Discrete Comput Geom (2010) 44: 195–222
DOI 10.1007/s00454-009-9200-4

On Sign Conditions Over Real Multivariate Polynomials

Gabriela Jeronimo · Daniel Perrucci · Juan Sabia

Received: 19 December 2008 / Revised: 19 March 2009 / Accepted: 4 May 2009 /
Published online: 23 June 2009

Abstract We present a new probabilistic algorithm to find a finite set of points intersecting the closure of each connected component of the realization of every sign condition over a family of real polynomials defining regular hypersurfaces that intersect transversally. This enables us to show a probabilistic procedure to list all feasible sign conditions over the polynomials. In addition, we extend these results to the case of closed sign conditions over an *arbitrary* family of real multivariate polynomials. The complexity bounds for these procedures improve the known ones.

Keywords Real multivariate polynomials · Sign conditions · Consistency problem · Complexity

1 Introduction

Given polynomials $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$, a sign condition $\sigma \in \{<, =, >\}^m$, or a closed sign condition $\sigma \in \{\leq, =, \geq\}^m$, is said to be *feasible* if the system

G. Jeronimo, D. Perrucci and J. Sabia partially supported by the following Argentinian research grants: UBACyT X847 (2006-2009), CONICET PIP 5852/05.
G. Jeronimo partially supported by ANPCYT PICT 2005 17–33018.

G. Jeronimo (✉) · D. Perrucci
Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina
e-mail: jeronimo@dm.uba.ar

J. Sabia
Departamento de Ciencias Exactas, Ciclo Básico Común, Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina

G. Jeronimo · J. Sabia
CONICET, Buenos Aires, Argentina

$f_1(x)\sigma_1 0, \ldots, f_m(x)\sigma_m 0$ has a solution in $\mathbb{R}^n$, and the set of its solutions is called the *realization* of σ. One of the basic problems in computational semialgebraic geometry is to decide whether a sign condition is feasible. This problem is a particular case of quantifier elimination and, on the other hand, many elimination algorithms use subroutines determining all the feasible sign conditions for a family of polynomials.

The first elimination algorithms over the reals are due to Tarski [41] and Seidenberg [39], but their complexities are not elementary recursive. Collins [16] was the first to obtain a doubly exponential complexity. In [21], Grigor'ev and Vorobjov present an algorithm with single exponential complexity to decide the consistency of a system of equalities and inequalities by studying the critical points of a function in order to obtain a finite set of points intersecting each connected component of the solution set. This same idea was used to obtain more efficient quantifier elimination procedures in [25, 32] and [7]. The procedure in this last paper relies on previous results from [8], where the authors obtain the best known complexity bound, in the deterministic model, for the computation of a set of points meeting every connected component of each feasible sign condition over an arbitrary family of polynomials: namely, for m polynomials in n variables of degrees bounded by d, this set can be computed within $m^{n+1}d^{O(n)}$ arithmetic operations. The specific problem of consistency for equalities over $\mathbb{R}$ was also treated through the critical point method afterwards. In [34], the non-emptiness of a real variety defined by a single equation is studied and, in [2], an algorithm is given to deal with arbitrary positive dimensional systems.

Several probabilistic procedures lead to successive complexity improvements. Using classical polar varieties, in [3] and [4], the case of a smooth compact variety given by a regular sequence is tackled within a complexity depending polynomially on an intrinsic degree of the systems involved and the input length. To achieve this complexity, straight-line program encoding of polynomials and an efficient procedure to solve polynomial equation systems over the complex numbers ([18]) are used. The compactness assumption is dropped in [5] and [6], by introducing generalized polar varieties. The main complexity result in these papers is that the computation of a finite set which contains at least one sample point for each connected component of the considered real variety can be achieved in time $O\big(\binom{n}{m}Ln^4m^2d^2\delta^2\big)$ up to poly-logarithmic factors, where $\delta \leq d^n m^{n-m}$ is a suitably defined degree of the real interpretation of the input reduced regular sequence of polynomials and L is the length of a straight-line program encoding these polynomials. The non-compact case is also considered in [36] for a smooth equidimensional variety defined by a radical ideal by studying projections over polar varieties, and an extension to the non-equidimensional situation is presented in [37]. Finally, [35] describes an algorithm computing at least one point in each connected component of a semi-algebraic set defined by a single inequality, which is based on the computation of generalized critical points, within $O(n^7d^{4n})$ arithmetic operations.

In this paper, we consider the problem of determining all feasible sign conditions (or closed sign conditions) over a given finite family of multivariate polynomials $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$. We first present a probabilistic algorithm that obtains a finite set of points intersecting the closure of each connected component of the realization of every sign condition over the given polynomials under the following regularity condition:

Assumption 1 For every $x \in \mathbb{C}^n$ and every $\{i_1, \ldots, i_s\} \subset \{1, \ldots, m\}$, if $f_{i_1}(x) = \cdots = f_{i_s}(x) = 0$, then $\{\nabla f_{i_1}(x), \ldots, \nabla f_{i_s}(x)\}$ is linearly independent.

In addition, for families of *arbitrary* polynomials, we show a probabilistic algorithm that computes a finite set of points intersecting each connected component of the realization of every *closed* sign condition. The input and intermediate computations in our algorithms are encoded by straight-line programs (see Sect. 2.2). The output is described by means of geometric resolutions, that is to say, by rational parametrizations of 0-dimensional varieties represented by univariate polynomials encoded in the usual way (namely, by their coefficient vectors). In both situations, the output of the algorithm enables us to determine all the feasible closed sign conditions over the polynomials by evaluating their signs at the computed points, which is done by using the techniques in [15]; moreover, in the first case, we can determine all feasible sign conditions (see Theorems 17 and 26).

A sketch of our main algorithms is the following. Given $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$, a generic change of variables prevents asymptotic behavior with respect to the projection to the first coordinate x_1 for each connected component $C \subset \mathbb{R}^n$ of every feasible (closed) sign condition over $f_1, \ldots, f_m$: either C projects onto $\mathbb{R}$ or its projection is a proper (possibly unbounded) interval whose endpoints have a non-empty finite fiber in $\overline{C}$. In the latter case, points in $\overline{C}$ are obtained as extremal points of x_1. These extremal points are solutions of particular systems of polynomial equations which are dealt with by deformation techniques that enable the computation of geometric resolutions of finite sets including them. To find points in the components projecting onto $\mathbb{R}$, the set is intersected with $\{x_1 = p_1\}$ for a particular value p_1, and the algorithm continues recursively.

The following theorem states our main results (see Theorems 15 and 25):

Theorem 2 *Let $\mathbb{K}$ be an effective subfield of $\mathbb{R}$. There are probabilistic algorithms to perform the following tasks*:

- *Given polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ satisfying Assumption 1, with degrees bounded by $d \geq 2$ and encoded by a straight-line program of length L, obtain a finite set of points intersecting the closure of each connected component of the realization of every sign condition over $f_1, \ldots, f_m$ within $O\big(\sum_{s=1}^{\min\{m,n\}} \binom{m}{s}\big(\binom{n-1}{s-1}d^n\big)^2 L\big)$ operations in $\mathbb{K}$ up to poly-logarithmic factors.*
- *Given* arbitrary *polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$, with degrees bounded by an even integer d and encoded by a straight-line program of length L, obtain a finite set of points intersecting each connected component of the realization of every* closed *sign condition over $f_1, \ldots, f_m$ within $O\big(\sum_{s=1}^{\min\{m,n\}} 2^s \binom{m}{s}\big(\binom{n-1}{s-1}d^n\big)^2 (L + d)\big)$ operations in $\mathbb{K}$ up to poly-logarithmic factors.*

The condition $d \geq 2$ is only required in order to simplify some complexity bounds. Even though Assumption 1 cannot be checked within the complexity order of our algorithms, it is met by generic polynomial families. The factor $\binom{n-1}{s-1}d^n$ in the com-

plexity estimates is an upper bound for the bihomogeneous Bézout numbers arising from the Lagrange characterization of critical points of projections (cf. [37]). In fact, one of the new tools to achieve the stated complexity order, which improves the previous ones depending on the same parameters, is the use of algorithmic deformation techniques specially designed for bihomogeneous systems (for a similar approach to solving bihomogeneous systems, see [24]). Up to now, the polynomial systems used to characterize critical points were handled with general algorithms solving polynomial equations over the complex numbers (see, for instance, [1, 20, 33], and [30]). Another important feature of the deformation techniques we use is that they enable us to locate a *finite* subset of representative points in the solution set of the considered Lagrange systems for arbitrary polynomial families.

A standard technique in real elimination is to take sums of squares and introduce infinitesimals to reduce the problem to the study of a smooth and compact real hypersurface. As this leads to an artificial growth of the parameters involved in the complexity estimates, a further advantage of our techniques is that we work directly with the input equations, as in [36] and [6], instead of using these constructions. Moreover, our work can be seen as an extension of [36] and [6] in the sense that we deal not only with equations but also with inequalities. In particular, the algorithm in [36], which only works for the case of smooth equidimensional varieties defined by a radical ideal, considers a family of equation systems equivalent to the ones introduced in the recursive stages of our algorithm, but those systems involve a large number of polynomials and do not have any evident structure. Let us remark that the use of infinitesimals in previous works serves also the purpose of finding representative points for *open* sign conditions defined by arbitrary polynomials. To achieve this task, which is not considered in this paper, the use of infinitesimals still seems to be unavoidable.

We also prove that our deformation based approach can be applied to deal with sign conditions over bivariate systems without any assumption on the polynomials. We expect this can be extended to general multivariate polynomials. This is the subject of our current research. Finally, we adapt our techniques to the case of an arbitrary multivariate polynomial.

All the complexity bounds in this paper refer to the number of arithmetic operations. The bit complexity analysis of our algorithms would require a further characterization of the generic choices involved as well as bit complexity estimates for some previous subroutines we use, which seem to be difficult to obtain.

This paper is organized as follows: In Sect. 2, we introduce some basic notions and notation that will be used throughout the paper. Section 3 is devoted to presenting the basic ingredients to be used in the design of our algorithms. In Sect. 4, we present our main algorithms to determine all feasible sign conditions over polynomial families satisfying regularity assumptions. In Sect. 5, we consider the same problem for closed sign conditions over arbitrary multivariate polynomials. The last section contains our results on sign conditions over bivariate polynomial families and over a single multivariate polynomial.

2 Preliminaries

2.1 Notation

Throughout this paper $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ denote the fields of rational, real and complex numbers, respectively, $\mathbb{N}$ denotes the set of positive integers and $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. If k is a field, $\bar{k}$ will denote an algebraic closure of k.

For $n \in \mathbb{N}$ and an algebraically closed field k, we denote by $\mathbb{A}^n_k$ and $\mathbb{P}^n_k$ (or simply by $\mathbb{A}^n$ or $\mathbb{P}^n$ if the base field is clear from the context) the n-dimensional affine space and projective space over k, respectively, equipped with their Zariski topologies. For a subset X of one of these spaces, we will denote by $\overline{X}$ its closure. We adopt the usual notions of dimension and degree of an algebraic variety V (see, for instance, [40] and [22]).

We will denote a projections on a set of coordinates x by π_x. For short, a projection on the kth coordinate will also be denoted by π_k.

For any non-empty set $A \subset \mathbb{R}^n$, $\overline{A}$ will denote its closure with respect to the usual Euclidean topology. We define $Z_{\inf}(A) = \{(x_1, \ldots, x_n) \in \overline{A} \mid x_1 = \inf \pi_1(A)\}$ if $\pi_1(A)$ is bounded from below, and $Z_{\inf}(A) = \emptyset$ otherwise. Similarly, $Z_{\sup}(A) = \{(x_1, \ldots, x_n) \in \overline{A} \mid x_1 = \sup \pi_1(A)\}$ if $\pi_1(A)$ is bounded from above, and $Z_{\sup}(A) = \emptyset$ otherwise. Finally, we denote $Z(A) = Z_{\inf}(A) \cup Z_{\sup}(A)$.

Throughout this paper, log will denote logarithm to the base 2.

2.2 Algorithms and Complexity

The algorithms we consider in this paper are described by arithmetic networks over an effective base field $\mathbb{K} \subset \mathbb{R}$ (see [43]). The notion of *complexity* of an algorithm we consider is the number of operations and comparisons over $\mathbb{K}$.

The objects we deal with are polynomials with coefficients in $\mathbb{K}$. Throughout our algorithms we represent each polynomial either as the array of all its coefficients in a pre-fixed order of its monomials (*dense form*) or by a *straight-line program*. Roughly speaking, a straight-line program (or slp, for short) over $\mathbb{K}$ encoding a list of polynomials in $\mathbb{K}[x_1, \ldots, x_n]$ is a program without branches (an arithmetic circuit) which enables us to evaluate these polynomials at any given point in $\mathbb{K}^n$. The number of instructions in the program is called the *length* of the slp (for a precise definition we refer to [14, Definition 4.2]; see also [23]).

We will do operations with polynomials encoded in both these ways. To estimate the complexities we will use the following results: Operations between univariate polynomials with coefficients in a field $\mathbb{K}$ of degree bounded by d in dense form can be done using $O(d \log(d) \log\log(d))$ operations in $\mathbb{K}$ (see [44, Chap. 8]). From an slp of length L encoding a polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$, we can compute an slp with length $O(L)$ encoding f and all its first order partial derivatives (see [10]).

2.3 Geometric Resolutions

A way of representing zero-dimensional affine varieties which is widely used in computer algebra nowadays is a *geometric resolution*. This notion was first introduced in

the works of Kronecker and König in the last years of the nineteenth century ([29] and [28]) and appears in the literature under different names (rational univariate representation, shape lemma, etc.). For a detailed historical account on its application in the algorithmic framework, we refer the reader to [20]. The precise definition we are going to use is the following:

Let k be a field of characteristic 0 and $V = \{\xi^{(1)}, \ldots, \xi^{(D)}\} \subset \mathbb{A}^n_{\overline{k}}$ be a zero-dimensional variety defined by polynomials in $k[x_1, \ldots, x_n]$. Given a *separating* linear form $\ell = u_1 x_1 + \cdots + u_n x_n \in k[x_1, \ldots, x_n]$ for V (that is, a linear form ℓ such that $\ell(\xi^{(i)}) \neq \ell(\xi^{(j)})$ if $i \neq j$), the following polynomials completely characterize the variety V:

- the *minimal polynomial* $q := \prod_{1 \leq i \leq D}(U - \ell(\xi^{(i)})) \in k[U]$ of ℓ over the variety V (where U is a new variable),
- a polynomial $\tilde{q} \in k[U]$ with $\deg(\tilde{q}) < D$ and relatively prime to q,
- polynomials $w_1, \ldots, w_n \in k[U]$ with $\deg(w_j) < D$ for every $1 \leq j \leq n$ satisfying

$$V = \left\{ \left(\frac{w_1}{\tilde{q}}(\eta), \ldots, \frac{w_n}{\tilde{q}}(\eta) \right) \in \overline{k}^n \;\middle|\; \eta \in \overline{k},\ q(\eta) = 0 \right\}.$$

The family of univariate polynomials $q, \tilde{q}, w_1, \ldots, w_n \in k[U]$ is called a *geometric resolution* of V (associated with the linear form ℓ).

We point out that the polynomial $\tilde{q}$ appearing in the above definition is invertible in $k[U]/(q(U))$. Setting $v_k(U) := \tilde{q}^{-1}(U) w_k(U) \mod (q(U))$ for every $1 \leq k \leq n$, we are lead to the standard notion of geometric resolution: a family of $n+1$ polynomials $q, v_1, \ldots, v_n$ in $k[U]$ satisfying $V = \{(v_1(\eta), \ldots, v_n(\eta)) \in \overline{k}^n \mid \eta \in \overline{k},\ q(\eta) = 0\}$. We will use both definitions alternatively, since the complexity of passing from one representation to the other does not modify the overall complexity of our algorithms. Which notion is used in each case will be clear from the number of polynomials.

3 General Approach

3.1 Avoiding Asymptotic Situations

For any non-empty set $A \subset \mathbb{R}^n$ we define $Z_{\inf}(A, k) = \{(x_1, \ldots, x_n) \in \overline{A} \mid x_k = \inf \pi_k(A)\}$ if $\pi_k(A)$ is bounded from below, and $Z_{\inf}(A, k) = \emptyset$ otherwise. Similarly, $Z_{\sup}(A, k) = \{(x_1, \ldots, x_n) \in \overline{A} \mid x_k = \sup \pi_k(A)\}$ whenever $\pi_k(A)$ is bounded from above, and $Z_{\sup}(A, k) = \emptyset$ otherwise. Finally, $Z(A, k) = Z_{\inf}(A, k) \cup Z_{\sup}(A, k)$. In particular, when $k = 1$, $Z_{\inf}(A, 1)$, $Z_{\sup}(A, 1)$ and $Z(A, 1)$ will be denoted by $Z_{\inf}(A)$, $Z_{\sup}(A)$ and $Z(A)$, respectively, as has already been stated in Sect. 2.1.

The precise conditions achieved by a generic linear change of variables are stated in the following proposition:

Proposition 3 *Let $f_1, \ldots, f_m$ be n-variate polynomials with real coefficients. After a generic linear change of variables over $\mathbb{Q}$, for every semialgebraic set $\mathcal{P}$ defined in $\mathbb{R}^n$ by a Boolean formula on the polynomials $f_1, \ldots, f_m$ involving equalities and inequalities to zero and every $p = (p_1, \ldots, p_n) \in \mathbb{R}^n$, if $1 \leq k \leq n$ and C is a connected component of $\mathcal{P} \cap \{x_1 = p_1, \ldots, x_{k-1} = p_{k-1}\}$, then $Z(C, k)$ is a finite set*

(*possibly empty*). *Moreover, if* $\pi_k(C)$ *is bounded from below, then* $Z_{\inf}(C,k)$ *is not empty, and, if* $\pi_k(C)$ *is bounded from above, then* $Z_{\sup}(C,k)$ *is not empty.*

To prove Proposition 3, we will use the following auxiliary lemma:

Lemma 4 *Let* $\{f_{ij}\}_{1\le i\le n, 1\le j\le l_i} \subset \mathbb{R}[x_1,\dots,x_n]$ *be a family of nonzero polynomials satisfying simultaneously*:

(a) *for* $1 \le i \le n$, $\{f_{ij}\}_{1\le j\le l_i}$ *is contained in* $\mathbb{R}[x_1,\dots,x_i]$, *it is closed under derivation with respect to the variable* x_i, *and every polynomial in it is quasi-monic* (*that is, monic up to a constant*) *with respect to* x_i,

(b) *for* $1 < i \le n$, $\{f_{(i-1)j}\}_{1\le j\le l_{i-1}}$ *slices* $\{f_{ij}\}_{1\le j\le l_i}$ *in the sense of* [13, *Definition* 2.3.4].

Let $p = (p_1,\dots,p_n) \in \mathbb{R}^n$, $1 \le i \le n$, *and* $\mathcal{P} \subset \mathbb{R}^i$ *be a semialgebraic set defined by a Boolean formula on the polynomials* f_{ij}, $1 \le j \le l_i$, *involving equalities and inequalities to zero. For* $1 \le k \le i$, *let* C *be a connected component of* $\mathcal{P} \cap \{x_1 = p_1,\dots,x_{k-1} = p_{k-1}\}$. *Then the set* $Z(C,k)$ *is finite* (*possibly empty*). *Moreover, if* $\pi_k(C)$ *is bounded from below, then* $Z_{\inf}(C,k) \ne \emptyset$, *and, if* $\pi_k(C)$ *is bounded from above, then* $Z_{\sup}(C,k) \ne \emptyset$.

Proof As for every $1 \le k \le n$ the family $\{f_{ij}(p_1,\dots,p_{k-1},x_k,\dots,x_n)\}_{k\le i\le n, 1\le j\le l_i} \subset \mathbb{R}[x_k,\dots,x_n]$ satisfies the hypotheses, it is enough to prove the lemma for $k = 1$.

For $i = 1$, the result is clear.

Suppose the statement is true for $i-1$. Let $\pi : \mathbb{R}^i \to \mathbb{R}^{i-1}$ be the projection on the first $i-1$ coordinates. Following the notation in [13, Chap. 2], let $A_1,\dots,A_\ell$ be the semialgebraic sets giving the slicing of $\mathbb{R}^{i-1}$ with respect to $f_{i1},\dots,f_{il_i}$ given by the polynomials $f_{(i-1)1},\dots,f_{(i-1)l_{i-1}}$ and, for $1 \le s \le \ell$, let $\xi_{s,1} < \cdots < \xi_{s,a_s} : A_s \to \mathbb{R}$ be the continuous semialgebraic functions that slice $A_s \times \mathbb{R}$. Let $A_{s,1},\dots,A_{s,u_s}$ be the connected components of A_s.

Note that C is a finite union of some sets of the partitions of the sets $A_{s,u} \times \mathbb{R}$ given by $\xi_{s,1},\dots,\xi_{s,a_s}$ and $\pi(C)$ is a finite union of sets $A_{s,u}$. If $\pi(C) = \bigcup_h A_{s_h,u_h}$, then $Z(\pi(C)) \subset \bigcup_h Z(A_{s_h,u_h})$. Since each A_{s_h,u_h} is a connected component of A_{s_h}, which can be described by a Boolean formula involving equalities and inequalities to zero of $f_{(i-1)1},\dots,f_{(i-1)l_{i-1}}$, by inductive hypothesis, each $Z(A_{s_h,u_h})$ is finite and, therefore, $Z(\pi(C))$ is finite too. Now, if $w \in Z(C)$, then $\pi(w) \in Z(\pi(C))$. Moreover, at least one of the quasi-monic polynomials $f_{i1},\dots,f_{il_i}$ vanishes at w and, therefore, $Z(C)$ is a finite set.

Suppose now that $\pi_1(C)$ is an interval bounded, for example, from below. Then, by the inductive assumption, there exists $z = (z_1,\dots,z_{i-1}) \in Z_{\inf}(\pi(C)) \subset \overline{\pi(C)}$. Assume further that $A_{1,1} \subset \pi(C)$, $z \in Z_{\inf}(A_{1,1})$ and $\gamma : [0,1] \to \overline{A}_{1,1}$ is a continuous semialgebraic curve such that $\gamma((0,1]) \subset A_{1,1}$ and $\gamma(0) = z$ (see [13, Theorem 2.5.5]). Let $\tilde{x} = \gamma(1)$. Since $\tilde{x} \in A_{1,1} \subset \pi(C)$, there exists $y \in \mathbb{R}$ such that $(\tilde{x},y) \in C$. Using [13, Lema 2.5.6], each $\xi_{1,a}$ can be extended continuously to $\overline{A}_1$. Let us denote by $\xi_{1,a}$ also this extension. Depending on the position of y with respect to the values $\xi_{1,1}(\tilde{x}) < \cdots < \xi_{1,a_1}(\tilde{x})$, it is easy in any case to define a continuous semialgebraic function $h : [0,1] \to \mathbb{R}$ such that the continuous function $\tilde{\gamma} : [0,1] \to \mathbb{R}^i$

defined as $\tilde{\gamma}(t) = (\gamma(t), h(t))$ satisfies $\tilde{\gamma}((0,1]) \subset C$ (note that the signs of the polynomials $f_{i1}, \ldots, f_{il_i}$ are constant over $\tilde{\gamma}((0,1])$) and, therefore, $(z, h(0)) = \tilde{\gamma}(0) \in \overline{C}$. Moreover, as $z_1 = \inf \pi_1(\pi(C)) = \inf \pi_1(C)$, $(z, h(0)) \in Z_{\inf}(C)$. □

Now, we can prove Proposition 3:

Proof By Lemma 4, it suffices to show that there exists a Zarisky open set $\mathcal{U} \subset Gl(n, \mathbb{C})$ such that, for every $V_0 \in \mathbb{Q}^{n\times n} \cap \mathcal{U}$ there exists a family of polynomials $\{f_{ij}\}_{1\le i\le n, 1\le j\le l_i} \subset \mathbb{R}[x]$ satisfying the hypotheses of the lemma, and such that, for $1 \le j \le m$, $f_{nj}(x) = f_j(V_0 x)$ with $m \le l_n$. Let V be a matrix whose entries are new variables v_{rs}, $1 \le r, s \le n$ and consider $\{F_{ij}\}_{1\le i\le n, 1\le j\le l_i} \subset \mathbb{R}[v, x]$ defined in the following way:

- Take $l'_n = m$ and, for $1 \le j \le l'_n$, let $F_{nj}(V, x) = f_j(Vx)$. Then, for $1 \le j_0 \le l'_n$, if $\deg_x F_{nj_0} = d_{nj_0}$, add the first $d_{nj_0} - 1$ derivatives of F_{nj_0} with respect to x_n to the list to obtain $\{F_{nj}\}_{1\le j\le l_n}$.
- From $\{F_{(i_0+1)j}\}_{1\le j\le l_{i_0+1}} \subset \mathbb{R}[v, x_1, \ldots, x_{i_0+1}]$, form $\{F_{i_0 j}\}_{1\le j\le l'_{i_0}} \subset \mathbb{R}[v, x_1, \ldots, x_{i_0}]$ by taking all possible resultants and subresultants with respect to the variable x_{i_0+1} between pairs of polynomials, not taking into account the ones that are identically zero. Then, for $1 \le j_0 \le l'_{i_0}$, if $\deg_x F_{i_0 j_0} = d_{i_0 j_0}$, add the first $d_{i_0 j_0} - 1$ derivatives of $F_{i_0 j_0}$ with respect to the variable x_{i_0} to obtain the family $\{F_{i_0 j}\}_{1\le j\le l_{i_0}}$.

Let $1 \le i \le n$ and $1 \le j \le l_i$. Let $d_{ij} := \deg_x F_{ij}$ and let $q_{ij} \in \mathbb{R}[v]$ be the coefficient of the monomial $x_i^{d_{ij}}$ in $F_{ij} \in \mathbb{R}[v][x]$. It can be shown inductively for $i = n, \ldots, 1$, that for every $1 \le j \le l'_i$ and $A \in \mathbb{Q}^{i\times i}$, $F_{ij}(V, Ax) = F_{ij}\big(V\left(\begin{smallmatrix} A & 0 \\ 0 & \mathrm{Id}_{n-i} \end{smallmatrix}\right), x\big)$, for every $l'_i + 1 \le j \le l_i$ and $B \in \mathbb{Q}^{(i-1)\times(i-1)}$, $F_{ij}\big(V, \left(\begin{smallmatrix} B & 0 \\ 0 & 1 \end{smallmatrix}\right)x\big) = F_{ij}\big(V\left(\begin{smallmatrix} B & 0 \\ 0 & Id_{n-i+1} \end{smallmatrix}\right), x\big)$, and (using these identities) that, for every $1 \le j \le l_i$, $q_{ij} \ne 0$.

Define $\mathcal{U} = \{V_0 \in \mathbb{C}^{n\times n} \mid q_{ij}(V_0) \ne 0 \text{ for } 1 \le i \le n, 1 \le j \le l_i\}$. By [9, Proposition 4.34 and Theorem 5.14], for every $V_0 \in \mathbb{Q}^{n\times n} \cap \mathcal{U}$, the set $\{f_{ij}(x)\}_{1\le i\le n, 1\le j\le l_i}$ defined by $f_{ij}(x) = F_{ij}(V_0, x)$ satisfies both conditions in Lemma 4. □

The following proposition is a major tool for our algorithms (cf. [36, Theorem 2]).

Proposition 5 *Let $f_1, \ldots, f_m$ be n-variate polynomials with real coefficients. After a generic change of variables, for every semialgebraic set $\mathcal{P}$ defined in $\mathbb{R}^n$ by a Boolean formula on $f_1, \ldots, f_m$ involving equalities and inequalities to zero, and every $p = (p_1, \ldots, p_n) \in \mathbb{R}^n$, if for $1 \le k \le n$, $\mathcal{P}(k, p)$ is the set of all the connected components of $\mathcal{P} \cap \{x_1 = p_1, \ldots, x_{k-1} = p_{k-1}\}$, then*

$$\{p\} \cup \left(\bigcup_{k=1}^{n} \bigcup_{C\in\mathcal{P}(k,p)} Z(C, k) \right)$$

is finite and intersects the closure of each connected component of $\mathcal{P}$.

Proof Proposition 3 ensures that this set is finite. Let $C_1 \in \mathcal{P}(1, p)$. If $\pi_1(C_1)$ is bounded from above or below, again Proposition 3 states that $Z(C_1, 1)$ is a finite non-empty set and is included in $\overline{C}_1$. Otherwise, $\pi_1(C_1) = \mathbb{R}$ and $C_1 \cap \{x_1 = p_1\} \neq \emptyset$. Let $C_2 \in \mathcal{P}(2, p)$ be a connected component of $C_1 \cap \{x_1 = p_1\}$. If $\pi_2(C_2)$ is bounded from above or below, $Z(C_2, 2) \neq \emptyset$ and is included in $\overline{C}_2 \subset \overline{C}_1$. Otherwise, $\pi_2(C_2) = \mathbb{R}$ and $C_1 \cap \{x_1 = p_1, x_2 = p_2\} \neq \emptyset$. Following this procedure, we obtain that either there exists $C_k \in \mathcal{P}(k, p)$ such that $Z(C_k, k) \neq \emptyset$ and is included in $\overline{C}_k \subset \overline{C}_1$ for some $1 \leq k \leq n$ or $p \in C_1$. □

The proof above leads to the recursive structure of our algorithm: For $2 \leq k \leq n$, we may think the kth variable as the first one for the polynomials $f_j(p_1, \ldots, p_{k-1}, x_k, \ldots, x_n)$ for $1 \leq j \leq m$. Therefore, it is enough to consider the problem of finding extremal points for the projection over the first coordinate of the closures of the connected components of a semialgebraic set.

3.2 Equations Defining Extremal Points

Let $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$ and let $S := \{i_1, \ldots, i_s\} \subset \{1, \ldots, m\}$. If $1 \leq s \leq n-1$, the implicit function theorem implies that a point z with maximum or minimum first coordinate in a connected component of $\{f_{i_1} = \cdots = f_{i_s} = 0\}$ satisfies

$$f_{i_1}(z) = \cdots = f_{i_s}(z) = 0, \quad \operatorname{rank} \begin{pmatrix} \frac{\partial f_{i_1}}{\partial x_2}(z) & \cdots & \frac{\partial f_{i_1}}{\partial x_n}(z) \\ \vdots & \ddots & \vdots \\ \frac{\partial f_{i_s}}{\partial x_2}(z) & \cdots & \frac{\partial f_{i_s}}{\partial x_n}(z) \end{pmatrix} < s. \tag{1}$$

This condition can be rewritten as

$$\begin{cases} f_{i_1}(z) = \cdots = f_{i_s}(z) = 0, \\ \sum_{j=1}^{s} \mu_j \overline{\nabla} f_{i_j}(z) = (0, \ldots, 0) \end{cases} \tag{2}$$

for $\mu_1, \ldots, \mu_s \in \mathbb{R}$ not simultaneously zero, where $\overline{\nabla} f_{i_j}(z)$ denotes the vector obtained by removing the first coordinate from the gradient $\nabla f_{i_j}(z)$.

When $s = 1$, for $z \in \mathbb{R}^n$, conditions (1) are equivalent to

$$f_{i_1}(z) = \frac{\partial f_{i_1}}{\partial x_2}(z) = \cdots = \frac{\partial f_{i_1}}{\partial x_n}(z) = 0. \tag{3}$$

When $s \geq n$, we will simply consider the conditions

$$f_{i_1}(z) = \cdots = f_{i_s}(z) = 0. \tag{4}$$

For every $2 \leq s \leq n-1$, as system (2) is homogeneous in the variables $\mu_1, \ldots, \mu_s$, we consider the variety $W_S \subset \mathbb{A}^n_{\mathbb{C}} \times \mathbb{P}^{s-1}_{\mathbb{C}}$ defined as the zero set of this system. If $s = 1$ or $s \geq n$, let W_S be the variety defined by systems (3) and (4) respectively.

The following result is an adaptation to our context of the Karush–Kuhn–Tucker conditions (see [31]) from non-linear optimization which generalize the Lagrange multipliers theorem in order to consider equality and inequality constraints.

Proposition 6 *Let* $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$ *and* $\sigma = (\sigma_1, \ldots, \sigma_m) \in \{\leq, <, =, >, \geq\}^m$. *Set* $E_\sigma = \{i \mid \sigma_i = \text{“}=\text{”}\}$. *Then, for every connected component* C *of the set* $\{x \in \mathbb{R}^n \mid f_1(x)\sigma_1 0, \ldots, f_m(x)\sigma_m 0\}$, *we have*

$$Z(C) \subset \bigcup_{\substack{S \neq \emptyset \\ E_\sigma \subset S \subset \{1,\ldots,m\}}} \pi_x(W_S).$$

Proof Without loss of generality, assume $E_\sigma = \{1, \ldots, l\}$ (or $E_\sigma = \emptyset$ and $l = 0$) and $\pi_1(C)$ is bounded from below. Let $z = (z_1, \ldots, z_n) \in Z_{\inf}(C)$ and $S_0 = \{i \in \{1, \ldots, m\} \mid f_i(z) = 0\}$. Note that $E_\sigma \subset S_0$ and, even when $l = 0$, $S_0 \neq \emptyset$; then, we may assume that $S_0 = \{1, \ldots, t\}$ with $\max\{1, l\} \leq t \leq m$. We will show that $z \in \pi_x(W_{S_0})$.

If $t \geq n$, we have $z \in \pi_x(W_{S_0})$ by the definition of this set.

Assume now that $t \leq n-1$. If $z \notin \pi_x(W_{S_0})$, the set $\{\overline{\nabla} f_i(z), i \in S_0\}$ is linearly independent. Let $f : \mathbb{R}^n \to \mathbb{R}^t$ be the map $f = (f_1, \ldots, f_t)$. We may assume that the minor corresponding to the variables $n-t+1, \ldots, n$ in the Jacobian matrix $Df(z)$ is not zero. Applying the inverse function theorem to $h(x) = (x_1 - z_1, \ldots, x_{n-t} - z_{n-t}, f_1(x), \ldots, f_t(x))$, there exist an open neighborhood U of z, $\varepsilon \in \mathbb{R}_{>0}$ and a map $g : (-\varepsilon, \varepsilon)^n \to U$ inverse to $h : U \to (-\varepsilon, \varepsilon)^n$. Moreover, we may assume that $f_{t+1}, \ldots, f_m$ have constant signs on U.

Let $w \in C \cap U$ and let $y = h(w)$. Let $\widetilde{\sigma} \in \{<, =, >\}^m$ be such that $f_i(w)\widetilde{\sigma}_i 0$ for $1 \leq i \leq m$. Then, the conditions $y_1 = w_1 - z_1 \geq 0$, $y_{n-t+1}\widetilde{\sigma}_1 0, \ldots, y_n \widetilde{\sigma}_t 0$ hold. Since $w \in C$, for $1 \leq i \leq m$, $\widetilde{\sigma}_i \in \{<, =\}$ if $\sigma_i = \text{“}\leq\text{”}$, $\widetilde{\sigma}_i \in \{>, =\}$ if $\sigma_i = \text{“}\geq\text{”}$ and $\widetilde{\sigma}_i = \sigma_i$ otherwise. Hence, every point satisfying $\widetilde{\sigma}$ also satisfies σ.

Let $\gamma : [-\varepsilon/2, y_1] \to (-\varepsilon, \varepsilon)^n$ be defined as $\gamma(u) = (u, y_2, \ldots, y_n)$. For $u \in [-\varepsilon/2, y_1]$ and $1 \leq i \leq t$, $f_i(g \circ \gamma(u)) = y_{n-t+i}\widetilde{\sigma}_i 0$. Taking into account that, for $t+1 \leq i \leq m$, f_i has constant sign over U and the image of $g \circ \gamma$ lies in U, we also have that $f_i(g \circ \gamma(u))\widetilde{\sigma}_i 0$ for $t+1 \leq i \leq m$. Therefore, the image of $g \circ \gamma$ is contained in the realization of σ and, since it is a connected curve with a point $g \circ \gamma(y_1) = w$ in the connected component C, we conclude that it is contained in C. Now, the first coordinate of $g \circ \gamma(-\varepsilon/2)$ is $-\varepsilon/2 + z_1 < z_1$, contradicting the fact that $z_1 = \inf \pi_1(C)$. □

3.3 Deformation Techniques for Bihomogeneous Systems

In this subsection, we present briefly a symbolic deformation introduced in [18–20, 26], and [38], adapted to the bihomogeneous setting following [24].

3.3.1 The Deformation

Given polynomials $h_1(x), \ldots, h_s(x), h_{s+1}(x, \mu), \ldots, h_r(x, \mu) \in \mathbb{K}[x_1, \ldots, x_n, \mu_1, \ldots, \mu_s]$, where $2 \leq s \leq n-1$ and $r = s + n - 1$ such that, for $1 \leq i \leq r$, $\deg_x(h_i) \leq d_i \leq d$ and, for $s+1 \leq i \leq r$, h_i is homogeneous of degree 1 in the variables μ, we consider the associated equation system:

$$h_1(x) = 0, \ldots, h_s(x) = 0, h_{s+1}(x, \mu) = 0, \ldots, h_r(x, \mu) = 0. \tag{5}$$

Let $W \subset \mathbb{A}^n \times \mathbb{P}^{s-1}$ be the variety this system defines. By the multihomogeneous Bézout theorem ([40, Chap. 4, Sect. 2.1]), the degree of W is bounded by

$$D := \left(\prod_{i=1}^{s} d_i\right)\left(\sum_{E\subset\{s+1,\dots,r\},\#E=n-s}\ \prod_{j\in E} d_j\right) \le \binom{n-1}{s-1} d^n. \tag{6}$$

Let $g_1(x), \dots, g_s(x), g_{s+1}(x,\mu), \dots, g_r(x,\mu) \in \mathbb{K}[x_1,\dots,x_n,\mu_1,\dots,\mu_s]$ be polynomials with $\deg_x(g_i) = d_i$ for $1 \le i \le r$ and homogeneous of degree 1 in the variables μ for $s+1 \le i \le r$, such that:

(H) $g_1, \dots, g_r$ define a 0-dimensional variety in $\mathbb{A}^n \times \{\mu_s \neq 0\} \subset \mathbb{A}^n \times \mathbb{P}^{s-1}$ with D points $s_1, \dots, s_D$ satisfying $\pi_x(s_i) \neq \pi_x(s_j)$ for $i \neq j$, and the Jacobian determinant of the polynomials obtained from $g_1, \dots, g_r$ by dehomogenizing them with $\mu_s = 1$ does not vanish at any of these points.

We will specify polynomial systems meeting these conditions in Definitions 12 and 19 below.

Let t be a new variable. For every $1 \le i \le r$, let

$$F_i := (1-t)h_i + t g_i. \tag{7}$$

Consider the variety $\hat{V} \subset \mathbb{A}^1 \times \mathbb{A}^n \times \mathbb{P}^{s-1}$ defined by $F_1, \dots, F_r$, and write

$$\hat{V} = V^{(0)} \cup V^{(1)} \cup V, \tag{8}$$

where $V^{(0)}$ is the union of the irreducible components of $\hat{V}$ contained in $\{t=0\}$, $V^{(1)}$ is the union of its irreducible components contained in $\{t=t_0\}$ for some $t_0 \in \mathbb{C}\setminus\{0\}$, and V is the union of the remaining irreducible components of $\hat{V}$.

Lemma 7 *With our previous assumptions and notation, $\pi_{x,\mu}(V \cap \{t=0\})$ is a finite subset of W containing all its isolated points.*

Proof Let V_1 be an irreducible component of V and $\overline{V}_1$ be its Zariski closure in $\mathbb{A}^1 \times \mathbb{P}^n \times \mathbb{P}^{s-1}$. The projection of $\overline{V}_1$ to $\mathbb{A}^1$ is onto and so, $\overline{V}_1 \cap \{t=1\} \neq \emptyset$. But our assumption on $g_1, \dots, g_r$ implies that $\overline{V}_1 \cap \{t=1\} = V_1 \cap \{t=1\}$; then, $V_1 \cap \{t=1\} \neq \emptyset$ and it is 0-dimensional. It follows that $\dim(V_1) = 1$. Therefore, V is a 1-equidimensional variety and thus $\pi_{x,\mu}(V \cap \{t=0\})$ is a finite set.

In order to prove the second part of the statement, note that $W = \pi_{x,\mu}(\hat{V} \cap \{t=0\}) = \pi_{x,\mu}(V^{(0)}) \cup \pi_{x,\mu}(V \cap \{t=0\})$. Now, an isolated point of W cannot belong to $\pi_{x,\mu}(V^{(0)})$, since the dimension of each of its irreducible components is at least 1; hence, it lies in $\pi_{x,\mu}(V \cap \{t=0\})$. □

The same deformation can be applied to a system $h_1(x), \dots, h_n(x) \in \mathbb{K}[x_1,\dots,x_n]$ with $g_1(x), \dots, g_n(x) \in \mathbb{K}[x_1,\dots,x_n]$ such that $\deg(g_i) = \deg(h_i)$ for every $1 \le i \le n$ and having $\prod_{i=1}^n \deg(g_i)$ common zeros in $\mathbb{A}^n$.

3.3.2 A Geometric Resolution

Lemma 8 *The variety defined in* $\mathbb{A}^n_{\overline{\mathbb{K}(t)}} \times \mathbb{P}^{s-1}_{\overline{\mathbb{K}(t)}}$ *by* $F_1, \ldots, F_r$ *as in* (7) *is* 0*-dimensional and has* D *points* $S_1, \ldots, S_D$ *in* $\{\mu_s \neq 0\}$ *such that* $\pi_x(S_i) \neq \pi_x(S_j)$ *for* $i \neq j$*. Moreover, these points can be considered as elements in* $\mathbb{K}[[t-1]]^r$*.*

Proof The multihomogeneous Bézout Theorem (see, for instance, [40, Chap. 4, Sect. 2.1]) states that the degree of the variety is bounded by D. If s_i, $1 \leq i \leq D$, are the common zeros of $g_1, \ldots, g_s, g_{s+1}, \ldots, g_r$, the Jacobian of $F_1, \ldots, F_r$ with respect to $x_1, \ldots, x_n, \mu_1, \ldots, \mu_{s-1}$ at $t = 1$ and $(x, \mu) = s_i$ is nonzero. The result follows applying the Newton–Hensel lifting (see, for example, [26, Lemma 3]). □

Consider now new variables $y_1, \ldots, y_n$ and define $\ell(x, \mu, y) = \ell(x, y) = \sum_{j=1}^n y_j x_j$. For $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, let $\ell_\alpha(x, \mu) = \ell_\alpha(x) = \sum_{j=1}^n \alpha_j x_j$. Let

$$P(t, U, y) = \prod_{i=1}^{D} \big(U - \ell(S_i, y)\big) = \frac{\sum_{h=0}^{D} p_h(t, y) U^h}{q(t)} = \frac{\hat{P}(t, U, y)}{q(t)} \in \mathbb{K}(t)[U, y], \tag{9}$$

with $\hat{P}(t, U, y) \in \mathbb{K}[t, U, y]$ with no factors in $\mathbb{K}[t] \setminus \mathbb{K}$.

In order to compute P, we will approximate its roots. The required precision is obtained from the following upper bound for the degree of its coefficients. A similar result in the general sparse setting appears in [27, Lemma 2.3], but to avoid a possibly cumbersome translation of our setting into sparse systems, we give an alternative statement and its proof here.

Lemma 9 *Using the notation in* (9), $\deg_t \hat{P}(t, U, y) \leq nD$.

Proof Let $\Phi : V \times \mathbb{A}^n \to \mathbb{A}^{n+2}$ be the morphism defined by $\Phi(t, x, \mu, y) = (t, \ell(x, y), y)$. It is easy to see that $\hat{P}(t, U, y)$ is a square-free polynomial defining $\overline{\operatorname{Im} \Phi}$.

For a generic $\beta = (\beta_0, \beta_1, \ldots, \beta_n) \in \mathbb{C}^{n+1}$, the polynomial $\hat{P}_\beta(t) = \hat{P}(t, \beta_0, \beta_1, \ldots, \beta_n)$ is square-free and satisfies $\deg_t \hat{P}(t, U, y) = \deg_t \hat{P}_\beta(t)$; moreover, this degree equals the number of isolated roots of the system

$$F_1(t, x) = 0, \ldots, F_s(t, x) = 0, F_{s+1}(t, x, \mu) = 0, \ldots, F_r(t, x, \mu) = 0,$$
$$\ell_{(\beta_1, \ldots, \beta_n)}(x) - \beta_0 = 0.$$

Using the multihomogeneous Bézout theorem in the three groups of variables x, μ and t, it can be seen easily that this system has at most nD isolated roots. □

Note that, if $\pi_x(V \cap \{t = 0\}) = \{z_1, \ldots, z_\nu\} \subset \mathbb{A}^n$, we have the factorization $\hat{P}(0, U, y) = \prod_{j=1}^a q_j(U, y)^{\delta_j}$ in $\mathbb{C}[U, y]$, where $q_l = U - \ell(z_l, y)$ for every $1 \leq l \leq \nu \leq a$. Let $Q(U, y) = \prod_{j=1}^a q_j^{\delta_j - 1}$.

For a generic $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{C}^n$, $\frac{\hat{P}(0, U, \alpha)}{Q(U, \alpha)}$ is square-free and vanishes at $\ell(z_l, \alpha)$ for $1 \leq l \leq \nu$. In addition, for $1 \leq l \leq \nu$, the kth coordinate of z_l $(1 \leq k \leq n)$

is the quotient of $-\frac{\frac{\partial \hat{P}}{\partial y_k}(0,\ell(z_l,\alpha),\alpha)}{Q(\ell(z_l,\alpha),\alpha)} = \delta_l(z_l)_k \prod_{j\neq l} q_j(\ell(z_l,\alpha),\alpha)$ by $\frac{\frac{\partial \hat{P}}{\partial U}(0,\ell(z_l,\alpha),\alpha)}{Q(\ell(z_l,\alpha),\alpha)} = \delta_l \prod_{j\neq l} q_j(\ell(z_l,\alpha),\alpha) \neq 0$. Then:

Proposition 10 *Let $\hat{P}(t,U,y)$ be as in (9). Then, for a generic $\alpha \in \mathbb{C}^n$,*

$$\left\{ \frac{\hat{P}(0,U,\alpha)}{Q(U,\alpha)}; \frac{\frac{\partial \hat{P}}{\partial U}(0,U,\alpha)}{Q(U,\alpha)}; -\frac{\frac{\partial \hat{P}}{\partial y_1}(0,U,\alpha)}{Q(U,\alpha)}, \ldots, -\frac{\frac{\partial \hat{P}}{\partial y_n}(0,U,\alpha)}{Q(U,\alpha)} \right\}$$

is a geometric resolution of a finite set containing $\pi_x(V \cap \{t=0\})$.

4 Regular Intersections

Let $f_1,\ldots,f_m \in \mathbb{R}[x_1,\ldots,x_n]$. As in Sect. 3.2, for $S=\{i_1,\ldots,i_s\} \subset \{1,\ldots,m\}$, consider the solution set W_S of the system (2), (3) or (4) depending on whether $2 \leq s \leq n-1$, $s=1$ or $s \geq n$, respectively. We will deal with the deformation (7) and the corresponding varieties (8) defined from the systems (2), (3) and (4) for $S \subset \{1,\ldots,m\}$ with $1 \leq \#S \leq n$, and an adequate initial system. We will add a subscript S in the notation $\hat{V}$, $V^{(0)}$, $V^{(1)}$ and V to indicate that the varieties are defined from the polynomial system associated with S.

Note that, under Assumption 1, W_S is the empty set whenever $s > n$. Moreover:

Lemma 11 *Under Assumption 1, after a generic linear change of variables, for every $S \subset \{1,\ldots,m\}$ with $1 \leq \#S \leq n$, the set W_S is finite and equals $\pi_{x,\mu}(V_S \cap \{t=0\})$.*

Proof If $s=n$, Assumption 1 implies that W_S is a finite set.

Now let $s \leq n-1$. Note that $\pi_x(W_S)$ is the set of critical points of the map $(x_1,\ldots,x_n) \mapsto x_1$ over the set $\{x \in \mathbb{C}^n \mid f_i(x)=0 \text{ for } i \in S\}$. By the arguments in [42, Sect. 2.1] based on Sard's theorem and a holomorphic Morse lemma, it follows that a generic linear form has a finite number of critical points on this complex variety. Therefore, taking any of these generic linear forms as the first coordinate, the set $\pi_x(W_S)$ turns to be finite. Moreover, for every $z \in \pi_x(W_S)$, since $\{\nabla f_i(z),\ i \in S\}$ is linearly independent and $\{\overline{\nabla} f_i(z),\ i \in S\}$ is linearly dependent, it follows that there is a unique $\mu \in \mathbb{P}^{s-1}$ such that $(z,\mu) \in W_S$.

The equality $W_S = \pi_{x,\mu}(V_S \cap \{t=0\})$ follows from Lemma 7. □

4.1 Symbolic Deformation Algorithms

First we introduce the initial systems for our first algorithmic deformation procedure.

Definition 12 For a given s with $1 < s < n$ and $r := s+n-1$, a *type* 1 *initial system* is a polynomial system of the form:

$$\begin{cases} g_i(x) = \prod_{1\leq j\leq d_i}(x_i - j) & \text{for } 1 \leq i \leq s, \\ g_i(x,\mu) = (\prod_{1\leq j\leq d_i} \phi_{ij}(x))\psi_i(\mu) & \text{for } s+1 \leq i \leq r, \end{cases}$$

where, for $s+1 \le i \le r$,

$$\phi_{ij}(x) = \left(\sum_{s+1 \le k \le n} \frac{1}{(i-s-1)d + j - 1 + k - s} x_k \right) + \frac{1}{(i-s-1)d + j - 1 + n + 1 - s} \quad (1 \le j \le d_i),$$

and

$$\psi_i(\mu) = \sum_{1 \le k \le s} \frac{1}{i - s - 1 + k} \mu_k.$$

For $s = 1$ and $s = n$, a type 1 initial system consists of n polynomials of the form $g_i(x) = \prod_{1 \le j \le d_i} (x_i - j)$ $(1 \le i \le n)$.

Using basic properties of Cauchy matrices, it follows that the solutions of the system introduced above are the D points obtained by combining each of the solutions of the first s equations with the solutions of the linear systems associated to all possible $\psi_{i_1}, \ldots, \psi_{i_{s-1}}, \phi_{i_s j_s}, \ldots, \phi_{i_{n-1} j_{n-1}}$ with $\{i_1, \ldots, i_{n-1}\} = \{s+1, \ldots, r\}$, and that all these points have different π_x-projections. Moreover, the Jacobian matrix of the system at each of these solutions is invertible, since it is the product of a diagonal matrix with nonzero entries with a block diagonal matrix whose blocks are an identity matrix and two Cauchy matrices. We conclude that Property (H) (see Sect. 3.3.1) holds for any type 1 initial system.

Now, we describe a probabilistic algorithm which computes a geometric resolution as in Proposition 10.

Proposition 13 *There is a probabilistic algorithm that, taking as input polynomials $h_1, \ldots, h_r$ in $\mathbb{K}[x_1, \ldots, x_n, \mu_1, \ldots, \mu_s]$ as in (5) encoded by an slp of length L, obtains a geometric resolution of a finite set containing $\pi_x(V \cap \{t = 0\})$ for a deformation defined from a type 1 initial system within complexity $O(n^2 D^2 \log(D) \log\log(D)(L + \log^2(D) \log\log(D)))$.*

Proof The procedure of this algorithm is standard. The main difference with previous known algorithms solving this task (see, for example, [20] or [26]) is that the Newton lifting is done pointwise.

First step: Form a type 1 initial system of polynomials of the same degree structure as $h_1, \ldots, h_r$ and compute the solutions $s_1, \ldots, s_D$ of this system. The computation of each solution amounts to solving two square linear systems of size $n - s$ and $s - 1$, respectively, with Cauchy matrices, which can be done within a complexity $O(n \log^2(n))$ by means of [12, Chap. 2, Algorithm 4.2]).

Second step: Construct an slp encoding $F_1, \ldots, F_r$ (see (7)). Since $g_1, \ldots, g_r$ can be encoded by an slp of length $O(dn^2)$, the length of this slp can be taken to be $L_1 = L + O(dn^2)$. Set F for the list of polynomials $F_1, \ldots, F_r$ dehomogenized with $\mu_s = 1$. The algorithm computes, for $i = 1, \ldots, D$, elements $\tilde{S}_i \in \mathbb{K}[t]^r$ such that for $1 \le k \le r$, $(\tilde{S}_i - S_i)_k \in (t-1)^{2nD+1} \mathbb{K}[[t-1]]$. Let $\tilde{S}_i^{(0)} = s_i$ be a solution of the initial system $g_1, \ldots, g_r$. By means of the Newton–Hensel operator we define recursively

$\tilde{S}_i^{(m+1)} = \tilde{S}_i^{(m)} - DF^{-1}(\tilde{S}_i^{(m)})F(\tilde{S}_i^{(m)}) \mod (t-1)^{2^{m+1}}\mathbb{K}[[t-1]]$. For $1 \le k \le r$ and $m \in \mathbb{N}_0$, $(\tilde{S}_i^{(m+1)})_k \equiv (\tilde{S}_i^{(m)})_k \mod (t-1)^{2^m}\mathbb{K}[[t-1]]$, and $(\tilde{S}_i^{(m)})_k$ is a polynomial in $t-1$ of degree less than 2^m. Since operations between polynomials of such degree can be done using $O(2^m m\log(m))$ operations in $\mathbb{K}$, the computation of $\tilde{S}_i^{(m+1)}$ from $\tilde{S}_i^{(m)}$ can be done within $O((nL_1+n^3)2^m m\log(m))$ operations. Therefore, the complexity of computing $\tilde{S}_i := \tilde{S}_i^{(\delta)}$ from s_i for $\delta = \lceil \log(2nD+1)\rceil$, for every $1 \le i \le D$, is $O(n(nL_1+n^3)D^2\log(D)\log\log(D))$.

Third step: This step consists in the computation of $\hat{P}(0,U,\alpha) = \sum_{h=0}^{D} p_h(0,\alpha)U^h$ and $\frac{\partial \hat{P}}{\partial y_k}(0,U,\alpha) = \sum_{h=0}^{D} \frac{\partial p_h}{\partial y_k}(0,\alpha)U^h$ for a generic $\alpha = (\alpha_1,\ldots,\alpha_n) \in \mathbb{Q}^n$. We have that $p_h(t,\alpha)/q(t)$ and $\frac{\partial p_h}{\partial y_k}(t,\alpha)/q(t)$ are the coefficients corresponding to U^h and $U^h(y_k-\alpha_k)$ $(1 \le k \le n,\ 0 \le h \le D)$, respectively, in the expansion of $P(t,U,y) = \sum_{h=0}^{D} \frac{p_h(t,y)}{q(t)}U^h \in \mathbb{K}[[t-1]][U, y-\alpha]$. As the degrees of the polynomials involved in these fractions are bounded by nD (see Lemma 9), they are uniquely determined by their power series expansions modulo $(t-1)^{2nD+1}\mathbb{K}[[t-1]]$ (see [44, Corollary 5.21]).

The algorithm proceeds as follows: First, it computes the coefficients of U^h and $U^h(y_k-\alpha_k)$ $(1 \le k \le n,\ 0 \le h \le D)$ in $\tilde{P}(t,U,y) = \prod_{i=1}^{D}(U - \ell(\tilde{S}_i, y)) \in \mathbb{K}[t][U,y]$ following [44, Algorithm 10.3] in $O(n^2D^2\log^3(D)\log\log^2(D))$ operations over $\mathbb{K}$. From these coefficients, $p_h(t,\alpha)$ and $\frac{\partial p_h}{\partial y_k}(t,\alpha)$ $(1 \le k \le n,\ 0 \le h \le D)$, and $q(t)$ are obtained within complexity $O(n^2D^2\log^2(D)\log\log(D))$ over $\mathbb{K}$ by using [44, Corollary 5.24 and Algorithm 11.4] and converting all rational fractions to a common denominator. Finally, the algorithm substitutes $t=0$ in these polynomials to obtain $\hat{P}(0,U,\alpha)$ and $\frac{\partial \hat{P}}{\partial y_k}(0,U,\alpha)$ for $1 \le k \le n$.

Fourth step: The algorithm computes $Q(U,\alpha) = \gcd(\hat{P}(0,U,\alpha), \frac{\partial \hat{P}}{\partial U}(0,U,\alpha))$ within complexity $O(D\log^2(D)\log\log(D))$ and makes the required exact divisions by $Q(U,\alpha)$ leading to the geometric resolution. This last step does not change the overall order of complexity, which is $O(n^2D^2\log(D)\log\log(D)(L+n^2d+\log^2(D)\log\log(D)))$. □

The algorithm underlying the proof of Proposition 13 can be adapted straightforwardly to handle the cases $s=1$ and $s=n$ within the same complexity bounds.

4.2 Main Algorithm

The main algorithm of this section is the following:

Algorithm 14

Input: Polynomials $f_1,\ldots,f_m \in \mathbb{K}[x_1,\ldots,x_n]$ satisfying Assumption 1 encoded by an slp of length L, and positive integers $d_1,\ldots,d_m$ such that $\deg f_i \le d_i$ for $1 \le i \le m$.

Output: A finite set $\mathcal{M} \subset \mathbb{A}^n$ intersecting the closure of each connected component of the realization of every feasible sign condition over $f_1,\ldots,f_m$ encoded by a list $\mathcal{G}$ of geometric resolutions of 0-dimensional varieties.

Procedure:

1. Make a random linear change of variables with coefficients in $\mathbb{Q}$.
2. Take a point $p = (p_1, \ldots, p_n) \in \mathbb{Q}^n$ at random.
3. Starting with $\mathcal{G} := \emptyset$, for $k = 1, \ldots, n-1$ and for every $S \subset \{1, \ldots, m\}$ with $1 \leq \#S \leq n-k+1$:
   (a) Obtain an slp encoding the polynomials which define the variety $W_{k,S}$ associated with the polynomials $f_1(p_1, \ldots, p_{k-1}, x_k, \ldots, x_n), \ldots, f_m(p_1, \ldots, p_{k-1}, x_k, \ldots, x_n)$ and the projection to the kth coordinate x_k.
   (b) Compute a geometric resolution $\{q^{(k,S)}(U), v_k^{(k,S)}(U), \ldots, v_n^{(k,S)}(U)\} \subset \mathbb{K}[U]$ of a finite set containing $\pi_x(W_{k,S}) = \pi_x(V_{k,S} \cap \{t = 0\}) \subset \mathbb{A}^{n-k+1}$ by means of a deformation from a type 1 initial system, and add the geometric resolution
   $$\left\{q^{(k,S)}(U), p_1, \ldots, p_{k-1}, v_k^{(k,S)}(U), \ldots, v_n^{(k,S)}(U)\right\}$$
   to the list $\mathcal{G}$.
4. Add to the list $\mathcal{G}$ the geometric resolutions $\{f_i(p_1, \ldots, p_{n-1}, U), p_1, \ldots, p_{n-1}, U\}$, for $1 \leq i \leq m$, and $\{U, p_1, \ldots, p_n\}$.

We point out that under Assumption 1, by Lemma 11, Step 3(b) of the previous algorithm could be achieved by any subroutine solving zero-dimensional polynomial systems. However, we use the deformation procedure we designed for the particular systems under consideration in order to obtain the complexity bounds stated in Theorem 2. The first part of this theorem is proved in the following:

Theorem 15 *Algorithm 14 is a probabilistic procedure that, from a family of polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ satisfying Assumption 1, obtains a finite set $\mathcal{M}$ intersecting the closure of each connected component of the realization of every sign condition over $f_1, \ldots, f_m$. If the input polynomials have degrees bounded by $d \geq 2$ and are encoded by an slp of length L, the algorithm performs $O\big(\big(\sum_{s=1}^{\min\{m,n\}} \binom{m}{s}\binom{n-1}{s-1}^2\big) d^{2n} n^4 \log(d)\ (\log(n) + \log\log(d))(L + n^2 + n\log^2(d)(\log(n) + \log\log(d)))\big)$ operations in $\mathbb{K}$.*

Proof Assuming that the random linear change of variables made in the first step of the algorithm is generic in the sense of Proposition 3, by Proposition 5, it suffices to show that

$$\{p\} \cup \left(\bigcup_{k=1}^{n} \bigcup_{C \in \mathcal{C}(k,p)} Z(C, k)\right) \subset \mathcal{M}$$

where $\mathcal{C}(k, p)$ denotes the set of all the connected components of the $\mathbb{R}^n$-subsets $\Gamma \cap \{x_1 = p_1, \ldots, x_{k-1} = p_{k-1}\}$ with Γ a connected component of a feasible sign condition over $f_1, \ldots, f_m$.

Note that for a generic point $p = (p_1, \ldots, p_n) \in \mathbb{K}^n$, for every $2 \leq k \leq n$, Assumption 1 also holds for the polynomials $f_i(p_1, \ldots, p_{k-1}, x_k, \ldots, x_n)$, $1 \leq i \leq n$. Thus, by taking p at random, we may assume that the assumption is met at each step of the recursion.

Then, for every $1 \leq k \leq n-1$, by Proposition 6 and Lemma 11, we have that

$$\bigcup_{C \in \mathcal{C}(k,p)} Z(C,k) \subset \bigcup_{\substack{S \subset \{1,\ldots,m\} \\ 1 \leq \#S \leq n-k+1}} \{p_1, \ldots, p_{k-1}\} \times \pi_x\big(V_{k,S} \cap \{t=0\}\big),$$

and Step 3 of the algorithm computes geometric resolutions for finite sets containing those in the right-hand side union; therefore, $\bigcup_{C \in \mathcal{C}(k,p)} Z(C,k) \subset \mathcal{M}$. Finally, note that $\bigcup_{C \in \mathcal{C}(n,p)} Z(C,n) \subset \bigcup_{i=1}^{m} \{f_i(p_1, \ldots, p_{n-1}, x_n) = 0\}$, which along with the point p, is added to the set $\mathcal{M}$ in Step 4 of the algorithm. This proves the correctness of Algorithm 14.

For every $1 \leq k \leq n-1$ and each $S \subset \{1, \ldots, m\}$ of cardinality at most $n-k+1$, the slp encoding the polynomials which define the variety $W_{k,S}$ computed at Step 2 of the algorithm can be taken of length $O(nL + n^3)$. Moreover, the number of points in $V_{k,S} \cap \{t=0\}$ is bounded by $\binom{n-k}{s-1} d^{n-k+1}$. Therefore, the result follows using the complexity estimate in Proposition 13. □

Now we will show how to get the entire list of feasible sign conditions over the polynomials $f_1, \ldots, f_m$ satisfying Assumption 1 using the output of Algorithm 14. The procedure relies on the following:

Proposition 16 *Let $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ be polynomials satisfying Assumption 1 and let $\mathcal{M}$ be a finite set such that $\mathcal{M} \cap \overline{C} \neq \emptyset$ for every connected component C of the realization of each feasible sign condition over $f_1, \ldots, f_m$. Then, the set of all feasible sign conditions over $f_1, \ldots, f_m$ is $\bigcup_{\sigma \in \mathcal{L}(\mathcal{M})} P_\sigma$ where $\mathcal{L}(\mathcal{M})$ is the set of all sign conditions satisfied by the elements of $\mathcal{M}$ and P_σ denotes the subset of $\{<, =, >\}^m$ consisting of all the elements that can be obtained from σ by replacing some of its "=" coordinates with "<" or ">".*

Proof Let $\hat{\sigma}$ be a feasible sign condition and C a connected component of $\{x \in \mathbb{R}^n \mid f_1(x)\hat{\sigma}_1 0, \ldots, f_m(x)\hat{\sigma}_m 0\}$. Consider a point $z \in \mathcal{M} \cap \overline{C}$ and let $\sigma \in \mathcal{L}(\mathcal{M})$ be the sign condition over $f_1, \ldots, f_m$ at z. By continuity, it follows that $\hat{\sigma} \in P_\sigma$.

Now, let $\sigma \in \mathcal{L}(\mathcal{M})$ and $z \in \mathcal{M}$ such that $f_i(z)\sigma_i 0$ for $1 \leq i \leq m$. Without loss of generality, assume $\sigma = (=, \ldots, =, >, \ldots, >)$ with t "=" and $m-t$ ">". If $t=0$, $P_\sigma = \{\sigma\}$. Suppose now $t > 0$, and let $\hat{\sigma} \in P_\sigma$. We may assume $\hat{\sigma} = (=, \ldots, =, >, \ldots, >)$ with l "=", where $0 \leq l \leq t$. Since the vectors $\nabla f_1(z), \ldots, \nabla f_t(z)$ are linearly independent, there exists $v \in \mathbb{R}^n$ such that $\langle \nabla f_i(z), v \rangle = 0$ for $1 \leq i \leq l$ and $\langle \nabla f_i(z), v \rangle > 0$ for $l+1 \leq i \leq t$. Consider a $\mathcal{C}^\infty$ curve $\gamma : [-1,1] \to \{f_1 = \cdots = f_l = 0\}$ such that $\gamma(0) = z$ and $\gamma'(0) = v$. For $l+1 \leq i \leq t$, $f_i \circ \gamma(0) = 0$ and $(f_i \circ \gamma)'(0) = \langle \nabla f_i(z), v \rangle > 0$; therefore, for a sufficiently small $u > 0$, $f_i \circ \gamma(u) > 0$ holds. In addition, for $1 \leq i \leq l$, $f_i \circ \gamma(u) = 0$ for every $u \in [-1,1]$. Finally, for $t+1 \leq i \leq m$, as $f_i \circ \gamma(0) > 0$, we have $f_i \circ \gamma(u) > 0$ for a sufficiently small u. We conclude that $\hat{\sigma}$ is feasible. □

Given a geometric resolution $\{q(U), v_1(U), \ldots, v_n(U)\} \subset \mathbb{K}[U]$ consisting of polynomials of degree bounded by δ, if $f_1, \ldots, f_m$ are encoded by an slp of length L, it is possible to obtain the signs they have at the points represented by the geometric resolution within complexity $O(L\delta \log(\delta) \log\log(\delta) + m\delta^\omega)$ (here $\omega \leq 2.376$ is a

positive real number such that for any field k it is possible to invert matrices in $k^{r\times r}$ with $O(r^\omega)$ operations, see [17]): first, for $1\le i\le m$, compute $f_i(v_1(U),\dots,v_n(U))$ mod $q(U)$ within complexity $O(L\delta\log(\delta)\log\log(\delta))$ ([44, Chap. 8]) and then, evaluate the signs of these polynomials at the roots of q by using the procedure described in [15, Sect. 3] within complexity $O(m\delta^\omega)$. Thus, we have:

Theorem 17 *There is a probabilistic algorithm that, given polynomials $f_1,\dots,f_m\in\mathbb{K}[x_1,\dots,x_n]$ of degrees bounded by $d\ge 2$ satisfying Assumption 1 and encoded by an slp of length L, computes the list of all feasible sign conditions over these polynomials within complexity $O\big(\sum_{s=1}^{\min\{m,n\}}\binom{m}{s}\big((L+n^2d)\binom{n-1}{s-1}^2 d^{2n}n^4\log(d)(\log(n)+\log\log(d))+md^{\omega n}\binom{n-1}{s-1}^\omega\big)\big)$.*

Our algorithms and complexity results can be refined if we are interested in a particular sign condition σ over $f_1,\dots,f_m$:

Remark 18 Let $\sigma\in\{<,=,>\}^m$ and $E_\sigma=\{i\mid\sigma_i=\text{“}=\text{”}\}$. Due to Proposition 6, in the third step of Algorithm 14 it suffices to consider those sets $S\subset\{1,\dots,m\}$ such that $E_\sigma\subset S$. Then, if $\#E_\sigma=l$, in the complexities of Theorems 15 and 17, the sum can be taken over $l\le s\le\min\{m,n\}$ and the combinatorial factor $\binom{m}{s}$ can be replaced by $\binom{m-l}{s-l}$.

5 Closed Sign Conditions Over Arbitrary Polynomials

In the case of arbitrary polynomials, the sets W_S may not be finite. To overcome this problem, we will consider the same kind of deformations as in the previous section but with different initial systems whose particular properties enable us to recover extremal points. This approach is similar to the one in [7].

5.1 Initial Systems for Deformations

Let d be an even positive integer and T the Tchebychev polynomial of degree d.

Definition 19 For a given $s\in\mathbb{N}$ with $1<s<n$ and $r:=s+n-1$, a *type* 2 *initial system* is a polynomial system of the form:

$$\begin{cases} g_i(x)=\tau_i(n+A_{i(n+1)}+\sum_{1\le k\le n}A_{ik}T(x_k)) & \text{for } 1\le i\le s,\\ g_i(x,\mu)=\sum_{1\le j\le s}\mu_j\frac{\partial g_j}{\partial x_{i-s+1}}(x) & \text{for } s+1\le i\le r,\end{cases}$$

where $\tau_i\in\{+,-\}$ for $1\le i\le s$, and $A\in\mathbb{Q}^{s\times(n+1)}$ is the Cauchy matrix defined as $A_{ik}=\frac{1}{a_i+k}$ for $1\le i\le s$, $1\le k\le n+1$, with $0\le a_1<\cdots<a_s$ integers such that a_s+n+1 is a prime number.

For $s=1$, a *type* 2 *initial system* consists of a polynomial $g_1(x)$ as above and its partial derivatives $\frac{\partial g_1(x)}{\partial x_2},\dots,\frac{\partial g_1(x)}{\partial x_n}$. Finally, for $s=n$, a *type* 2 *initial system* consists of n polynomials $g_1,\dots,g_n$ constructed as above from the Cauchy matrix $A\in\mathbb{Q}^{n\times(n+1)}$.

Note that if $\tau_i = \text{“}+\text{”}$, then $g_i(x) > 0$ for every $x \in \mathbb{R}^n$ and, if $\tau_i = \text{“}-\text{”}$, then $g_i(x) < 0$ for every $x \in \mathbb{R}^n$. Moreover, for $s+1 \le i \le r$,

$$g_i(x,\mu) = T'(x_{i-s+1})\left(\sum_{1\le j\le s} \tau_j A_{j(i-s+1)}\mu_j\right). \tag{10}$$

The Bézout number of a type 2 initial system is $D = \binom{n-1}{s-1}d^s(d-1)^{n-s} \le \binom{n-1}{s-1}d^n$.

Lemma 20 *Property* (H) (*see Sect.* 3.3.1) *holds for any type* 2 *initial system.*

Proof Assume $1 < s < n$. For $s+1 \le i \le r$, let $\bar{g}_i(x,\mu_1,\dots,\mu_{s-1}) = g_i(x,\mu_1,\dots,\mu_{s-1},1)$.

Let $B \subset \{2,\dots,n\}$ be a set with $n-s$ elements, let $e : B \to \{-1,1\}$ and suppose $e(k) = 1$ for a elements in B. Let $S_{B,e}$ be the set of solutions $(\bar{x},\bar{\mu})$ of the system

$$g_1(x) = \cdots = g_s(x) = \bar{g}_{s+1}(x,\mu) = \bar{g}_r(x,\mu) = 0 \tag{11}$$

which also satisfy

$$T'(x_k) = 0 \quad \text{and} \quad T(x_k) = e(k) \quad \text{for every } k \in B. \tag{12}$$

Since $\gcd(T', T+1) = T_{d/2}$ and $\gcd(T', T-1) = T'/T_{d/2}$ (where $T_{d/2}$ is the Tchebychev polynomial of degree $d/2$), the number of $(n-s)$-tuples satisfying (12) is $(d/2)^{n-s-a}(d/2-1)^a$. By using the explicit formula for the determinant of a Cauchy matrix and properties of Tchebychev polynomials, it can be seen that each of these $(n-s)$-tuples can be extended to a solution $(\bar{x},\bar{\mu})$ of (11) in d^s different ways. Then, $S_{B,e}$ has $(d/2)^{n-s-a}(d/2-1)^a d^s$ elements.

As for $(\bar{x},\bar{\mu}) \in S_{B,e}$, $T(\bar{x}_k) = e(k) = \pm 1$ for every $k \in B$, the sets $S_{B,e}$ are mutually disjoint. Then, if $(\bar{x}^{(1)},\bar{\mu}^{(1)})$, $(\bar{x}^{(2)},\bar{\mu}^{(2)})$ are two different solutions of (11), $\bar{x}^{(1)} \ne \bar{x}^{(2)}$. By taking into account every $B \subset \{2,\dots,n\}$, every a $(0 \le a \le n-s)$ and every function $e : B \to \{-1,1\}$ whose value is 1 at exactly a elements in B, we find $\binom{n-1}{n-s}\sum_{0\le a\le n-s}\binom{n-s}{a}(\frac{d}{2})^{n-s-a}(\frac{d}{2}-1)^a d^s = \binom{n-1}{n-s}(d-1)^{n-s}d^s$ solutions of (11).

Consider now the Jacobian matrix of this system evaluated at each of these solutions and suppose, without loss of generality, that the solution $(\bar{x},\bar{\mu})$ considered corresponds to $B = \{s+1,\dots,n\}$. Then, this matrix is of the form

$$\begin{array}{r} s \\ s-1 \\ n-s \end{array}\!\!\left\{\begin{array}{c|c|c} C_1 & 0 & 0 \\ \hline * & 0 & C_2 \\ \hline * & C_3 & * \end{array}\right.$$
$$\underbrace{}_{s}\ \underbrace{}_{n-s}\ \underbrace{}_{s-1}$$

with C_1, C_2 and C_3 invertible matrices.

For $s = 1$ and $s = n$, the proof is similar. □

5.2 Geometric Properties

Let $f_1, \ldots, f_m \in \mathbb{R}[x_1, \ldots, x_n]$ and let $S := \{i_1, \ldots, i_s\} \subset \{1, \ldots, m\}$ with $1 < s < n$. As explained in Sect. 3.2, for every point $z \in \mathbb{R}^n$ with maximum or minimum first coordinate over the set $\{x \in \mathbb{R}^n \mid f_{i_1}(x) = 0, \ldots, f_{i_s}(x) = 0\}$, there exists a nonzero vector $\mu = (\mu_1, \ldots, \mu_s)$ such that (z, μ) is a solution of the system

$$\begin{cases} f_{i_1}(z) = \cdots = f_{i_s}(z) = 0, \\ \sum_{1 \le j \le s} \mu_j \frac{\partial f_{i_j}}{\partial x_2}(z) = \cdots = \sum_{1 \le j \le s} \mu_j \frac{\partial f_{i_j}}{\partial x_n}(z) = 0. \end{cases} \tag{13}$$

Now, a homotopic deformation of this system by means of a type 2 initial system is as follows: for every $1 \le k \le s$, $F_k(t, x) = (1 - t) f_{i_k} + t g_k(x)$, and, for every $s + 1 \le k \le r$,

$$\begin{aligned} F_k(t, x, \mu) &= (1 - t) \sum_{1 \le j \le s} \mu_j \frac{\partial f_{i_j}}{\partial x_{k-s+1}}(x) + t \sum_{1 \le j \le s} \mu_j \frac{\partial g_j}{\partial x_{k-s+1}}(x) \\ &= \sum_{1 \le j \le s} \mu_j \frac{\partial F_j}{\partial x_{k-s+1}}(t, x). \end{aligned}$$

Thus, for any $t_0 \in \mathbb{R}$ and every $x_0 \in \mathbb{R}^n$ at which the first coordinate function attains a local maximum or minimum over the set $\{x \in \mathbb{R}^n \mid F_1(t_0, x) = \cdots = F_s(t_0, x) = 0\}$, by the implicit function theorem, there is a nonzero vector $\mu_0 \in \mathbb{R}^s$ such that $F_1(t_0, x_0) = \cdots = F_s(t_0, x_0) = F_{s+1}(t_0, x_0, \mu_0) = \cdots = F_s(t_0, x_0, \mu_0) = 0$.

In the sequel, we will consider deformations by means of specific type 2 initial systems.

Let $d \in \mathbb{N}$ be an even positive integer with $d \ge \deg f_i$ for every $1 \le i \le m$. Let $q_1 < \cdots < q_m$ be the first m prime numbers greater than n. For $1 \le i \le m$, let

$$g_i^+(x) = n + \frac{1}{q_i} + \sum_{1 \le k \le n} \frac{1}{q_i - n - 1 + k} T(x_k) \quad \text{and} \quad g_i^-(x) = -g_i^+(x).$$

Note that for each $S = \{i_1, \ldots, i_s\} \subset \{1, \ldots, m\}$ with $1 \le s \le n$ and every list $\tau_1, \ldots, \tau_s$ of $+$ and $-$ signs, the polynomials $g_{i_1}^{\tau_1}, \ldots, g_{i_s}^{\tau_s}$ form a type 2 initial system with $a_j = q_{i_j} - n - 1$ for $1 \le j \le s$ (see Definition 19). In addition, for $1 \le i \le m$, we denote

$$F_i^+(t, x) = (1 - t) f_i(x) + t g_i^+(x) \quad \text{and} \quad F_i^-(t, x) = (1 - t) f_i(x) + t g_i^-(x).$$

Lemma 21 *Let $S = \{i_1, \ldots, i_s\} \subset \{1, \ldots, m\}$ with $s > n$ and $\tau_1, \ldots, \tau_s$ a list of $+$ and $-$ signs. Then, the set $\{t \in \mathbb{C} \mid \exists x \in \mathbb{C}^n$ with $F_{i_1}^{\tau_1}(t, x) = \cdots = F_{i_s}^{\tau_s}(t, x) = 0\}$ is finite (possibly empty).*

Proof Denote by $\hat{F}_{i_1}^{\tau_1}, \ldots, \hat{F}_{i_s}^{\tau_s}, \hat{g}_{i_1}^{\tau_1}, \ldots, \hat{g}_{i_s}^{\tau_s}$ the polynomials obtained by homogenizing $F_{i_1}^{\tau_1}, \ldots, F_{i_s}^{\tau_s}$ and $g_{i_1}^{\tau_1}, \ldots, g_{i_s}^{\tau_s}$ with a new variable x_0. Let $Z \subset \mathbb{A}^1 \times \mathbb{P}^n$ be the set of common zeros of $\hat{F}_{i_1}^{\tau_1}, \ldots, \hat{F}_{i_s}^{\tau_s}$. In order to prove the statement it suffices to show

that $\pi_t(Z)$ is a finite set. Since π_t is a closed map, this can be proved by showing that $1 \notin \pi_t(Z)$, or equivalently, that the system $\hat{g}_{i_1}^{\tau_1}(x) = \cdots = \hat{g}_{i_s}^{\tau_s}(x) = 0$ has no solution in $\mathbb{P}^n$.

First, note that, if $(1 : x_1 : \cdots : x_n)$ is a solution of this system, then $(T(x_1), \ldots, T(x_n))$ is a solution of the linear system $B.\ y^t = -(n + \frac{1}{q_{i_1}}, \ldots, n + \frac{1}{q_{i_{n+1}}})^t$, where $B \in \mathbb{Q}^{(n+1)\times n}$ is the Cauchy matrix of coefficients of $g_{i_1}^{\tau_1}, \ldots, g_{i_{n+1}}^{\tau_{n+1}}$. But this linear system has no solutions, since its augmented matrix has a nonzero determinant. Finally, we have that, for $1 \leq j \leq s$, $\hat{g}_{i_j}^{\tau_j}(0, x_1, \ldots, x_n) = \pm 2^{d-1} \sum_{1\leq k\leq n} \frac{1}{q_{i_j}-n-1+k} x_k^d$. Considering the equations for $1 \leq j \leq n$, we deduce that $(x_1^d, \ldots, x_n^d)$ is in the kernel of the Cauchy matrix $(\frac{1}{q_{i_j}-n-1+k})_{1\leq j,k\leq n}$ and therefore, it is the zero vector. Thus, the system $\hat{g}_{i_1}^{\tau_1}(x) = \cdots = \hat{g}_{i_s}^{\tau_s}(x) = 0$ has no solutions in $\{x_0 = 0\}$. □

Notation 22 For $S = \{i_1, \ldots, i_s\} \subset \{1, \ldots, m\}$ with $1 \leq s \leq n$, and $\tau = (\tau_1, \ldots, \tau_s) \in \{+, -\}^s$, we denote $\hat{V}_{S,\tau} \subset \mathbb{A}^1 \times \mathbb{A}^n \times \mathbb{P}^{s-1}$ the variety defined by the polynomials constructed as in (7) by taking $h_1, \ldots, h_r$ as the polynomials in system (13) and $g_1, \ldots, g_r$ the type 2 initial system given by $g_{i_1}^{\tau_1}, \ldots, g_{i_s}^{\tau_s}$. We consider the decomposition $\hat{V}_{S,\tau} = V_{S,\tau}^{(0)} \cup V_{S,\tau}^{(1)} \cup V_{S,\tau}$ as in (8).

The following proposition will enable us to adapt Algorithm 14 in order to solve the problem in this general setting.

Proposition 23 *Let $\sigma \in \{\leq, =, \geq\}^m$, $E_\sigma = \{i \mid \sigma_i = \text{“}=\text{”}\}$, $U_\sigma = \{i \mid \sigma_i = \text{“}\geq\text{”}\}$ and $L_\sigma = \{i \mid \sigma_i = \text{“}\leq\text{”}\}$. For $S = \{i_1, \ldots, i_s\} \subset \{1, \ldots, m\}$ with $1 \leq s \leq n$, let $\mathcal{T}_S = \{\tau \in \{+, -\}^s \mid \tau_j = \text{“}+\text{”}$ if $i_j \in U_\sigma$ and $\tau_j = \text{“}-\text{”}$ if $i_j \in L_\sigma\}$. Then, after a generic linear change of variables, for each connected component C of $\{x \in \mathbb{R}^n \mid f_1(x)\sigma_1 0, \ldots, f_m(x)\sigma_m 0\}$, we have*

$$Z(C) \subset \bigcup_{\substack{S\subset\{1,\ldots,m\}\\ 1\leq \#S\leq n}} \bigcup_{\tau\in\mathcal{T}_S} \pi_x\big(V_{S,\tau} \cap \{t = 0\}\big).$$

Proof Without loss of generality, we may assume that $E_\sigma = \{1, \ldots, l\}$, $U_\sigma = \{l + 1, \ldots, k\}$, and $L_\sigma = \{k + 1, \ldots, m\}$ for some l, k with $0 \leq l \leq k \leq m$. By Proposition 3, after a generic linear change of variables, $Z(C)$ is finite. Moreover, since $\mathcal{P}$ is a closed set, $Z(C) \subset C$. Let $z \in Z_{\inf}(C)$ and $0 < \varepsilon < 1$ such that:

- $\overline{B(z,\varepsilon)} \cap \mathcal{P} \subset C$ and $\overline{B(z,\varepsilon)} \cap Z(C) = \{z\}$,
- for every $\hat{S} = \{i_1, \ldots, i_{\hat{s}}\} \subset \{1, \ldots, m\}$ with $\hat{s} > n$ and every $(\tau_1, \ldots, \tau_{\hat{s}}) \in \{+, -\}^{\hat{s}}$, $\varepsilon < |t_0|$ for every t_0 in $\{t \in \mathbb{C} \setminus \{0\} \mid \exists x \in \mathbb{C}^n$ with $F_{i_1}^{\tau_1}(t, x) = \cdots = F_{i_{\hat{s}}}^{\tau_{\hat{s}}}(t, x) = 0\}$,
- for every $S \subset \{1, \ldots, m\}$ with $1 \leq \#S \leq n$ and every $\tau \in \mathcal{T}_S$, $\varepsilon < |t_0|$ for every $t_0 \in \mathbb{C}$ such that $V_{S,\tau}^{(1)}$ has an irreducible component contained in $\{t = t_0\}$.

For $t \in \mathbb{R}$, let $R_t = \{x \in \overline{B(z,\varepsilon)} \mid F_1^+(t, x) \geq 0, \ldots, F_l^+(t, x) \geq 0, F_1^-(t, x) \leq 0, \ldots, F_l^-(t, x) \leq 0, F_{l+1}^+(t, x) \geq 0, \ldots, F_k^+(t, x) \geq 0, F_{k+1}^-(t, x) \leq 0, \ldots, F_m^-(t, x) \leq 0\}$. We have that $R_0 = C \cap \overline{B(z,\varepsilon)}$ and, for every $t \in [0, 1]$, $z \in R_t$.

Let $\nu > 0$ be the distance between the compact sets $\partial B(z,\varepsilon) \cap \{x_1 \le z_1\}$ and R_0. We claim that for some t_1, $0 < t_1 < \varepsilon$, the connected component C' of R_{t_1} containing z is included in $\{x \in \overline{B(z,\varepsilon)} \mid d(x,R_0) \le \nu/2\}$. Suppose this is not the case. Let $(t'_n)_{n\in\mathbb{N}}$ be a decreasing sequence of positive numbers converging to 0 and with $t'_1 < \varepsilon$, and for every $n \in \mathbb{N}$, let C'_n be the connected component of $R_{t'_n}$ containing z. Since C'_n intersects $\{x \in \overline{B(z,\varepsilon)} \mid d(x,R_0) > \nu/2\}$, there is a point $r_n \in C'_n$ such that $d(r_n,R_0) = \nu/2$. Then, there is a limit point $r \in \overline{B(z,\varepsilon)}$ with $d(r,R_0) = \nu/2$ such that, for $1 \le i \le k$, $F_i^+(0,r) \ge 0$, and for every $1 \le i \le l$ and $k+1 \le i \le m$, $F_i^-(0,r) \le 0$. Therefore, $r \in R_0$, contradicting the fact that $d(r,R_0) = \nu/2 > 0$.

Let $w \in C'$ be a point at which the function x_1 attains its minimum over C'. Since $z \in C'$, we have $w_1 \le z_1$. If $w \in \partial B(z,\varepsilon)$, then $w \in \partial B(z,\varepsilon) \cap \{x_1 \le z_1\}$, and so, $d(w,R_0) \ge \nu$, contradicting the fact that $d(w,R_0) \le \nu/2$. Therefore, $w \in B(z,\varepsilon)$.

As each of the polynomials $F_1^+,\dots,F_l^+,F_1^-,\dots,F_l^-,F_{l+1}^+,\dots,F_k^+,F_{k+1}^-,\dots,F_m^-$ that does not vanish at (t_1,w) takes a constant sign in a neighborhood of this point, we conclude that, if $F_{i_1}^{\tau_1},\dots,F_{i_s}^{\tau_s}$ are all the polynomials vanishing at (t_1,w), then the function x_1 attains a local minimum over the set $\{x \in \mathbb{R}^n \mid F_{i_1}^{\tau_1}(t_1,x) = 0,\dots,F_{i_s}^{\tau_s}(t_1,x) = 0\}$ at w. Let $S_0 = \{i_1,\dots,i_s\}$, which is not empty. For $1 \le i \le m$, $F_i^+(t_1,w)$ and $F_i^-(t_1,w)$ cannot be both zero; thus, $i_1,\dots,i_s$ are all distinct. Because of the way we chose ε, we also have that $s \le n$. Now, if $\tau_0 = (\tau_1,\dots,\tau_s)$, we have that $(t_1,w) \in \pi_{t,x}(\hat{V}_{S_0,\tau_0})$, but taking into account that $0 < t_1 < \varepsilon$, it follows that $(t_1,w) \in \pi_{t,x}(V_{S_0,\tau_0})$. Therefore, $(t_1,w) \in \bigcup_{\substack{S\subset\{1,\dots,m\}\\ 1\le \#S\le n}} \bigcup_{\tau\in\mathcal{T}_S} \pi_{t,x}(V_{S,\tau})$ and $0 < |(t_1,w)-(0,z)| < \sqrt{2}\varepsilon$.

Since the previous construction can be done for every $\varepsilon > 0$ sufficiently small and the sets $\pi_{t,x}(V_{S,\tau})$ are closed, we conclude that $(0,z) \in \bigcup_{\substack{S\subset\{1,\dots,m\}\\ 1\le \#S\le n}} \bigcup_{\tau\in\mathcal{T}_S} \pi_{t,x}(V_{S,\tau})$. □

5.3 Symbolic Deformation Algorithm

In the sequel, Ω will denote a positive real number such that for any ring R, addition, multiplication and the computation of determinant and adjoint of matrices in $R^{k\times k}$ can be performed within $O(k^\Omega)$ operations in R. We may assume $\Omega \le 4$ (see [11]) and, in order to simplify complexity estimations, we will also assume that $\Omega \ge 3$.

Proposition 24 *There is a probabilistic algorithm that, taking as input polynomials $h_1,\dots,h_r$ in $\mathbb{K}[x_1,\dots,x_n,\mu_1,\dots,\mu_s]$ as in (5) encoded by an slp of length L, obtains a geometric resolution of a finite set containing $\pi_x(V \cap \{t = 0\})$ for a deformation defined from a type 2 initial system within complexity $O(n^3(L+dn+n^{\Omega-1})D^2\log^2(D)\log\log^2(D))$, where d is an even integer such that $d \ge \deg_x(h_i)$ for every $1 \le i \le r$.*

Proof The structure of the algorithm is similar to that of the algorithm underlying the proof of Proposition 13.

First step: Take $\alpha = (\alpha_1,\dots,\alpha_n) \in \mathbb{Q}^n$ at random and compute a geometric resolution associated to the linear form $\ell_\alpha(x) = \alpha_1x_1 + \cdots + \alpha_nx_n$ of the variety defined in $\mathbb{A}^r$ by the (dehomogenized) type 2 initial system.

As shown in the proof of Lemma 20, this variety can be partitioned into subsets $S_{B,e}$. So, we first compute a geometric resolution associated with $\ell_\alpha(x)$ for

each $S_{B,e}$: after solving a linear system, the x-coordinates of points in $S_{B,e}$ turn to be defined by a square polynomial system in separated variables; then, the required computation can be achieved as in [27, Sect. 5.2.1] within complexity $O(D_{B,e}^2 \log^2(D_{B,e}) \log\log(D_{B,e}))$, where $D_{B,e}$ is the cardinality of $S_{B,e}$.

Finally, a geometric resolution of the whole variety is obtained following the splitting strategy given in [44, Algorithm 10.3], and noticing that, if $\{q, q_0, w_1, \ldots, w_r\}$ and $\{\tilde{q}, \tilde{q}_0, \tilde{w}_1, \ldots, \tilde{w}_r\}$ are geometric resolutions of disjoint sets with q and $\tilde{q}$ coprime polynomials, then $\{q\tilde{q}, q_0\tilde{q} + \tilde{q}_0 q, w_1\tilde{q} + \tilde{w}_1 q, \ldots, w_r\tilde{q} + \tilde{w}_r q\}$ is a geometric resolution of their union. This can be done within $O(nD\log^2(D)\log\log(D))$ operations in $\mathbb{Q}$.

The whole complexity of this step is $O(nD^2\log^2(D)\log\log(D))$.

Second step: Compute $P(t, U, y) \mod ((t-1)^{2nD+1} + (y_1 - \alpha_1, \ldots, y_n - \alpha_n)^2)\mathbb{K}[[t-1]][U, y]$.

First, from the geometric resolution computed in the previous step, obtain a geometric resolution associated with $\ell(x, y) = y_1x_1 + \cdots + y_nx_n$ of the variety defined by the initial system over $\overline{\mathbb{K}(y)}$, modulo the ideal $(y_1 - \alpha_1, \ldots, y_n - \alpha_n)^2$, applying [20, Algorithm 1] within complexity $O((dn^2 + n^\Omega)D^2\log^2(D)\log\log^2(D))$. Then, consider the variety defined by $F_1, \ldots, F_r$ over $\overline{\mathbb{K}(t, y)}$ (see Lemma 8). Since $F_1, \ldots, F_r$ can be encoded by an slp of length $L + O((d+s)n)$, a geometric resolution of this variety associated with the linear form $\ell(x, y)$ modulo the ideal $(t-1)^{2nD+1} + (y_1 - \alpha_1, \ldots, y_n - \alpha_n)^2$ can be obtained from the previously computed geometric resolution by applying [20, Algorithm 1] within complexity $O(n^3(L + dn + n^{\Omega-1})D^2\log^2(D)\log\log^2(D))$.

Third step: From the approximation to $P(t, U, y)$ obtain the required geometric resolution, by performing the same computations as in the third and forth steps of the algorithm underlying the proof of Proposition 13, which does not modify the overall complexity. □

The algorithm underlying the proof of Proposition 24 can be adapted straightforwardly to handle the cases $s = 1$ and $s = n$ within the same complexity bounds.

5.4 Main Algorithm

Here we prove the main result of this section, which is the second part of Theorem 2.

Theorem 25 *Given polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ with degrees bounded by an even integer d and encoded by an slp of length L, for generic choices of the parameters required at intermediate steps, the algorithm obtained from Algorithm 14 taking $p = (0, \ldots, 0)$ and replacing part* (b) *of Step* 3 *with*

(b′) *For every $\tau \in \{+, -\}^{\#S}$, compute a geometric resolution $\{q^{(k,S,\tau)}(U), v_k^{(k,S,\tau)}(U), \ldots, v_n^{(k,S,\tau)}(U)\} \subset \mathbb{K}[U]$ of a finite set containing $\pi_x(V_{k,S,\tau} \cap \{t = 0\})) \subset \mathbb{A}^{n-k+1}$ by means of a deformation from a type* 2 *initial system, and add the geometric resolution*

$$\left\{q^{(k,S,\tau)}(U), 0, \ldots, 0, v_k^{(k,S,\tau)}(U), \ldots, v_n^{(k,S,\tau)}(U)\right\}$$

to the list $\mathcal{G}$.

computes a finite set $\mathcal{M} \subset \mathbb{A}^n$ intersecting each connected component of the realization of every feasible closed sign condition over $f_1, \ldots, f_m$. The complexity of the algorithm is

$$O\left(n^6\big(L+d+n^2\big)\log^2(d)\big(\log(n)+\log\log(d)\big)^2 d^{2n}\left(\sum_{s=1}^{\min\{m,n\}} 2^s\binom{m}{s}\binom{n-1}{s-1}^2\right)\right).$$

Proof As in the proof of Theorem 15, by Proposition 5, it suffices to show that $\bigcup_{1\le k\le n-1}\bigcup_{C\in\mathcal{C}(k,p)} Z(C,k)\subset\mathcal{M}$, which is a consequence of Proposition 23.

Taking into account the linear change of variables performed at the first step of the algorithm, for $1\le k\le n-1$ and every $S\subset\{1,\ldots,m\}$ with $1\le \#S\le n-k+1$, we can obtain an slp of length $O(nL+n^3)$ encoding the polynomials involved in system (13). In (b′), the algorithm underlying the proof of Proposition 24 is used. The stated complexity is obtained by adding up the complexities of these steps for all (k,S,τ). □

As explained at the end of Sect. 4.2, from a geometric resolution of a finite set intersecting each feasible sign condition over $f_1,\ldots,f_m$, we can obtain the list of all closed sign conditions over these polynomials. We deduce:

Theorem 26 *There is a probabilistic algorithm which, given polynomials $f_1,\ldots,f_m\in\mathbb{K}[x_1,\ldots,x_n]$ of degrees bounded by an even integer d and encoded by an slp of length L, computes the list of all feasible closed sign conditions over these polynomials within $O\big(\sum_{s=1}^{\min\{m,n\}}\binom{m}{s}\binom{n-1}{s-1}^2 d^{2n}(2^s n^6(L+d+n^2)\log^2(d)(\log(n)+\log\log(d))^2+md^{(\omega-2)n}\binom{n-1}{s-1}^{\omega-2})\big)$ operations in $\mathbb{K}$.*

6 Some Particular Cases

6.1 The Bivariate Case

Here we will show that when $n=2$, Algorithm 14 solves our main problem for an *arbitrary* finite family of polynomials.

Lemma 27 *Let $f\in\mathbb{C}[x_1,x_2]$ be a nonzero polynomial with no factors in $\mathbb{C}[x_1]\setminus\{0\}$. Let g_1,g_2 be polynomials satisfying property* (H)*, with g_1 relatively prime to f. Let $F_1=(1-t)f+tg_1$ and $F_2=(1-t)\frac{\partial f}{\partial x_2}+tg_2$ and V be the variety defined in* (8)*. If $z\in\mathbb{C}^2$ satisfies that either two or more non-associate irreducible factors of f vanish at z or an irreducible factor of f and its derivative with respect to x_2 both vanish at z, then $z\in\pi_x(V\cap\{t=0\})$.*

Proof In order to simplify the notation, we write $f'=\frac{\partial f}{\partial x_2}$. Set $I=(F_1,F_2)\subset\mathbb{K}[t,x_1,x_2]$. Then $V\cap\{t=0\}=V((I:t^\infty)+(t))$.

Let $h_1=f/\gcd(f,f')$ and $h_2=f'/\gcd(f,f')$. We claim that $(I:t)=(F_1,F_2,h_2g_1-h_1g_2)$ holds: first note that $(h_2g_1-h_1g_2)t=h_2F_1-h_1F_2$, which shows the

inclusion $\supset$. Now, if $p(t,x) \in (I:t)$, we have $p(x,t)t = (\alpha_1(t,x)t + \alpha_0(x))F_1 + (\beta_1(t,x)t + \beta_0(x))F_2$ for polynomials $\alpha_1, \alpha_0, \beta_1, \beta_0$. Substituting $t = 0$, we obtain $\alpha_0 f = -\beta_0 f'$ and so, $\alpha_0 h_1 = -\beta_0 h_2$. Then, there exists $c \in \mathbb{C}[x]$ such that $\alpha_0 = ch_2$ and $\beta_0 = -ch_1$, and therefore, $p(t,x) = \alpha_1(t,x)F_1 + \beta_1(t,x)F_2 + c(h_2 g_1 - h_1 g_2)$.

Using similar arguments, it follows that $(I:t^2) \subset (I:t)$ and so, $(I:t^\infty) = (I:t) = (F_1, F_2, h_2 g_1 - h_1 g_2)$. Then, since each condition in the lemma implies that $h_1(z) = h_2(z) = 0$, we deduce that $(0,z) \in V(I:t^\infty)$, and therefore, $z \in \pi_x(V \cap \{t = 0\})$. □

Proposition 28 *Let $f_1, \ldots, f_m$ be arbitrary bivariate real polynomials and $\sigma \in \{<, =, >\}^m$. Then, after a generic linear change of variables, for each connected component C of $\{x \in \mathbb{R}^n \mid f_1(x)\sigma_1 0, \ldots, f_m(x)\sigma_m 0\}$ we have that $Z(C) \subset \bigcup_{S \subset \{1,\ldots,m\},\, 1 \le \#S \le 2} \pi_x(V_S \cap \{t = 0\})$, where the varieties V_S are defined from type 1 initial systems.*

Proof After a generic linear change of variables we may assume that, for each connected component C, either $\pi_1(C) = \mathbb{R}$ or $Z(C)$ is a non-empty finite set (see Proposition 3).

Assume $Z_{\inf}(C) \neq \emptyset$ and let $z = (z_1, z_2) \in Z_{\inf}(C)$. Since $z \in \partial C$, there is an index i_0 such that $f_{i_0} \neq 0$ and $f_{i_0}(z) = 0$. If f_{i_0} has two or more non-associate irreducible factors vanishing at z, or an irreducible factor vanishing at z and whose derivative with respect to x_2 also vanishes at z, by Lemma 27, $z \in \pi_x(V_{\{i_0\}} \cap \{t = 0\})$ (note that, because of the generic change of variables, f_{i_0} does not have factors of the form $x_i - \alpha$). Otherwise, there is a unique irreducible factor p of f_{i_0} vanishing at z which must have all real coefficients (since its complex conjugate also divides f_{i_0} and vanishes at z) such that $\frac{\partial p}{\partial x_2}(z) \neq 0$.

By the implicit function theorem applied to p at the point z, there is a continuous curve $(x_1, x_2(x_1))$ defined in a neighborhood of z_1, and a neighborhood of z such that the polynomial p (as well as any power of p and also f_{i_0}) has constant signs above, below and on the curve in this neighborhood. Since $z_1 = \inf \pi_1(C)$, there must be an index $i_1 \neq i_0$ such that $f_{i_1}(z) = 0$. Moreover, we may assume that f_{i_1} has a unique irreducible factor q vanishing at z that is not an associate to p. In this second case, z is an isolated point of $W_{\{i_0,i_1\}} = V(f_{i_0}, f_{i_1})$ and then, by Lemma 7, $z \in \pi_x(V_{\{i_0,i_1\}} \cap \{t = 0\})$. □

Using this proposition, following the proof of Theorem 15, we have:

Theorem 29 *Algorithm 14 is a probabilistic procedure that, given polynomials $f_1, \ldots, f_m \in \mathbb{K}[x_1, x_2]$ of degrees bounded by $d \ge 2$ that are encoded by an slp of length L, obtains a finite set $\mathcal{M}$ intersecting the closure of each connected component of the realization of every sign condition on the polynomials within complexity $O(m^2 d^4 \log(d) \log\log(d)(L + \log^2(d) \log\log(d)))$.* □

6.2 A Single Polynomial

In this section, we will show the procedure described in Sect. 5 can be adapted to solve the problem of computing a point in the closure of each connected component of $\{f=0\}$, $\{f>0\}$ and $\{f<0\}$ for an arbitrary polynomial $f \in \mathbb{K}[x_1,\ldots,x_n]$.

Let d be an even positive integer such that $d \geq \deg(f)$. Let T be the Tchebychev polynomial of degree d. We define $g(x) = n + \frac{1}{q} + \sum_{k=1}^{n} \frac{1}{q-n-1+k} T(x_k)$, where q is the smallest prime greater than n; $F(t,x) = (1-t)f(x) + tg(x)$, and, for $2 \leq i \leq n$, $F_i(t,x) = (1-t)\frac{\partial f}{\partial x_i}(x) + t\frac{\partial g}{\partial x_i}(x) = \frac{\partial F}{\partial x_i}(t,x)$. Note that $g > 0$ over $\mathbb{R}^n$, and therefore, $F > 0$ over the set $\{f=0\}$. Moreover, this is a deformation with a type 2 initial system (see Definition 19). As in Sect. 3.3.1, we let $\hat{V} = \{F = F_2 = \cdots = F_n = 0\} \subset \mathbb{A}^1 \times \mathbb{A}^n$, and consider its decomposition (8).

Lemma 30 *After a generic linear change of variables, for each connected component C of $\{f=0\}$, $\{f>0\}$ or $\{f<0\}$, we have $Z(C) \subset \pi_x(V \cap \{t=0\})$.*

Proof Consider first a connected component C of $\{f=0\}$ (for a similar approach in this case with an alternative deformation, see [34]). Let $z \in Z_{\inf}(C)$. Take $\varepsilon > 0$ such that $\overline{B(z,\varepsilon)}$ meets neither a connected component of $\{f=0\}$ different from C nor the finite set $Z(C) \setminus \{z\}$, and $\varepsilon < |t_0|$ for each $t_0 \in \mathbb{C}$ such that $V^{(1)}$ has a connected component contained in $\{t=t_0\}$.

Let $\mu \in (z_1, z_1+\varepsilon)$ be such that $\partial B(z,\varepsilon) \cap C \subset \{x_1 > \mu\}$. Without loss of generality, we may assume that f is positive over the compact set $\partial B(z,\varepsilon) \cap \{x_1 \leq \mu\}$. Let $\varepsilon_0 \in (0,\varepsilon)$ be such that F is positive over $[-\varepsilon_0,\varepsilon_0] \times (\partial B(z,\varepsilon) \cap \{x_1 \leq \mu\})$. Now, let $y \in B(z,\varepsilon)$ with $y_1 < z_1$ (thus, $f(y) \neq 0$). Since $F(-\varepsilon_0, z) < 0$, $F(\varepsilon_0, z) > 0$ and $F(0,y) \neq 0$, there is a point $(t_1, \tilde{y})$ in the union of the line segments joining $(-\varepsilon_0, z)$, $(0,y)$, and $(0,y)$, (ε_0, z), respectively, such that $F(t_1,\tilde{y}) = 0$. We have $t_1 \neq 0$ and $\tilde{y}_1 < z_1$. Let $w \in \{x \in \overline{B(z,\varepsilon)} \mid F(t_1,x) = 0\}$ be a point at which the coordinate function x_1 attains its minimum over this compact set. Note that $w \notin \partial B(z,\varepsilon)$, since $w_1 < \tilde{y}_1 < z_1 < \mu$ and F is positive over $[-\varepsilon_0,\varepsilon_0] \times (\partial B(z,\varepsilon) \cap \{x_1 \leq \mu\})$. Therefore, $w \in B(z,\varepsilon)$, and so $(t_1, w) \in \hat{V}$. Moreover, as $0 < |t_1| < \varepsilon$, we have $(t_1, w) \in V$. Since $0 < |(t_1,w) - (0,z)| < \sqrt{2}\varepsilon$, and the construction can be done for an arbitrary sufficiently small $\varepsilon > 0$, it follows that $(0,z) \in V$.

Assume now that C is a connected component of $\{f>0\}$ and let $z \in Z_{\inf}(C)$ (then, $f(z) = 0$). Let $\tilde{C}$ be the connected component of $\{f=0\}$ containing z, and $\varepsilon > 0$ such that $\overline{B(z,\varepsilon)}$ meets neither a connected component of $\{f=0\}$ different from $\tilde{C}$ nor the finite set $Z(C) \setminus \{z\}$, and $\varepsilon < |t_0|$ for every $t_0 \in \mathbb{C}$ such that $V^{(1)}$ has an irreducible component included in $\{t=t_0\}$.

Let $\mu \in (z_1, z_1+\varepsilon)$ be such that $\partial B(z,\varepsilon) \cap \overline{C} \subset \{x_1 > \mu\}$ and $\gamma : [0,1] \to \mathbb{R}^n$ a continuous semialgebraic curve such that $\gamma(0) = z$ and $\gamma((0,1]) \subset C \cap B(z,\varepsilon) \cap \{x_1 < \mu\}$. Let C_1 be the connected component of $C \cap B(z,\varepsilon)$ with $\gamma((0,1]) \subset C_1$. Take $t_1 \in (-\varepsilon, 0)$ small enough so that $F(t_1, \gamma(1)) > 0$. Since $F(t_1,\gamma(0)) < 0$, there exists $u \in (0,1)$ such that $F(t_1,\gamma(u)) = 0$. Let C' be the connected component of $\{x \in B(z,\varepsilon) \mid F(t_1,x) = 0\}$ containing $\gamma(u)$. As $\gamma(u) \in C' \cap C_1$, $C' \cup C_1$ is a connected set. Therefore $C' \subset C_1$, as $C' \subset B(z,\varepsilon) \setminus \tilde{C}$ and C_1 is a connected component of this set. Now let $K = C' \cup (\overline{B(z,\varepsilon)} \cap \{x_1 \geq \mu\})$, which is a compact set, since

$\overline{C'} = C' \cup (\partial B(z,\varepsilon) \cap \overline{C'}) \subset C' \cup (\partial B(z,\varepsilon) \cap \overline{C}) \subset K$. If $w \in K$ is a point at which the function x_1 attains its minimum over K, then $w \notin \overline{B(z,\varepsilon)} \cap \{x_1 \geq \mu\}$. Then, w is a minimum of x_1 over the set $C' \cap B(z,\varepsilon) \cap \{x_1 < \mu\}$. Therefore, $(t_1, w) \in \hat{V}$ and, since $0 < |t_1| < \varepsilon$, we have $(t_1, w) \in V$. As before, we conclude that $(0, z) \in V$. □

Then, due to Proposition 5 and proceeding as in the proof of Theorem 25, we have:

Theorem 31 *Given a polynomial $f \in \mathbb{K}[x_1, \ldots, x_n]$ of degree bounded by an even integer d and encoded by an slp of length L, for generic choices of the parameters required at intermediate steps, the algorithm obtained from Algorithm 14 modifying Step* 3(b) *in order to deal with type* 2 *initial systems, computes a finite set $\mathcal{M} \subset \mathbb{A}^n$ intersecting the closure of each connected component of the sets $\{f < 0\}$, $\{f = 0\}$ and $\{f > 0\}$. The complexity of the algorithm is $O(n^5(L + nd + n^{\Omega-1}) \log^2(d)(\log(n) + \log\log(d))^2 d^{2n})$.*

Acknowledgements The authors thank the referees for their useful suggestions and remarks.

References

1. Alonso, M.-E., Becker, E., Roy, M.-F., Wörmann, T.: Zeros, multiplicities, and idempotents for zero-dimensional systems. In: Algorithms in Algebraic Geometry and Applications. Progr. Math., vol. 143, pp. 1–15. Birkhäuser, Basel (1996)
2. Aubry, P., Rouillier, F., Safey El Din, M.: Real solving for positive dimensional systems. J. Symb. Comput. **34**(6), 543–560 (2002)
3. Bank, B., Giusti, M., Heintz, J., Mbakop, G.M.: Polar varieties, real equation solving, and data structures: the hypersurface case. J. Complex. **13**(1), 5–27 (1997)
4. Bank, B., Giusti, M., Heintz, J., Mbakop, G.M.: Polar varieties and efficient real elimination. Math. Z. **238**(1), 115–144 (2001)
5. Bank, B., Giusti, M., Heintz, J., Pardo, L.M.: Generalized polar varieties and an efficient real elimination procedure. Kybernetika (Prague) **40**(5), 519–550 (2004)
6. Bank, B., Giusti, M., Heintz, J., Pardo, L.M.: Generalized polar varieties: geometry and algorithms. J. Complex. **21**(4), 377–412 (2005)
7. Basu, S., Pollack, R., Roy, M.-F.: On the combinatorial and algebraic complexity of quantifier elimination. J. ACM **43**(6), 1002–1045 (1996)
8. Basu, S., Pollack, R., Roy, M.-F.: A new algorithm to find a point in every cell defined by a family of polynomials. In: Quantifier Elimination and Cylindrical Algebraic Decomposition, Linz, 1993. Texts Monogr. Symbol. Comput., pp. 341–350. Springer, Vienna (1998)
9. Basu, S., Pollack, R., Roy, M.-F.: Algorithms in Real Algebraic Geometry. Algorithms and Computation in Mathematics, vol. 10. Springer, Berlin (2003)
10. Baur, W., Strassen, V.: The complexity of partial derivatives. Theor. Comput. Sci. **22**(3), 317–330 (1983)
11. Berkowitz, S.: On computing the determinant in small parallel time using a small number of processors. Inf. Process. Lett. **18**(3), 147–150 (1984)
12. Bini, D., Pan, V.Y.: Polynomial and Matrix Computations. Vol. 1. Fundamental Algorithms. Progress in Theoretical Computer Science. Birkhäuser, Boston (1994)
13. Bochnak, J., Coste, M., Roy, M.-F.: Real Algebraic Geometry. Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 36. Springer, Berlin (1998)
14. Bürgisser, P., Clausen, M., Shokrollahi, M.A.: Algebraic Complexity Theory. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 315. Springer, Berlin (1997)
15. Canny, J.: Improved algorithms for sign determination and existential quantifier elimination. Comput. J. **36**(5), 409–418 (1993)

16. Collins, G.E.: Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In: Automata Theory and Formal Languages, Second GI Conf., Kaiserslautern, 1975. Lecture Notes in Comput. Sci., vol. 33, pp. 134–183. Springer, Berlin (1975)
17. Coppersmith, D., Winograd, S.: Matrix multiplication via arithmetic progressions. J. Symb. Comput. **9**(3), 251–280 (1990)
18. Giusti, M., Heintz, J., Hägele, K., Morais, J.E., Pardo, L.M., Montaña, J.L.: Lower bounds for Diophantine approximations. J. Pure Appl. Algebra **117/118**, 277–317 (1997)
19. Giusti, M., Heintz, J., Morais, J.E., Morgenstern, J., Pardo, L.M.: Straight-line programs in geometric elimination theory. J. Pure Appl. Algebra **124**(1–3), 101–146 (1998)
20. Giusti, M., Lecerf, G., Salvy, B.: A Gröbner free alternative for polynomial system solving. J. Complex. **17**(1), 154–211 (2001)
21. Grigor'ev, D.Y., Vorobjov, N.N. Jr.: Counting connected components of a semialgebraic set in subexponential time. Comput. Complex. **2**(2), 133–186 (1992)
22. Heintz, J.: Definability and fast quantifier elimination in algebraically closed fields. Theor. Comput. Sci. **24**(3), 239–277 (1983)
23. Heintz, J., Schnorr, C.-P.: Testing polynomials which are easy to compute. In: Logic and Algorithmic, Zurich, 1980. Enseign. Math., vol. 30, pp. 237–254. Univ. Genève, Geneva (1982)
24. Heintz, J., Jeronimo, G., Sabia, J., Solernó, P.: Intersection theory and deformation algorithms: the multi-homogeneous case. Manuscript
25. Heintz, J., Roy, M.-F., Solernó, P.: Sur la complexité du principe de Tarski–Seidenberg. Bull. Soc. Math. Fr. **118**(1), 101–126 (1990)
26. Heintz, J., Krick, T., Puddu, S., Sabia, J., Waissbein, A.: Deformation techniques for efficient polynomial equation solving. J. Complex. **16**(1), 70–109 (2000)
27. Jeronimo, G., Matera, G., Solernó, P., Waissbein, A.: Deformation techniques for sparse systems. Found. Comput. Math. **9**(1), 1–50 (2009)
28. König, J.: Einleitung in die allgemeine Theorie der algebraischen Größen. B.G. Teubner, Leipzig (1903)
29. Kronecker, L.: Grundzüge einer arithmetischen Theorie der algebraischen Grössen. Festschrift (1882)
30. Lecerf, G.: Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers. J. Complex. **19**(4), 564–596 (2003)
31. Pedregal, P.: Introduction to Optimization. Texts in Applied Mathematics, vol. 46. Springer, New York (2004)
32. Renegar, J.: On the computational complexity and geometry of the first-order theory of the reals. I, II, III. J. Symb. Comput. **13**(3), 255–352 (1992)
33. Rouillier, F.: Solving zero-dimensional systems through the rational univariate representation. Appl. Algebra Eng. Commun. Comput. **9**(5), 433–461 (1999)
34. Rouillier, F., Roy, M.-F., Safey El Din, M.: Finding at least one point in each connected component of a real algebraic set defined by a single equation. J. Complex. **16**(4), 716–750 (2000)
35. Safey El Din, M.: Testing sign conditions on a multivariate polynomial and applications. Math. Comput. Sci. **1**(1), 177–207 (2007)
36. Safey El Din, M., Schost, É.: Polar varieties and computation of one point in each connected component of a smooth algebraic set. In: Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation, pp. 224–231. ACM, New York (2003) (electronic)
37. Safey El Din, M., Trébuchet, P.: Strong bi-homogeneous Bézout theorem and its use in effective real algebraic geometry. INRIA Research Report RR-6001 (2006)
38. Schost, É.: Computing parametric geometric resolutions. Appl. Algebra Eng. Commun. Comput. **13**(5), 349–393 (2003)
39. Seidenberg, A.: A new decision method for elementary algebra. Ann. Math. (2) **60**, 365–374 (1954)
40. Shafarevich, I.R.: Basic Algebraic Geometry, study edition. Springer, Berlin (1977)
41. Tarski, A.: A Decision Method for Elementary Algebra and Geometry, 2nd edn. University of California Press, Berkeley (1951)
42. Voisin, C.: Hodge Theory and Complex Algebraic Geometry. II. Cambridge Studies in Advanced Mathematics, vol. 77. Cambridge University Press, Cambridge (2003)
43. von zur Gathen, J.: Parallel arithmetic computations: a survey. In: Mathematical Foundations of Computer Science, 1986, Bratislava, 1986. Lecture Notes in Comput. Sci., vol. 233, pp. 93–112. Springer, Berlin (1986)
44. von zur Gathen, J., Gerhard, J.: Modern Computer Algebra. Cambridge University Press, New York (1999)