J. Symbolic Computation (1992) 13, 255–299

On the Computational Complexity and Geometry of the First-order Theory of the Reals. Part I: Introduction. Preliminaries. The Geometry of Semi-algebraic Sets. The Decision Problem for the Existential Theory of the Reals

JAMES RENEGAR

School of Operations Research and Industrial Engineering, College of Engineering, Cornell University, Ithaca, New York 14853-7501, *USA*

(*Received* 18 *September* 1989)

This series of papers presents a complete development and complexity analysis of a decision method, and a quantifier elimination method, for the first order theory of the reals. The complexity upper bounds which are established are the best presently available, both for sequential and parallel computation, and both for the bit model of computation and the real number model of computation; except for the bounds pertaining to the sequential decision method in the bit model of computation, all bounds represent significant improvements over previously established bounds.

1. Introduction

1.1. This is the first part in a three part series of papers. This introduction provides an overview of the main results established in the series.

The decision problem for the first-order theory of the reals is the problem of determining if expressions of a certain form are true or false. Although a more general form is allowed, all allowable expressions can be reduced (as will be discussed later) to the form

$$(Q_1 x^{[1]} \in \mathbb{R}^{n_1})(Q_2 x^{[2]} \in \mathbb{R}^{n_2}) \cdots (Q_\omega x^{[\omega]} \in \mathbb{R}^{n_\omega}) P(x^{[1]}, \ldots, x^{[\omega]}), \tag{1.1}$$

where

(i) each Q_k is one of the quantifiers $\exists$ or $\forall$;

(ii) $P(x^{[1]}, \ldots, x^{[\omega]})$ is a quantifier free Boolean formula with "atomic predicates" of the form

$$g_i(x^{[1]}, \ldots, x^{[\omega]}) \Delta_i 0$$

each $g_i : \times_{k=1}^{\omega} \mathbb{R}^{n_k} \to \mathbb{R}$ being a real polynomial, and Δ_i being any one of the "standard relations"

$$>, \geq, =, \neq, \leq, <. \tag{1.2}$$

Such an expression is referred to as a "sentence". Catenating blocks of variables if necessary, it may be assumed that for each k, Q_k and Q_{k+1} are not the same quantifier. Hence, $\omega - 1$ is the number of "quantifier alternations".

0747-7171/92/030255+44 $03.00/0

As an example, given three polynomials g_1, g_2, $g_3:\mathbb{R}^{n_1}\times\mathbb{R}^{n_2}\to\mathbb{R}$ the sentence

$$(\exists x^{[1]}\in\mathbb{R}^{n_1})(\forall x^{[2]}\in\mathbb{R}^{n_2})[((g_1(x^{[1]},x^{[2]})=0)\wedge(g_2(x^{[1]},x^{[2]})>0))\vee\sim(g_3(x^{[1]},x^{[2]})\leq 0)]$$

declares that there exists $x^{[1]}$ such that given any $x^{[2]}$ the pair $(x^{[1]},x^{[2]})$ either satisfies

$$g_1(x^{[1]},x^{[2]})=0 \quad\text{and}\quad g_2(x^{[1]},x^{[2]})>0$$

or does not satisfy

$$g_3(x^{[1]},x^{[2]})\leq 0.$$

Depending on the specific polynomials g_1, g_2 and g_3, this assertion is either true or false.

The collection of all true sentences constitutes the first-order theory of the reals, denoted by Th($\mathbb{R}$). A decision method for Th($\mathbb{R}$) is an algorithm which, given a sentence, determines if the sentence is in Th($\mathbb{R}$). Tarski (1951) was the first to present a decision method for Th($\mathbb{R}$); he discovered his method around 1930 although it did not appear in print until later. We refer the reader to the introduction of his well-written monograph for a more formal discussion of Th($\mathbb{R}$).

The sentence (1.1) is said to be in prenex form; all quantifiers occur in front. It is the custom in the literature on the computational complexity of the decision problem to consider only sentences in prenex form. Throughout most of the introduction we focus on the prenex form; towards the end of the introduction we discuss sentences of a more general form. (Although all sentences can be reduced to prenex form, there is certainly a cost associated with doing so.)

Traditionally, attention has been restricted to sentences for which the coefficients of the polynomials g_i are rational numbers. Consequently, a decision method for Th($\mathbb{R}$) is an algorithm in the usual Turing machine sense. However, there is no ambiguity regarding what is meant for a sentence of the form (1.1) to be true or false if we allow the coefficients of the polynomials g_i to be real numbers. Borrowing a phrase from Blum & Smale (1992) we will refer to the resulting collection of true sentences as "the extended first order theory of the reals" and denote it by ETh($\mathbb{R}$). Thus, we view Th($\mathbb{R}$) as the subset of ETh($\mathbb{R}$) consisting of those sentences for which all of the polynomials occurring in the atomic predicates have rational coefficients.

An appropriate model of computation for defining what is meant by a "decision method for ETh($\mathbb{R}$)" is the model developed by Blum, Shub & Smale (1989). This model formalizes and extends what researchers often refer to as "arithmetic complexity". Computations are restricted to the arithmetic operations $+$, $-$, $\cdot$, $\div$, all assumed to be performed exactly on real numbers with no rounding errors (i.e. infinite precision), and branching decisions are made using the comparison operations $>$ and $=$. (A complete formalization of the model requires developing an appropriate notion of 'uniform algorithm', etc.; these issues are dealt with in Blum *et al.* (1989).)

When speaking of a decision method for Th($\mathbb{R}$) in the usual Turing machine sense we will, for brevity, speak of the "bit model" of computation. When speaking of a decision method for ETh($\mathbb{R}$) as an algorithm in the arithmetic complexity sense, we will speak of the "real number model" of computation. In this paper results are presented for both models of computation. Before proceeding we attempt to clarify the mathematical significance of the real number model.

The real number model aims at capturing what might be called the "algebraic complexity" of a problem. For the decision problem, relevant parameters to the real number model include (i) the number of variables, (ii) the number of atomic predicates, (iii) the degrees of the polynomials g_i occurring in the atomic predicates and (iv) the complexity of the procedure used to evaluate $\mathbb{P}$ where

> $\mathbb{P}$ is the Boolean expression obtained by replacing the atomic predicates in P with Boolean variables. (Thus, $g_i \Delta_i 0$ is replaced by B_i with allowable values 0 and 1.)

What cannot figure into complexity bounds in the real number model is any measure reflecting the "size" of a number; specifically, the size of the coefficients of the polynomials g_i can play no role in the bounds. In the real number model, "a number is a number is a number".

The bit model, although reflecting the finiteness of computations that are allowable in "reality", provides extra structure that is off-limits in the real number model. This is made especially apparent, for example, in recent work in linear programming (e.g. Khachian (1979), Karmarkar (1984), Renegar (1988*a*), etc.); among other things, in the bit model one has lower bounds on the separation between the vertices of the feasible region, and upper bounds on their pròximity to the origin. Although we now know many bit model polynomial-time algorithms for rational coefficient linear programming problems, none of these algorithms provides even a finite uniform bound in the real number model. Even though all of these algorithms rely primarily on the operations $+, -, \cdot, \div, >, =$, the number of such operations required by them can be made arbitrarily large with an appropriate choice of "large" coefficients even when the algebraic parameters are fixed, i.e. the number of variables and the number of constraints. The only known upper bounds in the real number model for linear programming are exponential in the number of variables. (The simplex method provides such a bound.) Even for the "simpler" feasibility decision problem the only known upper bounds are exponential in the number of variables; the feasibility decision problem is the problem of determining if a given set of linear inequalities can be satisfied simultaneously. Determining if the exponential dependence is an intrinsic part of the algebraic complexity of linear programming is widely considered as a foremost challenge among linear programming theorists. (Tardos (1986) has made some progress on this problem.)

A similar situation occurs for the first order theory of the reals. Certain tricks can be exploited in the bit model that are off-limits in the real number model. Algorithms have been discovered that provide "nice" bounds for the decision problem for Th($\mathbb{R}$) but which do not provide even a finite bound for the decision problem for ETh($\mathbb{R}$) in terms of the natural algebraic parameters of the problem. Although some of the algorithms are ingenious and their introduction provided dramatic new insight, they fall short of unravelling the complete algebraic structure underlying the problems. It seems that the ideal algorithm is one that provides a "nice" bound in the real number model and which when restricted to sentences with polynomials whose coefficients are rational numbers also provides a "nice" bound in the bit model.

Tarski's method provides algorithms for the decision problems of both ETh($\mathbb{R}$) and Th($\mathbb{R}$), but the costs of the algorithms are much worse than the costs of some of the newer algorithms.

Now we discuss another aspect of the complexity of the decision problem.

Given an arbitrary Boolean function $\mathbb{P}: \{0, 1\}^m \to \{0, 1\}$ and given m atomic predicates $g_i(x)\Delta_i 0$ there is an obvious and natural way to define a 0–1 valued function $P(x)$, namely

$$P(x) := \mathbb{P}(B_1(x), \ldots, B_m(x)),$$

where

$$B_i(x) := \begin{cases} 1 & \text{if } g_i(x)\Delta_i 0, \\ 0 & \text{otherwise.} \end{cases}$$

The perspective we take in these papers is that $\mathbb{P}$ is given, and the function P appearing in (1.1) is then defined as above.

In some way a measure of the cost of evaluating the Boolean function $\mathbb{P}$ must enter into the cost of a decision method. Traditionally, $\mathbb{P}$ has been assumed to be of restricted forms. For example, it is often assumed that $\mathbb{P}$ is initially given as a formula written using only "$\wedge$", "$\vee$", "$\sim$", "(", ")" and Boolean variables B_i. A measure of the "size" of $\mathbb{P}$ naturally follows; the size is then proportional to the cost of evaluating $\mathbb{P}$ when arbitrary values 0 or 1 are substituted for the Boolean variables.

Rather than requiring $\mathbb{P}$ to be of a restricted form, we assume that a procedure (i.e. oracle) is available for evaluating $\mathbb{P}$ when arbitrary values 0 or 1 are substituted for the variables B_i. A component of the bounds we state will be the number of "calls to $\mathbb{P}$", meaning the number of times the procedure for evaluating $\mathbb{P}$ is used. Of course we could restrict $\mathbb{P}$ to be of a specific form, such as in the previous paragraph, and then replace "calls to $\mathbb{P}$" with specific bounds on the operations required to make the calls. However, doing so would reduce the versatility of our results. Hence we choose to refer to "calls to $\mathbb{P}$".

When stating time bounds for parallel computation, we will use Time($\mathbb{P}$, N) to denote the worst-case time (over all 0–1 vectors) required to compute $\mathbb{P}$ using N processors.

As already noted, traditionally $\mathbb{P}$ has been assumed to be of restricted forms. Consequently, bounds appearing in the literature are stated with respect to these forms and are not stated in terms of the generic "calls to $\mathbb{P}$". However, once one becomes familiar with the underlying mathematics, it is not difficult to see how to extend slightly the analysis behind bounds appearing in the literature to obtain bounds which are stated in terms of "calls to $\mathbb{P}$". In the following brief survey of some of the highlights from the literature I have taken the liberty of doing this; this allows a more meaningful comparison of the bounds.

When we refer to "operations" it will be in the context of ETh($\mathbb{R}$). Formally, for the sequential operation bounds that follow, "operations" can be taken to refer to those allowed in the real number model of computation developed by Blum *et al.* (1989). For readers unfamiliar with that paper, "operations" can simply be taken to refer to the ordered field operations $+, -, \cdot, \div, >$ and $=$ (and operations for storing and retrieving data). Although a model for parallel computation over the reals is not formalized in Blum *et al.* (1989), the uniform and elementary nature of the algorithms designed for proving the "real number model parallel bounds" that follow guarantee that the bounds will hold for any reasonable real number model of parallel computation.

When we refer to "bit operations" it will be in the context of Th($\mathbb{R}$) and will refer to Turing machine operations. As with the real number model algorithms, the uniform and elementary nature of the algorithms designed for proving the "bit model parallel bounds" that follow guarantee that the bounds will hold for any reasonable bit model of parallel computation, of which there are several (e.g. the circuit model commonly used in defining NC).

In what follows we assume that $P(x^{[1]}, \ldots, x^{[\omega]})$ has m atomic predicates and we assume that $d \geq 2$ is an upper bound on the degrees of the polynomials occurring in the atomic predicates. Also recall that n_k is the number of variables occurring in $x^{[k]}$.

When referring to a decision method for Th($\mathbb{R}$) we may assume that the coefficients of the polynomials are integers; we then let L denote the maximum, over all of the coefficients, of the number of bits required to specify the coefficient.

The data specifying a sentence is ω, $n_1, \ldots, n_\omega$, $Q_1, \ldots, Q_\omega$, m, $\Delta_1, \ldots, \Delta_m$, d, the coefficients of the polynomials $g_1, \ldots, g_m$, and the Boolean function $\mathbb{P}$.

The following brief survey of results on the complexity of the decision problem is presented chronologically.

Both Seidenberg (1954) and Cohen (1969) made conceptual simplifications to Tarksi's design for a decision method. However, the first algorithm with a reasonable upper bound for the decision problem for Th($\mathbb{R}$) was obtained by Collins (1975). Relying on arguments and an algorithm specific to the bit model, he essentially proved an upper bound of $L^3(md)^{2^{O(\Sigma_k n_k)}}$ bit operations plus $(md)^{2^{O(\Sigma_k n_k)}}$ calls to $\mathbb{P}$. (Collins actually provided specific constants in his bound.) Thus, Collins' bound is "doubly exponential" in $\Sigma_k n_k$. Collins' work has been extremely influential in the development of computational real algebraic geometry.

In Ben-Or, Kozen & Reif (1986) a decision algorithm was introduced for ETh($\mathbb{R}$). They announced that, when restricted to sentences with integer coefficients, although possessing roughly the same sequential bounds as Collins' algorithm, the operations could be carried out in space only singly exponential in $\sum_k n_k$; moreover, they announced that their algorithm performs quickly in parallel. Unfortunately, a flaw was found in their complexity analysis. It is now apparent that the algorithm exactly as presented in Ben-Or *et al.* (1986) cannot achieve the claimed results for sentences with more than one variable. Modifications to the algorithm can be made so as to obtain the claimed bounds, as was shown by Fitchas *et al.* (1987) (discussed momentarily).

The Ben-Or *et al.* (1986) paper remains very significant. The complexity analysis for the clever univariate algorithm is certainly correct. In one respect the univariate case is the crucial case; all existing methods work by reducing the multivariate case to the univariate case. Ideas from the univariate algorithm of Ben-Or *et al.* form the backbone of several efficient decision methods for ETh($\mathbb{R}$). They are crucial for our method.

In Grigor'ev & Vorobjov (1988) a breakthrough was made regarding the decision problem for the existential theory of the reals; i.e. the decision problem for sentences where all variables have the same quantifier. Their algorithm and analysis are particular to the bit model of computation. The bound that follows from their work is $L^{O(1)}(md)^{O(n^2)}$ bit operations plus $(md)^{O(n)}$ calls to $\mathbb{P}$, n being the total number of variables. The significance of the bound is that it is only singly exponential in the number of variables.

Grigor'ev (1988) extended the ideas of Grigor'ev & Vorobjov (1988) to make a breakthrough on the more general decision problem for Th($\mathbb{R}$). Again the algorithm and analysis are particular to the bit model of computation. The upper bound that he announced is essentially $L^{O(1)}(md)^{(O(\Sigma_k n_k))^{4\omega-2}}$ bit operations plus $(md)^{O(\Sigma_k n_k)}$ calls to $\mathbb{P}$. Grigor'ev's bound is important in that the second exponent depends only on the number of quantifier alternations. Many interesting decision problems can be resolved by deciding the truth or falsity of sentences with only a few quantifier alternations.

In Fitchas, Galligo & Morgenstern (1987) a decision method was introduced for ETh($\mathbb{R}$) and was essentially announced to have an upper bound of $(md)^{2^{O(\Sigma_k n_k)}}$ operations plus $(md)^{2^{O(\Sigma_k n_k)}}$ calls to $\mathbb{P}$. Moreover, they announced that the algorithm can be implemented in parallel, requiring time $[2^{\Sigma_k n_k} \log(md)]^{O(1)} + \mathrm{Time}(\mathbb{P}, N)$ if $N(md)^{2^{O(\Sigma_k n_k)}}$ processors are used (for any $N \geq 1$). They also announced analogous complexity results for the bit model of computation. Their results were achieved by extending the ideas of Ben-Or *et al.*

In Canny (1988) it was announced that in the bit complexity model the existential theory of the reals can be decided in PSPACE. In Renegar (1988) it was announced that it can be decided in PSPACE much faster than with Canny's algorithm; moreover, the algorithm presented fully parallelized and, in the real number model, provided an $(md)^{O(n)}$ upper bound on the required number of operations (plus $(md)^{O(n)}$ calls to $\mathbb{P}$), where n is the number of variables.

Both Canny (1988) and Renegar (1988*b*) depend on the algorithm of Ben-Or *et al.* (1986) [BKR]. The methods of both papers require the determination of sign information for univariate polynomials whose coefficients are themselves polynomials in additional variables. This is the type of situation where the complexity analysis in Ben-Or *et al.* (1986) is incorrect. In Canny (1988) the errors of Ben-Or *et al.* are avoided by noting that in the applications, sign information is required only when the additional variables are "infinitesimally small". In essence, this allows the additional variables to be treated as fixed constants when the BKR algorithm is called on. In Renegar (1988), being unaware of the errors in Ben-Or, Roy & Solernó (1986), the BKR algorithm was simply called on and the fact that the additional variables introduced could be treated as fixed constants in the same way was ignored. Strictly speaking, the proof given in Renegar (1988) is thus incorrect. Canny alerted me to the problems in Ben-Or *et al.* (1986). It was largely the unsettling idea that I did not completely understand the mathematics I was basing my work on that led me to undertake the research contained in the present series of papers.

In Heintz, Roy & Solernó (1989) a bit model decision algorithm was presented for the existential theory of the reals. They essentially announced that the algorithm requires only $L^{O(1)}(md)^{n^{O(1)}}$ sequential operations and $(md)^{O(n)}$ calls to $\mathbb{P}$, where n is the number of variables. The algorithm can be implemented in parallel, requiring time $[n\log(Lmd)]^{O(1)}+\mathrm{Time}(\mathbb{P}, N)$ if $L^{O(1)}(md)^{n^{O(1)}}$ processors are used for the operations and $N(md)^{O(n)}$ processors are used for the calls (for any $N\geq 1$).

We now state our results for the decision problem.

Theorem 1.1. *There is an algorithm for the decision problem for* ETh($\mathbb{R}$) *that requires only*

$$(md)^{2^{O(\omega)}\sum_k n_k} \textit{ operations and } (md)^{O(\sum_k n_k)} \textit{ calls to } \mathbb{P}.$$

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

$$\left[2^{\omega}\left(\prod_k n_k\right)\log(md)\right]^{O(1)}+\mathrm{Time}(\mathbb{P}, N)$$

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

When restricted to sentences involving only polynomials with integer coefficients, the algorithm becomes a decision method for Th($\mathbb{R}$) *requiring only*

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

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

$$\log(L)\left[2^{\omega}\left(\prod_k n_k\right)\log(md)\right]^{O(1)}+\mathrm{Time}(\mathbb{P}, N)$$

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

There are several ways in which the above theorem is an advance over previous results. It provides the first operation bound in the real number model that is doubly exponential only in the number of quantifier alternations. It provides the first time bound for parallel computation for both the real number model and the bit model that is exponential only in the number of quantifier alternations. It establishes a very low dependence on L with regard to bit complexity.

Simultaneously and independently, Heintz, Roy & Solernó (1990) have proven a similar theorem, the main difference being that the exponent $2^{O(\omega)}\prod_k n_k$ occurring in our theorem is replaced by $[O(\sum_k n_k)]^{O(\omega)}$. Their work is based firmly in Grigor'ev (1988).

The exponent occurring in the operation bounds in our theorem is of a very nice form. This is made most noticeable by comparing it with the other established exponents, written slightly differently:

$$\text{Collins' exponent: } \prod_k 2^{O(n_k)}$$

$$\text{Grigor'ev's exponent:} \approx \prod_k O\Big(\sum_j n_j\Big)^4$$

$$\text{our exponent: } \prod_k O(n_k)$$

$$\text{Heintz, Roy \& Solernó: } \prod_k O\Big(\sum_j n_j\Big)^{O(1)}.$$

Grigor'ev's exponent is generally much, much better than Collins' but is much worse when there are many blocks $x^{[k]}$ of variables, most of which contain only a few variables. Our exponent is strictly better than Grigor'ev's, is generally much, much better than Collins', and is always at least as good as Collins'.

The various bounds are best understood by realizing that decision methods typically work by passing through a sentence from back to front. First the vector $x^{[\omega]}$ is focused on, then the vector $x^{[\omega-1]}$, and so on. The work arising from each vector results in a factor for the exponent in the operation bounds. For Collins' method, the factor corresponding to $x^{[k]}$ in $2^{O(n_k)}$. For our method the factor is $O(n_k)$. The factor corresponding to Grigorev's decision method is $\approx O(\sum_j n_j)^4$ independently of the number of variables in $x^{[k]}$. In that method a vector with few variables can potentially create as large of a factor as one with many variables. Similarly, the factor corresponding to the method of Heintz *et al.* is $O(\sum_j n_j)^{O(1)}$ independently of $x^{[k]}$.

Many interesting formulae have blocks of variables of various sizes. For example, sentences asserting continuity generally have $(\forall\varepsilon)(\exists\delta)$, along with large blocks of variables. The exponent in our operation bound is especially relevant for such sentences as the factors contributed from the smaller blocks are of modest size.

The theorem is proven in Part II. The bit complexity bounds are easily established because no divisions occur in the algorithm. Verifying the bit complexity results essentially amounts to verifying that all numbers occurring during the execution of the algorithm are integers of nicely bounded bit length (assuming that the coefficients of the polynomials occurring in the atomic predicates are integers). The $L(\log L)(\log\log L)$ factor occurring in the theorem arises from the well known bit complexity bound for multiplying integers. Similarly, the $\log L$ and L^2 occurring in the parallel bounds arise from the well-known parallel bounds for multiplying integers.

Tarski developed more than a decision method for sentences, he developed a quantifier elimination method for formulae. A formula is defined exactly as a sentence is, except that in a formula not all variables are required to be quantified. The variables that are not quantified are referred to as the "free" variables; when specific values are substituted for the free variables, the formula becomes a sentence.

A formula

$$(Q_1 x^{[1]} \in \mathbb{R}^{n_1}) \cdots (Q_\omega x^{[\omega]} \in \mathbb{R}^{n_\omega}) P(y, x^{[1]}, \ldots, x^{[\omega]}) \tag{1.3}$$

with free variables $y = (y_1, \ldots, y_l)$ is said to be equivalent to a quantifier free formula $\bar{P}(y)$ if the sentence obtained by substituting $\bar{y}$ into (1.3) is true precisely for those values $\bar{y} \in \mathbb{R}^l$ satisfying $\bar{P}(y)$, i.e. $\bar{P}(\bar{y}) = 1$. A quantifier elimination method is an algorithm which, given an arbitrary formula, constructs an equivalent quantifier free formula.

Tarski's quantifier elimination method provides both a real number model algorithm for formulae with real coefficients, and a bit model algorithm for formulae with rational coefficients.

In Collins (1975) a quantifier elimination method was introduced, not just a decision method for Th($\mathbb{R}$). His quantifier elimination is designed specifically for formulae with rational coefficients, and requires only $L^3(md)^{2^{O(l+\Sigma_k n_k)}}$ bit operations and $(md)^{2^{O(l+\Sigma_k n_k)}}$ calls to $\mathbb{P}$. (Again, Collins provides specific constants.)

Fitchas *et al.* (1987) presented a real number model quantifier elimination method and essentially announced that it requires only $(md)^{2^{O(l+\Sigma_k n_k)}}$ operations and $(md)^{2^{O(l+\Sigma_k n_k)}}$ calls to $\mathbb{P}$. Moreover, they announced that the algorithm can be implemented in parallel, requiring time $[2^{l+\Sigma_k n_k} \log(md)]^{O(1)} + \mathrm{Time}(\mathbb{P}, N)$ if $(md)^{2^{O(l+\Sigma_k n_k)}}$ processors are used for the operations and $N(md)^{2^{O(l+\Sigma_k n_k)}}$ processors are used for the calls (for any $N \geq 1$). They also announced analogous bounds with respect to the bit complexity model.

The above bounds are by far the best bounds that had appeared in the literature before the following theorem was established.

Now we state our quantifier elimination results. We assume that l, the number of free variables occurring in (1.3), is at least one.

THEOREM 1.2. *There is a real number model quantifier elimination method that requires only*

$$(md)^{2^{O(\omega)} l \Pi_k n_k} \textit{ operations and } (md)^{O(l+\Sigma_k n_k)} \textit{ calls to } \mathbb{P}.$$

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

$$\left[2^\omega \left(l \prod_k n_k\right) \log(md)\right]^{O(1)} + \mathrm{Time}(\mathbb{P}, N)$$

if $(md)^{2^{O(\omega)} l \Pi_k n_k}$ *processors are used for the operations and* $N(md)^{O(l+\Sigma_k n_k)}$ *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

$$L(\log L)(\log\log L)(md)^{2^{O(\omega)} l \Pi_k n_k}$$

sequential bit operations and $(md)^{O(l+\Sigma_k n_k)}$ *calls to* $\mathbb{P}$*. When implemented in parallel the algorithm requires time*

$$(\log L)\left[2^\omega \left(l \prod_k n_k\right) \log(md)\right]^{O(1)} + \mathrm{Time}(\mathbb{P}, N)$$

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

The algorithm constructs a quantifier free formula of the following simple form:

$$\bigvee_{i=1}^{I}\bigwedge_{j=1}^{J_i}(h_{ij}(y)\Delta_{ij}0), \tag{1.4}$$

where

$$I\leq (md)^{2^{O(\omega)}l\prod_k n_k};$$

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

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

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

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* $(L+l)(md)^{2^{O(\omega)}\prod_k n_k}$.

The above theorem is an advance over previous quantifier elimination results in the same ways that Theorem 1.1 is an advance over previous decision method results.

Quantifier elimination methods generally work inductively. First, the variables $x^{[\omega]}$ are eliminated from the formula $(Q_\omega x^{[\omega]}\in\mathbb{R}^{n_\omega})P(y, x^{[1]},\dots, x^{[\omega]})$ to obtain an equivalent quantifier free formula $\bar{P}(y, x^{[1]},\dots, x^{[\omega-1]})$. Then $x^{[\omega-1]}$ is eliminated from $(Q_{\omega-1}x^{[w-1]}\in\mathbb{R}^{n_{\omega-1}})\bar{P}$, and so on. However, the above theorem is not established in this way. The problem with this approach is the exponential dependence on l of the size of the number I occurring in (1.4). The inductive approach results in an exponent $(O(\sum_k n_k))^\omega$ as opposed to the exponent $2^{O(\omega)}\prod_k n_k$ appearing in the theorem. (Of course this raises the question of whether there is a quantifier elimination method which produces quantifier free formulae with the number of atomic predicates not depending exponentially on l.)

The quantifier elimination method is designed by extending the ideas used in designing the decision method. The above theorem is proven in Part III.

Heintz *et al.* (1990) have simultaneously and independently proven a similar theorem and, just as before, the main difference is in the exponent occurring in the operation bounds. Where we have $2^{O(\omega)}l\prod_k n_k$, they have $[O(l+\sum_j n_k)]^{O(\omega)}$; as before, in their method a vector with few variables can potentially create as large a factor in the exponent as one with many variables.

It should be noted that although Grigor'ev's theorem (Grigor'ev, 1988) pertained only to the decision problem, it is now apparent that he was not far from having an analogous theorem for the sequential bit complexity of quantifier elimination; results from Grigor'ev (1988) combined with modifications of ideas in Ben-Or *et al.* (1986) can be used to prove such a theorem; Grigor'ev conjectured such a theorem.

Now we briefly discuss sentences and formulae not in prenex form. We do not do this in full generality here; we only provide enough discussion to indicate how complexity bounds for more general sentences and formulae can be obtained from the two theorems.

There are various ways to reduce a sentence to prenex form. One way is to introduce new variables. For example, a sentence of the form

$$(\forall s\in\mathbb{R})[(\forall t\in\mathbb{R})P_1(s, t)\vee(\exists t\in\mathbb{R})P_2(s, t)] \tag{1.5}$$

is equivalent to the sentence

$$(\forall(s, t_1)\in\mathbb{R}^2)(\exists t_2\in\mathbb{R})[P_1(s, t_1)\vee P_2(s, t_2)].$$

The problem with introducing new variables is the excessive dependence of the cost of decision methods on the number of variables.

An efficient quantifier elimination method for formulae in prenex form provides a better means of reducing a sentence (or a formula) to prenex form. The method is first applied to the largest portions of the sentence that are formulae in prenex form, reducing the sentence somewhat, then applied to the largest portions of the resulting sentence that are formulae in prenex form, and so on. For example, for the sentence (1.5), the quantifier elimination method would be applied to the portion $(\forall t \in \mathbb{R}) P_1(s, t)$, and separately to the portion $(\exists t \in \mathbb{R}) P_2(s, t)$, to obtain equivalent quantifier free formulae $\bar{P}_1(s)$ and $\bar{P}_2(s)$. The sentence (1.5) would then be equivalent to the prenex form sentence $(\forall s \in \mathbb{R})[\bar{P}_1(s) \vee \bar{P}_2(s)]$.

Using the quantifier elimination method designed to prove Theorem 1.2, and relying on the simple form (1.4) of quantifier free formulae it produces, the above approach yields by far the most efficient decision method (quantifier elimination method) known for general sentences (formulae). However, I know that a general method that is somewhat better can be designed. The problem with the above inductive approach is again the size of the number I occurring in (1.4). For example, when applied to a sentence of the form

$$\begin{aligned}&(Q_1 x^{[1]} \in \mathbb{R}^{n_1})[P_1(x^{[1]})\\ &\qquad \wedge (Q_2 x^{[2]} \in \mathbb{R}^{n_2})[P_2(x^{[1]}, x^{[2]}) \wedge \cdots \wedge (Q_\omega x^{[\omega]} \in \mathbb{R}^{n_\omega}) P_\omega(x^{[1]}, \ldots, x^{[\omega]})] \cdots]\end{aligned}$$

the approach results in an exponent $(O(\sum_k n_k))^\omega$ when in fact an exponent $2^{O(\omega)} \prod_k n_k$ is attainable by extending the ideas behind the algorithms designed to prove Theorems 1.1 and 1.2. I may make this the subject of a future paper.

Results on the computational complexity of approximating "solutions" for real formulae can be found in Renegar (1992*a*); $\bar{y} \in \mathbb{R}^l$ is said to be a solution for the formula (1.3) if the sentence obtained by substituting $\bar{y}$ for y is true. The analysis in Renegar (1992*a*) relies heavily on the results established in the present series of papers.

Similar bounds to those provided by our theorems have been proven in cases involving algebraically closed fields. In that setting only atomic predicates of the form $g_i = 0$ and $g_i \neq 0$ are allowed. The algebraic completeness and the absence of an ordering make the algorithmic construction and analysis significantly easier. Especially noteworthy for establishing record bounds are the results of Grigor'ev (1987), and Chistov & Grigor'ev (1984), where analogs to the results of Grigor'ev (1988) are presented, the results essentially being established for the bit model of computation. Also especially noteworthy for establishing record bounds are the results of Ierardi (1989), and of Fitchas, Galligo & Morgenstern (1990), where analogs to the results contained in the present paper are presented; the results are essentially established for the "real number model" (or rather, an appropriate generalization), specialize to give the main results of Chistov & Grigor'ev (1984), and also include appropriate bounds for parallel implementation. However, in all of these papers the exponent arrived at is of the form $(O(l + \sum_k n_k))^{2\omega}$ (or worse), rather than $2^{O(\omega)} l \prod_k n_k$.

An excellent bibliography of research related to constructive aspects of quantifier elimination for real closed fields has been compiled by Arnon (1988). An interesting survey on research in logic stemming from Tarski's work was written by Van den Dries (1988).

In section 1.2 we provide a synopsis of the results established in this paper. The introductions of Parts II and III state the main results, in addition to the above theorems, that are proven in those papers.

This series of papers is obviously very long. I have attempted to explain the mathematics in a way that will be understandable to any motivated reader, even one who has been unfamiliar with the subject area until now. Having myself studied the decision problem only in the last 2 years, I know from my attempts to learn the recent literature that this type of exposition is missing. The lengthy exposition is also called for because our approach is significantly different from earlier ones. Through the use of appendices, the series is self-contained; the mathematics is developed from a very basic level. The second and third papers each contain a "preliminaries" section listing those results proven earlier in the series that will be relied on in the paper.

A synopsis of the main ideas in this series of papers can be found in Renegar (1992*b*), where the myriad of subtle details that arise are purposely ignored.

For the initial reading of this three part series we suggest the following sequence. Part I, section 2.1, 2.2, 2.3. (Ignore the proofs in the appendices that are referred to.)

Section 3.1, 3.8, 3.9, 3.10. (Think about 3.8, but only read 3.9 and 3.10 lightly.)

Section 4. (Read this short section carefully! Understand the arguments, assuming the validity of the propositions referred to. The ideas in this section are elaborated on in Part II to construct the general decision procedure.)

Part II, section 1. (A short introduction.)

Section 2. (Read this lightly as a review.)

Section 3. (Only read the first three paragraphs and the statement of proposition 3.4; the proposition is crucial in what follows.)

Section 4. (Read this section carefully. It slowly develops all of the crucial ideas for the general decision procedure, but in the "simple" case of only a single quantifier alternation.)

Section 5. (Theorem 1.1 is proven here. The analysis in this section is a fairly straightforward generalization of the analysis of section 4.)

Section 6.1. (The analysis in section 6.2 is very similar to that in section 5, and so is best skipped on a first reading.)

Part III, section 1. (A short introduction.)

Sections 2, 3. (Read these lightly as reviews.)

Section 4.1. (Ignore section 4.2.)

Sections 5, 6, 7, 8, 9. (An accurate understanding of the quantifier elimination method requires a good understanding of the details developed in these sections except that the proofs of Propositions 8.1 and 8.2 can be ignored.)

1.2. Here we present a synopsis of the material contained in this paper.

Section 2 contains algebraic preliminaries that are relied on throughout the series. Several of the preliminaries are only stated in the section, but are proven in appendices.

Section 3 is a technical section that is the heart of this paper and the cornerstone for the series. We now introduce a definition so that we can convey an idea of what section 3 is about.

Let $g_1, \ldots, g_m : \mathbb{R}^n \to \mathbb{R}$ be arbitrary polynomials. The "connected sign partition" $\mathrm{CSP}\{g_i\}_i$ generated by $\{g_i\}_i$ is the partition of $\mathbb{R}^n$ whose elements are the maximal connected subsets of $\mathbb{R}^n$ with the following property: if $\bar{x}$ and $\hat{x}$ are in the same element then the sign of $g_i(\bar{x})$ is the same as the sign of $g_i(\hat{x})$ for all i (the sign is 1, 0 or -1 depending on whether the value is positive, zero or negative).

Section 3 is devoted to constructing a set of polynomials, from the coefficients of $\{g_i\}_i$, which contains easily extractable information regarding $\mathrm{CSP}\{g_i\}_i$. In particular, the polynomials constructed provide a foundation for computing approximations to representatives from all elements of CSP$\{g_i\}_i$. In Part II, we use the polynomials to obtain "symbolic" representatives for all of the elements.

One of the important facts about the polynomials constructed in section 3 is that the procedure for their construction is dependent only on m, n and d (the maximal degree of the polynomials g_i). Also, no branching occurs during the construction. So what is actually constructed is a set of polynomials some of whose variables represent the coefficients of $\{g_i\}_i$, the constructed polynomials being independent of $\{g_i\}_i$; to obtain information about CSP$\{g_i\}_i$ for specific $\{g_i\}_i$, one can just plug in the specific coefficients. The independence of the construction from the specific $\{g_i\}_i$ appears to be crucial in obtaining exponents of the form $2^{O(\omega)}\prod_k n_k$ as opposed to $(O(\sum_k n_k))^{O(\omega)}$.

In recent years several works in complexity theory have made use of upper bounds on the number of connected components of real algebraic varieties implied by Milnor (1964). For example, these bounds are crucial in the arguments establishing the lower bounds found in Steele & Yao (1982), and Ben-Or (1983). Together with results from Heintz (1983), they are also crucial in establishing the upper bound in Grigor'ev (1988).

The machinery we develop in section 3 trivially provides an upper bound of $(md)^{O(n)}$ on the number of elements in CSP$\{g_i\}_i$. However, whereas Milnor (1964) relies on Morse theory, our development proceeds from only elementary arguments.

The facts from section 3 that will be used in this series of papers are summarized in sections 3.8, 3.9 and 3.10.

The results from sections 2 and 3, together with the algorithm of Ben-Or *et al.* (1986) for determining the "consistent sign vectors" of a set of univariate polynomials, easily provide an efficient decision algorithm for the existential theory of the reals, as is shown in section 4. A full discussion of (a slightly modified version of) the Ben-Or *et al.* univariate algorithm can be found in sections 5 and 7 of Part III; the ideas behind the algorithm are crucial in designing the quantifier elimination procedure in that paper.

2. Preliminaries

2.1. In this section we discuss algebraic preliminaries including a certain construction related to the "u-resultant". Although the reader who is familiar with the u-resultant will only want to skim the subsections describing the construction, it should be noted that the construction and the proofs of its properties are based only on very elementary arguments. We actually construct a certain well-known polynomial that only has the u-resultant as a factor. We do not need the full power of the u-resultant. We avoid referring the reader to detailed proofs regarding properties of the u-resultant by focusing on the simpler construction.

In the remainder of section 2.1, and in sections 2.4 and 2.5, we present preliminaries that will be necessary for a thorough understanding of the mathematics behind the algorithms; the preliminaries in sections 2.2 and 2.3 are necessary to even motivate the algorithms.

A well-known fact that is crucial for us is that the determinant of a matrix can be computed quickly in parallel. A proof of the following proposition is contained in Appendix A.

PROPOSITION 2.1.1. (Csanky, 1976.) *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 $Ln^{O(1)}$.

Another important fact for us is that the "consistent sign vectors" of a set of univariate polynomials $g_1, \ldots, g_m : \mathbb{R} \to \mathbb{R}$ can be constructed efficiently; a vector $\sigma \in \{-1, 0, 1\}^m$ is said to be a consistent sign vector for $\{g_i\}_i$ if there exists $\bar{x} \in \mathbb{R}$ such that the sign of $g_i(\bar{x})$ is σ_i for all i.

PROPOSITION 2.1.2. (Ben-Or *et al.*, 1986.) *Assume that $g_1, \ldots, g_m$ are real univariate polynomials of degree at most $d \geq 2$. The consistent sign vectors of $\{g_i\}_i$ can be determined with $(md)^{O(1)}$ operations (no divisions) in time $[\log(md)]^{O(1)}$ using $(md)^{O(1)}$ parallel processors. If the coefficients of $\{g_i\}_i$ are integers of bit length at most L, then $L(\log L)(\log \log L)(md)^{O(1)}$ sequential bit operations suffice, or time $\log(L)[\log(md)]^{O(1)}$ using $L^2(md)^{O(1)}$ parallel processors.*

The "no division" claim is not a direct consequence of Ben-Or *et al.* (1986), but comes from the slight variant of their algorithm presented in sections 5 and 8 of Part III of this series.

Another well-known fact that is important for us is that multivariate interpolation, without divisions, can be accomplished quickly in parallel; the polynomial returned will be a non-zero constant multiple of the actual polynomial. The following easily proven lemma is established in Appendix B.

LEMMA 2.1.3. *Assume that $f : \mathbb{C}^n \to \mathbb{C}$ is a polynomial of degree at most $d \geq 2$. Then $[\prod_{0 \leq j < k \leq d} (k-j)]^n f$ can be computed solely from the values $f(\bar{x})$, $\bar{x} \in \{0, 1, \ldots, d\}^n$, using $d^{O(n)}$ operations (no divisions). The computations can be implemented in parallel, requiring time $[n \log(d)]^{O(1)}$ if $d^{O(n)}$ processors are used. If the values $f(\bar{x})$, $\bar{x} \in \{0, 1, \ldots, d\}^n$, are integers of bit length at most L, all numbers occurring during the computation will be integers of bit length at most $L + nd^{O(1)}$.*

A well-known, and easily proven, fact that we use is that the zeros of a complex univariate polynomial vary continuously in the coefficients if the leading coefficient does not vanish; if $\bar{z}$ is a zero of multiplicity k, then for all sufficiently small perturbations of the coefficients, the resulting polynomials will have exactly k zeros near $\bar{z}$, counting multiplicities. The proof is left to the reader.

Assume that $g_1, \ldots, g_m : \mathbb{R}^n \to \mathbb{R}$ are polynomials and let $\mathrm{CSP}\{g_i\}_i$ be the connected sign partition of $\mathbb{R}^n$ generated by $g_1, \ldots, g_m$, as defined in section 1.2. Our arguments implicitly use the fact that $\mathrm{CSP}\{g_i\}_i$ consists of a finite number of elements and, at one point, explicitly uses the fact that each of the elements is path-connected. Although these facts are well known, for completeness we have included an elementary proof in Appendix C.

Another well-known fact that we use is that "most" systems of homogeneous polynomials $F : \mathbb{C}^n \to \mathbb{C}^m$, $m \geq n$, have only the trivial solution, i.e. 0. More specifically, consider the set of all homogeneous systems $F : \mathbb{C}^n \to \mathbb{C}^m$ for which either degree $(F_i) = d_i$ or F_i is identically zero. By identifying each of these systems with the vector of its coefficients we identify the entire set with $\mathbb{C}^N$ for the appropriate N. It is proven in Appendix D that there exists a finite set $\{\Phi_i\}_i$ of polynomials $\Phi_i : \mathbb{C}^N \to \mathbb{C}$ such that F has a non-trivial zero if and only if $\Phi_i(F) = 0$ for all i.

Note that the above fact implies the following. Assume that $F:\mathbb{C}\times\mathbb{C}^n\to\mathbb{C}^m$, $m\ge n$, is a system of polynomials satisfying both (i) for all δ the system $x\mapsto F(\delta,x)$ is homogeneous and (ii) for some δ the system $x\mapsto F(\delta,x)$ has only the trivial zero. Then for all but finitely many values of δ the system $x\mapsto F(\delta,x)$ has only the trivial zero. This is important in some of our proofs.

The above facts can be used to establish similar properties for homogeneous systems $F:\mathbb{C}^n\to\mathbb{C}^{n-1}$. Because of homogeneity, the zero set of F is a union of complex lines through the origin, the so-called "zero lines". In Appendix D we also establish the well-known fact that "most" homogeneous systems $F:\mathbb{C}^n\to\mathbb{C}^{n-1}$ have only finitely many zero lines.

As a consequence of the last fact we have the following. Assume that $F:\mathbb{C}\times\mathbb{C}^n\to\mathbb{C}^{n-1}$ is a system of polynomials satisfying both (i) for all δ the system $x\mapsto F(\delta,x)$ is homogeneous and (ii) for some δ the system $x\mapsto F(\delta,x)$ has only finitely many zero lines. Then for all but finitely many values of δ the system $x\mapsto F(\delta,x)$ has only finitely many zero lines.

This concludes the algebraic preliminaries except for the development of the "u-resultant".

2.2. In this section we discuss an algebraic construction referred to as the "u-resultant".

Let $f:\mathbb{C}^n\to\mathbb{C}^n$ be a system of polynomials each of degree at most d. Let $F:\mathbb{C}^{n+1}\to\mathbb{C}^n$ denote its degree d homogenization, i.e. the monomials of F_i are obtained from those of f_i by multiplying by the appropriate powers of x_{n+1} so as to become of degree d.

For $X\in\mathbb{C}^{n+1}$ satisfying $X_{n+1}\neq 0$, define

$$\mathrm{Aff}(X)=\frac{1}{X_{n+1}}(X_1,\ldots,X_n),$$

the "affine image" of X.

If $f(\bar{x})=0$ then $F(t\bar{x},t)=0$ for all $t\in\mathbb{C}$. If $F(\bar{X})=0$ and $\bar{X}_{n+1}\neq 0$ then $f(\mathrm{Aff}(\bar{X}))=0$. Hence, to every zero of f there corresponds a "zero line" for F and to every zero line $\{t\bar{X};\ t\in\mathbb{C}\}$ of F, where $\bar{X}_{n+1}\neq 0$, there corresponds a zero for f. The zero lines $\{t\bar{X};\ t\in\mathbb{C}\}$ of F satisfying $\bar{X}_{n+1}=0$ are sometimes referred to as "the zeros of f at infinity". The system f is said to have finitely many zeros including those at infinity if F has only finitely many zero lines.

Let $\mathbb{C}\mathrm{Poly}(n,n,d)$ denote the vector space of polynomial systems $f=(f_1,\ldots,f_n):\mathbb{C}^n\to\mathbb{C}^n$ for which each coordinate polynomial f_i is of degree at most d. By identifying systems of polynomials with their vector of coefficients, we can view $\mathbb{C}\mathrm{Poly}(n,n,d)$ as $\mathbb{C}^N$ for the appropriate N.

There exists a polynomial $R:\mathbb{C}\mathrm{Poly}(n,n,d)\times\mathbb{C}^{n+1}\to\mathbb{C}$ with the following properties. If $f\in\mathbb{C}\mathrm{Poly}(n,n,d)$ has infinitely many zeros, including those at infinity, then the polynomial $U\mapsto R(f,U)$ is identically zero. If f has only finitely many zeros, including those at infinity, then $U\mapsto R(f,U)$ factors linearly

$$U\mapsto R(f,U)=\prod_{i=1}^{d^n}\xi^{(i)}\cdot U. \tag{2.2.1}$$

where $\xi^{(i)}\cdot U:=\sum_{j=1}^{n+1}\xi_j^{(i)}U_j$; moreover, the zero lines of F are then precisely the lines $\{t\xi^{(i)};\ t\in\mathbb{C}\}$. Hence, the zeros of f are the affine images of those $\xi^{(i)}$ satisfying $\xi_{n+1}^{(i)}\neq 0$.

The polynomial R is sometimes referred to as the u-resultant of F. The u-resultant provides the basis for a multi-variate analogue to univariate factorization.

A detailed discussion of the u-resultant can be found in earlier editions of Van der Waerden (1950).

We do not need the full power of the u-resultant. What we need is an easily constructed polynomial $R : \mathbb{C}\mathrm{Poly}(n, n, d) \times \mathbb{C}^{n+1} \to \mathbb{C}$ which has the following two properties: (i) if $U \mapsto R(f, U)$ is not identically zero, then $U \mapsto R(f, U)$ factors linearly as in (2.2.1), where the zeros of f are precisely the points $\mathrm{Aff}(\xi^{(i)})$ that are well-defined; (ii) for very particular f to be specified in a later section, $U \mapsto R(f, U)$ is not identically zero.

Although the u-resultant has the properties that we need, a polynomial R with the above properties can be constructed using only elementary arguments. The polynomial R thus obtained will be a multiple of the u-resultant, where the factor is a polynomial expression only in the coefficients of f. The polynomial can vanish for particular f for which the u-resultant does not vanish, but this is of no concern for our applications.

We now discuss the construction of R. It is obtained as the determinant of a certain linear transformation.

Let $\mathbb{H}$ denote the vector space of complex homogeneous polynomials $h : \mathbb{C}^{n+1} \to \mathbb{C}$ of degree $n(d-1)+1$; of course the identically zero polynomial must also be included to obtain a vector space. The monomials in $\mathbb{H}$ clearly form a basis $\mathbb{B}$ for $\mathbb{H}$.

Let F_i denote the degree d homogenization of f_i.

We now define a linear transformation $T : \mathbb{H} \to \mathbb{H}$ by defining it on the elements of $\mathbb{B}$ and then extending linearly. Besides the homogeneous polynomials $F_1, \ldots, F_n$ of interest to us, the linear transformation will also depend on an additional polynomial

$$U \cdot x = \sum_{j=1}^{n+1} U_j x_j.$$

For now U should be thought of as a vector in $\mathbb{C}^{n+1}$; momentarily it will become a vector of variables.

For $x_1^{d_1} \cdots x_{n+1}^{d_{n+1}} \in \mathbb{B}$, let i denote the least index satisfying $i \le n$ and $d \le d_i$ if such an i exists; otherwise let $i = n+1$. Note that because the monomials in $\mathbb{B}$ have degree $n(d-1)+1$, if $i = n+1$ then $d_{n+1} \ge 1$. If $i \le n$, then define

$$T(x_1^{d_1} \cdots x_{n+1}^{d_{n+1}}) = x_1^{d_1} \cdots x_i^{d_i - d} \cdots x_{n+1}^{d_{n+1}} F_i(x).$$

If $i = n+1$, then define

$$T(x_1^{d_1} \cdots x_{n+1}^{d_{n+1}}) = x_1^{d_1} \cdots x_n^{d_n} x_{n+1}^{d_{n+1}-1} U \cdot x.$$

Extend T linearly to define a linear transformation $T : \mathbb{H} \to \mathbb{H}$. Let $M(f, U)$ denote the matrix representing T with respect to the basis $\mathbb{B}$. This matrix can be efficiently constructed from the coefficients of the original system f and the vector U; each coordinate is either 0, a coefficient from f or a coordinate U_j.

Let $R : \mathbb{C}\mathrm{Poly}(n, n, d) \times \mathbb{C}^{n+1} \to \mathbb{C}$ be defined by

$$R(f, U) = D! \det M(f, U), \tag{2.2.2}$$

where $M(f, U)$ is a $D \times D$ matrix; we add the factor of $D!$ so as to avoid divisions when computing R. This is a polynomial of degree $d^{O(n)}$ in the coefficients of $f \in \mathbb{C}\mathrm{Poly}(n, n, d)$ as can be verified simply from the fact that the size of $M(f, U)$ is $d^{O(n)}$. Because $U \cdot x$ was used in defining T only for the d^n monomials $x_1^{d_1} \cdots x_{n+1}^{d_{n+1}}$ satisfying $d_1 < d, \ldots, d_n < d$, the degree of $R(f, U)$ in U is exactly d^n.

The polynomial $R(f, U)$ is not identically zero. In fact, if f is the system $f_i(x) = x_i^d$ for all i, then it is easily established tht $R(f, U) = (D!)U_{n+1}^{d^n}$.

We now argue that for any f such that $U \mapsto R(f, U)$ is not identically zero, $U \mapsto R(f, U)$ factors linearly

$$U \mapsto R(f, U) = \prod_{i=1}^{d^n} \xi^{(i)} \cdot U,$$

where the zero lines of F are precisely the lines $\{t\xi^{(i)}; t \in \mathbb{C}\}$; hence the zeros of f are precisely the points $\mathrm{Aff}(\xi^{(i)})$ that are well-defined.

Assume that ξ is a zero of the system

$$\begin{gathered} F_1(x) = 0 \\ \vdots \\ F_n(x) = 0 \\ U \cdot x = 0. \end{gathered}$$

Then, by the definition of T, for every monomial $h \in \mathbb{B}$ we have that $T(h)(\xi) = 0$, i.e. the polynomial $T(h)$ has ξ as a zero. The same is then true for all $h \in \mathbb{H}$. Hence the image of T contains only polynomials with ξ as a zero. In particular if $\xi \neq 0$ (say $\xi_1 \neq 0$) then T is not an isomorphism (because the polynomial $x_1^{n(d-1)+1}$ cannot be in its image).

The above argument establishes the fact that if $\xi \neq 0$ is a zero of F, and U satisfies $\xi \cdot U = 0$, then $R(f, U) = 0$. Hence $U \mapsto R(f, U)$ vanishes on the set $\{U \in \mathbb{C}^{n+1}; \xi \cdot U = 0\}$. Assuming that $U \mapsto R(f, U)$ is not identically zero, it follows that $\xi \cdot U$ is a factor of $U \mapsto R(f, U)$. (For an elementary proof of this, first note that by a linear transformation we may assume $\xi = e_1$, the first unit vector. The statement just corresponds to the fact that any non-trivial polynomial in $U_1, \ldots, U_{n+1}$ that vanishes whenever $U_1 = 0$ has U_1 as a factor.)

We have now established that if f is such that $U \mapsto R(f, U)$ is not identically zero then for each non-trivial zero ξ of F, the linear polynomial $\xi \cdot U$ is a factor of $U \mapsto R(f, U)$. If f has d^n distinct zeros, then because $U \mapsto R(f, U)$ is of degree d^n it follows that

$$U \mapsto R(f, U) = \prod_{i=1}^{d^n} \xi^{(i)} \cdot U,$$

where $\{t\xi^{(i)}; t \in \mathbb{C}\}$ are precisely the zero lines of F.

It only remains to establish the linear factorization for the case that f does not have d^n distinct zeros. To do this we show in Appendix E that there is a "nice" system of polynomials $\bar{f}$ such that for all but finitely many values of ε, the system

$$x \mapsto \varepsilon \bar{f}(x) + (1 - \varepsilon) f(x)$$

has d^n distinct zeros and

$$U \mapsto R(\varepsilon \bar{f} + (1 - \varepsilon) f, U)$$

is not identically zero. Then an elementary limit argument can be used to show that if $U \mapsto R(f, U)$ is not identically zero, it factors linearly $\prod_{i=1}^{d^n} \xi^{(i)} \cdot U$ where each $\xi^{(i)}$ is a zero of F. (The limit argument is provided by the proof of Proposition 2.4.1, letting $k = 0$ there.) Since we already know that $\xi \cdot U$ is a factor of $U \mapsto R(f, U)$ if $F(\xi) = 0$ and $\xi \neq 0$, the proof of the linear factorization is complete, assuming the proof of the existence of $\bar{f}$ in Appendix E.

The proof of the existence of $\bar{f}$ is a tedious digression; that is why it has been placed in the appendix.

The following proposition is now established. We use $\mathbb{R}\mathrm{Poly}(n, n, d)$ to denote the subset of systems in $\mathbb{C}\mathrm{Poly}(n, n, d)$ with real coefficients.

PROPOSITION 2.2.1. *There exists a constructible non-trivial (i.e. not identically zero) polynomial* $R:\mathbb{C}\mathrm{Poly}(n, n, d)\times\mathbb{C}^{n+1}\to\mathbb{C}$ *of degree* $d^{O(n)}$ *with the following properties*:

(i) *if* $f\in\mathbb{C}\mathrm{Poly}(n, n, d)$ *is such that* $U\mapsto R(f, U)$ *is not identically zero, then* $U\mapsto R(f, U)$ *factors linearly*

$$U\mapsto R(f, U)=\prod_{i=1}^{d^n}\xi^{(i)}\cdot U,$$

where the zeros of f *are precisely the points* $\mathrm{Aff}(\xi^{(i)})$ *that are well-defined, i.e.* $\xi^{(i)}_{n+1}\neq 0$;

(ii) $R:\mathbb{R}\mathrm{Poly}(n, n, d)\times\mathbb{R}^{n+1}\mapsto\mathbb{R}$, *i.e. R restricted to real arguments yields real values*; *in particular, for* $f\in\mathbb{R}\mathrm{Poly}(n, n, d)$, $U\mapsto R(f, U)$ *is a real polynomial.*

2.3. The polynomial R càn be used to reduce some multi-variate polynomial problems to univariate ones. For example, it allows the problem of approximating the zeros of $f:\mathbb{C}^n\to\mathbb{C}^n$ to essentially be reduced to the problem of approximating the zeros of a univariate polynomial. We now indicate how this can be done. The perspective gained from the following presentation is very important in motivating the later algorithms.

Assume that $f\in\mathbb{C}\mathrm{Poly}(n, n, d)$ is such that $U\mapsto R(f, U)$ is not identically zero and hence

$$U\mapsto R(f, U)=\prod_{i=1}^{d^n}\xi^{(i)}\cdot U, \tag{2.3.1}$$

where the zeros of f are precisely those points $\mathrm{Aff}(\xi^{(i)})$ that are well-defined.

Fix $\beta\in\mathbb{C}^{n+1}$. Assume that β is such that if $\xi^{(i)}$ corresponds to a zero at infinity, then $\xi^{(i)}\cdot\beta\neq 0$. Then $\xi^{(i)}\cdot(\beta+te_{n+1})$ is a non-zero constant independent of t; here, e_{n+1} is the $n+1$th standard unit vector.

For each $\xi^{(i)}$ corresponding to a finite zero, there exists exactly one $t^{(i)}\in\mathbb{C}$ satisfying $\xi^{(i)}\cdot(\beta+t^{(i)}e_{n+1})=0$. Assume that $t^{(i)}\neq t^{(j)}$ if $i\neq j$. (This assumption will be eliminated shortly.)

Consider the univariate polynomial $t\mapsto R(f, \beta+te_{n+1})$. From our assumptions and the linear factorization (2.3.1) we find that this polynomial has precisely the $t^{(i)}$ as zeros. Moreover, invoking the product rule for differentiation shows that $\nabla_U R(f, \beta+t^{(i)}e_{n+1})$ is a non-zero multiple of $\xi^{(i)}$. (Throughout this paper, $\nabla_U R(f, U)$ is the vector with jth coordinate $\partial R/\partial U_j$.) Hence, the finite zeros of f are precisely the points $\mathrm{Aff}[\nabla_U R(f, \beta+t^{(i)}e_{n+1})]$. By approximating the zeros $t^{(i)}$ of the univariate polynomial one can obtain, in the obvious manner, approximations to the zeros of f.

Although we never actually approximate the zeros of f in this paper, what is important about the preceding discussion is the correspondence

$$\mathrm{Aff}(\xi^{(i)})=\mathrm{Aff}[\nabla_U R(f, \beta+t^{(i)}e_{n+1})].$$

However, this correspondence rests on some strong assumptions.

Perhaps the most restrictive assumption made in the above argument is that $t^{(i)}\neq t^{(j)}$ if $i\neq j$. This assumption is not difficult to remove. To see how, first replace the assumption that $t^{(i)}\neq t^{(j)}$ if $i\neq j$ with the weaker assumption that $t^{(i)}=t^{(j)}$ if and only if $\xi^{(i)}$ is a multiple of $\xi^{(j)}$. (We will remove this weaker assumption shortly.) Then, for example, if multiples of $\xi^{(1)}$ occur exactly k times among the $\xi^{(i)}$, the product rule applied to the linear factorization (2.3.1) shows the vector

$$\frac{\mathrm{d}^{k-1}}{\mathrm{d}t^{k-1}}\nabla_U R(f,\beta+t^{(1)}e_{n+1})$$

is a non-zero multiple of $\xi^{(1)}$. Hence, as is very important in this paper, each zero of f is then of the form $\mathrm{Aff}(\bar{\xi})$ where

$$\bar{\xi}=\frac{\mathrm{d}^j}{\mathrm{d}t^j}\nabla_U R(f,\beta+\bar{t}e_{n+1}),$$

$$\bar{t}\text{ is a zero of } t\mapsto R(f,\beta+te_{n+1}),$$

$$0\leq j\leq d^n.$$

Of course all such points $\mathrm{Aff}(\bar{\xi})$ may not be zeros of f, but that will be of no concern to us.

Finally, we show that all of the assumptions on β can be removed. These assumptions are now (i) $\xi^{(i)}\cdot\beta\neq 0$ if $\xi^{(i)}$ corresponds to a zero at infinity; (ii) the polynomial $t\mapsto R(f,\beta+te_{n+1})$ defined by β is such that $t^{(i)}=t^{(j)}$ iff $\xi^{(i)}$ is a multiple of $\xi^{(j)}$. We show that a certain finite set contains an appropriate β. Computational methods exist for determining exactly which elements in this set are appropriate, but our applications only require the knowledge that at least one is indeed appropriate.

The set is simply

$$\{(i^{n-1},i^{n-2},\ldots,i,1,0);\ i\text{ an integer, } 0\leq i\leq nd^{2n}\}. \tag{2.3.2}$$

The crucial property this set possesses is that each subset of n vectors is linearly independent. (Otherwise there would exist numbers a_i, not all zero, such that the degree $n-1$ polynomial $z\mapsto\sum_{i=0}^{n-1}a_iz^i$ has at least n (integer) zeros.) In particular, if $\xi^{(i)}$ corresponds to a zero at infinity, then at most $n-1$ elements β of (2.3.2) satisfy $\xi^{(i)}\cdot\beta=0$. Similarly, if $\xi^{(i)}$ and $\xi^{(j)}$ correspond to finite zeros and $\xi^{(i)}$ is not a multiple of $\xi^{(j)}$, then at most $n-1$ elements in (2.3.2) can lie in the projection of $\{U;\ \xi^{(i)}\cdot U=0=\xi^{(j)}\cdot U\}$ onto $\mathbb{C}^n\times\{0\}$. A simple counting argument now shows that (2.3.2) must contain at least one β satisfying both (i) and (ii) of the preceding paragraph.

In the foregoing discussion we assumed that $f\in\mathbb{C}\mathrm{Poly}(n,n,d)$. Under the more restrictive assumption $f\in\mathbb{R}\mathrm{Poly}(n,n,d)$, note that if $\mathrm{Aff}(\xi^{(i)})$ and β are real, then so is $t^{(i)}$.

For positive integers n and D, define

$$\mathcal{B}(n+1,D):=\{(i^{n-1},i^{n-2},\ldots,i,1,0);\ 0\leq i\leq nD^2\}. \tag{2.3.3}$$

We have now established the following crucial proposition.

Proposition 2.3.1. *Assume that $f\in\mathbb{R}\mathrm{Poly}(n,n,d)$ is such that $U\mapsto R(f,U)$ is not identically zero. Assume that $\bar{x}\in\mathbb{R}^n$ satisfies $f(\bar{x})=0$. Then there exist $\beta\in\mathcal{B}(n+1,d^n)$ and $0\leq j\leq d^n$ such that $t\mapsto R(f,\beta+te_{n+1})$ is not identically zero and for some real zero $\bar{t}$ of $t\mapsto R(f,\beta+te_{n+1})$,*

$$\bar{x}=\mathrm{Aff}\left(\frac{\mathrm{d}^j}{\mathrm{d}t^j}\nabla_U R(f,\beta+\bar{t}e_{n+1})\right).$$

More generally, given any polynomial $R:\mathbb{R}^{n+1}\mapsto\mathbb{R}$ of degree at most D that is not identically zero and factors linearly (over the complex numbers) $\prod_i\xi^{(i)}\cdot U$, for each $\xi^{(i)}$ for *which* $\mathrm{Aff}(\xi^{(i)})$ *is well-defined and real there exist* $\beta \in \mathscr{B}(n+1, D)$ *and* $0 \le j \le D$ *such that* $t \mapsto R(\beta + te_{n+1})$ *is not identically zero, and for some real zero* $\bar{t}$ *of* $t \mapsto R(\beta + te_{n+1})$, *the vector*

$$\bar{\xi} := \frac{\mathrm{d}^j}{\mathrm{d}t^j} \nabla R(\beta + \bar{t}e_{n+1})$$

satisfies $\mathrm{Aff}(\bar{\xi}) = \mathrm{Aff}(\xi^{(i)})$.

2.4. In our applications we will need to handle certain "degenerate" cases in the sense that $U \mapsto R(f, U)$ will be identically zero for the underlying system f. To do this our constructions will rely on limits of systems of polynomials.

More specifically, assume that $f, \bar{f}: \mathbb{R}^n \to \mathbb{R}^n$ are systems of polynomials each of degree at most d and assume that $U \mapsto R(\bar{f}, U)$ is not identically zero. For particular f and $\bar{f}$, our constructions will require knowledge about the limit points of zeros of

$$x \mapsto \varepsilon \bar{f}(x) + (1-\varepsilon) f(x)$$

as $\varepsilon \downarrow 0$. If the polynomial $U \mapsto R(f, U)$ is not identically zero then it encodes the requisite knowledge. If it is identically zero then we need another trick.

With f and $\bar{f}$ fixed, consider the polynomial

$$\bar{R}(\varepsilon, U) := R(\varepsilon \bar{f} + (1-\varepsilon) f, U).$$

Having assumed that $U \mapsto R(\bar{f}, U)$ is not identically zero, neither is $\bar{R}$. Thus we can expand $\bar{R}$ in powers of ε to obtain

$$\bar{R}(\varepsilon, U) = \sum_{i \ge k} \varepsilon^i R_i(U),$$

where R_k is not identically zero. The polynomial R_k encodes the information that we need.

PROPOSITION 2.4.1. (Canny (1990); similar results are in Grigor'ev (1988).) *The polynomial* R_k *factors linearly*

$$R_k(U) = \prod_{i=1}^{d^n} \xi^{(i)} \cdot U,$$

where the limit points of the zeros of

$$x \mapsto \varepsilon \bar{f}(x) + (1-\varepsilon) f(x)$$

as $\varepsilon \downarrow 0$ *are precisely those points* $\mathrm{Aff}(\xi^{(i)})$ *that are well-defined, i.e.* $\xi^{(i)}_{n+1} \neq 0$.

PROOF. Define

$$\hat{R}(\varepsilon, U) := R_k(U) + \sum_{i > k} \varepsilon^{i-k} R_i(U),$$

i.e. $\hat{R}$ is $1/\varepsilon^k$ times $\bar{R}$. Choose $U' \in \mathbb{C}^{n+1}$ such that $R_k(U') \neq 0$.

Since $\hat{R}$ is a polynomial and R_k is not identically zero, there are only finitely many values of ε for which $U \mapsto \hat{R}(\varepsilon, U)$ is identically zero. Hence for all $\varepsilon \neq 0$ in some open neighbourhood of 0, $U \mapsto \hat{R}(\varepsilon, U)$ factors

$$\hat{R}(\varepsilon, U) = \prod_{i=1}^{d^n} \xi^{(i)}(\varepsilon) \cdot U, \tag{2.4.1}$$

where the zeros of $x \mapsto \varepsilon \bar{f}(x) + (1-\varepsilon) f(x)$ are precisely those points $\mathrm{Aff}(\xi^{(i)}(\varepsilon))$ that are well-defined. Moreover, we may assume that $\hat{R}(\varepsilon, U') \neq 0$ for ε in this neighbourhood by restricting it further if necessary; hence we may assume that $\xi^{(i)}(\varepsilon) \cdot U' \neq 0$ for ε in this neighbourhood.

From the factorization (2.4.1) it is easily seen that the zeros of the univariate polynomial $t \mapsto \hat{R}(\varepsilon, -e_j + tU')$ are precisely the points

$$\xi_j^{(i)}(\varepsilon) / \xi^{(i)}(\varepsilon) \cdot U'. \tag{2.4.2}$$

(Here, e_j is the jth standard unit vector.) Since the zeros of a univariate polynomial vary continuously in the coefficients of the polynomial, the zeros of the degree d^n polynomial $t \mapsto \hat{R}(0, -e_j + tU')$ are the limit points of (2.4.2) as $\varepsilon \downarrow 0$. Hence we may define

$$\bar{\xi}^{(i)} := \lim_{\varepsilon \downarrow 0} \left(\frac{1}{\xi^{(i)}(\varepsilon) \cdot U'} \right) \xi^{(i)}(\varepsilon).$$

Clearly, the limit points of the zeros of $x \mapsto \varepsilon \bar{f}(x) + (1-\varepsilon) f(x)$ as $\varepsilon \downarrow 0$ are precisely those points $\mathrm{Aff}(\bar{\xi}^{(i)})$ that are well-defined.

Since

$$\prod_{i=1}^{d^n} \left(\frac{1}{\xi^{(i)}(\varepsilon) \cdot U'} \right) \xi^{(i)}(\varepsilon) \cdot U = \frac{\hat{R}(\varepsilon, U)}{\hat{R}(\varepsilon, U')},$$

it is now easily argued that $\hat{R}(0, U) = 0$ if and only if $\bar{\xi}^{(i)} \cdot U = 0$ for some i. From this the factorization of $R_k(U) = \hat{R}(0, U)$ follows. Furthermore, the resulting $\xi^{(i)}$ are simply non-zero multiples of the $\bar{\xi}^{(i)}$, and hence $\mathrm{Aff}(\xi^{(i)}) = \mathrm{Aff}(\bar{\xi}^{(i)})$ if either of these points (and hence both) is well-defined; hence the limit points of the zeros of $x \mapsto \varepsilon \bar{f}(x) + (1-\varepsilon) f(x)$ as $\varepsilon \downarrow 0$ are precisely those points $\mathrm{Aff}(\xi^{(i)})$ that are well-defined.

2.5. We close this section with a simple lemma that will allow us to work with projections in an easy way.

Lemma 2.5.1. *Assume that $R : \mathbb{C}^{n+2} \to \mathbb{C}$ is not identically zero and factors linearly $R(\bar{U}) = \prod_i \bar{\xi}^{(i)} \cdot \bar{U}$ where $\bar{U} = (U_0, \ldots, U_{n+1})$. Let the expansion of R in powers of U_0 be*

$$R(\bar{U}) = \sum_{i \geq k} U_0^i R_i(U),$$

where $U = (U_1, \ldots, U_{n+1})$ and R_k is not identically zero. Then R_k factors linearly

$$R_k(U) = \prod_j \xi^{(j)} \cdot U.$$

Moreover, the points $\mathrm{Aff}(\xi^{(j)}) \in \mathbb{C}^n$ that are well-defined are precisely the projection onto $(x_1, \ldots, x_n)$ of the points $(\bar{x}_0, \ldots, \bar{x}_n) = \mathrm{Aff}(\bar{\xi}^{(i)})$ that are well-defined.

Proof. Assume without loss of generality that those $\bar{\xi}^{(i)}$ for which $\bar{\xi}_1^{(i)} = \cdots = \bar{\xi}_{n+1}^{(i)} = 0$ are precisely $\bar{\xi}^{(1)}, \ldots, \bar{\xi}^{(k')}$. Then, trivially, $k = k'$ and R_k is a non-zero multiple of

$$\prod_{i > k} \xi^{(i)} \cdot U,$$

where $\xi^{(i)} := (\bar{\xi}_1^{(i)}, \ldots, \bar{\xi}_{n+1}^{(i)})$. The remaining claims follow easily.

3. The Construction of a "Small" Set of "Low" Degree Polynomials Which Encodes "Easily" Extractable Information About Connected Sign Partitions

3.1. Define $\mathbb{R}\text{Poly}(m, n, d)$ to be the vector space of tuples $g = (g_1, \ldots, g_m)$ of polynomials $g_i : \mathbb{R}^n \to \mathbb{R}$ of degree at most d. Recall that the elements of the connected sign partition $\text{CSP}\{g_i\}_i$ were defined as the maximal connected sets in $\mathbb{R}^n$ satisfying the property that two points $\bar{x}$ and $\hat{x}$ are in the same element only if the sign of g_i at $\bar{x}$ is the same as that at $\hat{x}$ for all i.

By identifying systems in $\mathbb{R}\text{Poly}(m, n, d)$ with their vector of coefficients, we can view $\mathbb{R}\text{Poly}(m, n, d)$ as $\mathbb{R}^N$ for the appropriate N.

In this section we construct a set $\mathcal{R}(m, n, d)$ of $(md)^{O(n)}$ polynomials $R : \mathbb{R}\text{Poly}(m, n, d) \times \mathbb{R}^{n+1} \to \mathbb{R}$ of degree at most $(md)^{O(n)}$ with the following property: for each $g \in \mathbb{R}\text{Poly}(m, n, d)$ and each element of $\text{CSP}\{g_i\}_i$ there exists $R \in \mathcal{R}(m, n, d)$ such that $U \mapsto R(g, U)$ is not identically zero and factors linearly $\prod_i \xi^{(i)} \cdot U$ where for some i, $\text{Aff}(\xi^{(i)})$ is in the element.

As an obvious corollary we have the well-known fact discussed in the Introduction that the number of elements in $\text{CSP}\{g_i\}_i$ is $(md)^{O(n)}$.

The construction is "elementary", but our description is lengthy. We have tried to isolate the ideas behind the construction, introducing each when it becomes naturally apparent that something more is needed for the construction.

The results of this section are summarized in subsections 3.8, 3.9 and 3.10.

3.2. For $S \subseteq \{1, \ldots, m\}$ define

$$\text{Feas}\{g_i\}_{i \in S} := \{x;\ g_i(x) \geq 0\ \forall i \in S\}.$$

The major step in the overall construction is the construction of a particular set of polynomials $R : \mathbb{R}\text{Poly}(m, n, d) \times \mathbb{R}^{n+1} \to \mathbb{R}$ with the following property: for each $g \in \mathbb{R}\text{Poly}(m, n, d)$, each $S \subseteq \{1, \ldots, m\}$ and each connected component of $\text{Feas}\{g_i\}_{i \in S}$ there exists a polynomial R in the set such that $U \mapsto R(g, U)$ is not identically zero and factors linearly $\prod \xi^{(i)} \cdot U$ where for some i, $\text{Aff}(\xi^{(i)})$ is in the component.

Our approach to this construction is through consideration of the following non-linear programming problem:

$$\min f(x) := \sum_j (m+1)^j x_j^{d'}.$$

NLP(S)

$$\text{s.t. } g_i(x) \geq 0\ \forall i \in S,$$

where d' is the least even integer at least as great as d.

It is easily proven that each connected component of $\text{Feas}\{g_i\}_{i \in S}$ contains a local optimum of NLP(S)—a point x^* is said to be a local optimum if there exists $\varepsilon > 0$ such that for all x satisfying both $\|x - x^*\| \leq \varepsilon$ and $x \in \text{Feas}\{g_i\}_i$, $f(x^*) \leq f(x)$.

The following proposition provides a partial algebraic characterization of local optima of NLP(S).

Recall that $\nabla f(x)$ denotes the gradient of f at x.

PROPOSITION 3.2.1. *Assume that x^* is a local optimum of* NLP(S). *Define*

$$\mathcal{A} := \{i \in S;\ g_i(x^*) = 0\},$$

the indices of the constraints that are "active" at x^*. Then $\{\nabla f(x^*), \nabla g_i(x^*);\ i \in \mathscr{A}\}$ is a linearly dependent set.

Proof. Assume otherwise. Let $k = \#\mathscr{A}$, the number of elements in $\mathscr{A}$, and let M denote the $(k+1)\times n$ matrix with rows $\nabla f(x^*)$, $\nabla g_i(x^*)$, $i \in \mathscr{A}$. Then M maps $\mathbb{R}^n$ onto $\mathbb{R}^{k+1}$ so that there exists $v \in \mathbb{R}^n$ satisfying $\nabla f(x^*)v = -1$, $\nabla g_i(x^*)v = 1$ for all $i \in \mathscr{A}$. For all sufficiently small $\varepsilon > 0$, $f(x^* + \varepsilon v) < f(x^*)$ and $g_i(x^* + \varepsilon v) > 0$ for all $i \in S$, contradicting x^* being a local optimum.

Another way of stating the proposition is as follows. Assume that x^* is a local optimum and $\mathscr{A}$ is the (possibly empty) set of indices of those constraints that are active at x^*. Let $M_{\mathscr{A}}(x)$ be the matrix whose rows are precisely the vectors $\nabla g_i(x)$, $i \in \mathscr{A}$ and $\nabla f(x)$—for definiteness in what is to follow, specify $M_{\mathscr{A}}(x)$ uniquely as the matrix with last row $\nabla f(x)$ and with earlier rows $\nabla g_i(x)$, where $\nabla g_i(x)$ occurs before $\nabla g_j(x)$ if $i < j$. Then $\det M_{\mathscr{A}}(x^*)M_{\mathscr{A}}^T(x^*) = 0$.

Hence, x^* is a local optimum of NLP(S) only if there exists $\mathscr{A} \subseteq S$ such that x^* is a zero of

$$h_{\mathscr{A}}(x) := \det M_{\mathscr{A}}(x)M_{\mathscr{A}}^T(x) + \sum_{i \in \mathscr{A}} g_i^2(x). \tag{3.2.1}$$

We have now established the following fact. For each $S \subseteq \{1, \ldots, m\}$ and for each connected component of Feas$\{g_i\}_{i\in S}$ there exists $\mathscr{A} \subseteq S$ such that some real zero of $h_{\mathscr{A}}(x)$ lies in the component.

For $\mathscr{A} \subseteq \{1, \ldots, m\}$ let

$$d(\mathscr{A}) := 2d(1 + \#\mathscr{A})$$

where $\#\mathscr{A}$ is the number of elements of $\mathscr{A}$. In particular, $d(\mathscr{A})$ is an even integer at least as great as the degree of $h_{\mathscr{A}}$.

3.3. To motivate our approach we introduce an assumption that will later be eliminated. Assume that for all $\mathscr{A} \subseteq \{1, \ldots, m\}$, $h_{\mathscr{A}}(x)$ has only finitely many real zeros.

Consider the unconstrained minimization problem

$$\min_x [x \mapsto \tilde{h}_{\mathscr{A}}(\varepsilon, x)], \tag{3.3.1}$$

where

$$\tilde{h}_{\mathscr{A}}(\varepsilon, x) := -\varepsilon \sum_j x_j^{d(\mathscr{A})} + (1 - \varepsilon)h_{\mathscr{A}}(x).$$

Note that $\tilde{h}_{\mathscr{A}}(0, x) = h_{\mathscr{A}}(x)$. Of course x^* is a local optimum for this problem only if $\nabla_x \tilde{h}_{\mathscr{A}}(\varepsilon, x^*) = 0$.

Clearly, since $d(\mathscr{A})$ is even, the limit points of the set $\{x;\ \tilde{h}_{\mathscr{A}}(\varepsilon, x) \le 0\}$ as $\varepsilon \downarrow 0$ are precisely the points in the set $\{x;\ h_{\mathscr{A}}(x) \le 0\}$. Since $h_{\mathscr{A}}(x) \ge 0$ for all x, the limit points are simply the zeros of $h_{\mathscr{A}}(x)$. Consequently, under the assumption that there are only finitely many real zeros for $h_{\mathscr{A}}(x)$, it follows that each of the real zeros is the limit point of an entire connected component of $\{x;\ \tilde{h}(\varepsilon, x) \le 0\}$ as $\varepsilon \downarrow 0$. Thus, each of the real zeros for $h_{\mathscr{A}}(x)$ is the limit point of local optima of (3.3.1) as $\varepsilon \downarrow 0$ and hence, each of the zeros is the limit point of zeros of $x \mapsto \nabla_x \tilde{h}_{\mathscr{A}}(\varepsilon, x)$ as $\varepsilon \downarrow 0$.

Fix $\mathscr{A}\subseteq\{1,\dots,m\}$. Let $R:\mathbb{R}\mathrm{Poly}(n,n,d(\mathscr{A})-1)\times\mathbb{R}^{n+1}\to\mathbb{R}^n$ denote the "u-resultant" polynomial constructed in section 2.2. Define the polynomial

$$\bar{R}_{\mathscr{A}}:\mathbb{R}\mathrm{Poly}(m,n,d)\times\mathbb{R}\times\mathbb{R}^{n+1}\to\mathbb{R}^n$$

by

$$\bar{R}_{\mathscr{A}}(g,\varepsilon,U):=R(x\mapsto\nabla_x\tilde{h}_{\mathscr{A}}(\varepsilon,x),U).$$

It is easily determined from the definitions that $\bar{R}_{\mathscr{A}}(g,1,U)$ is a non-zero multiple of $U_{n+1}^{(d(a)-1)^n}$, in particular, $U\mapsto\bar{R}_{\mathscr{A}}(g,1,U)\not\equiv 0$ (i.e. is not identically zero). Hence, (i) expanding $\bar{R}_{\mathscr{A}}(g,\varepsilon,U)$ in powers of ε,

$$\bar{R}_{\mathscr{A}}(g,\varepsilon,U)=\sum_i\varepsilon^i\bar{R}_{\mathscr{A}}^{(i)}(g,U),$$

(ii) fixing g and (iii) letting $i'=i(g,\mathscr{A})$ be the smallest integer i for which $U\mapsto\bar{R}_{\mathscr{A}}^{(i)}(g,U)\not\equiv 0$, it follows from Proposition 2.4.1 that $U\mapsto\bar{R}_{\mathscr{A}}^{(i')}(g,U)$ factors linearly $\prod_i\xi^{(i)}\cdot U$ and the limit points of $\{x;\nabla_x\tilde{h}_{\mathscr{A}}(\varepsilon,x)=0\}$ as $\varepsilon\downarrow 0$ are precisely the points $\mathrm{Aff}(\xi^{(i)})$ that are well-defined. In particular, if $h_{\mathscr{A}}(x)$ has only finitely many real zeros, then for each real zero x^* there exists i such that $x^*=\mathrm{Aff}(\xi^{(i)})$.

Recall that presently we are working towards constructing a set of polynomials such that for each $S\subseteq\{1,\dots,m\}$ and connected component of $\mathrm{Feas}\{g_i\}_{i\in S}$ at least one of these polynomials factors linearly to yield a point with affine image in the component. The set we desire to construct could be defined simply as the set of $R_{\mathscr{A}}^{(i)}$ as $\mathscr{A}$ ranges over all subsets of $\{1,\dots,m\}$ were it not for two problems: (i) if g is such that $h_{\mathscr{A}}(x)$ has infinitely many real zeros for some $\mathscr{A}$, then there is no guarantee from our analysis that for each connected component of $\mathrm{Feas}\{g_i\}_{i\in S}$ there would exist R in the set for which $U\mapsto R(g,U)$ is not identically zero and factors linearly $\prod_i\xi^{(i)}\cdot U$ where for some i, $\mathrm{Aff}(\xi^{(i)})$ is in the component; (ii) the set thus defined would contain at least 2^m polynomials—we definitely want to avoid exponential dependence on m.

3.4. To circumvent these problems we introduce another construction based on taking a limit. Define $\bar{g}_i:\mathbb{R}\times\mathbb{R}^n\to\mathbb{R}$ by

$$\bar{g}_i(\delta,x)=(1-\delta)g_i(x)+\delta\left(1+\sum_j i^jx_j^{d'}\right),$$

where, again, d' is the least even integer at least as great as d. Because for each $S\subseteq\{1,\dots,m\}$ the limit points of

$$\{x;\ \bar{g}_i(\delta,x)\geq 0\ \forall i\in S\}$$

as $\delta\downarrow 0$ are precisely the points in $\mathrm{Feas}\{g_i\}_{i\in S}$, it is easily proven that each connected component of $\mathrm{Feas}\{g_i\}_{i\in S}$ contains a limit point of local optima of the non-linear programming problem

$$\min_x f(x)\left(:=\sum_j(m+1)^jx_j^{d'}\right).$$

NLP(δ,S)

$$\text{s.t. } x\mapsto\bar{g}_i(\delta,x)\geq 0\quad\forall i\in S$$

as $\delta \downarrow 0$. (For assume that C denotes a connected component of Feas$\{g_i\}_{i\in S}$. Noting that d' is even, there exists a point x^* which minimizes f over the closed set C and, moreover, there exists r such that for any $x \in \mathbb{R}^n$ satisfying $\|x\| \geq r$, $f(x) > f(x^*)$. Now, since the closed set Feas$\{g_i\}_i$ is precisely the set of limit points of $\{x;\ \bar{g}_i(\delta, x) \geq 0\ \forall i \in S\}$ as $\delta \downarrow 0$, and since C is contained in each of these sets (assuming $\delta \geq 0$), $C \cap \{x;\ \|x\| \leq r\}$ is the set of limit points of a connected component $C'(\delta)$ of $\{x;\ \bar{g}_i(\delta, x) \geq 0\ \forall i \in S\} \cap \{x;\ \|x\| \leq r\}$ as $\delta \downarrow 0$; moreover, $C \cap \{x;\ \|x\| \leq r\} \subseteq C'(\delta)$ and hence $x^* \in C'(\delta)$. Let $C''(\delta)$ denote the connected component of $\{x;\ \bar{g}_i(\delta, x) \geq 0\ \forall i \in S\}$ containing $C'(\delta)$. Since $x^* \in C'(\delta)$, the definition of r implies that f restricted to $C''(\delta)$ has a local minimum in $C'(\delta)$; since $C'(\delta)$ converges to a bounded subset of C as $\delta \downarrow 0$, the proof is complete.)

Of course NLP(0, S) is just the non-linear programming problem we denoted by NLP(S) in section 3.2.

For $\mathscr{A} \subseteq \{1, \ldots, m\}$, define $M_{\mathscr{A}}(\delta, x)$ to be the matrix whose rows are precisely the vectors $\nabla_x g_i(\delta, x)$ for $i \in \mathscr{A}$, and the vector $\nabla_x f(x)$, ordered in the obvious manner. Define

$$h_{\mathscr{A}}(\delta, x) := \det M_{\mathscr{A}}(\delta, x) M_{\mathscr{A}}^T(\delta, x) + \sum_{i \in \mathscr{A}} \bar{g}_i^2(\delta, x).$$

Then the local optima of NLP(δ, S) are contained in the set

$$\bigcup_{\mathscr{A} \subseteq \{1, \ldots, m\}} \{x;\ h_{\mathscr{A}}(\delta, x) = 0\}. \tag{3.4.1}$$

Hence, each connected component of Feas$\{g_i\}_{i\in S}$ contains a limit point of the set (3.4.1) as $\delta \downarrow 0$.

Of course $x \mapsto h_{\mathscr{A}}(0, x)$ is just the polynomial we denoted by $h_{\mathscr{A}}(x)$ in section 3.2.

For all but finitely many values of δ the polynomials $h_{\mathscr{A}}(\delta, x)$ have a particulary nice structure as is made evident by the following lemma. The proof of the lemma is somewhat lengthy and is deferred to section 3.1.1. The lemma is absolutely crucial to our approach.

LEMMA 3.4.1. *For all but finitely many values of δ the following is true. Let $\mathscr{A} \subseteq \{1, \ldots, m\}$. If $\#\mathscr{A} > n$ then $x \mapsto h_{\mathscr{A}}(\delta, x)$ has no real zeros. If $\#\mathscr{A} \leq n$ then $x \mapsto h_{\mathscr{A}}(\delta, x)$ has only finitely many real zeros.*

Again let $d(\mathscr{A}) := 2d(1 + \#\mathscr{A})$. For each $\mathscr{A} \subseteq \{1, \ldots, m\}$ define $\tilde{h}_{\mathscr{A}} : \mathbb{R} \times \mathbb{R} \times \mathbb{R}^n \to \mathbb{R}$ by

$$\tilde{h}_{\mathscr{A}}(\varepsilon, \delta, x) = -\varepsilon \sum_j x_j^{d(\mathscr{A})} + (1 - \varepsilon) h_{\mathscr{A}}(\delta, x).$$

Of course $x \mapsto \tilde{h}_{\mathscr{A}}(\varepsilon, 0, x)$ is just the polynomial we denoted by $\tilde{h}_{\mathscr{A}}(\varepsilon, x)$ in section 3.3. Just as we showed that if $x \mapsto h_{\mathscr{A}}(x)$ has only finitely many real zeros then every real zero is a limit point of real zeros of $x \mapsto \nabla_x \tilde{h}_{\mathscr{A}}(\varepsilon, x)$ as $\varepsilon \downarrow 0$, one can show that if $x \mapsto h_{\mathscr{A}}(\delta, x)$ has only finitely many real zeros then every real zero is a limit point of real zeros of $x \mapsto \nabla_x \tilde{h}_{\mathscr{A}}(\varepsilon, \delta, x)$ as $\varepsilon \downarrow 0$.

Fix $\mathscr{A} \subseteq \{1, \ldots, m\}$. Again let $R : \mathbb{R}\text{Poly}(n, n, d(\mathscr{A}) - 1) \times \mathbb{R}^{n+1} \to \mathbb{R}$ denote the "u-resultant" polynomial constructed in section 2.2. Define $\bar{R}_{\mathscr{A}} : \mathbb{R}\text{Poly}(m, n, d) \times \mathbb{R} \times \mathbb{R} \times \mathbb{R}^{n+1} \to \mathbb{R}$ by

$$\bar{R}_{\mathscr{A}}(g, \varepsilon, \delta, U) := R(x \mapsto \nabla_x \tilde{h}_{\mathscr{A}}(\varepsilon, \delta, x), U).$$

Expand $\bar{R}_{\mathscr{A}}$ in powers of ε and δ:

$$\bar{R}_{\mathscr{A}}(g, \varepsilon, \delta, U) = \sum_i \sum_j \varepsilon^i \delta^j \bar{R}_{\mathscr{A}}^{(i,j)}(g, U).$$

Lemma 3.4.2. *The following is true for each $g \in \mathbb{R}\mathrm{Poly}(m, n, d)$. For every $\mathscr{A} \subseteq \{1, \ldots, m\}$, the polynomial*

$$(\varepsilon, \delta, U) \mapsto \bar{R}_{\mathscr{A}}(g, \varepsilon, \delta, U)$$

is not identically zero. Hence there exists $i' = i(g, \mathscr{A})$, $j' = j(g, \mathscr{A})$ such that

$$U \mapsto \bar{R}^{\langle i', j' \rangle}_{\mathscr{A}}(g, U) \not\equiv 0 \quad \textit{but} \quad U \mapsto \bar{R}^{\langle i, j \rangle}_{\mathscr{A}}(g, U) \equiv 0$$

if either (i) $i < i'$ *or* (ii) $i = i'$ *and* $j < j'$. *The polynomial*

$$U \mapsto \bar{R}^{\langle i', j' \rangle}_{\mathscr{A}}(g, U)$$

factors linearly $\prod_i \xi^{(i)}_{\mathscr{A}} \cdot U$ *over the complex numbers. For each $S \subseteq \{1, \ldots, m\}$ and each connected component of* $\mathrm{Feas}\{g_i\}_{i \in S}$ *there exists $\mathscr{A}$ satisfying $\# \mathscr{A} \le n$ and such that for some i,* $\mathrm{Aff}(\xi^{(i)}_{\mathscr{A}})$ *is in the component.*

Proof. Fix g. For brevity let $\bar{R}_{\mathscr{A}}(\varepsilon, \delta, U) := \bar{R}_{\mathscr{A}}(g, \varepsilon, \delta, U)$, $\bar{R}^{\langle i, j \rangle}_{\mathscr{A}}(U) := \bar{R}^{\langle i, j \rangle}_{\mathscr{A}}(g, U)$.

First, $\bar{R}_{\mathscr{A}}$ is not identically zero. In fact, by tracing back through the definitions one can easily show that $\bar{R}_{\mathscr{A}}(1, 0, U)$ is a non-zero multiple of $U_{n+1}^{(d(\mathscr{A})-1)^n}$.

Consider the expansion of $\bar{R}_{\mathscr{A}}$ in powers of ε:

$$\bar{R}_{\mathscr{A}}(\varepsilon, \delta, U) = \sum_i \varepsilon^i \bar{R}^{\langle i \rangle}_{\mathscr{A}}(\delta, U).$$

Then $i' = i'(g, \mathscr{A})$ as defined in the statement of the proposition is the smallest integer i such that $\bar{R}^{\langle i \rangle}_{\mathscr{A}}(\delta, U)$ is not identically zero in both δ and U.

Assume that $\bar{\delta} > 0$ is such that for all $\mathscr{A} \subseteq \{1, \ldots, m\}$, the interval $(0, \bar{\delta})$ does not contain any of the finitely many values of δ excluded by Lemma 3.4.1. Decreasing $\bar{\delta}$ if necessary, we may assume that for all $\delta \in (0, \bar{\delta})$ and all $\mathscr{A}$, $U \mapsto \bar{R}^{\langle i' \rangle}_{\mathscr{A}}(\delta, U) \not\equiv 0$.

Assume that $\delta \in (0, \bar{\delta})$. By definition, $x \mapsto h_{\mathscr{A}}(\delta, x)$ has only finitely many real zeros. Then the discussion of section 3.3 applied to the polynomial $x \mapsto h_{\mathscr{A}}(\delta, x)$ rather than to the polynomial $h_{\mathscr{A}}(x)$ shows that $U \mapsto \bar{R}^{\langle i' \rangle}_{\mathscr{A}}(\delta, U)$ factors linearly

$$U \mapsto \bar{R}^{\langle i' \rangle}_{\mathscr{A}}(\delta, U) := \prod_i \xi^{(i)}_{\mathscr{A}, \delta} \cdot U$$

and for each real zero $\bar{x}$ of $x \mapsto h_{\mathscr{A}}(\delta, x)$ there exists i such that $\bar{x} = \mathrm{Aff}(\xi^{(i)}_{\mathscr{A}, \delta})$. From Proposition 2.4.1 it now follows that $\bar{R}^{\langle i', j' \rangle}_{\mathscr{A}}$ factors linearly

$$\bar{R}^{\langle i', j' \rangle}_{\mathscr{A}}(U) = \prod_i \xi^{(i)}_{\mathscr{A}} \cdot U$$

and the limit points of $\{x \in \mathbb{R}^n;\ h_{\mathscr{A}}(\delta, x) = 0\}$ as $\delta \downarrow 0$ are contained among those points $\mathrm{Aff}(\xi^{(i)}_{\mathscr{A}})$ that are well-defined.

As discussed just prior to Lemma 3.4.1, each connected component of $\mathrm{Feas}\{g_i\}_{i \in S}$ has a limit point of

$$\bigcup_{\mathscr{A} \subseteq \{1, \ldots, m\}} \{x;\ h_{\mathscr{A}}(\delta, x) = 0\}$$

as $\delta \downarrow 0$. Since $x \mapsto h_{\mathscr{A}}(\delta, x)$ has no real zeros if both $\delta \in (0, \bar{\delta})$ and $\# \mathscr{A} > n$, the proof is complete.

3.5. In the preceding we have been concerned with constructing a set of polynomials such that for each $S \subseteq \{1, \ldots, m\}$ and each connected component of $\text{Feas}\{g_i\}_{i\in S}$ at least one of the polynomials factors linearly to yield a point in $\text{Feas}\{g_i\}_{i\in S}$; Lemma 3.4.2 shows the set of polynomials $\bar{R}^{(i,j)}_{\mathscr{A}}$ for all i, j and $\mathscr{A}$ satisfying $\#\mathscr{A} \leq n$ to be an appropriate choice. Now we consider a slightly different problem, that of constructing a set of polynomials such that for each $\Delta = (\Delta_1, \ldots, \Delta_m) \in \{\leq, =, \geq\}^m$ and each connected component of

$$\text{Feas}_\Delta\{g_i\}_i := \{x \in \mathbb{R}^n;\ g_i(x)\Delta_i 0\ \forall i = 1, \ldots, m\}$$

at least one of the polynomials factors linearly to yield a point in the component.

For $i = 1, \ldots, m$, define $g_{m+i} := -g_i$. It is easily seen that an appropriate set of polynomials would be a set with the property that for each $S \subseteq \{1, \ldots, 2m\}$ and each connected component of $\text{Feas}\{g_i\}_{i\in S}$ at least one of the polynomials factors linearly to yield a point in the component. However, if in section 3.4 we replace $(g_1, \ldots, g_m)$ with $(g_1, \ldots, g_{2m}) = (g_1, \ldots, g_m, -g_1, \ldots, -g_m)$ and $\mathscr{A} \subseteq \{1, \ldots, m\}$ with $\mathscr{A} \subseteq \{1, \ldots, 2m\}$ we obtain such a set of polynomials $\bar{R}^{(i,j)}_{\mathscr{A}} : \mathbb{R}\text{Poly}(m, n, d) \times \mathbb{R}^{n+1} \to \mathbb{R}$ where $\mathscr{A}$ can be restricted to satisfy $\#\mathscr{A} \leq n$.

3.6. We are now in a position to accomplish the real goal of this section, the construction of a set $\mathscr{R}(m, n, d)$ of polynomials $R : \mathbb{R}\text{Poly}(m, n, d) \times \mathbb{R}^{n+1} \to \mathbb{R}$ such that for each $g \in \mathbb{R}\text{Poly}(m, n, d)$ and each element of the connected sign partition $\text{CSP}\{g_i\}_i$ there exists $R \in \mathscr{R}(m, n, d)$ such that $U \mapsto R(g, U)$ is not identically zero and factors linearly $\prod_i \xi^{(i)} \cdot U$ where for some i, $\text{Aff}(\xi^{(i)})$ is in the element.

We accomplish this goal through a simple construction involving one additional variable. Let $\{h_i\}_i$ be the set consisting of the following $3m+1$ polynomials in $(x_0, x) \in \mathbb{R} \times \mathbb{R}^n$:

$$\begin{array}{ll} h_i(x_0, x) = g_i(x) & i = 1, \ldots, m \\ h_{m+i}(x_0, x) = x_0 g_i(x) - 1 & i = 1, \ldots, m \\ h_{2m+i}(x_0, x) = x_0 g_i(x) + 1 & i = 1, \ldots, m \\ h_{3m+1}(x_0, x) = x_0 - 1. & \end{array} \tag{3.6.1}$$

For $\sigma \in \{-1, 0, 1\}^m$ define $\Delta_j \in \{\leq, =, \geq\}$, $j = 1, \ldots, 3m+1$ as follows:

$$\Delta_i \text{ is} \left\{ \begin{array}{ll} \leq & \text{if } \sigma_i = -1 \\ = & \text{if } \sigma_i = 0 \\ \geq & \text{if } \sigma_i = 1 \end{array} \right\} \quad \text{for } i = 1, \ldots, m$$

$$\Delta_{m+i} \text{ is} \left\{ \begin{array}{ll} \leq & \text{if } \sigma_i = -1 \\ \leq & \text{if } \sigma_i = 0 \\ \geq & \text{if } \sigma_i = 1 \end{array} \right\} \quad \text{for } i = 1, \ldots, m$$

$$\Delta_{2m+i} \text{ is} \left\{ \begin{array}{ll} \leq & \text{if } \sigma_i = -1 \\ \geq & \text{if } \sigma_i = 0 \\ \geq & \text{if } \sigma_i = 1 \end{array} \right\} \quad \text{for } i = 1, \ldots, m$$

$$\Delta_{3m+1} \text{is} \geq$$

Note that if $(x_0, x) \in \text{Feas}_\Delta\{h_i\}_i$ then the sign vector of g at x is σ. Also note that if $x \in \mathbb{R}^n$ is such that the sign vector of g at x is σ then for all sufficiently large $x_0 > 0$,

$(x_0, x) \in \mathrm{Feas}_\Delta\{h_i\}_i$. It follows that for each element of $\mathrm{CSP}\{g_i\}_i$ there exists Δ such that the element is the union of projections of connected components of $\mathrm{Feas}_\Delta\{h_i\}_i$.

Let

$$\bar{R}^{\langle i,j\rangle}_{\mathscr{A}}: \mathbb{R}\mathrm{Poly}(3m+1, n+1, d+1) \times \mathbb{R}^{n+2} \to \mathbb{R}$$

be the polynomials as in section 3.5. Let $h := (h_1, \ldots, h_{3m+1})$. Thus, for each $\Delta \in \{\leq, =, \geq\}^{3m+1}$ and each connected component of $\mathrm{Feas}_\Delta\{h_i\}_i$ there exists an $\bar{R}^{\langle i,j\rangle}_{\mathscr{A}}$ such that

$$\bar{U} = (U_0, \ldots, U_{n+1}) \mapsto \bar{R}^{\langle i,j\rangle}_{\mathscr{A}}(h, \bar{U})$$

factors linearly to yield a point with affine image in the component.

Expand each $\bar{R}^{\langle i,j\rangle}_{\mathscr{A}}$ in powers of U_0:

$$\bar{R}^{\langle i,j\rangle}_{\mathscr{A}}(h, \bar{U}) = \sum_k U_0^k \bar{R}^{\langle i,j,k\rangle}_{\mathscr{A}}(h, U),$$

where $U = (U_1, \ldots, U_{n+1})$. By Lemma 2.5.1, if $\bar{U} \mapsto \bar{R}^{\langle i,j\rangle}_{\mathscr{A}}(h, \bar{U})$ factors linearly $\prod_l \bar{\xi}^l \cdot \bar{U}$ and if $k' = k(h, \mathscr{A}, i, j)$ is the smallest integer k such that

$$U \mapsto \bar{R}^{\langle i,j,k\rangle}_{\mathscr{A}}(h, U) \neq 0$$

then

$$U \mapsto \bar{R}^{\langle i,j,k'\rangle}_{\mathscr{A}}(h, U)$$

factors linearly $\prod_l \xi^{(l)} \cdot U$ where the projections of those points $\mathrm{Aff}(\bar{\xi}^{(l)})$ that are well-defined are precisely those points $\mathrm{Aff}(\xi^{(l)})$ that are well-defined.

Defining

$$R^{\langle i,j,k\rangle}_{\mathscr{A}}: \mathbb{R}\ \mathrm{Poly}(m, n, d) \times \mathbb{R}^{n+1} \to \mathbb{R}$$

by

$$R^{\langle i,j,k\rangle}_{\mathscr{A}}(g, U) := \bar{R}^{\langle i,j,k\rangle}_{\mathscr{A}}(h, U),$$

where h is as in (3.6.1) it should be clear that we finally have the set of polynomials $\mathscr{R}(m, n, d)$ that we have been seeking; all $R^{\langle i,j,k\rangle}_{\mathscr{A}}$ for which $\#\mathscr{A} \leq n+1$.

3.7. Now we consider the number of operations required for vital constructions based on the polynomials $R^{\langle i,j,k\rangle}_{\mathscr{A}}$. Letting $U = (U_1, \ldots, U_{n+1})$ and letting $\mathscr{A} \subseteq \{1, \ldots, 6m+2\}$, tracing back through the definitions we have that

$$R((x_0, x) \mapsto \nabla_{(x_0,x)} \tilde{h}_{\mathscr{A}}(\varepsilon, \delta, x_0, x), U_0, U) = \sum_i \sum_j \sum_k \varepsilon^i \delta^j U_0^k R^{\langle i,j,k\rangle}_{\mathscr{A}}(g, U), \quad (3.7.1)$$

where

(i) $R: \mathbb{R}\mathrm{Poly}(n+1, n+1, d(\mathscr{A})) \times \mathbb{R}^{n+2} \to \mathbb{R}$ is the "u-resultant" polynomial constructed in section 2.2;

(ii) $d(\mathscr{A}) := 2(d+1)(\#\mathscr{A}+1)$;

(iii) $\tilde{h}_{\mathscr{A}}(\varepsilon, \delta, x_0, x) := -\varepsilon \sum_{j=0}^{n+1} x_j^{d(\mathscr{A})} + (1-\varepsilon) h_{\mathscr{A}}(\delta, x_0, x)$;

(iv) $h_{\mathscr{A}}(\delta, x_0, x) = \det M_{\mathscr{A}}(\delta, x_0, x) M^T_{\mathscr{A}}(\delta, x_0, x) + \sum_{i \in \mathscr{A}} \bar{h}_i^2(\delta, x_0, x)$;

(v) $M_{\mathscr{A}}(\delta, x_0, x)$ is the matrix with last row $d(\mathscr{A}) \sum_{j=0}^{n} x_j^{d(\mathscr{A})-1}$ and with earlier rows $\nabla_{(x_0,x)} \bar{h}_i(\delta, x_0, x)$, $i \in \mathscr{A}$, ordered by increasing indices i;

(vi) $\bar{h}_i(\delta, x_0, x) := (1-\delta) h_i(x_0, x) + \delta(1 + \sum_{j=0}^{n} i^j x_j^{d'})$;

(vii) d' is the least even integer at least as great as $d+1$;

(viii) for $i = 1, \ldots, 3m+1$, h_i is defined by (3.6.1) and $h_{3m+1+i} := -h_i$.

Since the left hand side of (3.7.1) is defined as the determinant of a $d(\mathcal{A})^{O(n)} \times d(\mathcal{A})^{O(n)}$ matrix whose coordinates are zeros, coefficients of the system

$$(x_0, x) \mapsto \nabla_{(x_0,x)} \tilde{h}_{\mathcal{A}}(\varepsilon, \delta, x_0, x)$$

and the variables $U_0, \ldots, U_{n+1}$, it is a polynomial of degree $d(\mathcal{A})^{O(n)}$ in

$$(g, \varepsilon, \delta, U_0, U) \in \mathbb{R}\mathrm{Poly}(m, n, d) \times \mathbb{R}^{n+4}.$$

Given $g \in \mathrm{Poly}(m, n, d)$, $\beta \in \mathbb{R}^{n+1}$ and the ith unit vector e_i, and relying on the definition of R (i.e. (2.2.2)), a non-zero constant multiple of the polynomial

$$(\varepsilon, \delta, U_0, s, t) \mapsto R((x_0, x) \mapsto \nabla_{(x_0,x)} \tilde{h}_{\mathcal{A}}(\varepsilon, \delta, x_0, x), U_0, \beta + se_i + te_{n+1})$$

can be constructed using determinant evaluation and multi-variate interpolation with $d(\mathcal{A})^{O(n)}$ operations (no divisions). From this, the non-zero constant multiple of each of the bivariate polynomials

$$(s, t) \mapsto R^{(i,j,k)}_{\mathcal{A}}(g, \beta + se_i + te_{n+1}) \tag{3.7.2}$$

are easily determined with an additional $d(\mathcal{A})^{O(n)}$ operations (no divisions). Finally, with an additional $d(\mathcal{A})^{O(n)}$ operations (no divisions), one can then construct the non-zero constant multiple of each of the univariate polynomials

$$t \mapsto R^{(i,j,k)}_{\mathcal{A}}(g, \beta + te_{n+1}),$$

$$t \mapsto \frac{\mathrm{d}^l}{\mathrm{d}t^l} \nabla_U R^{(i,j,k)}_{\mathcal{A}}(g, \beta + te_{n+1}), \qquad l = 0, \ldots, D,$$

where D is the maximal degree of these polynomials (which is no greater than the size of the matrix defining R). Relying on the parallel determinant evaluation procedure of Proposition 2.1.1 and the multi-variate interpolation algorithm of Lemma 2.1.3, the above constructions easily parallelize, requiring time $(n \log d(\mathcal{A}))^{O(1)}$ using $[d(\mathcal{A})]^{O(n)}$ processors. Moreover, if the coefficients of β and $\{g_i\}_i$ are integers of bit length at most L, then all numbers occurring during the construction are easily verified to be integers of bit length at most $Ld(\mathcal{A})^{O(n)}$.

3.8. We summarize the results thus far in two propositions. The second proposition is an elaboration of the first, but is not important in this series of papers. The second proposition is included because the author needs the additional details it provides in another paper. The polynomials R occurring in the propositions refer to the positive multiples of the polynomials $R^{(i,j,k)}$ that arise from the computations of the preceding section; the properties of the polynomials $R^{(i,j,k)}$ that we are interested in are shared by all non-zero constant multiples of the $R^{(i,j,k)}$.

As before, $g = (g_1, \ldots, g_m)$ and $\{g_i\}_i$ both refer to the same set of polynomials.

Proposition 3.8.1. *Let $\bar{m} := \min\{m, n\}$. There exists a set $\mathcal{R}(m, n, d)$ of $(md)^{O(n)}$ polynomials $R : \mathbb{R}\mathrm{Poly}(m, n, d) \times \mathbb{R}^{n+1} \to \mathbb{R}$ of degree at most $D = (\bar{m}d)^{O(n)}$ with the following properties*:

(i) *if for $g \in \mathbb{R}\mathrm{Poly}(m, n, d)$ we define*

$$\mathcal{R}\{g_i\}_i := \{U \mapsto R(g, U);\ R \in \mathcal{R}(m, n, d)\}$$

then for each element of $\mathrm{CSP}\{g_i\}_i$ *there exists* $R \in \mathcal{R}\{g_i\}_i$ *such that R is not identically zero and factors linearly (over the complex numbers)* $\prod_i \xi^{(i)} \cdot U$ *where for some i,* $\mathrm{Aff}(\xi^{(i)})$ *is in the element;*

(ii) *for each* $g \in \mathbb{R}\mathrm{Poly}(m, n, d)$ *and each* $\beta \in \mathbb{R}^{n+1}$ *the entire set of univariate polynomials*

$$t \mapsto R(\beta + te_{n+1}),$$

$$t \mapsto \frac{\mathrm{d}^j}{\mathrm{d}t^j} \nabla R(\beta + te_{n+1}), \qquad j = 0, \ldots, D,$$

obtained from all $R \in \mathcal{R}\{g_i\}_i$ *can be constructed from* β *and the coefficients of* $\{g_i\}_i$ *with* $(md)^{O(n)}$ *operations (no divisions) in time* $[n \log(md)]^{O(1)}$ *using* $(md)^{O(n)}$ *processors; if the coefficients of g and* β *are integers of bit length at most L, then all numbers occurring during the construction are integers of bit length at most* $L(md)^{O(n)}$.

PROPOSITION 3.8.2. *Elements of the set* $\mathcal{R}(m, n, d)$ *of Proposition* 3.8.1 *are naturally indexed as*

$$R_{\mathscr{A}}^{(i,j,k)} \quad \text{where } 0 \le i, j, k \le D,$$
$$\mathscr{A} \subseteq \{1, \ldots, 6m+2\},$$
$$\#\mathscr{A} \le n+1.$$

For each g and $\mathscr{A}$ *at least one of the polynomials* $U \mapsto R_{\mathscr{A}}^{(i,j,k)}(g, U)$ *is not identically zero. Define*

$$i' = i(g, \mathscr{A}), \qquad j' = j(g, \mathscr{A}), \qquad k' = k(g, \mathscr{A}),$$

to be the non-negative integers satisfying

$$U \mapsto R_{\mathscr{A}}^{(i',j',k')}(g, U) \not\equiv 0 \quad \text{but} \quad U \mapsto R_{\mathscr{A}}^{(i,j,k)}(g, U) \equiv 0$$

if either (i) $i < i'$, (ii) $i = i', j < j'$ *or* (iii) $i = i', j = j', k < k'$. *Then*

$$U \mapsto R_{\mathscr{A}}^{(i',j',k')}(g, U) \tag{3.8.1}$$

factors linearly (over the complex numbers) $\prod_i \xi^{(i)} \cdot U$. *Finally, the polynomial R of part* (i) *of Proposition* 3.8.1 *may be assumed to be* (3.8.1) *for some* $\mathscr{A}$.

3.9. In our applications, the coefficients of the polynomials considered will themselves be polynomials in a limited number of variables. We now record a slight variation on Proposition 3.8.1 that will be useful in the applications. The proof is immediate from the arguments leading to Proposition 3.8.1, again relying on the algorithms of Proposition 2.1.1 and Lemma 2.1.3 to determine the polynomials arising as determinants of matrices with polynomial coefficients.

For $g_1, \ldots, g_m : \mathbb{R}^{n_1} \times \mathbb{R}^{n_2} \to \mathbb{R}$ and $\bar{x}_1 \in \mathbb{R}^{n_1}$, define $\mathrm{CSP}\{x^{[2]} \mapsto g_i(\bar{x}^{[1]}, x^{[2]})\}_i$ as the connected sign partition of $\mathbb{R}^{n_2}$ generated by the polynomials $x^{[2]} \mapsto g_i(\bar{x}^{[1]}, x^{[2]})$.

PROPOSITION 3.9.1. *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* $d \ge 2$. *Let* $\bar{m} := \min\{m, n_2\}$. *There exists a set* $\mathcal{R}\{g_i\}_i(x^{[1]})$ *of* $(md)^{O(n_2)}$ *polynomials in the variables* $(x^{[1]}, U) \in \mathbb{R}^{n_1} \times \mathbb{R}^{n_2+1}$, *of degree at most* $D = (\bar{m}d)^{O(n_2)}$, *with the following properties:*

(i) *for each* $\bar{x}^{[1]} \in \mathbb{R}^{n_1}$ *and for each element of the connected sign partition* $\mathrm{CSP}\{x^{[2]} \mapsto g_i(\bar{x}^{[1]}, x^{[2]})\}_i$ *of* $\mathbb{R}^{n_2}$ *there exists* $R \in \mathcal{R}\{g_i\}_i(x^{[1]})$ *such that* $U \mapsto R(\bar{x}^{[1]}, U)$ *is not identically zero and factors linearly (over the complex numbers)* $\prod \xi^{(i)} \cdot U$ *where for some* i, $\mathrm{Aff}(\xi^{(i)})$ *is in the element*;

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

$$(x^{[1]}, t) \mapsto R(x^{[1]}, \beta + te_{n_2+1}),$$

$$(x^{[1]}, t) \mapsto \frac{\mathrm{d}^j}{\mathrm{d}t^j} \nabla_U R(x^{[1]}, \beta + te_{n_2+1}), \qquad j = 0, \ldots, D,$$

obtained from all $R \in \mathcal{R}\{g_i\}_i(x^{[1]})$ *can be constructed from* β *and the coefficients of* $\{g_i\}_i$ *with* $(md)^{O(n_1 n_2)}$ *operations (no divisions) in time* $[n_1 n_2 \log(md)]^{O(1)}$ *using* $(md)^{O(n_1 n_2)}$ *parallel processors; if the coefficients of* β *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* $(L + n_1)(\bar{m}d)^{O(n_2)}$.

The operation bounds arise from the fact that in the above setting the computations will involve evaluating the determinants of $(md)^{O(n_2)}$ matrices of size $(\bar{m}d)^{O(n_2)} \times (\bar{m}d)^{O(n_2)}$ whose coefficients are polynomials, of degree $O(\bar{m}d)$, in the variables $x^{[1]}$, t and s (the latter variable being used to construct the gradient, as in (3.7.2)).

3.10. The last two propositions of this section are slight extensions of Proposition 3.9.1 to technical forms that will be easy to use at a certain juncture in our analysis. In stating the proposition we use notation that will be relied on later. On a first reading the reader should look at this section lightly, then return to it when the results are called for in the next paper in the series.

Assume that

$$g_i^{(j)} : \bigtimes_{k=1}^{j} \mathbb{R}^{n_k} \mapsto \mathbb{R}, \qquad i = 1, \ldots, m_j,$$

are polynomials of degree at most d_j. For $\bar{x}^{j-1]} = (\bar{x}^{[1]}, \ldots, \bar{x}^{[j-1]}) \in \bigtimes_{k=1}^{j-1} \mathbb{R}^{n_k}$, define $\mathrm{CSP}\{x^{[j]} \mapsto g_i^{(j)}(\bar{x}^{j-1]}, x^{[j]})\}_i$ as the connected sign partition of $\mathbb{R}^{n_j}$ generated by the polynomials $x^{[j]} \mapsto g_i^{(j)}(\bar{x}^{j-1]}, x^{[j]})$.

We will want a set of polynomials $R : \bigtimes_{k=1}^{j} \mathbb{R}^{n_k+1} \mapsto \mathbb{R}$ with the following property: for each tuple

$$\bar{X}^{j-1]} = (\bar{X}^{[1]}, \ldots, \bar{X}^{[j-1]}) \in \bigtimes_{k=1}^{j-1} \mathbb{R}^{n_k+1}$$

such that $\bar{X}^{[k]}_{n_k+1} \neq 0$ for all k, and for each element of $\mathrm{CSP}\{x^{[j]} \mapsto g_i^{(j)}(\bar{x}^{j-1]}, x^{[j]})\}_i$ where

$$\bar{x}^{j-1]} := (\bar{x}^{[1]}, \ldots, \bar{x}^{[j-1]}) \quad \text{and} \quad \bar{x}^{[k]} := \mathrm{Aff}(\bar{X}^{[k]}),$$

there exists a polynomial R in the set such that

$$U \mapsto R(\bar{X}^{j-1]}, U)$$

is not identically zero and factors linearly (over the complex numbers) $\prod_i \xi^{(i)} \cdot U$ where for some i, $\mathrm{Aff}(\xi^{(i)})$ is in the element.

We actually have such a set at hand. For let $G_i^{(j)}$ be any non-zero constant multiple of the polynomial obtained from $g_i^{(j)}$ by homogenizing (to degree d_j) with respect to each $x^{[k]}$, $k=1,\dots,j-1$, separately. (Thus, $G_i^{(j)}$ is homogeneous of degree d_j in each $X^{[k]}\in \mathbb{R}^{n_k+1}$, $k=1,\dots,j-1$, and is of degree at most d_j in $x^{[j]}\in\mathbb{R}^{n_j}$.) Observe that under the stated condition $\bar{X}^{[k]}_{n_k+1}\neq 0$ for all $k=1,\dots,j-1$,

$$\mathrm{CSP}\{x^{[j]}\mapsto g_i^{(j)}(\bar{x}^{j-1]},x^{[j]})\}_i=\mathrm{CSP}\{x^{[j]}\mapsto G_i^{(j)}(\bar{X}^{j-1]},x^{[j]})\}_i.$$

Hence, letting $\mathcal{R}(m_j,n_j,d_j)$ be the polynomials as in Proposition 3.8.1 and letting $G^{(j)}:=(G_1^{(j)},\dots,G_{m_j}^{(j)})$, we can define the set to be the set of all polynomials of the form

$$(X^{j-1]},U)\mapsto R[x^{[j]}\mapsto G^{(j)}(X^{j-1]},x^{[j]}),U],$$

where R ranges over all elements of $\mathcal{R}(m_j,n_j,d_j)$.

The operation bound in part (ii) of the following proposition is again obtained by relying on the algorithms of Proposition 2.1.1 and Lemma 2.1.3 to determine the polynomials arising as determinants of matrices with polynomial coefficients.

PROPOSITION 3.10.1. *Assume that* $g_i^{(j)}:\bigtimes_{k=1}^{j}\mathbb{R}^{n_k}\mapsto\mathbb{R}$, $i=1,\dots,m_j$, *are polynomials of degree at most* $d_j\geq 2$. *Let* $G_i^{(j)}$ *be any non-zero constant multiple of the polynomial obtained from* $g_i^{(j)}$ *by homogenizing (to degree* d_j*) with respect to each* $x^{[k]}$, $k=1,\dots,j-1$, *separately. Define* $\bar{m}_j:=\min\{m_j,n_j\}$. *There exists a set* $\mathcal{R}\{G_i^{(j)}\}_i(X^{j-1]})$ *of* $M_j=(m_jd_j)^{O(n_j)}$ *polynomials* $R:\bigtimes_{k=1}^{j}\mathbb{R}^{n_k+1}\to\mathbb{R}$ *of degree at most* $D_j=j(\bar{m}_jd_j)^{O(n_j)}$ *with the following properties:*

(i) *for each* $\bar{X}^{j-1]}=(\bar{X}^{[1]},\dots,\bar{X}^{[j-1]})\in\bigtimes_{k=1}^{j-1}\mathbb{R}^{n_k+1}$ *satisfying* $\bar{X}^{[k]}_{n_k+1}\neq 0$ *for all k, and for each element of* $\mathrm{CSP}\{x^{[j]}\mapsto g_i^{(j)}(\bar{x}^{j-1]},x^{[j]})\}_i$, *where*

$$\bar{x}^{j-1]}:=(\bar{x}^{[1]},\dots,\bar{x}^{[j-1]}),\qquad \bar{x}^{[k]}:=\mathrm{Aff}(\bar{X}^{[k]}),$$

there exists $R\in\mathcal{R}\{G_i^{(j)}\}_i(X^{j-1]})$ *such that* $U\mapsto R(\bar{X}^{j-1]},U)$ *is not identically zero and factors linearly (over the complex numbers)* $\prod_i \xi^{(i)}\cdot U$ *where for some i,* $\mathrm{Aff}(\xi^{(i)})$ *is in the element;*

(ii) *for any system of polynomials*

$$q^{j-1]}:\mathbb{R}^{j-1}\to\bigtimes_{k=1}^{j-1}R^{n_k+1}$$

of degree at most $d'_{j-1}\geq 1$, *and for any* $\beta\in\mathbb{R}^{n_j+1}$, *the entire set of polynomials in the variables* $(t^{j-1]},t_j):=(t_1,\dots,t_j)$

$$(t^{j-1]},t_j)\mapsto R[q^{j-1]}(t^{j-1]}),\beta+t_je_{n_j+1}],$$

$$(t^{j-1]},t_j)\mapsto\frac{\mathrm{d}^i}{\mathrm{d}t_j^i}\nabla_U R[q^{j-1]}(t^{j-1]}),\beta+t_je_{n_j+1}],\qquad i=0,\dots,D_j,$$

obtained from all $R\in\mathcal{R}\{G_i^{(j)}\}_i(X^{j-1]})$ *can be constructed from* β *and the coefficients of the polynomials* $\{(t^{j-1]},x^{[j]})\mapsto G_i^{(j)}(q^{j-1]}(t^{j-1]}),x^{[j]})\}_i$ *with* $(jd'_{j-1})^{O(j)}(m_jd_j)^{O(jn_j)}$ *operations (no divisions), in time* $[jn_j\log(d'_{j-1}m_jd_j)]^{O(1)}$ *using* $(jd'_{j-1})^{O(j)}(m_jd_j)^{O(jn_j)}$ *parallel processors; if the coefficients of* β *and the polynomials* $\{(t^{j-1]},x^{[j]})\mapsto G_i^{(j)}(q^{j-1]}(t^{j-1]}),x^{[j]})\}_i$ *are integers of bit length at most L, then all numbers occurring during the construction will be integers of bit length at most* $[L+(jd'_{j-1})^{O(1)}](\bar{m}_jd_j)^{O(n_j)}$.

The operation bounds arise from the fact that in the above setting the computations will involve evaluating the determinants of $(m_jd_j)^{O(n_j)}$ matrices of size $(\bar{m}_jd_j)^{O(n_j)}\times(\bar{m}_jd_j)^{O(n_j)}$ whose coefficients are polynomials of degree $O(jd'_{j-1}\bar{m}_jd_j)$, in the variables $t^{j-1]}$, t_j and s (the latter variable being used to construct the gradient as in (3.7.2)).

The proof of the following proposition is essentially identical to the proof of the preceding proposition.

Proposition 3.10.2. *Assume that*

$$g_i^{\langle j\rangle}:\mathbb{R}^l\times\left(\bigtimes_{k=1}^{j}\mathbb{R}^{n_k}\right)\to\mathbb{R},\qquad i=1,\dots,m_j,$$

are polynomials of degree at most d_j. *Let* $G_i^{\langle j\rangle}$ *be any non-zero constant multiple of the polynomial obtained from* $g_i^{\langle j\rangle}$ *by homogenizing (to degree* d_j*) with respect to each* $x^{[k]}$, $k=1,\dots,j-1$, *separately. Define* $\bar{m}_j:=\min\{m_j,n_j\}$. *There exists a set* $\mathcal{R}\{G_i^{\langle j\rangle}\}_i(y,X^{j-1]})$ *of* $M_j=(m_jd_j)^{O(n_j)}$ *polynomials* $R:\mathbb{R}^l\times(\bigtimes_{k=1}^{j}\mathbb{R}^{n_k+1})\to\mathbb{R}$ *of degree at most* $D_j=j(\bar{m}_jd_j)^{O(n_j)}$ *with the following properties:*

(i) *for each* $(\bar{y},\bar{X}^{j-1]})=(\bar{y},\bar{X}^{[1]},\dots,\bar{X}^{[j-1]})\in\mathbb{R}^l\times(\bigtimes_{k=1}^{j-1}\mathbb{R}^{n_k+1})$ *satisfying* $\bar{X}_{n_k+1}^{[k]}\neq 0$ *for all k, and for each element of* $\mathrm{CSP}\{x^{[j]}\mapsto g_i(\bar{y},\bar{x}^{j-1]},x^{[j]})\}_i$, *where*

$$\bar{x}^{j-1]}:=(\bar{x}^{[1]},\dots,\bar{x}^{[j-1]}),\qquad \bar{x}^{[k]}:=\mathrm{Aff}(\bar{X}^{[k]}),$$

there exists $R\in\mathcal{R}\{G_i^{\langle j\rangle}\}_i(y,X^{j-1]})$ *such that* $U\mapsto R(\bar{y},\bar{X}^{j-1]},U)$ *is not identically zero and factors linearly (over the complex numbers)* $\prod_i\xi^{(i)}\cdot U$ *where for some i,* $\mathrm{Aff}(\xi^{(i)})$ *is in the element;*

(ii) *for any system of polynomials*

$$q^{j-1]}:\mathbb{R}^l\times\mathbb{R}^{j-1}\mapsto\bigtimes_{k=1}^{j-1}\mathbb{R}^{n_k+1}$$

of degree at most $d'_{j-1}\geq 1$ *and for any* $\beta\in\mathbb{R}^{n_j+1}$, *the entire set of polynomials in the variables* $(y,t^{j-1]},t_j)$

$$(y,t^{j-1]},t_j)\mapsto R[y,q^{j-1]}(y,t^{j-1]}),\beta+t_je_{n_j+1}],$$

$$(y,t^{j-1]},t_j)\mapsto\frac{\mathrm{d}^i}{\mathrm{d}t_j^i}\nabla_U R[y,q^{j-1]}(y,t^{j-1]}),\beta+t_je_{n_j+1}],\qquad i=0,\dots,D_j,$$

obtained from all $R\in\mathcal{R}\{G_i^{\langle j\rangle}\}_i(y,X^{j-1]})$ *can be constructed from* β *and the coefficients of the polynomials*

$$\{(y,t^{j-1]},x^{[j]})\mapsto G_i^{\langle j\rangle}(y,q^{j-1]}(t^{j-1]}),x^{[j]})\}_i$$

with $(jd'_{j-1})^{O(j+l)}(m_jd_j)^{O((j+l)n_j)}$ *operations in time* $[(j+l)n_j\log(d'_{j-1}m_jd_j)]^{O(1)}$ *using* $(jd'_{j-1})^{O(j+l)}(m_jd_j)^{O((j+l)n_j)}$ *parallel processors; if the coefficients of* β *and the polynomials* $\{(y,t^{j-1]},x^{[j]})\mapsto G_i^{\langle j\rangle}(y,q^{j-1]}(t^{j-1]}),x^{[j]})\}_i$ *are integers of bit length at most L, then all numbers occurring during the construction are integers of bit length at most* $[L+l(jd'_{j-1})^{O(1)}](\bar{m}_jd_j)^{O(n_j)}$.

3.11. The final task of this section is to give the proof of Lemma 3.4.1. The proof proceeds via several other lemmas. The notation we use is that developed just prior to the statement of Lemma 3.4.1.

Lemma 3.11.1. *Assume that* $\mathcal{A}\subseteq\{1,\dots,m\}$ *is such that* $\#\mathcal{A}>n$. *Then the system of polynomials*

$$x\mapsto\bar{g}_i(1,x),\qquad i\in\mathcal{A},$$

has no complex zeros, even at infinity.

Proof. Assume otherwise, so that after homogenizing there exists $\bar{x}\in\mathbb{C}^{n+1}$, $\bar{x}\neq 0$, satisfying $\bar{x}_{n+1}^{d'}+\sum_{j=1}^{n} i^j\bar{x}_j^{d'}=0$ for all $i\in\mathscr{A}$. Then the non-zero polynomial

$$t\mapsto\bar{x}_{n+1}^{d'}+\sum_{j=1}^{n} t^j\bar{x}_j^{d'}$$

of degree at most n has at least $n+1$ zeros, namely, $t=i$ for all $i\in\mathscr{A}$. Of course this cannot be.

Recall that in section 2.1 we discussed the fact that if for some choice $\bar{\delta}$ a system of polynomials F in the variables δ and x has the property that $x\mapsto F(\bar{\delta},x)=0$ has no solutions, even at infinity, then the same is true for $x\mapsto F(\delta,x)$ except for finitely many values of δ. Hence, by the previous lemma, if $\#\mathscr{A}>n$,

$$x\mapsto\bar{g}_i(\delta,x),\qquad i\in\mathscr{A},$$

has no complex zeros, even at infinity, except for finitely many values of δ; then $x\mapsto h_{\mathscr{A}}(\delta,x)$ has no real zeros except for finitely many values of δ. We have now established the first claim of Lemma 3.4.1.

For $\#\mathscr{A}\leq n$ the proof is more involved, especially for the case $\#\mathscr{A}<n$.

Lemma 3.11.2. (Descarte's Rule.) *Suppose that $p(t)=\sum_i a_it^i\neq 0$ is a complex univariate polynomial with at least $k>0$ distinct non-negative real zeros. Then at least k of the coefficients a_i, $i>0$, satisfy $a_i\neq 0$.*

Proof. Without loss of generality we may assume that p is a real polynomial by replacing it with $p(t)+\bar{p}(t)$, "$\bar{\ }$" only here denoting conjugate (or replacing it with $\sqrt{-1}\,p(t)$ if all a_i are purely imaginary).

Let $\bar{d}$ denote the degree of p. For $i=0,1,\ldots,\bar{d}$, let n_i denote the number of distinct non-negative zeros of $p^{(i)}$, the ith derivative of p. The mean value theorem implies that $p^{(i+1)}$ has at least n_i-1 distinct strictly positive zeros. Hence, $n_{i+1}\geq n_i-1$, and $n_{i+1}\geq n_i$ if $a_{i+1}=0$. It follows that if fewer than k of the coefficients a_i, $i>0$, satisfied $a_i\neq 0$ then $n_{\bar{d}}\geq 1$, which of course is not possible.

In what follows let $S_l:\mathbb{C}^n\to\mathbb{C}$ denote the symmetric homogeneous polynomial

$$S_l(x):=\sum_{j_1<\cdots<j_l} x_{j_1}^{d'-1}\cdots x_{j_l}^{d'-1}.$$

Lemma 3.11.3. *Assume that $k=\#\mathscr{A}\leq n$. Then the system of n polynomials in n variables*

$$x\mapsto\bar{g}_i(1,x),\qquad i\in\mathscr{A},$$

$$S_l(x)\qquad k+1\leq l\leq n,$$

has only finitely many complex zeros including those at infinity. (Note that no polynomial S_l appears in the above system if $\#\mathscr{A}=n$.)

Proof. First note that if $\bar{x}\in\mathbb{C}^{n+1}$ is such that

$$\bar{x}_{n+1}^{d'}+\sum_{j=1}^{n} i^j\bar{x}_j^{d'}=0\quad\text{for all } i\in\mathscr{A},$$

then by Lemma 3.11.2 applied to the polynomial

$$p(t) := \bar{x}_{n+1}^{d'} + \sum_{j=1}^{n} t^j \bar{x}_j^{d'},$$

at least k of the coordinates $\bar{x}_j$, $j < n+1$, must satisfy $\bar{x}_j \neq 0$.

Next note by inductively decreasing k, that if $\bar{x} \in \mathbb{C}^{n+1}$ is a zero of

$$(x_1, \ldots, x_{n+1}) \mapsto S_l(x_1, \ldots, x_n) \quad \text{for all } k+1 \leq l \leq n,$$

then at most k of the coordinates $\bar{x}_j$, $j < n+1$, satisfy $\bar{x}_j \neq 0$. (Hence we may assume that $k \geq 1$ since otherwise the lemma follows trivially.)

We have now established that if $\bar{x} \in \mathbb{C}^{n+1}$ is a zero of the homogenization of the system in the statement of the lemma, then exactly k of the coordinates $\bar{x}_j$, $j < n+1$, satisfy $\bar{x}_j \neq 0$.

To prove the lemma it now suffices to show that for every $K \subseteq \{1, \ldots, n\}$ satisfying $\# K = k$, there are only finitely many complex zeros, including those at infinity, for the following system of k polynomials in the k variables x_j, $j \in K$:

$$1 + \sum_{j \in K} i^j x_j^{d'}, \qquad i \in \mathscr{A}.$$

In fact, there are at most $(d')^k$ such zeros. For suppose $\bar{x}_j$ $(j \in K)$, $\bar{x}_{n+1}$ together form one non-trivial zero of the homogenization, and suppose that $\hat{x}_j$ $(j \in K)$, $\hat{x}_{n+1}$ form another. We will show that there then exists $w \in \mathbb{C}$ such that both $w\bar{x}_{n+1}^{d'} = \hat{x}_{n+1}^{d'}$ and $w\bar{x}_j^{d'} = \hat{x}_j^{d'}$ for all $j \in K$. From this claim that there are "at most $(d')^k$ such zeros" follows.

Now to show that such a w exists. Suppose otherwise. Then by an appropriate linear sum of the polynomials

$$t \mapsto \bar{x}_{n+1}^{d'} + \sum_{j \in K} t^j \bar{x}_j^{d'} \quad \text{and} \quad t \mapsto \hat{x}_{n+1}^{d'} + \sum_{j \in K} t^j \hat{x}_j^{d'}$$

we can obtain a non-zero polynomial $p(t) = \sum a_i t^i$ for which at most $k-1$ of the coefficients a_i, $i > 0$, satisfy $a_i \neq 0$, but for which each $i \in \mathscr{A}$ is a zero. This contradicts Lemma 3.11.2.

We can now prove Lemma 3.4.1 for the case $\# \mathscr{A} = n$. For then, by the previous lemma, the system

$$x \mapsto \bar{g}_i(1, x), \qquad i \in \mathscr{A}$$

has only finitely many complex zeros, including those at infinity. Hence the same is true of the system

$$x \mapsto \bar{g}_i(\delta, x), \qquad i \in \mathscr{A}$$

except for finitely many values of δ. Thus, except for finitely many values of δ, $x \mapsto \sum_{i \in \mathscr{A}} \bar{g}_i^2(\delta, x)$ has only finitely many real zeros. The same is then true of $x \mapsto h_{\mathscr{A}}(\delta, x)$.

Finally we prove Lemma 3.4.1 for the case $\# \mathscr{A} < n$. In what follows, let $k = \# \mathscr{A}$.

Recall that $M_{\mathscr{A}}(\delta, x)$ is the matrix with rows $\nabla_x \bar{g}_i(\delta, x)$ for $i \in \mathscr{A}$, and last row $d'(m+1) \times (x_1^{d'-1}, \ldots, x_n^{d'-1})$. Assuming that $k = \# \mathscr{A} < n$, for $1 \leq j_1 < \cdots < j_{k+1} \leq n$ define $M_{\mathscr{A}}^{\langle j_1, \ldots, j_{k+1} \rangle}(\delta, x)$ to be the square matrix consisting of the j_1th, $\ldots$, j_{k+1}th columns of $M_{\mathscr{A}}(\delta, x)$.

Noting that the jth column of $M_{\mathscr{A}}(1, x)$ has coordinates $d' i^j x_j^{d'-1}$ where i ranges over $\mathscr{A} \cup \{m+1\}$, define $A_{\mathscr{A}}^{\langle j_1, \ldots, j_{k+1} \rangle}$ to be the constant matrix satisfying

$$M_{\mathscr{A}}^{\langle j_1, \ldots, j_{k+1} \rangle}(1, x) = A_{\mathscr{A}}^{\langle j_1, \ldots, j_{k+1} \rangle} \operatorname{diag}[d' x_{j_1}^{d'-1}, \ldots, d' x_{j_{k+1}}^{d'-1}],$$

where diag[ ] is the obvious diagonal matrix. The $(k+1)\times(k+1)$ constant matrix $A_{\mathscr{A}}^{\langle j_1,\dots,j_{k+1}\rangle}$ is non-singular. For if $v=(v_{j_1},\dots,v_{j_{k+1}})^T$, then $A_{\mathscr{A}}^{\langle j_1,\dots,j_{k+1}\rangle}v$ is the vector with coordinates $v_{j_1}(i)^{j_1}+\cdots+v_{j_{k+1}}(i)^{j_{k+1}}$, where i ranges over $\mathscr{A}\cup\{m+1\}$. If $v\neq 0$ yet this vector was zero, we would have a polynomial $t\mapsto\sum a_jt^j$ with $k+2$ non-negative real zeros (i.e. 0, $m+1$ and $i\in\mathscr{A}$) but with at most $k+1$ non-zero coefficients a_j, $j>0$, satisfying $a_j\neq 0$. This would contradict Lemma 3.11.2.

Note that for each $l\geq k+1$ and $j_1<\cdots<j_l$,

$$x_{j_1}^{d'-1}\cdots x_{j_l}^{d'-1}=[(d')^{k+1}\det A_{\mathscr{A}}^{\langle j_1,\dots,j_{k+1}\rangle}]^{-1}[\det M_{\mathscr{A}}^{\langle j_1,\dots,j_{k+1}\rangle}(1,x)]x_{j_{k+2}}^{d'-1}\cdots x_l^{d'-1}.$$

Consequently, for $l\geq k+1$ there exist polynomials $p_{\mathscr{A},l}^{\langle j_1,\dots,j_{k+1}\rangle}(x)$ such that

$$S_l(x)=\sum_{j_1<\cdots<j_{k+1}}p_{\mathscr{A},l}^{\langle j_1,\dots,j_{k+1}\rangle}(x)\det M_{\mathscr{A}}^{\langle j_1,\dots,j_{k+1}\rangle}(1,x). \tag{3.11.1}$$

Fixing δ, consider the system of n polynomials in n variables

$$\begin{aligned}\bar{g}_i(\delta,x)&=0, \qquad i\in\mathscr{A},\\ \sum_{j_1<\cdots<j_{k+1}}p_{\mathscr{A},l}^{\langle j_1,\dots,j_{k+1}\rangle}(x)\det M_{\mathscr{A}}^{\langle j_1,\dots,j_{k+1}\rangle}(\delta,x)&, \qquad k+1\leq l\leq n.\end{aligned} \tag{3.11.2}$$

From (3.11.1) and Lemma 3.11.3 we find that this system has only finitely many complex zeros, including those at infinity, when $\delta=1$. Hence the same is true for all but finitely many values of δ.

Finally, note that if $\bar{x}$ is a real zero of $x\mapsto h_{\mathscr{A}}(\delta,x)$ then $\bar{g}_i(\delta,x)=0$ for all $i\in\mathscr{A}$ and $M_{\mathscr{A}}(\delta,\bar{x})$ is not of full rank, i.e., not of rank $k+1$. But if $M_{\mathscr{A}}(\delta,\bar{x})$ is not of rank $k+1$, then $\det M_{\mathscr{A}}^{\langle j_1,\dots,j_{k+1}\rangle}(\delta,\bar{x})=0$ for all $j_1<\cdots<j_{k+1}$. Hence, $\bar{x}$ is a solution of (3.11.2). Since (3.11.2) has only finitely many solutions except for finitely many values of δ, the proof of Lemma 3.4.1 is complete.

4. Determining the Consistent Sign Vectors of a Set of Polynomials and a Decision Method for the Existential Theory of the Reals

Let $g_1,\dots,g_m:\mathbb{R}^n\to\mathbb{R}$ be polynomials of degree at most d. The "sign vector" of $g_1,\dots,g_m:\mathbb{R}^n\to\mathbb{R}$ at $\bar{x}\in\mathbb{R}^n$ is the vector $\sigma\in\{-1,0,1\}^m$ defined by

$$\sigma_i=\begin{cases}-1 & \text{if } g_i(\bar{x})<0\\ 0 & \text{if } g_i(\bar{x})=0\\ 1 & \text{if } g_i(\bar{x})>0.\end{cases}$$

The set of "consistent sign vectors" for $g_1,\dots,g_m$ is the set of all sign vectors obtained as $\bar{x}$ ranges over $\mathbb{R}^n$. In this section we present a method for determining the set of consistent sign vectors for arbitrary polynomials $g_1,\dots,g_m$. Once all consistent sign vectors can be determined, a decision method for the existential theory of the reals easily follows as we will show.

Now we discuss the procedure for determining the consistent sign vectors.

Let $\mathscr{R}\{g_i\}_i$ be the set of $(md)^{O(n)}$ polynomials $R:\mathbb{R}^{n+1}\to\mathbb{R}$ of degree at most $D=(\bar{m}d)^{O(n)}$ as in Proposition 3.8.1(i), where $\bar{m}:=\min\{m,n\}$. Hence for each element of the connected sign partition CSP$\{g_i\}_i$ there exists $R\in\mathscr{R}\{g_i\}_i$ such that R is not identically zero and factors linearly $R(U)=\prod_i\xi^{(i)}\cdot U$ and for some i, Aff$(\xi^{(i)})$ is in the element.

Let $\mathcal{B}(n+1, D)\subset\mathbb{R}^{n+1}$ be the set of $O(nD^2)$ vectors as defined by (2.3.2). The second half of Proposition 2.3.1 shows that for each polynomial $R:\mathbb{R}^{n+1}\to\mathbb{R}$ of degree at most D that factors linearly $\prod_i \xi^{(i)}\cdot U\not\equiv 0$, and for each i such that $\mathrm{Aff}(\xi^{(i)})$ is well-defined and real, there exist $\beta\in\mathcal{B}(n+1, D)$ and $0\le j\le D$ with the following property: for some real zero t' of $t\mapsto R(\beta+te_{n+1})$,

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

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

Let $G_i:\mathbb{R}^{n+1}\to\mathbb{R}$ denote the homogenization of g_i. Combining the facts of the last two paragraphs, for each consistent sign vector $\sigma=(\sigma_1,\dots,\sigma_m)$ of $(g_1,\dots,g_m)$ there exist $R\in\mathcal{R}\{g_i\}_i$, $\beta\in\mathcal{B}(n+1, D)$ and $0\le j\le D$ such that $(\sigma_1,\dots,\sigma_m, 1)$ is a consistent sign vector either for the univariate system

$$\begin{aligned} &t\mapsto G_i(q(t)), \qquad i=1,\dots,m,\\ &t\mapsto q_{n+1}(t), \end{aligned} \tag{4.1}$$

or for the univariate system

$$\begin{aligned} &t\mapsto G_i(-q(t)), \qquad i=1,\dots,m,\\ &t\mapsto -q_{n+1}(t), \end{aligned} \tag{4.2}$$

where

$$q(t) := \frac{\mathrm{d}^j}{\mathrm{d}t^j}\nabla R(\beta+te_{n+1}).$$

Conversely, it is easily seen that if $(\sigma_1,\dots,\sigma_m, 1)$ is a consistent sign vector for either of the latter systems, then $(\sigma_1,\dots,\sigma_m)$ is a consistent sign vector for $(g_1,\dots,g_m)$.

To determine the consistent sign vectors of $\{g_i\}_i$ it thus suffices to determine the consistent sign vectors for all of the univariate systems (4.1) and (4.2) obtained as (R, β, j) ranges over $\mathcal{R}\{g_i\}_i\times\mathcal{B}(n+1, D)\times\{0,\dots,D\}$. Relying on Propositions 2.1.2 and 3.8.1, we obtain the following proposition.

Proposition 4.1. *Any set of polynomials $g_1,\dots,g_m:\mathbb{R}^n\to\mathbb{R}$, 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 $L^2(md)^{O(n)}$ parallel processors.*

It is now trivial to present an efficient decision method for the existential theory of the reals. Assume that we are concerned with determining if the sentence

$$(Qx\in\mathbb{R}^n)P(x) \tag{4.3}$$

is true or false, where Q is "$\exists$" or "$\forall$" and $P(x)$ is a quantifier free formula with distinct atomic predicates $g_i(x)\Delta_i 0$, $i=1,\ldots,m$, Δ_i being any of the standard relations (1.2).

Let $\mathbb{P}$ and Time$(\mathbb{P}, N)$ be as defined in the introduction. For $\sigma\in\{-1,0,1\}^m$, define $B(\sigma)\in\{0,1\}^m$ by

$$B_i(\sigma)=\begin{cases} 1 & \text{if } \sigma_i=1 \text{ and } \Delta_i\in\{>,\geq,\neq\} \\ 1 & \text{if } \sigma_i=0 \text{ and } \Delta_i\in\{\geq,=,\leq\} \\ 1 & \text{if } \sigma_i=-1 \text{ and } \Delta_i\in\{\neq,\leq,<\} \\ 0 & \text{otherwise.} \end{cases}$$

Here is the decision method for the existential theory of the reals. First construct the set S of all consistent sign vectors for $\{g_i\}_i$. Then simply verify if the "sentence"

$$(Q\sigma\in S)\mathbb{P}(B(\sigma))$$

it true; this sentence is true iff (4.3) is true.

Proposition 4.2. *There exists an algorithm for the existential theory of the reals, which when applied to the sentence* (4.3), *requires* $(md)^{O(n)}$ *operations and* $(md)^{O(n)}$ *calls to* $\mathbb{P}$. *The computations can be accomplished in time* $[n\log(md)]^{O(1)}+\text{Time}(\mathbb{P},N)$ *if* $(md)^{O(n)}$ *processors are used for the operations and* $N(md)^{O(n)}$ *processors are used for the calls* (*for any* $N\geq 1$). *If the coefficients of* $\{g_i\}_i$ *are integers of bit length at most L, then the algorithm requires* $L(\log L)(\log\log L)(md)^{O(n)}$ *sequential bit operations and* $(md)^{O(n)}$ *calls to* $\mathbb{P}$, *or time* $\log(L)[n\log(md)]^{O(1)}+\text{Time}(\mathbb{P},N)$ *using* $L^2(md)^{O(n)}$ *processors for the operations and* $N(md)^{O(n)}$ *processors for the calls* (*for any* $N\geq 1$).

I would like to thank several people who have had a very positive influence on this work; Lenore Blum, Doug Ierardi, Dexter Kozen, John Canny, Steve Smale, Mike Shub, my typist Kathy King and, most of all, my wife, Katie Barnaby. Thanks!

This research was supported by NSF Grant DMS-8800835.

References

Arnon, D. S. (1988). A bibliography of quantifier elimination for real closed fields. *J. Symbolic Computation* **5**, 267-274.

Ben-Or, M. (1983). Lower bounds for algebraic computation trees. *Proceedings of the 1983 ACM Symposium on Symbolic and Algebraic Computation*, 80-86.

Ben-Or, M., Kozen, D., Reif, J. (1986). The complexity of elementary algebra and geometry. *J. Comp. System Sci.* **32**, 251-264.

Blum, L., Shub, M., Smale, S. (1989). On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bulletin of the American Mathematical Society* **21**, 1-46.

Blum, L., Smale, S. (1992). The Godel incompleteness theorem and decidability over a ring. In: *From Topology to Computation*, Proceedings of the Smalefest. Springer-Verlag.

Canny, J. (1988). Some algebraic and geometric computations in PSPACE. *Proceedings of the 20th Annual ACM Symposium on the Theory of Computing*, 460-467.

Canny, J. (1990). Generalized characteristic polynomials. *J. Symbolic Computation* **9**, 241-250.

Chistov, A. L., Grigor'ev, D. Yu. (1984). Complexity of quantifier elimination in the theory of algebraically closed fields. *Lecture Notes in Computer Science* **176**, 17-31.

Cohen, P. J. (1969). Decision procedures for real and *p*-adic fields. *Communications in Pure and Applied Mathematics* **22**, 131-151.

Collins, G. E. (1975). Quantifier elimination for real closed fields by cylindrical algebraic decomposition. Second GI Conference on Automata Theory and Formal Languages. *Lecture Notes in Computer Science* **33**, 134-183.

Csanky, L. (1976). Fast parallel matrix inversion algorithms. *SIAM Journal on Computing* **5**, 618-623.

Fitchas, N., Galligo, A., Morgenstern, J. (1987). Algorithmes rapides en séquential et en parallele pour l'élimination de quantificateurs en géométrie élémentaire. In: *Séminaire Structures Algébriques Ordonnées*, UER de Mathématiques Universite de Paris VII.

Fitchas, N., Galligo, A., Morgenstern, J. (1990). Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields. *J. Pure App. Algebra* **67**, 1-14.

Grigor'ev, D. Yu. (1987). The complexity of the decision problem for the first order theory of algebraically closed fields. *Math. USSR Izvestiya* **29**, 459-475.

Grigor'ev, D. Yu. (1988). The complexity of deciding Tarski algebra. *J. Symbolic Computation* **5**, 65-108.

Grigor'ev, D. Yu., Vorobjov, N. N. (1988). Solving systems of polynomial inequalities in subexponential time. *J. Symbolic Computation* **5**, 37-64.

Heintz, J. (1983). Definability and fast quantifier elimination in algebraically closed fields. *Theoretical Computer Science* **24**, 239-277.

Heintz, J., Roy, M., Solernó, P. (1989). On the complexity of semialgebraic sets. *Proc. IFIP*, 293-298. San Francisco: North-Holland.

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

Ierardi, D. (1989). Quantifier elimination in the first-order theory of algebraically closed fields. *Proceedings of the 21st Annual ACM Symposium on the Theory of Computing;* also PhD thesis, Department of Computer Science, Cornell University.

Karmarkar, N. (1984). A new polynomial-time algorithm for linear programming. *Combinatorica* **4**, 373-395.

Khachiyan, L. G. (1979). A polynomial algorithm in linear programming. *Soviet Mathematics Doklady* **20**, 191-194.

Milnor, J. (1964). On the Betti numbers of real varieties. *Proceedings of the American Mathematical Society* **15**, 275-280.

Renegar, J. (1988*a*). A polynomial time algorithm, based on Newton's method, for linear programming. *Mathematical Programming* **40**, 59-93.

Renegar, J. (1988*b*). A faster PSPACE algorithm for the existential theory of the reals. *Proceedings of the 29th Annual IEEE Symposium on the Foundations of Computer Science*, 291-295.

Renegar, J. (1992*a*). On the computational complexity of approximating solutions for real algebraic formulae. *SIAM Journal on Computing.*

Renegar, J. (1992*b*). Recent progress on the complexity of the decision problem for the reals. *Proceedings of the DIMACS Workshop on Algebraic Methods in Geometric Computations.*

Seidenberg, A. (1954). A new decision method for elementary algebra. *Annals of Mathematics* **60**, 365-374.

Steele, J. M., Yao, A. C. (1982). Lower bounds for algebraic decision trees. *J. Algorithms* **3**, 1-8.

Tardos, É. (1986). A strongly polynomial algorithm for solving combinatorial linear programs. *Operations Research* **34**, 250-256.

Tarski, A. (1951). *A Decision Method for Elementary Algebra and Geometry.* University of California Press.

Van Den Dries, L. (1988). Alfred Tarski's elimination theory for real closed fields. *J. Symbolic Logic* **53**, 7-19.

Van Der Waerden, B. L. (1950). *Modern Algebra*, Vol. 2. Frederick Ungar Publishing Co.

Appendix A

Here we review a fast parallel method for computing determinants as was first presented by Csanky (1976). To avoid division we actually compute the determinant times $n!$.

The algorithm is based on Leverrier's method for finding the coefficients of the characteristic polynomial of a matrix.

Let A be the $n \times n$ matrix whose characteristic polynomial is to be computed and let $\lambda^n + \sum_{i=1}^n c_i \lambda^{n-i}$ denote its characteristic polynomial; of course $c_n = \det(A)$. Let $\lambda_1, \ldots, \lambda_n$ denote the zeros of the characteristic polynomial. The algorithm is based on the obvious fact that $s_i := \sum_k \lambda_k^i = \operatorname{trace}(A^i)$ can be computed quickly in parallel.

For $j = 1, \ldots, n$, let $\{\lambda_{jk}\}_{k=1}^j$ denote the zeros of $\lambda^j + \sum_{i=1}^j c_i \lambda^{j-i}$. Of course

$$0 = \sum_{k=1}^{j} \left[\lambda_{jk}^j + \sum_{i=1}^{j} c_i \lambda_{jk}^{j-i} \right] = \left(\sum_{k=1}^{j} \lambda_{jk}^j \right) + \sum_{i=1}^{j} c_i \left(\sum_{k=1}^{j} \lambda_{jk}^{j-i} \right). \tag{A.1}$$

Since the value of the ith elementary symmetric polynomial (in n variables) at the point $(\lambda_1, \ldots, \lambda_n)$ is c_i, as is the value at the point $(\lambda_{j1}, \ldots, \lambda_{jj}, 0, \ldots 0)$ for all $i \leq j$, the theorem on symmetric polynomials implies that the value of the symmetric polynomial

$(x_1,\dots,x_n)\mapsto\sum_k x_k^i$ is the same at the two points for all $i\le j$; thus, $s_i=\sum_{k=1}^{j}\lambda_{jk}^i$ for all $j\ge i$. Substituting into (A.1) we obtain the following system of linear equations:

$$\begin{bmatrix} 1 & & & & & \\ s_1 & 2 & & & & \\ s_2 & s_1 & 3 & & & \\ s_3 & s_2 & s_1 & 4 & & \\ \vdots & \vdots & \vdots & \vdots & & \\ s_{n-1} & s_{n-2} & s_{n-3} & s_{n-4} & \cdots & n \end{bmatrix}\begin{bmatrix} c_1 \\ c_2 \\ \\ \vdots \\ \\ c_n \end{bmatrix} = -\begin{bmatrix} s_1 \\ s_2 \\ \\ \vdots \\ \\ s_n \end{bmatrix}.$$

Defining $\bar{c}_1 := i\,!\,c_i$, the above equations are equivalent to

$$\bar{c}_i=-(i-1)\,!\,s_i-\sum_{j<i}(i-1)\cdots(j+1)s_{i-j}\bar{c}_j,\qquad i=1,\dots,n. \tag{A.2}$$

Assuming for simplicity of exposition that $n=2^N$, these equations can be solved quickly in parallel as follows.

At the end of the jth time interval the variables will be viewed as occurring in "blocks"

$$B_{jk}:=\{\bar{c}_i;\,(k-1)2^j<i\le k2^j\},\qquad k=1,\dots,2^{N-j},$$

and the right hand side of the identities (A.2) for $\bar{c}_i\in B_{jk}$ will have been replaced with linear expressions involving only the variables in $\bigcup_{k'<k}B_{jk'}$. Denote these identities by I_{jk}; the identities I_{j1} simply state the solution values for the variables in B_{j1}. (The algorithm begins with $j=0$.)

During the $j+1$th time interval new identities I'_{jk} are computed to replace I_{jk} if k is even. The new identities are simply obtained by substituting the right hand side of identities in $I_{j,k-1}$ for the variables $\bar{c}_i\in B_{j,k-1}$ occurring in the right hand side of identities in I_{jk}. Then, for $k=1,\dots,2^{N-j-1}$, we let

$$B_{j+1,k}=B_{j,2k-1}\cup B_{j,2k}$$
$$I_{j+1,k}:=I_{j,2k-1}\cup I'_{j,2k}.$$

Proposition 2.1.1 easily follows.

Appendix B

In this appendix we establish Lemma 2.1.3 regarding the cost of multi-variate interpolation for determining the coefficients of a polynomial $f:\mathbb{C}^n\to\mathbb{C}$ of degree d from the value of f at the points in $\{0,1,\dots,d\}^n$. To avoid divisions we will actually compute the non-zero multiple of the coefficients stated in the lemma.

First assume that f is a univariate polynomial. Then, for i,j and k restricted to the set $\{0,1,\dots,d\}$, we have the identity

$$f(x)\prod_{k>j}(k-j)=\sum_i\left[(-1)^{d-i}f(i)\prod_{j\ne i}\left[(x-j)\prod_{\substack{k>j\\k\ne i}}(k-j)\right]\right]$$

because the value of the polynomial on the left agrees with that on the right at the $d+1$ points $0,1,\dots,d$. Lemma 2.1.3 follows easily for the univariate case.

Now assume that $f:\mathbb{C}^n\to\mathbb{C}$ where $n\ge 2$. For $x=(x_1,\dots,x_n)$ define $x^{i]}:=(x_1,\dots,x_i)$. Let

$$f(x)=\sum_{i_j,\dots,i_n}a_{i_j\cdots i_n}(x^{j-1]})x_j^{i_j}\cdots x_n^{i_n}$$

denote the Taylor expansion of f in powers of $x_j,\dots,x_n$; so $a_{i_j\cdots i_n}(x^{j-1]})$ is a polynomial in $x_1,\dots,x_{j-1}$.

We proceed inductively. Applying the univariate interpolation algorithm to the polynomials $x_n \mapsto f(\bar{x}^{n-1]}, x_n)$ for $\bar{x}^{n-1]} \in \{0,\dots,d\}^{n-1}$, we obtain the values $a_{i_n}(\bar{x}^{n-1]}) \prod_{k>j}(k-j)$.

Applying the univariate algorithm to the polynomials $x_{n-1} \mapsto a_{i_n}(\bar{x}^{n-2]}, x_{n-1}) \prod_{k>j}(k-j)$ for $\bar{x}^{n-2]} \in \{0,\dots,d\}^{n-2}$, from the previously computed values we obtain the values $a_{i_{n-1}i_n}(\bar{x}^{n-2]})[\prod_{k>j}(k-j)]^2$.

And so on.

Lemma 2.1.3 follows.

Appendix C

Assume that $g_1,\dots,g_m:\mathbb{R}^n \to \mathbb{R}$ are polynomials of degree at most d. Here we show that $\mathrm{CSP}\{g_i\}_i$ consists of a finite number of elements and that each of these is path-connected. The proof depends on Lemma 3.1 from the second paper in the series, restated as follows.

LEMMA C.1. *Assume that*

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

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*

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

(*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* $\det M^T M = 0$.

Now to prove that $\mathrm{CSP}\{g_i\}_i$ consists of a finite number of elements and that each of these is path-connected. The proof proceeds by induction. It is trivial for $n=1$. Assume that it has been established for sets of polynomials in $n-1$ variables.

For each $I \subseteq \{1,\dots,m\}$, consider the polynomial in $(x^{n-1]}, t) \in \mathbb{R}^{n-1}\times\mathbb{R}$,

$$G_I(x^{n-1]}, t) := \prod_{i\in I} g_i(x^{n-1]}, t) = \sum_{j=0}^{md} a_{I,j}(x^{n-1]}) t^j,$$

where the right hand side denotes the expansion in powers of t, the $a_{I,j}(x^{n-1]})$ being polynomials in $x^{n-1]}$. For each pair of integers e and k satisfying $1 \leq e \leq md$ and $0 \leq k < e$ form the polynomial

$$h_{I,e,k}(x^{n-1]}) := \det M^T M,$$

where M is the $(2e-k-1)\times(2e-2k-1)$ matrix as defined in Lemma C.1 with respect to the truncated univariate polynomials

$$p(t) = \sum_{j=0}^{e} a_{I,j}(x^{n-1]}) t^j, \qquad q(t) = \sum_{j=1}^{e} j a_{I,j}(x^{n-1]}) t^{j-1}.$$

(Of course the entries of M involve the polynomials $a_{I,j}(x^{n-1]})$.) Let $\{h_i\}_i$ denote the resulting set of polynomials, obtained as I ranges over all subsets of $\{1,\dots,m\}$, along with the polynomials

$$x^{n-1]} \mapsto a_{I,j}(x^{n-1]}), \qquad j = 0,\dots,md. \tag{C.1}$$

By inductive hypothesis, CSP$\{h_i\}_i$ contains only finitely many elements and each element is path connected.

We claim that the projection of each element of CSP$\{g_i\}_i$ onto $\mathbb{R}^{n-1}$ is a union of elements in CSP$\{h_i\}_i$. Once this is established it follows that CSP$\{g_i\}_i$ is finite, because the number of elements of CSP$\{g_i\}_i$ that project onto a given point $\bar{x}^{n-1]} \in \mathbb{R}^{n-1}$ is at most equal to the number of elements in the connected sign partition of $\mathbb{R}$ generated by the polynomials $t \mapsto g_i(\bar{x}^{n-1]}, t)$.

Now to establish the claim. Assume that $\bar{x}^{n-1]}$ and $\hat{x}^{n-1]}$ lie in the same element of CSP$\{h_i\}_i$. We want to prove that they lie in the projections of exactly the same elements of CSP$\{g_i\}_i$. Assume otherwise; assume that $\bar{x}^{n-1]}$ lies in the projection of some element of CSP$\{g_i\}_i$ that $\hat{x}^{n-1]}$ does not.

Let $\gamma:[0,1] \to \mathbb{R}^{n-1}$ be a continuous path from $\gamma(0) = \bar{x}^{n-1]}$ to $\gamma(1) = \hat{x}^{n-1]}$ contained entirely within an element of CSP$\{h_i\}_i$. Let I denote the set of indices i for which there exists $0 \leq s \leq 1$ such that $t \mapsto g_i(\gamma(s), t)$ is not identically zero. Because the polynomials (C.1) are contained in $\{h_i\}_i$, the degree of $t \mapsto G_I(\gamma(s), t)$ must be the same for all $0 \leq s \leq 1$. Call this degree $\bar{e}$. (It is easily established that we may assume $\bar{e} \geq 1$; otherwise $\bar{x}^{n-1]}$ and $\hat{x}^{n-1]}$ would lie in the projections of the same elements of CSP$\{g_i\}_i$.)

Since the zeros of degree $\bar{e}$ polynomials vary continuously in the coefficients and since $\bar{x}^{n-1]}$ lies in the projection of some element of CSP$\{g_i\}_i$ that $\hat{x}^{n-1]}$ does not, it follows from the definition of G_I that there exist $0 \leq s_1, s_2 \leq 1$ such that the number of common complex zeros counting multiplicities for

$$t \mapsto G_I(\gamma(s_1), t) \quad \text{and} \quad t \mapsto \frac{\mathrm{d}}{\mathrm{d}t} G_I(\gamma(s_1), t)$$

is different than for the pair obtained by replacing s_1 with s_2. But since the polynomials $h_{I,e,k}$ are contained in $\{h_i\}_i$, Lemma C.1 then implies $\gamma(s_1)$ and $\gamma(s_2)$ must then lie in different elements of CSP$\{h_i\}_i$, contradicting the definition of γ. The claim is thus established.

Now we inductively establish path-connectedness for the elements of CSP$\{g_i\}_i$. Momentarily we will show that each element of CSP$\{g_i\}_i$ is a finite union of path-connected sets. Although each $S \in$ CSP$\{g_i\}_i$ is connected, it does not then follow that each S is path-connected. However, since the g_i are arbitrary polynomials in n-variables it does follow for all $\bar{x} \in \mathbb{R}^n$, $\varepsilon \geq 0$ that each connected component of $S \cap \{x;\ \|x - \bar{x}\| \leq \varepsilon\}$ is a finite union of path-connected components (since each such connected component is an element of the connected sign partition generated by $\{g_i\}_i \cup \{x \mapsto \varepsilon^2 - \sum_j x_j^2\}$). Elementary point-set topology arguments show that any connected set S possessing this latter property is in fact path-connected.

Now to prove that each element of CSP$\{g_i\}_i$ is a finite union of path-connected sets. Define

$$\{f_i\}_i := \{g_i\}_i \cup \{x^{n]} \mapsto h_i(x^{n-1]})\}_i,$$

where $x^{n]} = (x_1, \ldots, x_n)$. Relying on the already established fact that connected sign partitions contain only finitely many elements, each element of CSP$\{g_i\}_i$ is the finite union of elements of CSP$\{f_i\}_i$. It suffices to establish path-connectedness for the elements of CSP$\{f_i\}_i$.

Let $S \in$ CSP$\{f_i\}_i$. Since, as we have seen, the projection of any element of CSP$\{g_i\}_i$ onto $\mathbb{R}^{n-1}$ is a union of a finite number of elements from CSP$\{h_i\}_i$, the projection of S onto $\mathbb{R}^{n-1}$ is precisely an element $\bar{S}$ of CSP$\{h_i\}_i$.

Let I denote the set of indices i for which there exists $x^{n-1]} \in \bar{S}$ such that $t \mapsto g_i(x^{n-1]}, t)$ is not identically zero. Because the polynomials (C.1) are contained in $\{h_i\}_i$, the degree of $t \mapsto G_I(x^{n-1]}, t)$ is the same for all $x^{n-1]} \in \bar{S}$. If the degree is 0, then relying on the notation $x^{n]} = (x^{n-1]}, x_n)$, we have that

$$S = \{x^{n]}; x^{n-1]} \in \bar{S}\},$$

and the path-connectedness of S follows from that of $\bar{S}$. We may thus assume that the degree is at least 1.

From the definition of $\{h_i\}_i$ and Lemma C.1 it is easily argued that the number of distinct real zeros of $t \mapsto G_I(x^{n-1]}, t)$ is independent of $x^{n-1]} \in \bar{S}$. Denote this number by e'. We may assume that $e' \geq 1$ since otherwise path-connectedness follows easily.

For $x^{n-1]} \in \bar{S}$, let $t^{(1)}(x^{n-1]}) < \cdots < t^{(e')}(x^{n-1]})$ denote the distinct real zeros of $t \mapsto G_I(x^{n-1]}, t)$; we may assume that each $t^{(i)}$ is continuous in $x^{n-1]}$. Then, clearly, S is of one of the following forms:

$$\{(x^{n-1]}, t); x^{n-1]} \in \bar{S} \text{ and } t < t^{(1)}(x^{n-1]})\},$$
$$\{(x^{n-1]}, t^{(i)}(x^{n-1]}); x^{n-1]} \in \bar{S}\},$$
$$\{(x^{n-1]}, t); x^{n-1]} \in \bar{S} \text{ and } t^{(i)}(x^{n-1]}) < t < t^{(i+1)}(x^{n-1]})\},$$
$$\{(x^{n-1]}, t); x^{n-1]} \in \bar{S} \text{ and } t > t^{(e')}(x^{n-1]})\}.$$

Since $\bar{S}$ is path-connected and $t^{(i)}(x^{n-1]})$ varies continuously in $x^{n-1]} \in \bar{S}$, it follows that S is path-connected.

Appendix D

Here we establish the well-known facts that "most" systems of homogeneous polynomials $F: \mathbb{C}^n \to \mathbb{C}^m$, $m \geq n$, have only the trivial zero, and "most" systems of homogeneous polynomials $F: \mathbb{C}^n \to \mathbb{C}^{n-1}$ have only finitely many zero lines. We begin with the first fact. The proof we present is a simplification of the proof presented in section 80 (via sections 18 and 77) of Van der Waerden (1950). The proof depends on the following easily proven and very well-known proposition. (A proof of the proposition follows immediately from the proof of Lemma 3.1 in Part II in this series.)

PROPOSITION D.1. *Assume that*

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

are complex univariate polynomials of formal degrees d and e, respectively. Define M to be the $(d+e) \times (d+e)$ matrix $[m_{ij}]$ where

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

(*Here we define $a_i = 0$ if $i < 0$ or $i > d$, and similarly for b_i.*) *Then* $\det M = 0$ *if and only if either* (i) *p and q have a common zero or* (ii) $a_d = 0 = b_e$.

The matrix M is generally referred to as the "Sylvester matrix" of p and q, and its determinant is generally referred to as the "Sylvester resultant" of p and q.

Let $d_1, \ldots, d_m$ be positive integers and consider the set of all homogeneous systems $F: \mathbb{C}^n \to \mathbb{C}^m$ for which either degree $(F_i) = d_i$ or F_i is identically zero. By identifying each of these systems with the vector of its coefficients we identify the entire set with $\mathbb{C}^N$ for the appropriate N. We wish to show that there exists a finite set $\{\Phi_i\}_i$ of polynomials $\Phi_i:\mathbb{C}^N\to\mathbb{C}$ such that F has a non-trivial zero if and only if $\Phi_i(F)=0$ for all i.

We begin by claiming that we may assume all d_i to be the same positive integer. This is simply because F, as above, has a non-trivial zero if and only if the system $\tilde{F}:\mathbb{C}^n\to C^m$ does, where $\tilde{F}_i\equiv(F_i)^{\prod_{j\neq i}d_j}$. Since the coefficients of $\tilde{F}$ are polynomial expressions in the coefficients of F, the claim follows.

Let $\mathbb{C}H\mathrm{Poly}(m,n,d)$ denote the vector space of systems of polynomials $F:\mathbb{C}^n\to\mathbb{C}^m$ with coordinate polynomials F_i which are either homogeneous of degree d, or identically zero. We now prove that there does indeed exist a finite set $\{\Phi_i\}_i$ of polynomials $\Phi_i:\mathbb{C}H\mathrm{Poly}(m,n,d)\to\mathbb{C}$ such that $\Phi_i(F)=0$ for all i if and only if F has a non-trivial zero.

The proof proceeds by induction. It is trivially true when $n=1$; then only the identically zero system has a non-trivial zero. We now establish it for general n assuming that it is true for $n-1$.

In what follows we use $x^{n-1]}$ to denote a vector of $n-1$ variables, and for $u\in\mathbb{C}^m$, $F\in\mathbb{C}H\mathrm{Poly}(m,n,d)$, we define $u\cdot F:=\sum_i u_iF_i$, a single polynomial in n variables.

Consider the polynomial $\psi:\mathbb{C}^m\times\mathbb{C}^m\times\mathbb{C}H\mathrm{Poly}(m,n,d)\times\mathbb{C}^{n-1}\to\mathbb{C}$ whose value at $(u,v,F,x^{n-1]})$ is the value of the Sylvester resultant of the two univariate polynomials $t\mapsto u\cdot F(x^{n-1]},t)$ and $t\mapsto v\cdot F(x^{n-1]},t)$. It follows from Proposition D.1 that if $(u,v,F,x^{n-1]})$ is a zero of ψ, then so are all multiples of $(u,v,F,x^{n-1]})$. Consequently, ψ is homogeneous. Let D denote its degree.

Expanding ψ in powers of u and v, let $\{\psi_i\}_i$ denote the coefficient polynomials; these are polynomials in $(F,x^{n-1]})\in\mathbb{C}H\mathrm{Poly}(m,n,d)\times\mathbb{C}^{n-1}$. For $F\in\mathbb{C}H\mathrm{Poly}(m,n,d)$, let $\tilde{F}$ denote the system consisting of the polynomials $x^{n-1]}\mapsto\psi_i(F,x^{n-1]})$. From the definition and homogeneity of ψ, it is easily seen that polynomials of $\tilde{F}$ are either homogeneous of degree $d':=D-4d$, or are identically zero. Consequently, letting m' denote the number of elements in $\{\psi_i\}_i$, we have that $F\mapsto\tilde{F}$ is a polynomial mapping from $\mathbb{C}H\mathrm{Poly}(m,n,d)$ to $\mathbb{C}H\mathrm{Poly}(m',n-1,d')$. (In fact, it is a homogeneous polynomial mapping.)

By assumption, there exists a finite set $\{\Phi_i'\}_i$ of polynomials $\Phi_i':\mathbb{C}H\mathrm{Poly}(m',n-1,d')\to\mathbb{C}$ such that $\Phi_i'(G)=0$ if and only if G has a non-trivial zero.

We claim that F has a non-trivial zero if and only if $\tilde{F}$ does. Consequently, the set $\{\Phi_i\}_i$ of polynomials that we seek can be defined simply as the composition of the polynomials Φ_i' with $F\mapsto\tilde{F}$.

Now to prove the claim.

First assume that the homogeneous system F is such that the monomial x_n^d does not occur among the non-zero terms of any of the coordinate polynomials F_i. Then F has a non-trivial zero, namely, $(0,\ldots,0,1)$. Also, by (ii) of Proposition D.1, $(u,v,x^{n-1]})\mapsto\psi(u,v,F,x^{n-1]})$ is identically zero. Consequently, $\tilde{F}$ is the identically zero system; it certainly has a non-trivial zero.

Henceforth, we may assume that x_n^d does occur among the non-zero terms of at least one of the F_i. Note that then any non-trivial zero $(\bar{x}^{n-1]},\bar{t})$ of F satisfies $\bar{x}^{n-1]}\neq0$.

Assume that F has a non-trivial zero $(\bar{x}^{n-1]},\bar{t})$. Then for all u and v, the univariate polynomials $t\mapsto u\cdot F(\bar{x}^{n-1]},t)$ and $t\mapsto v\cdot F(\bar{x}^{n-1]},t)$ share the common zero $\bar{t}$. Consequently, by (i) of Proposition D.1, $(u,v)\mapsto\psi(u,v,F,\bar{x}^{n-1]})$ is identically zero. It follows that $\tilde{F}(\bar{x}^{n-1]})=0$.

Conversely, assume that $\tilde{F}$ has a non-trivial zero, say, $\bar{x}^{n-1]}$. Then $(u,v)\mapsto\psi(u,v,F,\bar{x}^{n-1]})$ is identically zero.

Fix $\bar{u}$ such that $t\mapsto\bar{u}\cdot F(\bar{x}^{n-1]},t)$ is of degree d. Let $\bar{t}_1,\ldots,\bar{t}_d$ denote the zeros of this univariate polynomial. Define $T_i:\mathbb{C}^m\mapsto\mathbb{C}$ by $T_i(v)=v\cdot F(\bar{x}^{n-1]},\bar{t}_i)$. To prove that

F has a non-trivial zero it suffices to show that for some i, the linear map T_i is identically zero (because then $(\bar{x}^{n-1}, \bar{t}_i)$ will be a non-trivial zero of F). In turn, to prove this, by the linearity of the maps T_i it suffices to show that for each v there exists i such that $T_i(v)=0$. But this is true by (i) of Proposition D.1 and the fact that $v \mapsto \psi(\bar{u}, v, F, \bar{x}^{n-1]})$ is identically zero (since $(u, v) \mapsto \psi(u, v, F, \bar{x}^{n-1]})$ is identically zero).

We have now proven that there does indeed exist a finite set $\{\Phi_i\}_i$ of polynomials Φ_i: $\mathbb{C}H\text{Poly}(m, n, d) \to \mathbb{C}$ such that $\Phi_i(F)=0$ for all i if and only if F has non-trivial zero.

Next we prove the second fact to be established in this appendix: there exists a finite set of polynomials from $\mathbb{C}H\text{Poly}(n-1, n, d)$ to $\mathbb{C}$ all of which vanish at F if and only if F has infinitely many zero lines.

To each system $F \in \mathbb{C}H\text{Poly}(n-1, n, d)$ add an additional polynomial $u \cdot x := \sum_j u_j x_j$. Here, the u_j are the coefficients but momentarily they will be viewed as variables. Let the resulting system be denoted by $(F, u \cdot x): \mathbb{C}^n \to \mathbb{C}^n$.

We know that there exists a finite set of polynomials $\{\Phi_i\}_i$ such that $(F, u \cdot x)$ has other than the trivial zero if and only if $\Phi_i(F, u \cdot x)=0$ for all i. Expand the polynomials $\Phi_i(F, u \cdot x)$ in powers of the variables u; the coefficients of the powers of u are then polynomials in the coefficients of F. Denote these polynomials in the coefficients of F by Φ_{ij} where i corresponds to the subscript of the polynomial Φ_i whose expansion produced Φ_{ij}.

We claim that F has infinitely many distinct zero lines if and only if $\Phi_{ij}(F)=0$ for all i and j.

For first assume that F has only finitely many zero lines. For each of these lines choose a non-zero vector on that line. Assume that $\alpha^{(1)}, \ldots, \alpha^{(l)}$ are the chosen vectors. There exists $\bar{u} \in \mathbb{C}^n$ such that $\bar{u} \cdot \alpha^{(k)} \neq 0$ for all k. Then the system $x \mapsto (F(x), \bar{u} \cdot x)$ has no non-trivial zero. Hence, there exists i' such that $\Phi_{i'}(F, \bar{u} \cdot x) \neq 0$. Consequently, there exists j such that $\Phi_{i'j}(F) \neq 0$.

Now assume that F has infinitely many zero lines. By considering the limit set of a sequence of zero lines of F it is easy to prove that for each $\bar{u} \in \mathbb{C}^n$ there exists a complex line $L \subset \mathbb{C}^n$ which contains the point $\bar{u}$ and which intersects the set

$$\{y \in \mathbb{C}^n;\, \exists x \neq 0 \ni F(x)=0 \text{ and } y \cdot x = 0\}$$

in infinitely many points. However, for each of these intersection points y the map $x \mapsto (F(x), y \cdot x)$ has a non-trivial zero so that for all i, $\Phi_i(F, y \cdot x)=0$. Hence, all of the univariate polynomials obtained by restricting $u \mapsto \Phi_i(F, u \cdot x)$ to $u \in L$ have infinitely many zeros and thus must be identically zero. In particular, $\Phi_i(F, \bar{u} \cdot x)=0$ for all i. Since $\bar{u}$ was arbitrary, it follows that $\Phi_{ij}(F) \equiv 0$ for all i and j.

Appendix E

Here we establish the existence of a "nice" $\bar{f}$ as claimed just prior to Proposition 2.2.1.

Let $\bar{f}^{(1)}$ be the system defined by $\bar{f}_i^{(1)}(x) = x_i^d$ for all i and let $\bar{f}^{(2)}$ be the system defined by $\bar{f}_i^{(2)}(x) = x_i^d - 1$ for all i. Because $U \mapsto R(\bar{f}_i^{(1)}, U) = (D!) U_{n+1}^{d^n}$, it easily follows that for all except finitely many values of $\varepsilon \in \mathbb{C}$

$$U \mapsto R(\varepsilon \bar{f}^{(1)} + (1-\varepsilon)\bar{f}^{(2)}, U) \tag{E.1}$$

is not identically zero.

Next, since the homogenization of the system of $n+1$ polynomials in n variables

$$\bar{f}^{(2)}(x)$$
$$\det[D\bar{f}^{(2)}(x)]$$

has no non-trivial solution (here $D\bar{f}^{(2)}$ is the Jacobian matrix) it follows from the discussion of section 2.1 that for all but finitely many values of ε the system

$$\begin{aligned} &x \mapsto \varepsilon\bar{f}^{(1)}(x)+(1-\varepsilon)\bar{f}^{(2)}(x)\\ &x \mapsto \det[D(\varepsilon\bar{f}^{(1)}+(1-\varepsilon)\bar{f}^{(2)})(x)] \end{aligned} \tag{E.2}$$

has no non-trivial solution when homogenized.

Let $\bar{f} := \varepsilon\bar{f}^{(1)}+(1-\varepsilon)\bar{f}^{(2)}$ be such that (E.1) is not identically zero and (E.2) has no non-trivial solutions when homogenized.

Invoking the same arguments again, for all but finitely many values of $\varepsilon \in \mathbb{C}$

$$U \mapsto R(\varepsilon f+(1-\varepsilon)\bar{f}, U)$$

is not identically zero and the system

$$\begin{aligned} &x \mapsto \varepsilon f(x)+(1-\varepsilon)\bar{f}(x)\\ &x \mapsto \det D(\varepsilon f+(1-\varepsilon)\bar{f})(x) \end{aligned} \tag{E.3}$$

has no non-trivial solution when homogenized. We will have proven that $\bar{f}$ is nice in the sense that we desire if we can establish the fact that except for the finitely many values of ε excluded,

$$x \mapsto \varepsilon f(x)+(1-\varepsilon)\bar{f}(x) \tag{E.4}$$

has exactly d^n distinct zeros, including those at infinity.

Assume that ε' is not an excluded value. Let $\gamma:[0, 1] \mapsto \mathbb{C}$ be a continuously differentiable path from $\gamma(0)=0$ to $\gamma(1)=\varepsilon'$ that avoids excluded values.

We now argue that if $\varepsilon=\gamma(t)$, then (E.4) has no zeros at infinity. Assume otherwise and let $\bar{X} \in \mathbb{C}^{n+1}$ be a non-trivial zero of the homogenization of (E.4) satisfying $\bar{X}_{n+1}=0$. Let $h:\mathbb{C}^n \to \mathbb{C}^n$ be the homogeneous system composed of the terms of degree d in (E.4). Letting $\bar{x} := (\bar{X}_1, \ldots, \bar{X}_n)$, then the homogenization of the last equation in (E.3) at $\bar{X}$ is easily seen to equal $\det Dh(\bar{x})$. But since h is homogeneous and $h(\bar{x})=0$, $\det Dh(\bar{x})$ must equal zero. Hence $\bar{X}$ must be a zero of the homogenization of (E.3) contradicting $\varepsilon=\gamma(t)$ not being an excluded value. Hence, if $\varepsilon=\gamma(t)$ then (E.4) has no zeros at infinity.

Fix $0 \le t' \le 1$ and let x' be a zero of (E.4) for $\varepsilon=\gamma(t')$. Because ε is not an excluded value, the Jacobian matrix

$$D(\varepsilon f+(1-\varepsilon)\bar{f})(x')$$

is non-singular. The implicit function theorem and the fact that (E.4) has no zeros at infinity for any non-excluded value of ε then imply that for all t in a relatively open interval of t' in $[0, 1]$, the number of zeros of (E.4) when $\varepsilon=t$ is the same as the number when $\varepsilon=t'$. Since $[0, 1]$ cannot be expressed as the disjoint union of more than one relatively open subinterval of $[0, 1]$ it follows that the number of zeros of (E.4) for $\varepsilon=\gamma(1)=\varepsilon'$ is the same as the number of zeros of $\bar{f}$. By exactly the same arguments applied to (E.2), the number of distinct zeros of $\bar{f}$ equals that of $\bar{f}^{(2)}$, i.e. d^n. Hence, the number of zeros of (E.4) for $\varepsilon=\varepsilon'$ is d^n.