Found Comput Math (2009) 9: 1–50
DOI 10.1007/s10208-008-9024-2

FOUNDATIONS OF COMPUTATIONAL MATHEMATICS
The Journal of the Society for the Foundations of Computational Mathematics

Deformation Techniques for Sparse Systems

Gabriela Jeronimo · Guillermo Matera · Pablo Solernó · Ariel Waissbein

Received: 13 September 2006 / Revised: 13 April 2007 / Accepted: 6 August 2007 /
Published online: 22 February 2008

Abstract We exhibit a probabilistic symbolic algorithm for solving zero-dimensional sparse systems. Our algorithm combines a symbolic homotopy procedure, based on a

Communicated by Mike Shub.

Research was partially supported by the following grants: UBACyT X112 (2004–2007), UBACyT X847 (2006–2009), PIP CONICET 2461, PIP CONICET 5852/05, ANPCyT PICT 2005 17-33018, UNGS 30/3005, MTM2004-01167 (2004–2007), MTM2007-62799 and CIC 2007–2008.

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

P. Solernó
e-mail: psolerno@dm.uba.ar

G. Jeronimo · G. Matera · P. Solernó
National Council of Science and Technology (CONICET), Buenos Aires, Argentina

G. Matera
Instituto de Desarrollo Humano, Universidad Nacional de General Sarmiento, J.M. Gutiérrez 1150, 1613 Los Polvorines, Buenos Aires, Argentina
e-mail: gmatera@ungs.edu.ar

A. Waissbein
CoreLabs, CORE Security Technologies, Humboldt 1967, C1414CTU Buenos Aires, Argentina

A. Waissbein
Doctorado en Ingeniería, Instituto Tecnológico de Buenos Aires, Av. Eduardo Madero 399, C1106ACD Buenos Aires, Argentina
e-mail: ariel.waissbein@corest.com

flat deformation of a certain morphism of affine varieties, with the polyhedral deformation of Huber and Sturmfels. The complexity of our algorithm is cubic in the size of the combinatorial structure of the input system. This size is mainly represented by the cardinality and mixed volume of Newton polytopes of the input polynomials and an arithmetic analogue of the mixed volume associated to the deformations under consideration.

Keywords Sparse system solving · Symbolic homotopy algorithms · Polyhedral deformations · Mixed volume · Non-Archimedean height · Puiseux expansions of space curves · Newton–Hensel lifting · Geometric solutions · Probabilistic algorithms · Complexity

Mathematics Subject Classification (2000) Primary: 14Q05 · 52B20 · 68W30 · Secondary: 12Y05 · 13F25 · 14Q20 · 68W40

1 Introduction

This paper deals with the symbolic computation of all solutions to zero-dimensional multivariate polynomial equation systems, i.e., systems with a finite number of common complex zeros. We focus our attention on systems of *sparse* polynomials, namely, polynomials with nonzero coefficients only at a prescribed set of monomials.

The algorithms presented in this paper rely on *deformation* techniques. Roughly speaking, a deformation method to solve a zero-dimensional polynomial system obtains a perturbation of the given system. This perturbation consists of a parametric family of zero-dimensional systems with a parametric instance easy to solve, enabling one to recover the solutions of the original system by continuation.

Deformation methods for computing all solutions of a given zero-dimensional polynomial system have been applied extensively in the numeric solving framework (see, e.g., [1, 7, 37, 53]). This kind of algorithm has also appeared (both for symbolic and numeric solving) in a number of recent research papers (see, e.g., [8, 17, 25, 26, 28, 32, 34, 41, 46, 52, 56, 57]). The cost of such algorithms is usually determined by geometric invariants associated to the family of systems under consideration, typically in the form of a suitable (arithmetic or geometric) Bézout number (for instance, the product of the degrees of the polynomials, the mixed volume of their Newton polytopes, etc.; see [24, 26, 27, 35, 38, 45, 49]).

From the symbolic point of view, every instance of a deformation procedure is regarded as a fiber of a suitable morphism π (customarily a flat linear projection with generic finite fiber) of an affine variety W. In this case, the continuation step is achieved by a symbolic Newton–Hensel lifting. This method, implicitly considered in the papers [20, 21], is isolated in [25] and refined in [8, 52] (see also [24, 41]). The cost of this procedure can be roughly estimated by the product of two geometric invariants: the number of points in a typical fiber of π and the degree of the variety W. This technique is nearly optimal in the worst case [13], and has good performance over certain well-posed families of polynomial systems of practical interest (see [8, 12, 25, 41, 52]).

The origins of sparse elimination theory can be traced back to the results by D.N. Bernstein, A.G. Kushnirenko and A.G. Khovanski ([5, 29, 30]) that bound the number of solutions of a polynomial system in terms of a combinatorial invariant associated to the set of exponents of the monomials arising with nonzero coefficients in the defining polynomials. More precisely, the Bernstein–Kushnirenko–Khovanski (BKK for short) theorem asserts that the number of isolated solutions in the n-dimensional complex torus $(\mathbb{C}^*)^n$ of a polynomial system of n equations in n unknowns is bounded by the *mixed volume* of the family of Newton polytopes of the corresponding polynomials.

Numeric (homotopy continuation) methods for sparse systems are typically based on a specific family of deformations called polyhedral homotopies ([26, 48, 56, 57]). Polyhedral homotopies preserve the Newton polytope of the input polynomials and yield an effective version of the BKK theorem (see, e.g., [26, 27]).

In this paper we combine the homotopic procedures of [26] with the above mentioned symbolic deformation techniques, particularly in the version of [8], in order to derive a symbolic probabilistic algorithm for solving sparse zero-dimensional polynomial systems with cubic cost in the size of the combinatorial structure of the input system. Our main result may be stated as follows (see Theorem 6.2 below for a precise statement).

Main Theorem *Let $f_1, \ldots, f_n$ be polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ such that the system $f_1 = 0, \ldots, f_n = 0$ defines a zero-dimensional affine subvariety V of $\mathbb{C}^n$. Denote by $\Delta_1, \ldots, \Delta_n \subset \mathbb{Z}^n_{\geq 0}$ the supports of $f_1, \ldots, f_n$, and assume that $0 \in \Delta_i$ for $1 \leq i \leq n$ and the mixed volume D of the Newton polytopes $Q_1 := \mathrm{Conv}(\Delta_1), \ldots, Q_n := \mathrm{Conv}(\Delta_n)$ is nonzero.*

Then, we can probabilistically compute a geometric solution of the variety V using $O^{\sim}(NDD')$ arithmetic operations in $\mathbb{Q}$, with $N := \sum_{1 \leq i \leq n} \#\Delta_i$ and $D' := \sum_{1 \leq i \leq n} \mathcal{M}(\Delta, Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n)$, where Δ denotes the standard n-dimensional simplex and $\mathcal{M}$ stands for mixed volume.

Here $O^{\sim}$ refers to the standard Soft-Oh notation which does not take into account logarithmic terms. Further, we have ignored terms depending polynomially on n and the size of certain combinatorial objects associated to the polyhedral deformation.

Our algorithms are of *Monte Carlo* or *BPP* type (see, e.g., [3, 59, 61]), i.e., they return the correct output with probability at least a fixed value strictly greater than $1/2$. This means that the error probability can be made arbitrarily small by iteration of the algorithms. On the other hand, our algorithms do not seem to be of *Las Vegas* or *ZPP* type, i.e., we have no means of checking the correctness of our output results. We observe that the probabilistic aspect of our algorithms is related to the random choice of points outside certain Zariski closed subsets of suitable affine spaces, whose probability of success is explicitly estimated.

We assume that the combinatorics of the polyhedral deformation mentioned above are known. More precisely, we assume that we are given a certain collection of subsets of the input supports $\Delta_1, \ldots, \Delta_n$, which defines a *fine-mixed subdivision* of

$\Delta_1, \ldots, \Delta_n$, together with the *lifting function* which yields such a subdivision (for precise definitions see [26, Sect. 2] or Sect. 2.1 below). For an efficient algorithm computing these objects see, for instance, [33].

The input of our algorithm is the standard sparse representation of the polynomials $f_1, \ldots, f_n \in \mathbb{Q}[X_1, \ldots, X_n]$, that is, the list of exponents of all nonzero monomials arising in $f_1, \ldots, f_n$ together with the corresponding coefficients. Nevertheless, n-variate polynomials which arise as intermediate results of our algorithm will be usually represented by an algorithm which allows their evaluation at a generic value of $\mathbb{C}^n$ by means of a sequence of arithmetic operations or *straight-line program* (see Sect. 2.2). We observe that in our setting there are no significant differences between the sparse and the straight-line program representation. Indeed, any polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$ of degree at most $d > 0$ having support $\Delta \subset \mathbb{Z}^n_{\geq 0}$ can be evaluated with $O(n\#\Delta \log d)$ arithmetic operations in $\mathbb{C}$. In this sense, we see that f has a straight-line program representation whose size is of the same order as its standard sparse representation, and can be efficiently obtained from the latter. On the other hand, from a straight-line program which evaluates a polynomial $f \in \mathbb{Q}[X_1, \ldots, X_n]$ of (known) support Δ with $\mathcal{L}$ arithmetic operations, the corresponding sparse representation can be easily obtained by a process of multipoint evaluation and interpolation with cost $O(\mathcal{L}\#\Delta)$, up to logarithmic terms. Since the routines of our procedure are of black-box type (cf. [13]), that is, they only call the input polynomials and their first derivatives for substitutions of the variables $X_1, \ldots, X_n$ into values belonging to suitable commutative zero-dimensional algebras, we conclude that the straight-line program representation of intermediate results is better suited than the sparse one. In particular, we note that computing the first derivatives of a multivariate polynomial can be done more efficiently for polynomials given by straight-line programs than by their sparse encoding (cf. [4]).

The output of the algorithm is a *geometric solution* (also called a *rational univariate representation*) of the zero-dimensional variety V. Roughly speaking, the points of V are parametrized by the values of the image of a linear projection $V \to \mathbb{C}$ defined by a generic linear form with rational coefficients. In order to obtain a "rational" algorithm, we compute a univariate polynomial with rational coefficients whose roots are precisely these values (see Sect. 2.3 for a precise definition of this notion).

The complexity of our algorithm is mainly expressed in terms of three quantities which measure the size of the combinatorial structure of the input system: the number of nonzero coefficients $N := \sum_{1 \leq i \leq n} \#\Delta_i$ and the mixed volumes $D := \mathcal{M}(Q_1, \ldots, Q_n)$ and $D' := \sum_{1 \leq i \leq n} \mathcal{M}(\Delta, Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n)$. While D represents the (optimal) number of paths which are followed during our homotopy, the quantity D' is an arithmetic analogue of D (see [43, 44]) which measures the "precision" at which the paths of our homotopy must be followed. We observe that the invariant D' is also optimal for a generic choice of the coefficients of the polynomials $f_1, \ldots, f_n$ (see Lemma 2.3 below; compare also with [45, Theorem 1.1]). Therefore, we may paraphrase our complexity estimate as saying that it is *cubic* in the combinatorial structure of the input system, with a geometric component, an arithmetic component and a component related to the size of the input data. In this sense, we see that the cost of our algorithm

strongly resembles the cost $O(NDμ^2)$ of numerical continuation algorithms, where $μ$ is the highest sparse condition number arising from the application of the Implicit Function Theorem to the points of the paths which are followed (cf. [15]; see also [36] for a probability analysis of the condition numbers of sparse systems).

Our result improves and refines the estimate of [8] in the case of a sparse system, which is expressed as a fourth power of D and the maximum of the degrees of two varieties associated with the input (we observe that this maximum is an upper bound for the parameter D'). On the other hand, it also improves [46, 47], which solve a sparse system with a complexity which is roughly quartic in the size of the combinatorial structure of the input system. Finally, throughout the paper we provide explicit estimates of the error probability of all the steps of our algorithm. This might be seen as a further contribution to the symbolic stage of the probabilistic seminumeric method of [26], which lacks such analysis of error probability.

The algorithm proceeds in two main steps: in the first step, the polyhedral deformation introduced in [26] is applied to solve an auxiliary generic sparse system with the same structure as the input polynomials (Sect. 5; see also Sect. 4 for a discussion on the genericity conditions underlying the choice of the coefficients of the corresponding polynomials). In the second step, the solutions of this generic system enable us to recover the solutions of the given system by means of a standard homotopic deformation (see Sect. 6).

In the first step, in order to solve a generic sparse system $h_1 = 0, \ldots, h_n = 0$ with supports $Δ_1, \ldots, Δ_n$, the polyhedral homotopy of [26] introduces a new variable T and deforms the polynomial h_i by multiplying each nonzero monomial of h_i by a power of T (which is determined by the given lifting function). The roots of the resulting parametric system are algebraic functions of the parameter T whose expansions as Puiseux series can be obtained by "lifting" the solutions to certain associated zero-dimensional polynomial systems that can be easily solved due to their specific structure (see Sect. 5.2 for details). This enables us to compute a geometric solution of the zero set of this parametric system (Sect. 5.3). Substituting 1 for T in the computed polynomials, a geometric solution of the set of common zeros of $h_1, \ldots, h_n$ is obtained (Sect. 5.4).

For the sake of comprehensiveness, throughout Sects. 4 and 5 the whole first step of the algorithm will be illustrated with a bivariate polynomial example borrowed from [26, Example 2.7].

After solving the system $h_1 = 0, \ldots, h_n = 0$, in the second step the solutions to the input system $f_1 = 0, \ldots, f_n = 0$ are recovered by considering a second homotopy of type $Tf_1 + (1 - T)h_1, \ldots, Tf_n + (1 - T)h_n$ (see Sect. 6). As in the first step, the algorithm first solves this parametric system (Sect. 6.1) and then, substituting 1 for T, a complete representation of the solution set of the input system is obtained. This representation eventually includes multiplicities, which are removed in a further computation (Sect. 6.2).

2 Preliminaries

2.1 Sparse Elimination

Here we introduce some notions and notations of convex geometry and sparse elimination theory (see, e.g., [19, 26, 48]) that will be used in the sequel.

2.1.1 Basic Notions

Let $X_1, \ldots, X_n$ be indeterminates over $\mathbb{Q}$ and write $X := (X_1, \ldots, X_n)$. For $q := (q_1, \ldots, q_n) \in \mathbb{Z}^n$, we use the notation $X^q := X_1^{q_1} \cdots X_n^{q_n}$. Let $f := \sum_q c_q X^q$ be a Laurent polynomial in $\mathbb{Q}[X, X^{-1}] := \mathbb{Q}[X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}]$. By the support of f we understand the subset of $\mathbb{Z}^n$ defined by the elements $q \in \mathbb{Z}^n$ for which $c_q \neq 0$ holds. The Newton polytope of f is the convex hull of the support of f in $\mathbb{R}^n$.

A sparse polynomial system with supports $\Delta_1, \ldots, \Delta_n \subset \mathbb{Z}^n_{\geq 0}$ is defined by polynomials

$$f_i(X) := \sum_{q \in \Delta_i} a_{i,q} X^q \quad (1 \leq i \leq n),$$

with $a_{i,q} \in \mathbb{C} \setminus \{0\}$ for each $q \in \Delta_i$ and $1 \leq i \leq n$.

For a finite subset Δ of $\mathbb{Z}^n$, we denote by $Q := \mathrm{Conv}(\Delta)$ its convex hull in $\mathbb{R}^n$. The usual Euclidean volume of a polytope Q in $\mathbb{R}^n$ will be denoted by $\mathrm{Vol}_{\mathbb{R}^n}(Q)$.

Let $Q_1, \ldots, Q_n$ be polytopes in $\mathbb{R}^n$. For $\lambda_1, \ldots, \lambda_n \in \mathbb{R}_{\geq 0}$, we use the notation $\lambda_1 Q_1 + \cdots + \lambda_n Q_n$ to refer to the Minkowski sum $\lambda_1 Q_1 + \cdots + \lambda_n Q_n := \{x \in \mathbb{R}^n : x = \lambda_1 x_1 + \cdots + \lambda_n x_n \text{ with } x_1 \in Q_1, \ldots, x_n \in Q_n\}$. Consider the real-valued function $(\lambda_1, \ldots, \lambda_n) \mapsto \mathrm{Vol}_{\mathbb{R}^n}(\lambda_1 Q_1 + \cdots + \lambda_n Q_n)$. This is a homogeneous polynomial function of degree n in the λ_i (see, e.g., [14, Chap. 7, Proposition §4.4.9]). The mixed volume $\mathcal{M}(Q_1, \ldots, Q_n)$ of $Q_1, \ldots, Q_n$ is defined as the coefficient of the monomial $\lambda_1 \cdots \lambda_n$ in $\mathrm{Vol}_{\mathbb{R}^n}(\lambda_1 Q_1 + \cdots + \lambda_n Q_n)$.

For $i = 1, \ldots, n$, let Δ_i be a finite subset of $\mathbb{Z}^n_{\geq 0}$ and let $Q_i := \mathrm{Conv}(\Delta_i)$ denote the corresponding polytope. Let $f_1, \ldots, f_n$ be a sparse polynomial system with respect to $\Delta_1, \ldots, \Delta_n$. The BKK theorem ([5, 29, 30]) asserts that the system $f_1 = 0, \ldots, f_n = 0$ has at most $\mathcal{M}(Q_1, \ldots, Q_n)$ isolated common solutions in the n-dimensional torus $(\mathbb{C}^*)^n$, with equality for generic choices of the coefficients of $f_1, \ldots, f_n$. Furthermore, if the condition $0 \in Q_i$ holds for $1 \leq i \leq n$, then $\mathcal{M}(Q_1, \ldots, Q_n)$ bounds the number of solutions in $\mathbb{C}^n$ (see [35]).

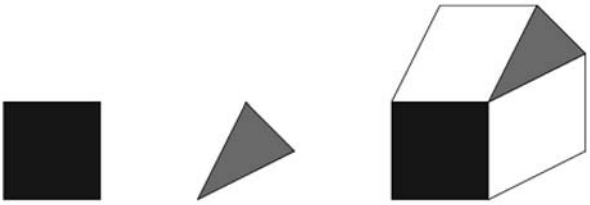
Example Let $\Delta_1 := \{(0,0), (2,0), (0,2), (2,2)\}$ and $\Delta_2 := \{(0,0), (1,2), (2,1)\}$ in $\mathbb{Z}^2$. A sparse polynomial system with supports Δ_1, Δ_2 is a system defined by polynomials of the following type:

$$\begin{cases} f_1 = a_{(0,0)} + a_{(2,0)} X_1^2 + a_{(0,2)} X_2^2 + a_{(2,2)} X_1^2 X_2^2, \\ f_2 = b_{(0,0)} + b_{(1,2)} X_1 X_2^2 + b_{(2,1)} X_1^2 X_2, \end{cases} \tag{2.1}$$

with $a_q, b_q \in \mathbb{C} \setminus \{0\}$.

Let $Q_1 := \mathrm{Conv}(\Delta_1)$ and $Q_2 := \mathrm{Conv}(\Delta_2)$. Then $\mathcal{M}(Q_1, Q_2) = \mathrm{Vol}_{\mathbb{R}^2}(Q_1 + Q_2) - \mathrm{Vol}_{\mathbb{R}^2}(Q_1) - \mathrm{Vol}_{\mathbb{R}^2}(Q_2) = 8$.

The pictures of Q_1, Q_2 and $Q_1 + Q_2$ are, respectively,



2.1.2 Mixed Subdivisions

Assume that the union of the sets $\Delta_1, \ldots, \Delta_n$ affinely generates $\mathbb{Z}^n$, and consider the partition of $\Delta_1, \ldots, \Delta_n$ defined by the relation $\Delta_i \sim \Delta_j$ if and only if $\Delta_i = \Delta_j$. Let $s \in \mathbb{N}$ denote the number of classes in this partition, and let $\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(s)} \subset \mathbb{Z}^n$ denote a member in each class. Write $\mathcal{A} := (\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(s)})$. For $\ell = 1, \ldots, s$, let $k_\ell := \#\{i : \Delta_i = \mathcal{A}^{(\ell)}\}$. Without loss of generality, we will assume that $\Delta_1 = \cdots = \Delta_{k_1} = \mathcal{A}^{(1)}$, $\Delta_{k_1+1} = \cdots = \Delta_{k_1+k_2} = \mathcal{A}^{(2)}$ and so on.

A cell of $\mathcal{A}$ is a tuple $C = (C^{(1)}, \ldots, C^{(s)})$ with $C^{(\ell)} \neq \emptyset$ and $C^{(\ell)} \subset \mathcal{A}^{(\ell)}$ for $1 \leq \ell \leq s$. We define

$$\begin{aligned}
\mathrm{type}(C) &:= \big(\dim\big(\mathrm{Conv}\big(C^{(1)}\big)\big), \ldots, \dim\big(\mathrm{Conv}\big(C^{(s)}\big)\big)\big),\\
\mathrm{Conv}(C) &:= \mathrm{Conv}\big(C^{(1)} + \cdots + C^{(s)}\big),\\
\#(C) &:= \#\big(C^{(1)}\big) + \cdots + \#\big(C^{(s)}\big),\\
\mathrm{Vol}_{\mathbb{R}^n}(C) &:= \mathrm{Vol}_{\mathbb{R}^n}\big(\mathrm{Conv}(C)\big).
\end{aligned}$$

A face of a cell C is a cell $\mathcal{C} = (\mathcal{C}^{(1)}, \ldots, \mathcal{C}^{(s)})$ of C with $\mathcal{C}^{(\ell)} \subset C^{(\ell)}$ for $1 \leq \ell \leq s$ such that there exists a linear functional $\gamma : \mathbb{R}^n \to \mathbb{R}$ that takes its minimum over $C^{(\ell)}$ at $\mathcal{C}^{(\ell)}$ for $1 \leq \ell \leq s$. One such functional γ is called an inner normal of C.

A mixed subdivision of $\mathcal{A}$ is a collection of cells $\mathfrak{C} = \{C_1, \ldots, C_m\}$ of $\mathcal{A}$ satisfying conditions (1)–(4) below:

(1) $\dim(\mathrm{Conv}(C_j)) = n$ for $1 \leq j \leq m$.
(2) The intersection $\mathrm{Conv}(C_i) \cap \mathrm{Conv}(C_j) \subset \mathbb{R}^n$ is either the empty set or a face of both $\mathrm{Conv}(C_i)$ and $\mathrm{Conv}(C_j)$ for $1 \leq i < j \leq m$.
(3) $\bigcup_{j=1}^m \mathrm{Conv}(C_j) = \mathrm{Conv}(\mathcal{A})$.
(4) $\sum_{\ell=1}^s \dim(\mathrm{Conv}(C_j^{(\ell)})) = n$ for $1 \leq j \leq m$.

If $\mathfrak{C}$ also satisfies the condition:

(5) $\#(C_j) = n + s$ for $1 \leq j \leq m$

we say that $\mathfrak{C}$ is a fine-mixed subdivision of $\mathcal{A}$. Observe that, as a consequence of conditions (4) and (5), for each cell $C_j = (C_j^{(1)}, \ldots, C_j^{(s)})$ in a fine-mixed subdivision

the identity $\dim(\mathrm{Conv}(C_j^{(\ell)})) = \#C_j^{(\ell)} - 1$ holds for $1 \le \ell \le s$. In the sequel, we are going to consider only those cells of type $(k_1, \ldots, k_s)$ in a fine-mixed subdivision.

We point out that a mixed subdivision $\mathfrak{C}$ of $\mathcal{A}$ enables us to compute the mixed volume of the family $Q_1 = \mathrm{Conv}(\Delta_1), \ldots, Q_n = \mathrm{Conv}(\Delta_n)$ by means of the following identity (see [26, Theorem 2.4]):

$$\mathcal{M}(Q_1, \ldots, Q_n) = \sum_{\substack{C_i \in \mathfrak{C} \\ \mathrm{type}(C_i) = (k_1, \ldots, k_s)}} k_1! \ldots k_s! \cdot \mathrm{Vol}_{\mathbb{R}^n}(C_i). \tag{2.2}$$

A fine-mixed subdivision of $\mathcal{A}$ can be obtained by means of a lifting process as explained in what follows. For $1 \le \ell \le s$, let $\omega_\ell : \mathcal{A}^{(\ell)} \to \mathbb{R}$ be an arbitrary function. The tuple $\omega := (\omega_1, \ldots, \omega_s)$ is called a lifting function for $\mathcal{A}$. Once a lifting function ω is fixed, the graph of any subset $C^{(\ell)}$ of $\mathcal{A}^{(\ell)}$ will be denoted by $\widehat{C}^{(\ell)} := \{(q, \omega_\ell(q)) \in \mathbb{R}^{n+1} : q \in C^{(\ell)}\}$. Then, for a sufficiently generic lifting function ω, the set of cells C of $\mathcal{A}$ satisfying the conditions:

(i) $\dim(\mathrm{Conv}(\widehat{C}^{(1)} + \cdots + \widehat{C}^{(s)})) = n$; and
(ii) $(\widehat{C}^{(1)}, \ldots, \widehat{C}^{(s)})$ is a face of $(\widehat{\mathcal{A}}^{(1)}, \ldots, \widehat{\mathcal{A}}^{(s)})$ whose inner normal has positive last coordinate

is a fine-mixed subdivision of $\mathcal{A}$ (see [26, Sect. 2]).

Example We continue with the example introduced at the end of the previous subsection. Here $\mathcal{A} := (\mathcal{A}^{(1)}, \mathcal{A}^{(2)})$, where $\mathcal{A}^{(1)} := \Delta_1$ and $\mathcal{A}^{(2)} := \Delta_2$.

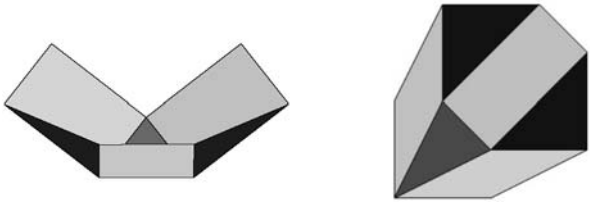
Following [26, Example 2.7], the lifting function $\omega = (\omega_1, \omega_2)$ defined by

$$\omega_1(q) := \begin{cases} 0 & \text{for } q = (0,0), \\ 1 & \text{for } q \in \mathcal{A}^{(1)} \backslash \{(0,0)\}, \end{cases} \quad \text{and} \quad \omega_2(q) := 0 \text{ for every } q \in \mathcal{A}^{(2)}, \tag{2.3}$$

induces a fine-mixed subdivision of $\mathcal{A}$. More precisely, such a fine-mixed subdivision consists of the set of cells satisfying conditions (i) and (ii) above, which are listed below together with the inner normals of the faces they come from:

- $C_1 := \{\{(0,0), (0,2)\}, \{(0,0), (1,2)\}\}$, $\gamma^{(1)} := (2, -1, 2)$.
- $C_2 := \{\{(0,0), (2,0)\}, \{(0,0), (2,1)\}\}$, $\gamma^{(2)} := (-1, 2, 2)$.
- $C_3 := \{\{(0,0), (2,2)\}, \{(1,2), (2,1)\}\}$, $\gamma^{(3)} := (-1, -1, 4)$.
- $C_4 := \{\{(0,0)\}, \{(0,0), (1,2), (2,1)\}\}$, $\gamma^{(4)} := (0, 0, 1)$.
- $C_5 := \{\{(0,0), (0,2), (2,2)\}, \{(1,2)\}\}$, $\gamma^{(5)} := (0, -1, 2)$.
- $C_6 := \{\{(0,0), (2,0), (2,2)\}, \{(2,1)\}\}$, $\gamma^{(6)} := (-1, 0, 2)$.

The pictures below show the lower envelope of $\widehat{\mathcal{A}}^{(1)} + \widehat{\mathcal{A}}^{(2)} \subset \mathbb{R}^3$ and its projection to $\mathbb{R}^2$, respectively.



Note that the cells of type $(k_1, k_2) = (1, 1)$ are C_1, C_2 and C_3.

The following result (cf. [26, Sect. 2]) states a generic condition for a lifting function to induce a fine-mixed subdivision.

Lemma 2.1 *The lifting process associated to a lifting function ω yields a fine-mixed subdivision of $\mathcal{A}$ if the following condition holds*: *for every $r_1, \ldots, r_s \in \mathbb{Z}_{\geq 0}$ with $\sum_{\ell=1}^{s} r_\ell > n$ and every cell $(C^{(1)}, \ldots, C^{(s)})$ with $C^{(\ell)} := \{q_{\ell,0}, \ldots, q_{\ell,r_\ell}\} \subset \mathcal{A}^{(\ell)}$ $(1 \leq \ell \leq s)$, if*

$$V(C) := \begin{pmatrix} q_{1,1} - q_{1,0} \\ \vdots \\ q_{1,r_1} - q_{1,0} \\ \cdots \\ \cdots \\ q_{s,1} - q_{s,0} \\ \vdots \\ q_{s,r_s} - q_{s,0} \end{pmatrix} \quad \textit{and} \quad V\big(\widehat{C}\big) := \begin{pmatrix} q_{1,1} - q_{1,0} & \omega_1(q_{1,1}) - \omega_1(q_{1,0}) \\ \vdots & \vdots \\ q_{1,r_1} - q_{1,0} & \omega_1(q_{1,r_1}) - \omega_1(q_{1,0}) \\ \cdots & \cdots \\ \cdots & \cdots \\ q_{s,1} - q_{s,0} & \omega_s(q_{s,1}) - \omega_s(q_{s,0}) \\ \vdots & \vdots \\ q_{s,r_s} - q_{s,0} & \omega_s(q_{s,r_s}) - \omega_s(q_{s,0}) \end{pmatrix},$$

then $\operatorname{rank}(V(C)) = n$ *implies* $\operatorname{rank}(V(\widehat{C})) = n + 1$.

Proof Notice that (1)–(3) are automatically satisfied by the set of cells defined by conditions (i)–(ii). Assume that the condition of the statement of the lemma is met and consider a cell $C = (C^{(1)}, \ldots, C^{(s)})$ of $\mathcal{A}$ satisfying conditions (i) and (ii) above. $\widehat{C}$ being a *lower* facet of $\mathcal{A}$, the identity $\dim(\operatorname{Conv}(C^{(1)} + \cdots + C^{(s)})) = \dim(\operatorname{Conv}(\widehat{C}^{(1)} + \cdots + \widehat{C}^{(s)}))$ must hold. Write $C^{(\ell)} = \{q_{\ell,0}, \ldots, q_{\ell,r_\ell}\}$ for $1 \leq \ell \leq s$. Then we have that $\operatorname{rank}(V(C)) = \dim(\langle q_{\ell,j} - q_{\ell,0} : 1 \leq \ell \leq r_\ell,\ 1 \leq j \leq r_j \rangle) = \dim(\operatorname{Conv}(C^{(1)} + \cdots + C^{(s)})) = n$ and $\operatorname{rank}(V(\widehat{C})) = \dim(\operatorname{Conv}(\widehat{C}^{(1)} + \cdots + \widehat{C}^{(s)})) = n$. Now, the condition stated on ω implies that $\sum_{\ell=1}^{s} r_\ell \leq n$ and, taking into account that the $\sum_{\ell=1}^{s} r_\ell$ many vectors $q_{\ell,j} - q_{\ell,0}$ $(1 \leq \ell \leq s,\ 1 \leq j \leq r_\ell)$ span a linear space of dimension n, we conclude that the equality $\sum_{\ell=1}^{s} r_\ell = n$ holds, which shows that condition (5) in the definition of a fine-mixed subdivision is met. Moreover, as $\sum_{\ell=1}^{s} \dim(\operatorname{Conv}(C^{(\ell)})) \geq \dim(\operatorname{Conv}(C^{(1)} + \cdots + C^{(s)}))$ holds for an arbitrary cell C, we see that $\dim(\operatorname{Conv}(C^{(\ell)})) = r_\ell$ holds for every $1 \leq \ell \leq s$, which implies that condition (4) is also valid. This finishes the proof of the lemma. □

Note that the condition $\operatorname{rank}(V(\widehat{C})) = n + 1$ can be restated as the nonvanishing of the maximal minors of the matrix $V(\widehat{C})$. Since $\operatorname{rank}(V(C)) = n$, these maximal minors are nonzero linear forms in the unknown values $\omega_\ell(q_{\ell,j})$ of the lifting function. Thus, if $\mathcal{N}_\ell = \#\mathcal{A}^{(\ell)}$ for every $1 \leq \ell \leq s$, a sufficiently generic lifting function can be obtained by randomly choosing the values $\omega_\ell(q_{\ell,j})$ of ω at the points of $\mathcal{A}^{(\ell)}$ from the set $\{1, 2, \ldots, \rho 2^{\mathcal{N}_1 + \cdots + \mathcal{N}_s}\}$, with probability of success at least $1 - 1/\rho$ for $\rho \in \mathbb{N}$.

In this paper we shall assume that a sufficiently generic lifting function and the induced fine-mixed subdivision of $\mathcal{A}$ are given.

2.2 Complexity Model and Complexity Estimates

In this section we describe our computational model and briefly mention efficient algorithms for some basic specific algebraic tasks.

2.2.1 Complexity Model

Algorithms in computational algebraic geometry are usually described using the standard dense or sparse complexity model, i.e., encoding multivariate polynomials by means of the vector of all or of all nonzero coefficients. Nevertheless, for algorithms of black-box type (cf. [13]), that is, algorithms that only call the input polynomials for substitutions of their variables into values belonging to suitable commutative zero-dimensional algebras, other representations more suitable for evaluation may be convenient. In this paper we are going to use an alternative encoding of intermediate results of our computations by means of straight-line programs (cf. [11, 23, 40, 55]). A straight-line program β in $\mathbb{Q}(X) := \mathbb{Q}(X_1, \ldots, X_n)$ is a finite sequence of rational functions $(f_1, \ldots, f_k) \in \mathbb{Q}(X)^k$ such that for $1 \le i \le k$, the function f_i is an element of the set $\{X_1, \ldots, X_n\}$, or an element of $\mathbb{Q}$ (a *parameter*), or there exist $1 \le i_1, i_2 < i$ such that $f_i = f_{i_1} \circ_i f_{i_2}$ holds, where $\circ_i$ is one of the arithmetic operations $+, -, \times, \div$. The straight-line program β is called division-free if $\circ_i$ is different from $\div$ for $1 \le i \le k$. A natural measure of the complexity of β is its time or length (cf. [11, 51]), which is the total number of arithmetic operations performed during the evaluation process defined by β. We say that the straight-line program β computes or represents a subset S of $\mathbb{Q}(X)$ if $S \subset \{f_1, \ldots, f_k\}$ holds.

Our model of computation is based on the concept of straight-line programs. However, a model of computation consisting *only* of straight-line programs is not expressive enough for our purposes. Therefore we allow our model to include decisions and selections (subject to previous decisions). For this reason we shall also consider computation trees, which are straight-line programs with branchings. Time of the evaluation of a given computation tree is defined similarly to the case of straight-line programs (see, e.g., [11, 58] for more details on the notion of computation trees).

2.2.2 Probabilistic Identity Testing

A difficult point in the manipulation of multivariate polynomials given by straight-line programs is the so-called identity testing problem: given two elements f and g of $\mathbb{C}[X] := \mathbb{C}[X_1, \ldots, X_n]$, decide whether f and g represent the same polynomial function on $\mathbb{C}^n$. Indeed, all known deterministic algorithms solving this problem have complexity at least $\max\{\deg f, \deg g\}^{\Omega(1)}$. In this paper we are going to use *probabilistic* algorithms to solve the identity testing problem, based on the following result.

Theorem 2.2 [59, Lemma 6.44] *Let f be a nonzero polynomial of $\mathbb{C}[X]$ of degree at most d and let $\mathcal{S}$ be a finite subset of $\mathbb{C}$. Then the number of zeros of f in $\mathcal{S}^n$ is at most $d(\#\mathcal{S})^{n-1}$.*

For the analysis of our algorithms, we shall interpret the statement of Theorem 2.2 in terms of probabilities. More precisely, given a fixed nonzero polynomial f in

$\mathbb{C}[X_1, \ldots, X_n]$ of degree at most d, we conclude from Theorem 2.2 that the probability of choosing randomly a point $a \in \mathcal{S}^n$ such that $f(a) = 0$ holds is bounded from above by $d/\#\mathcal{S}$ (assuming a uniform distribution of probability on the elements of $\mathcal{S}^n$).

2.2.3 Basic Complexity Estimates

In order to estimate the complexity of our procedures we shall frequently use the notation $\mathsf{M}(m) := m \log^2 m \log\log m$. Here and in the sequel log will denote logarithm to the base 2. Let R be a commutative ring of characteristic zero with unity. We recall that the number of arithmetic operations in R necessary to compute the multiplication or division with remainder of two univariate polynomials in $R[T]$ of degree at most m is $O(\mathsf{M}(m)/\log(m))$ (cf. [6, 59]). Multipoint evaluation and interpolation of univariate polynomials of $R[T]$ of degree m at *invertible* points $a_1, \ldots, a_m \in R$ can be performed with $O(\mathsf{M}(m))$ arithmetic operations in R (see, e.g., [9]).

If $R = k$ is a field, then we shall use algorithms based on the Extended Euclidean Algorithm (EEA for short) in order to compute the gcd or resultant of two univariate polynomials in $k[T]$ of degree at most m with $O(\mathsf{M}(m))$ arithmetic operations in k (cf. [6, 59]). We use Padé approximation in order to compute the dense representation of the numerator and denominator of a rational function $f = p/q \in k(T)$ with $\max\{\deg p, \deg q\} \leq m$ from its Taylor series expansion up to order $2m$. This also requires $O(\mathsf{M}(m))$ arithmetic operations in k ([6, 59]).

For brevity, we will denote by Ω the exponent that appears in the complexity estimate $O(n^\Omega)$ for the multiplication of two $(n \times n)$-matrices with coefficients in $\mathbb{Q}$. We remark that the (theoretical) bound $\Omega < 2.376$ is typically impractical and we prefer to take $\Omega := \log 7 \sim 2.81$ (cf. [6]).

2.3 Geometric Solutions

The notion of a geometric solution of an algebraic variety was first introduced in the works of Kronecker and König in the last years of the nineteenth century. Nowadays, geometric solutions are widely used in computer algebra as a suitable representation of algebraic varieties, especially in the zero-dimensional case.

In this subsection we first introduce this notion in the case of zero-dimensional varieties and curves. Then we state degree estimates for the polynomials involved in a geometric solution of a variety defined by a sparse system. Finally, we show how to extend any algorithm computing generic eliminating polynomials to a procedure for the computation of a geometric solution.

2.3.1 Geometric Solutions of Zero-Dimensional Varieties and Curves

Let $\overline{K}$ denote an algebraic closure of a field K of characteristic zero, let $\mathbb{A}^n(\overline{K})$ be the n-dimensional space $\overline{K}^n$ endowed with its Zariski topology, and let $V = \{\xi^{(1)}, \ldots, \xi^{(D)}\}$ be a zero-dimensional subvariety of $\mathbb{A}^n(\overline{K})$ defined over K. A geometric solution of V consists of:

- A linear form $u = u_1 X_1 + \cdots + u_n X_n \in K[X]$ which separates the points of V, i.e., satisfying $u(\xi^{(i)}) \neq u(\xi^{(k)})$ if $i \neq k$.

- The minimal polynomial $m_u := \prod_{1 \le i \le D}(Y - u(\xi^{(i)})) \in K[Y]$ of u in V (where Y is a new variable).
- Polynomials $w_1, \ldots, w_n \in K[Y]$ with $\deg w_j < D$ for every $1 \le j \le n$ satisfying

$$V = \left\{\left(w_1(\eta), \ldots, w_n(\eta)\right) \in \overline{K}^n : \eta \in \overline{K}, m_u(\eta) = 0\right\}.$$

In the sequel, we shall be given a polynomial system $f_1 = 0, \ldots, f_n = 0$ of n-variate polynomials of $\mathbb{Q}[X]$ defining a zero-dimensional affine variety $V \subset \mathbb{A}^n := \mathbb{A}^n(\mathbb{C})$. We shall consider the system $f_1 = 0, \ldots, f_n = 0$ (symbolically) "solved" if we obtain a geometric solution of V as defined above.

Example Let $f_1, f_2 \in \mathbb{Q}[X_1, X_2]$ be the following polynomials:

$$f_1 := X_1^3 - 3X_1^2X_2 + 3X_1X_2^2 - X_2^3 - 11X_1 + 9X_2 + 8,$$
$$f_2 := X_1^2 - 2X_1X_2 + X_2^2 - 3X_1 + 2X_2 + 1,$$

which define the zero-dimensional variety $V := \{(4, 1), (0, -1), (9, 11)\}$ in $\mathbb{C}^2$. Let $u := X_1 - X_2 \in \mathbb{Q}[X_1, X_2]$. Note that u is a separating linear form for V. The geometric solution of V associated with u consists of:

- The minimal polynomial $m_u := (Y - 3)(Y - 1)(Y + 2) = Y^3 - 2Y^2 - 5Y + 6$.
- The polynomials $w_1 := Y^2 - 2Y + 1$ and $w_2 := Y^2 - 3Y + 1$, which satisfy the identities $(w_1(3), w_2(3)) = (4, 1)$, $(w_1(1), w_2(1)) = (0, -1)$ and $(w_1(-2), w_2(-2)) = (9, 11)$.

The notion of geometric solution can be extended to equidimensional varieties of positive dimension. For our purposes, it will be sufficient to consider the case of an algebraic curve defined over $\mathbb{Q}$.

Suppose that we are given a curve $V \subset \mathbb{A}^{n+1}$ defined by polynomials $f_1, \ldots, f_n \in \mathbb{Q}[X, T]$. Assume that for each irreducible component C of V, the identity $I(C) \cap \mathbb{Q}[T] = \{0\}$ holds. Let u be a nonzero linear form of $\mathbb{Q}[X]$ and $\pi_u : V \to \mathbb{A}^2$ the morphism defined by $\pi_u(x, t) := (t, u(x))$. Our assumptions on V imply that the Zariski closure $\overline{\pi_u(V)}$ of the image of V under π_u is a hypersurface of $\mathbb{A}^2$ defined over $\mathbb{Q}$. Let Y be a new indeterminate. Then there exists a unique (up to scaling by nonzero elements of $\mathbb{Q}$) polynomial $M_u \in \mathbb{Q}[T, Y]$ of minimal degree defining $\overline{\pi_u(V)}$. Let $m_u \in \mathbb{Q}(T)[Y]$ denote the (unique) monic multiple of M_u with $\deg_Y(m_u) = \deg_Y(M_u)$. We call m_u the *minimal polynomial* of u in V. In these terms, a geometric solution of the curve V consists of:

- A *generic* linear form $u \in \mathbb{Q}[X]$.
- The minimal polynomial $m_u \in \mathbb{Q}(T)[Y]$.
- Elements $v_1, \ldots, v_n$ of $\mathbb{Q}(T)[Y]$ such that $(\partial m_u/\partial Y)(u)X_i \equiv v_i(u) \bmod \mathbb{Q}(T) \otimes \mathbb{Q}[V]$ and $\deg_Y(v_i) < \deg_Y(m_u)$ holds for $1 \le i \le n$.

We observe that $\deg_Y m_u$ equals the cardinality of the zero-dimensional variety defined by $f_1, \ldots, f_n$ over $\mathbb{A}^n(\overline{\mathbb{Q}(T)})$.

2.3.2 Degree Estimates in the Sparse Setting

In the sequel, we shall deal with curves $V := V(f_1, \ldots, f_n) \subset \mathbb{A}^{n+1}$ as above. The complexity of the algorithms for solving the systems $f_1 = 0, \ldots, f_n = 0$ defining such curves will be expressed mainly by means of two discrete invariants: the *degree* and the *height* of the projection $\pi : V \to \mathbb{A}^1$. The degree of π is defined as the degree $\deg m_u = \deg_Y M_u$ of the minimal polynomial of a generic linear form $u \in \mathbb{Q}[X_1, \ldots, X_n]$ and can be considered as a measure of the "complexity" of the curve V. On the other hand, the height of π is defined as $\deg_T M_u$ and may be considered as a measure of the "complexity of the description" of the curve V.

In the sparse setting, we can estimate $\deg_Y M_u$ and $\deg_T M_u$ in terms of combinatorial quantities (namely, mixed volumes) associated to the polynomial system under consideration (see also [45]).

Lemma 2.3 *Let assumptions and notations be as above. For $1 \le i \le n$, let $Q_i \subset \mathbb{R}^n$ be the Newton polytope of f_i, considering f_i as an element of $\mathbb{Q}(T)[X]$. Let $\widehat{Q}_1, \ldots, \widehat{Q}_n \subset \mathbb{R}^{n+1}$ be the Newton polytopes of $f_1, \ldots, f_n$, considering $f_1, \ldots, f_n$ as elements of $\mathbb{Q}[X, T]$, and let $\Delta \subset \mathbb{R}^{n+1}$ be the standard n-dimensional simplex in the hyperplane $\{T = 0\}$, i.e., the Newton polytope of a generic linear form $u \in \mathbb{Q}[X]$. Assume that $0 \in \widehat{Q}_i$ for every $1 \le i \le n$. Then the following estimates hold*:

$$\deg_Y M_u \le \mathcal{M}(Q_1, \ldots, Q_n), \qquad \deg_T M_u \le \mathcal{M}\big(\Delta, \widehat{Q}_1, \ldots, \widehat{Q}_n\big). \tag{2.4}$$

Furthermore, if there exist $c_1, \ldots, c_n \in \mathbb{R}_{\ge 0}$ such that $\widehat{Q}_i \subset Q_i \times [0, c_i]$ for $1 \le i \le n$, then the following inequality holds:

$$\deg_T M_u \le \sum_{i=1}^{n} c_i \, \mathcal{M}(\Delta, Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n). \tag{2.5}$$

Proof The upper bound $\deg_Y M_u \le \mathcal{M}(Q_1, \ldots, Q_n)$ follows straightforwardly from the BKK bound and the affine root count in [35].

In order to obtain an upper bound for $\deg_T M_u$, we observe that substituting a generic value $y \in \mathbb{Q}$ for Y we have $\deg_T M_u(T, Y) = \deg_T M_u(T, y) = \#\{t \in \mathbb{C};\, M_u(t, y) = 0\}$. Moreover, it follows that $M_u(t, y) = 0$ if and only if there exists a point $x \in \mathbb{A}^n$ with $y = u(x)$ and $(x, t) \in V$. Therefore, it suffices to estimate the number of points $(x, t) \in \mathbb{A}^{n+1}$ satisfying $u(x) - y = 0$, $f_1(x, t) = 0, \ldots, f_n(x, t) = 0$. Since u is a generic linear form, the system

$$u(X) - y = 0,\ f_1(X, T) = 0, \ldots, f_n(X, T) = 0, \tag{2.6}$$

has finitely many common zeros in $\mathbb{A}^{n+1}$. Combining the BKK bound with the affine root count of [35] we see that there are at most $\mathcal{M}(\Delta, \widehat{Q}_1, \ldots, \widehat{Q}_n)$ solutions of (2.6). We conclude that $\deg_T M_u \le \mathcal{M}(\Delta, \widehat{Q}_1, \ldots, \widehat{Q}_n)$ holds, showing thus (2.4).

In order to prove (2.5), we make use of basic properties of the mixed volume (see, for instance, [18, Chap. IV]). Since $\widehat{Q}_i \subset Q_i \times [0, c_i]$ holds for $1 \le i \le n$, by the monotonicity of the mixed volume we have

$$\mathcal{M}\big(\Delta, \widehat{Q}_1, \ldots, \widehat{Q}_n\big) \le \mathcal{M}\big(\Delta, Q_1 \times [0, c_1], \ldots, Q_n \times [0, c_n]\big).$$

Note that $Q_i \times [0, c_i] = S_{i,0} + S_{i,1}$, where $S_{i,0} = Q_i \times \{0\}$ and $S_{i,1} = \{0\} \times [0, c_i]$ for $i = 1, \ldots, n$. Hence, by multilinearity,

$$\mathcal{M}\big(\Delta, Q_1 \times [0, c_1], \ldots, Q_n \times [0, c_n]\big) = \sum_{(j_1, \ldots, j_n) \in \{0,1\}^n} \mathcal{M}(\Delta, S_{1,j_1}, \ldots, S_{n,j_n}). \tag{2.7}$$

If the vector $(j_1, \ldots, j_n)$ has at least two nonzero coordinates, then two of the sets $S_{1,j_1}, \ldots, S_{n,j_n}$ are parallel line segments; therefore, $\mathcal{M}(\Delta, S_{1,j_1}, \ldots, S_{n,j_n}) = 0$. On the other hand, if j_i is the only nonzero coordinate, the corresponding term in the sum of the right-hand side of (2.7) is

$$\begin{aligned}&\mathcal{M}\big(\Delta, Q_1 \times \{0\}, \ldots, Q_{i-1} \times \{0\}, \{0\} \times [0, c_i], Q_{i+1} \times \{0\}, \ldots, Q_n \times \{0\}\big)\\ &\quad = c_i\, \mathcal{M}(\Delta, Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n).\end{aligned}$$

Finally, for $(j_1 \ldots, j_n) = (0, \ldots, 0)$ we have $\mathcal{M}(\Delta, Q_1 \times \{0\}, \ldots, Q_n \times \{0\}) = 0$ since all the polytopes are included in an n-dimensional subspace.

We conclude that the right-hand side of (2.7) equals the right-hand side of (2.5). This finishes the proof of the lemma. □

Example For the system

$$\begin{cases} a_{(0,0)} + a_{(2,0)} X_1^2 T + a_{(0,2)} X_2^2 T + a_{(2,2)} X_1^2 X_2^2 T = 0, \\ b_{(0,0)} + b_{(1,2)} X_1 X_2^2 + b_{(2,1)} X_1^2 X_2 = 0, \end{cases} \tag{2.8}$$

we have:

- $Q_1 = \mathrm{Conv}(\{(0,0), (0,2), (2,0), (2,2)\})$.
- $Q_2 = \mathrm{Conv}(\{(0,0), (1,2), (2,1)\})$.
- $\widehat{Q}_1 = \mathrm{Conv}(\{(0,0,0), (0,2,1), (2,0,1), (2,2,1)\})$.
- $\widehat{Q}_2 = \mathrm{Conv}(\{(0,0,0), (1,2,0), (2,1,0)\})$.

Therefore, the following upper bounds for the degree of the polynomial M_u hold for any separating linear form u:

$$\deg_Y M_u \le \mathcal{M}(Q_1, Q_2) = 8 =: D, \tag{2.9}$$

$$\deg_T M_u \le \mathcal{M}\big(\Delta, \widehat{Q}_1, \widehat{Q}_2\big) = 3 =: E, \tag{2.10}$$

where $\Delta := \mathrm{Conv}(\{(0,0,0), (1,0,0), (0,1,0)\})$.

2.3.3 Algorithmic Aspects

From the algorithmic point of view, the crucial step towards the computation of a geometric solution of the variety V is the computation of the minimal polynomial m_u of a generic linear form u which separates the points of V. In the remaining part of this section we shall show how we can derive an algorithm for computing the entire geometric solution of a zero-dimensional variety V defined over $\mathbb{Q}$ from a procedure for computing the minimal polynomial of a generic linear form u (cf. [2, 22, 52]).

Let $\Lambda := (\Lambda_1, \ldots, \Lambda_n)$ be a vector of new indeterminates and let $K := \mathbb{Q}(\Lambda)$. Denote by I_K the ideal in $K[X_1, \ldots, X_n]$ which is the extension of the ideal $I := I(V) \subset \mathbb{Q}[X_1, \ldots, X_n]$ of the zero-dimensional variety V, and denote by $B := K[X_1, \ldots, X_n]/I_K$ the corresponding zero-dimensional quotient algebra. Write $V = \{\xi^{(1)}, \ldots, \xi^{(D)}\}$.

Set $U := \Lambda_1 X_1 + \cdots + \Lambda_n X_n \in K[X_1, \ldots, X_n]$ and let $m_U(\Lambda, Y) = \prod_{j=1}^{D}(Y - U(\xi^{(j)})) \in \mathbb{Q}[\Lambda, Y]$ be the minimal polynomial of the linear form U in the extension $K \hookrightarrow B$. Note that $\deg m_U = D$ holds, and that $\partial m_U/\partial Y$ is not a zero divisor in $\mathbb{Q}[\mathbb{A}^n \times V]$. Furthermore, $m_U(\Lambda, U) \in I(\mathbb{A}^n \times V) \subset \mathbb{Q}[\Lambda, X_1, \ldots, X_n]$ holds. Since $I(\mathbb{A}^n \times V)$ is generated by polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$, taking the partial derivative of $m_U(\Lambda, U)$ with respect to the variable Λ_k for $1 \le k \le n$, we conclude that

$$\frac{\partial m_U}{\partial Y}(\Lambda, U)\, X_k + \frac{\partial m_U}{\partial \Lambda_k}(\Lambda, U) \in I\big(\mathbb{A}^n \times V\big). \tag{2.11}$$

Observe that the degree estimate $\deg_Y(\partial m_U/\partial \Lambda_k) \le D - 1$ holds.

Assume that a linear form $u = u_1 X_1 + \cdots + u_n X_n \in \mathbb{Q}[X_1, \ldots, X_n]$ which separates the points of V is given. Substituting u_k for Λ_k in the polynomial $m_U(\Lambda, Y)$ we obtain the minimal polynomial $m_u(Y)$ of u. Furthermore, making the same substitution in the polynomials $(\partial m_U/\partial Y)(\Lambda, Y)\, X_k + (\partial m_U/\partial \Lambda_k)(\Lambda, Y)$ of (2.11) for $1 \le k \le n$ and reducing modulo $m_u(Y)$, we obtain polynomials $(\partial m_u/\partial Y)(Y)X_k - v_k(Y) \in I(V)$ $(1 \le k \le n)$. In particular, we have that the identities

$$\frac{\partial m_u}{\partial Y}(u)X_k = v_k(u) \quad (1 \le k \le n) \tag{2.12}$$

hold in $\mathbb{Q}[V]$. Observe that the minimal polynomial $m_u(Y)$ is square-free, since the linear form u separates the points of V. Therefore, $m_u(Y)$ and $\partial m_u/\partial Y(Y)$ are relatively prime. Thus, multiplying modulo $m_u(Y)$ the polynomials $v_k(Y)$ by the inverse of $(\partial m_u/\partial Y)(Y)$ modulo $m_u(Y)$ we obtain polynomials $w_k(Y) := (\partial m_u/\partial Y)^{-1} v_k(Y)$ $(1 \le k \le n)$ of degree at most $D - 1$ such that

$$X_k = w_k(u) \tag{2.13}$$

holds in $\mathbb{Q}[V]$ for $1 \le k \le n$. The polynomials $m_u, w_1, \ldots, w_n \in \mathbb{Q}[Y]$ form a geometric solution of V.

Now, suppose that we are given an algorithm Ψ over $\mathbb{Q}(\Lambda)$ for computing the minimal polynomial of the linear form $U = \Lambda_1 X_1 + \cdots + \Lambda_n X_n$. Suppose further that we are given a separating linear form $u := u_1 X_1 + \cdots + u_n X_n \in \mathbb{Q}[X_1, \ldots, X_n]$ such that the vector $(u_1, \ldots, u_n)$ does not annihilate any denominator in $\mathbb{Q}[\Lambda]$ of any intermediate result of the algorithm Ψ. In order to compute the polynomials $v_1, \ldots, v_n$ of (2.12), we observe that the Taylor expansion of $m_U(\Lambda, Y)$ in powers of $\Lambda - u := (\Lambda_1 - u_1, \ldots, \Lambda_n - u_n)$ has the following expression:

$$m_U(\Lambda, Y) = m_u(Y) + \sum_{k=1}^{n} \left(\frac{\partial m_u}{\partial Y}(Y)X_k - v_k(Y) \right)(\Lambda_k - u_k) \mod (\Lambda - u)^2.$$

We shall compute this first-order Taylor expansion by computing the first-order Taylor expansion of each intermediate result in the algorithm Ψ. In this way, each arithmetic operation in $\mathbb{Q}(\Lambda)$ arising in the algorithm Ψ becomes an arithmetic operation between two polynomials of $\mathbb{Q}[\Lambda]$ of degree at most 1, and is truncated up to order $(\Lambda - u)^2$. Since the first-order Taylor expansion of an addition, multiplication or division of two polynomials of $\mathbb{Q}[\Lambda]$ of degree at most 1 requires $O(n)$ arithmetic operations in $\mathbb{Q}$, we have that the whole step requires $O(n\mathsf{T})$ arithmetic operations in $\mathbb{Q}$, where T is the number of arithmetic operations in $\mathbb{Q}(\Lambda)$ performed by the algorithm Ψ.

Finally, the computation of the polynomials $w_1, \ldots, w_n$ of (2.13) requires the inversion of $\partial m_u/\partial Y$ modulo $m_u(Y)$ and the modular multiplication $w_k(Y) := (\partial m_u/\partial Y)^{-1} v_k(Y)$ for $1 \le k \le n$. These steps can be executed with additional $O(n\mathsf{M}(D))$ arithmetic operations in $\mathbb{Q}$. Summarizing, we have the following result.

Lemma 2.4 *Suppose that we are given*:

(1) *An algorithm Ψ in $\mathbb{Q}(\Lambda)$ which computes the minimal polynomial $m_U \in \mathbb{Q}[\Lambda, Y]$ of $U := \Lambda X_1 + \cdots + \Lambda_n X_n$ with T arithmetic operations in $\mathbb{Q}(\Lambda)$.*
(2) *A separating linear form $u := u_1 X_1 + \cdots + u_n X_n \in \mathbb{Q}[X_1, \ldots, X_n]$ such that the vector $(u_1, \ldots, u_n)$ does not annihilate any denominator in $\mathbb{Q}[\Lambda]$ of any intermediate result of the algorithm Ψ.*

Then a geometric solution of the variety V can be (deterministically) computed with $O(n(\mathsf{T} + \mathsf{M}(D)))$ arithmetic operations in $\mathbb{Q}$.

3 Statement of the Problem and Outline of the Main Algorithm

Let $\Delta_1, \ldots, \Delta_n$ be fixed finite subsets of $\mathbb{Z}^n_{\ge 0}$ with $0 \in \Delta_i$ for $1 \le i \le n$ and let $D := \mathcal{M}(Q_1, \ldots, Q_n)$ denote the mixed volume of the polytopes $Q_1 := \mathrm{Conv}(\Delta_1), \ldots, Q_n := \mathrm{Conv}(\Delta_n)$. Assume that $D > 0$ holds or, equivalently, that $\dim(\sum_{i \in I} Q_i) \ge |I|$ for every nonempty subset $I \subset \{1, \ldots, n\}$ (see, for instance, [39, Chap. IV, Proposition 2.3]).

Let $f_1, \ldots, f_n \in \mathbb{Q}[X]$ be polynomials defining a sparse system with respect to $\Delta_1, \ldots, \Delta_n$ and let $d_1, \ldots, d_n$ be their total degrees. Let $d := \max\{d_1, \ldots, d_n\}$. Suppose that $f_1, \ldots, f_n$ define a zero-dimensional variety V in $\mathbb{A}^n$. As in the previous section, we group equal supports into $s \le n$ distinct supports $\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(s)}$. Write $\mathcal{A} := (\mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(s)})$ and denote by k_ℓ the number of polynomials f_i with support $\mathcal{A}^{(\ell)}$ for $1 \le \ell \le s$.

From now on we assume that we are given a sufficiently generic lifting function $\omega := (\omega_1, \ldots, \omega_s)$ and the fine-mixed subdivision of $\mathcal{A}$ induced by ω. We assume further that the function $\omega_\ell : \mathcal{A}^{(\ell)} \to \mathbb{Z}$ takes only nonnegative values and $\omega_\ell(0, \ldots, 0) = 0$ for every $1 \le \ell \le s$. The lifting function ω and the corresponding fine-mixed subdivision of $\mathcal{A}$ can be used in order to define an appropriate deformation of the system $f_1 = 0, \ldots, f_n = 0$, the so-called *polyhedral deformation* introduced by Huber and Sturmfels in [26]. Our purpose here is to use this polyhedral deformation to derive a symbolic probabilistic algorithm which computes a geometric solution of the system $f_1 = 0, \ldots, f_n = 0$.

Since the polyhedral deformation requires that the coefficients of the input polynomials satisfy certain generic conditions, we introduce some auxiliary *generic* polynomials $g_1, \ldots, g_n$ with the same supports $\Delta_1, \ldots, \Delta_n$ and consider the perturbed polynomial system defined by $h_i := f_i + g_i$ for $1 \le i \le n$. The genericity conditions underlying the choice of $g_1, \ldots, g_n$ and $h_1, \ldots, h_n$ are discussed in Sect. 4. We observe that if the coefficients of the polynomials $f_1, \ldots, f_n$ satisfy these conditions then our method can be directly applied to $f_1, \ldots, f_n$.

Otherwise, we first solve the system $h_1 = 0, \ldots, h_n = 0$ and then recover the solutions to the input system $f_1 = 0, \ldots, f_n = 0$ by considering the standard homotopy $f_1 + (1-T)g_1 = 0, \ldots, f_n + (1-T)g_n = 0$.

4 The Polyhedral Deformation: Genericity Conditions

4.1 The Polyhedral Deformation

This section is devoted to introducing the polyhedral deformation of Huber and Sturmfels [26].

Let $h_i := \sum_{q \in \Delta_i} c_{i,q} X^q$ for $1 \le i \le n$ be polynomials in $\mathbb{Q}[X]$ and let V_1 denote the set of their common zeros in $\mathbb{A}^n$. For $i = 1, \ldots, n$, let ℓ_i be the (unique) integer with $\Delta_i = \mathcal{A}^{(\ell_i)}$, and let $\widetilde{\omega}_i := \omega_{\ell_i}$ be the lifting function associated to the support Δ_i. In order to simplify notations, the n-tuple $\widetilde{\omega} := (\widetilde{\omega}_1, \ldots, \widetilde{\omega}_n)$ will be denoted simply by $\omega = (\omega_1, \ldots, \omega_n)$. As before, we denote by $\widehat{C}^{(\ell)} := \{(q, \omega_\ell(q)) \in \mathbb{R}^{n+1} : q \in C^{(\ell)}\}$ the graph of any subset $C^{(\ell)}$ of $\mathcal{A}^{(\ell)}$ for $1 \le \ell \le s$, and extend this notation correspondingly. For a new indeterminate T, we deform the polynomials $h_1, \ldots, h_n$ into polynomials $\widehat{h}_1, \ldots, \widehat{h}_n \in \mathbb{Q}[X, T]$ defined in the following way:

$$\widehat{h}_i(X, T) := \sum_{q \in \Delta_i} c_{i,q} X^q T^{\omega_i(q)} \quad (1 \le i \le n). \tag{4.1}$$

Let I denote the ideal of $\mathbb{Q}[X, T]$ generated by $\widehat{h}_1, \ldots, \widehat{h}_n$ and let J denote the Jacobian determinant of $\widehat{h}_1, \ldots, \widehat{h}_n$ with respect to the variables $X_1, \ldots, X_n$. We set

$$\widehat{V} := V\big(I : J^\infty\big) \subset \mathbb{A}^{n+1}. \tag{4.2}$$

We shall show that, under a generic choice of the coefficients of $h_1, \ldots, h_n$, the system defined by the polynomials in (4.1) constitutes a deformation of the input system $h_1 = 0, \ldots, h_n = 0$, in the sense that the morphism $\pi : \widehat{V} \to \mathbb{A}^1$ defined by $\pi(x, t) := t$ is a dominant map with $\pi^{-1}(1) = V_1 \times \{1\}$. We shall further exhibit degree estimates on the genericity condition underlying such choice of coefficients. These estimates will allow us to obtain suitable polynomials $h_1, \ldots, h_n$ by randomly choosing their coefficients in an appropriate finite subset of $\mathbb{Z}$.

According to [26, Sect. 3], the solutions over an algebraic closure $\overline{\mathbb{Q}(T)}$ of $\mathbb{Q}(T)$ to the system defined by the polynomials (4.1) are algebraic functions of the parameter T which can be represented as Puiseux series of the form

$$\begin{aligned} x(T) := \big(&x_{1,0} T^{\frac{\gamma_1}{\gamma_{n+1}}} + \text{higher-order terms}, \ldots, x_{n,0} T^{\frac{\gamma_n}{\gamma_{n+1}}} \\ &+ \text{higher-order terms}\big), \end{aligned} \tag{4.3}$$

where $\gamma := (\gamma_1, \ldots, \gamma_n, \gamma_{n+1}) \in \mathbb{Z}^{n+1}$ is an inner normal with positive last coordinate $\gamma_{n+1} > 0$ of a (lower) facet $\widehat{C} = (\widehat{C}^{(1)}, \ldots, \widehat{C}^{(s)})$ of $\widehat{\mathcal{A}}$ of type $(k_1, \ldots, k_s)$, and $x_0 := (x_{1,0}, \ldots, x_{n,0}) \in (\mathbb{C}^*)^n$ is a solution to the polynomial system defined by

$$h_{i,\gamma}^{(0)} := \sum_{q \in C^{(\ell_i)}} c_{i,q} X^q \quad (1 \le i \le n), \tag{4.4}$$

where, as defined before, ℓ_i is the integer with $1 \le \ell_i \le s$ and $\Delta_i = \mathcal{A}^{(\ell_i)}$. For a generic choice of the polynomials $h_1, \ldots, h_n$ there are $k_1! \cdots k_s! \cdot \mathrm{Vol}(C)$ distinct solutions $x_0 \in (\mathbb{C}^*)^n$ to the system defined by the polynomials (4.4) and hence, there are $k_1! \cdots k_s! \cdot \mathrm{Vol}(C)$ distinct Puiseux series $x(T)$ as in (4.3). We shall "lift" each solution x_0 to this system to a solution of the form (4.3) to the system defined by (4.1). This means that, on input x_0, we shall compute the Puiseux series expansion of the corresponding solution (4.3) truncated up to a suitable order.

Let

$$V_{0,\gamma} := \left\{ x \in \left(\mathbb{C}^*\right)^n : h_{1,\gamma}^{(0)}(x) = 0, \ldots, h_{n,\gamma}^{(0)}(x) = 0 \right\}. \tag{4.5}$$

A particular feature of the polynomials (4.4) which makes the associated equation system "easy to solve" is that the vector of their supports is $(C^{(1)})^{k_1} \times \cdots \times (C^{(s)})^{k_s}$, where $(C^{(1)}, \ldots, C^{(s)})$ is a cell of type $(k_1, \ldots, k_s)$ in a fine-mixed subdivision of $\mathcal{A}$. Therefore, for every $1 \le \ell \le s$, the set $C^{(\ell)}$ consists of $k_\ell + 1$ points and hence, up to monomial multiplication so that each polynomial has a nonzero constant term, the (Laurent) polynomials in (4.4) are linear combinations of $n + 1$ distinct monomials in n variables.

Denote $\Gamma \subset \mathbb{Z}^{n+1}$ the set of all primitive integer vectors of the form $\gamma := (\gamma_1, \ldots, \gamma_n, \gamma_{n+1}) \in \mathbb{Z}^{n+1}$ with $\gamma_{n+1} > 0$ for which there is a cell $C = (C^{(1)}, \ldots, C^{(s)})$ of type $(k_1, \ldots, k_s)$ of the subdivision of $\mathcal{A}$ induced by ω such that $\widehat{C}$ has inner normal γ.

Fix a cell $C = (C^{(1)}, \ldots, C^{(s)})$ of type $(k_1, \ldots, k_s)$ of the subdivision of $\mathcal{A}$ induced by ω associated with a primitive inner normal $\gamma \in \Gamma$ with positive last coordinate. In order to lift the points of the variety $V_{0,\gamma}$ of (4.5) to a solution of the system defined by the polynomials in (4.1), we will work with a family of auxiliary polynomials $h_{1,\gamma}, \ldots, h_{n,\gamma} \in \mathbb{Q}[X, T]$ which we define as follows:

$$h_{i,\gamma}(X, T) := T^{-m_i} \widehat{h}_i\left(T^{\gamma_1} X_1, \ldots, T^{\gamma_n} X_n, T^{\gamma_{n+1}}\right) \quad (1 \le i \le n), \tag{4.6}$$

where $m_i \in \mathbb{Z}$ is the lowest power of T appearing in $\widehat{h}_i(T^{\gamma_1} X_1, \ldots, T^{\gamma_n} X_n, T^{\gamma_{n+1}})$ for every $1 \le i \le n$. Note that the polynomials obtained by substituting $T = 0$ into $h_{1,\gamma}, \ldots, h_{n,\gamma}$ are precisely those introduced in (4.4). Now we illustrate the objects introduced in this subsection with a particular sparse polynomial system with the same structure as the generic system (2.1).

Example Here we illustrate the previous constructions. Consider the polynomials $h_1, h_2 \in \mathbb{Q}[X_1, X_2]$ defined as

$$\begin{cases} h_1 := 1 - X_1^2 - X_2^2 - X_1^2 X_2^2, \\ h_2 := 1 + X_1^2 X_2 + X_1 X_2^2. \end{cases} \tag{4.7}$$

Observe that the polynomials above are a specialization of the generic polynomials introduced in (2.1).

We deform the polynomials h_1, h_2 using the lifting function ω defined in (2.3), obtaining thus the following polynomials:

$$\begin{cases} \widehat{h}_1 := 1 - X_1^2 T - X_2^2 T - X_1^2 X_2^2 T, \\ \widehat{h}_2 := 1 + X_1^2 X_2 + X_1 X_2^2. \end{cases} \tag{4.8}$$

These polynomials $\widehat{h}_1, \widehat{h}_2$ define the curve

$$\widehat{V} := V\big(\langle \widehat{h}_1, \widehat{h}_2 \rangle : J^\infty\big) = V\big(\widehat{h}_1, \widehat{h}_2\big), \tag{4.9}$$

where J is the Jacobian determinant of $\widehat{h}_1$ and $\widehat{h}_2$ with respect to the variables X_1, X_2.

According to the remark at the end of the example of Sect. 2.1.2, the cells of type $(1,1)$ in the fine-mixed subdivision of the support sets induced by ω, and the corresponding inner normals are:

- $C_1 := \{\{(0,0),(0,2)\},\{(0,0),(1,2)\}\}$, $\gamma^{(1)} := (2,-1,2)$.
- $C_2 := \{\{(0,0),(2,0)\},\{(0,0),(2,1)\}\}$, $\gamma^{(2)} := (-1,2,2)$.
- $C_3 := \{\{(0,0),(2,2)\},\{(1,2),(2,1)\}\}$, $\gamma^{(3)} := (-1,-1,4)$.

Therefore, the polynomial systems defined by the polynomials $h^{(0)}_{i,\gamma}$ of (4.4) and their solution sets $V_{0,\gamma}$ are

$$\begin{cases} h^{(0)}_{1,\gamma^{(1)}} = 1 - X_2^2, \\ h^{(0)}_{2,\gamma^{(1)}} = 1 + X_1 X_2^2, \end{cases} \qquad V_{0,\gamma^{(1)}} = \big\{(-1,1),(-1,-1)\big\}, \tag{4.10}$$

$$\begin{cases} h^{(0)}_{1,\gamma^{(2)}} = 1 - X_1^2, \\ h^{(0)}_{2,\gamma^{(2)}} = 1 + X_1^2 X_2, \end{cases} \qquad V_{0,\gamma^{(2)}} = \big\{(1,-1),(-1,-1)\big\}, \tag{4.11}$$

$$\begin{cases} h^{(0)}_{1,\gamma^{(3)}} = 1 - X_1^2 X_2^2, \\ h^{(0)}_{2,\gamma^{(3)}} = X_1^2 X_2 + X_1 X_2^2, \end{cases} \qquad \begin{aligned} V_{0,\gamma^{(3)}} = \big\{&(1,-1), \\ &(-1,1),(i,-i),(-i,i)\big\}. \end{aligned} \tag{4.12}$$

Finally, the polynomials $h_{i,\gamma}$ defined in (4.6) are

$$\begin{cases} h_{1,\gamma^{(1)}} = 1 - X_1^2 T^6 - X_2^2 - X_1^2 X_2^2 T^4, \\ h_{2,\gamma^{(1)}} = 1 + X_1^2 X_2 T^3 + X_1 X_2^2, \end{cases} \tag{4.13}$$

$$\begin{cases} h_{1,\gamma^{(2)}} = 1 - X_1^2 - X_2^2 T^6 - X_1^2 X_2^2 T^4, \\ h_{2,\gamma^{(2)}} = 1 + X_1^2 X_2 + X_1 X_2^2 T^3, \end{cases} \tag{4.14}$$

$$\begin{cases} h_{1,\gamma^{(3)}} = 1 - X_1^2 T^2 - X_2^2 T^2 - X_1^2 X_2^2, \\ h_{2,\gamma^{(3)}} = T^3 + X_1^2 X_2 + X_1 X_2^2. \end{cases} \tag{4.15}$$

4.2 On the Genericity of the Initial System

Here we discuss the genericity conditions underlying the choice of the polynomials $g_1, \ldots, g_n$ that enable us to apply the polyhedral deformation defined by the lifting form ω to the system $h_1 := f_1 + g_1 = 0, \ldots, h_n := f_n + g_n = 0$.

The first condition we require is that the set of common zeros of the perturbed polynomials $h_1, \ldots, h_n$ is a zero-dimensional variety with the maximum number of points for a sparse system with the given structure. More precisely, we require that the following condition holds:

(H1) The set $V_1 := \{x \in \mathbb{A}^n : h_1(x) = 0, \ldots, h_n(x) = 0\}$ is a zero-dimensional variety with $D := \mathcal{M}(Q_1, \ldots, Q_n)$ distinct points.

In addition, we need that the system (4.4) giving the initial points to our first deformation for every $\gamma \in \Gamma$ has as many roots as possible, namely, the mixed volume of their support vectors.

For each cell $C = (C^{(1)}, \ldots, C^{(s)})$ of type $(k_1, \ldots, k_s)$ of the induced fine-mixed subdivision, set an order on the $n+1$ points appearing in any of the sets $C^{(\ell)}$, after a suitable translation so that $0 \in C^{(\ell)}$ for every $1 \le \ell \le s$. Assume that $0 \in \mathbb{Z}^n$ is the last point according to this order. Denote $\gamma \in \mathbb{Z}^{n+1}$ the primitive inner normal of C with positive last coordinate. Consider the $n \times (n+1)$ matrix whose ith row is the coefficient vector of $h^{(0)}_{i,\gamma}$ in the prescribed monomial order and set $\mathcal{M}_\gamma \in \mathbb{Q}^{n\times n}$ and $\mathcal{B}_\gamma \in \mathbb{Q}^{n\times 1}$ for the submatrices consisting of the first n columns (coefficients of nonconstant monomials) and the last column (constant coefficients), respectively. Then the coefficients of $g_1, \ldots, g_n$ are to be chosen so that the following condition holds:

(H2) For every $\gamma \in \Gamma$, the $(n \times n)$-matrix $\mathcal{M}_\gamma$ is nonsingular and all the entries of $(\mathcal{M}_\gamma)^{-1}\mathcal{B}_\gamma$ are nonzero.

Our next results assert that the above conditions can be met with good probability by randomly choosing the coefficients of $g_1, \ldots, g_n$ in a certain set $\mathcal{S} \subset \mathbb{Z}$. We observe that our estimate on the size of $\mathcal{S}$ is not intended to be accurate, but to show that the growth of the size of the integers involved in the subsequent computations is not likely to create complexity problems.

Let $\{\Omega_{i,q} : 1 \le i \le n,\ q \in \Delta_i\}$ be a set of new indeterminates over $\mathbb{Q}$. For $1 \le i \le n$, write $\Omega_i := (\Omega_{i,q} : q \in \Delta_i)$ and let $H_i \in \mathbb{Q}[\Omega_i, X]$ be the generic polynomial

$$H_i(\Omega_i, X) := \sum_{q\in\Delta_i} \Omega_{i,q} X^q, \tag{4.16}$$

with support Δ_i and $N_i := \#\Delta_i$ coefficients. Let $\Omega := (\Omega_1, \ldots, \Omega_n)$ and let $N := N_1 + \cdots + N_n$ be the total number of indeterminate coefficients.

We start the analysis of the required generic conditions with the following quantitative version of Bernstein's result on the genericity of zero-dimensional sparse systems (see [5, Theorem B, 26, Theorem 6.1]).

Lemma 4.1 *There exists a nonzero polynomial* $P^{(0)} \in \mathbb{Q}[\Omega]$ *with* $\deg P^{(0)} \le 3n^{2n+1}d^{2n-1}$ *such that for any* $c \in \mathbb{Q}^N$ *with* $P^{(0)}(c) \ne 0$, *the system* $H_1(c_1, X) = 0, \ldots, H_n(c_n, X) = 0$ *has* D *solutions in* $\mathbb{A}^n$, *counting multiplicities.*

Proof Due to [26, Theorem 6.1] combined with [35], the system $H_1(c_1, X) = 0, \ldots, H_n(c_n, X) = 0$ has D solutions in $\mathbb{A}^n$ counting multiplicities if and only if for every facet inner normal $\mu \in \mathbb{Z}^n$ of $Q_1 + \cdots + Q_n$, the sparse resultant $\mathrm{Res}_{\Delta_1^\mu, \ldots, \Delta_n^\mu}$ does not vanish at $c := (c_1, \ldots, c_n)$. Here Δ_i^μ denotes the set of points of Δ_i where the linear functional induced by μ attains its minimum for $1 \leq i \leq n$.

Therefore, the polynomial $P^{(0)} := \prod_\mu \mathrm{Res}_{\Delta_1^\mu, \ldots, \Delta_n^\mu} \in \mathbb{Q}[\Omega]$, where the product ranges over all primitive inner normals $\mu \in \mathbb{Z}^n$ to facets of $Q_1 + \cdots + Q_n$, satisfies the required condition.

In order to estimate the degree of $P^{(0)}$, we observe that for every facet inner normal $\mu \in \mathbb{Z}^n$ the following upper bound holds:

$$\deg(\mathrm{Res}_{\Delta_1^\mu, \ldots, \Delta_n^\mu}) \leq \sum_{i=1}^{n} \mathcal{M}\big(\Delta_1^\mu, \ldots, \Delta_{i-1}^\mu, \Delta_{i+1}^\mu, \ldots, \Delta_n^\mu\big) \leq n d^{n-1},$$

where $d := \max\{d_1, \ldots, d_n\}$. On the other hand, it is not difficult to see that the number of facets of an n-dimensional integer convex polytope $P \subset \mathbb{R}^n$ which has an integer point in its interior is bounded by $n!\,\mathrm{Vol}_{\mathbb{R}^n}(P)$. Now, taking $P := (n+1)Q$, we obtain an integer polytope with the same number of facets as Q having an integer interior point. Then, the number of facets of Q is bounded by $n!\,\mathrm{Vol}_{\mathbb{R}^n}(P) = n!\,\mathrm{Vol}_{\mathbb{R}^n}((n+1)Q) = (n+1)^n\, n!\,\mathrm{Vol}_{\mathbb{R}^n}(Q) \leq (n+1)^n (nd)^n$, since Q is included in the n-dimensional simplex of size nd. This proves the upper bound for the degree of $P^{(0)}$ of the statement of the lemma. □

The next lemma is concerned with the genericity of a smooth sparse system.

Lemma 4.2 *With the same notations as in Lemma 4.1 and before, there exists a nonzero polynomial $P^{(1)} \in \mathbb{Q}[\Omega]$ of degree at most $4n^{2n+1}d^{2n-1}$ such that for any $c \in \mathbb{Q}^N$ with $P^{(1)}(c) \neq 0$, the system $H_1(c_1, X) = 0, \ldots, H_n(c_n, X) = 0$ has exactly D distinct solutions in $\mathbb{A}^n$.*

Proof Consider the incidence variety associated to $(\Delta_1, \ldots, \Delta_n)$-sparse systems, namely,

$$W := \left\{ (x, c) \in \big(\mathbb{C}^*\big)^n \times \big(\mathbb{A}^{N_1} \times \cdots \times \mathbb{A}^{N_n}\big) : \sum_{q \in \Delta_i} c_{i,q} x^q = 0 \text{ for } 1 \leq i \leq n \right\}.$$

As in [42, Proposition 2.3], it follows that W is a $\mathbb{Q}$-irreducible variety. Let $\pi_\Omega : W \to \mathbb{A}^{N_1} \times \cdots \times \mathbb{A}^{N_n}$ be the canonical projection, which is a dominant map.

By [39, Chap. V, Corollary (3.2.1)], there is a nonempty Zariski open set $\mathcal{U}(\Delta_1, \ldots, \Delta_n) \subset \mathbb{A}^{N_1} \times \cdots \times \mathbb{A}^{N_n}$ of coefficients $c = (c_1, \ldots, c_n)$ for which the polynomials $H_1(c_1, X), \ldots, H_n(c_n, X)$ have supports $\Delta_1, \ldots, \Delta_n$, respectively, and the set of their common zeros in $(\mathbb{C}^*)^n$ is a nondegenerate complete intersection variety. Then the Jacobian $J_H := \det(\partial H_i / \partial X_j)_{1 \leq i,j \leq n}$ does not vanish at any point of $\pi_\Omega^{-1}(c)$ for every $c \in \mathcal{U}(\Delta_1, \ldots, \Delta_n)$.

Let $\mathbb{Q}(\Omega) \hookrightarrow \mathbb{Q}(W)$ be the finite field extension induced by the dominant projection π_Ω. By the preceding paragraph we have that the rational function defined by

J_H in $\mathbb{Q}(W)$ is nonzero. Therefore, its primitive minimal polynomial $M_J \in \mathbb{Q}[\Omega, Y]$ is well defined and satisfies the degree estimates

$$\deg_\Omega M_J \le \deg W \cdot \deg J_H \le \prod_{i=1}^{n}(d_i+1)\cdot \sum_{i=1}^{n} d_i \le 2^n d^{n+1} n$$

(see [50, 52]).

Let $P^{(1)} := P^{(0)} M_J^{(0)}$, where $P^{(0)}$ is the polynomial given by Lemma 4.1 and $M_J^{(0)}$ denotes the constant term of the expansion of M_J in powers of Y. We claim that $P^{(1)}$ satisfies the requirements of the statement of the lemma. Indeed, let $c \in \mathbb{Q}^N$ satisfy $P^{(1)}(c) \neq 0$. Then $P^{(0)}(c) \neq 0$ holds and, hence, Lemma 4.1 implies that $H_1(c, X) = 0, \ldots, H_n(c, X) = 0$ is a zero-dimensional system. Furthermore, $M_J^{(0)}(c)$ is a nonzero multiple of the product $\prod_{x \in \pi_\Omega^{-1}(c)} J_H(c, x)$. Thus, the nonvanishing of $M_J^{(0)}(c)$ shows that all the points of $\pi_\Omega^{-1}(c)$ are smooth and therefore, from, e.g., [39, IV, Theorem 2.2], it follows that $\pi_\Omega^{-1}(c)$ consists of exactly D simple points in $(\mathbb{C}^*)^n$. Moreover, combining the assumption that $0 \in \Delta_i$ for $1 \le i \le n$ with [35, Theorem 2.4], we deduce that $\pi_\Omega^{-1}(c)$ consists of D simple points in $\mathbb{A}^n$. The estimate $\deg M_J^{(0)} \le \deg_\Omega M_J \le 2^n d^{n+1} n \le n^{2(n+1)} d^{2n-1}$ implies the statement of the lemma. □

Finally, we exhibit a generic condition on the coefficients $h_1, \ldots, h_n$ which implies that assumption (H2) holds.

Lemma 4.3 *With the previous assumptions and notations, there exists a nonzero polynomial* $P^{(2)} \in \mathbb{Q}[\Omega]$ *with* $\deg P^{(2)} \le n(n+1)\#\Gamma$ *such that for every* $c := (c_1, \ldots, c_n) \in \mathbb{Q}^N$ *with* $P^{(2)}(c) \neq 0$, *the polynomials* $h_i := H_i(c_i, X)$ $(1 \le i \le n)$ *satisfy condition* (H2).

Proof Fix a primitive integer inner normal $\gamma \in \Gamma$ to a lower facet of $\widehat{\mathcal{A}}$. Let $\mathcal{M}_\gamma \in \mathbb{Q}[\Omega]^{n\times n}$ and $\mathcal{B}_\gamma \in \mathbb{Q}[\Omega]^{n\times 1}$ be the matrices constructed from the generic polynomials $H_1, \ldots, H_n \in \mathbb{Q}[\Omega][X]$ as explained in the paragraph preceding condition (H2). Let $D_{0,\gamma} \in \mathbb{Q}[\Omega]$ be the (nonzero) determinant of $\mathcal{M}_\gamma$, and for every $1 \le j \le n$, let $D_{j,\gamma}$ be the determinant of the matrix obtained from $\mathcal{M}_\gamma$ by replacing its jth column with $\mathcal{B}_\gamma$. Set $P_\gamma := \prod_{j=0}^{n} D_{j,\gamma}$. Finally, take $P^{(2)} := \prod_{\gamma\in\Gamma} P_\gamma$. By Cramer's rule, whenever $P^{(2)}(c) \neq 0$, we have that the system $h_1, \ldots, h_n$ with coefficient vector $c = (c_1, \ldots, c_n)$ meets condition (H2).

The degree estimate for $P^{(2)}$ follows from the fact that $\deg P_\gamma \le n(n+1)$ holds for every $\gamma \in \Gamma$, since each of the entries of the matrices whose determinants are involved has degree 1 in the variables Ω. □

Now we are ready to state a generic condition on the coefficients of $h_1, \ldots, h_n$ which implies that (H1) and (H2) hold.

Proposition 4.4 *Under the previous assumptions and notations, there exists a nonzero polynomial* $P \in \mathbb{Q}[\Omega]$ *with* $\deg P \le 4n^{2n+1} d^{2n-1} + n(n+1)D$ *such that*

for every $c \in \mathbb{Q}^N$ *with* $P(c) \neq 0$, *the polynomials* $h_i := H_i(c_i, X)$ $(1 \leq i \leq n)$ *satisfy conditions* (H1) *and* (H2).

Proof Set $P := P^{(1)}P^{(2)}$, where $P^{(1)}$ is the polynomial of the statement of Lemma 4.2 and $P^{(2)}$ is the one defined in the statement of Lemma 4.3. The result follows from Lemmas 4.2 and 4.3, and the upper bound $\#\Gamma \leq D$ for the cardinality of the set of the distinct inner normal vectors considered (one for each cell of type $(k_1, \ldots, k_s)$ in the given fine-mixed subdivision). □

5 The Polyhedral Deformation: The Algorithm

5.1 Outline of the Algorithm

Now we have all the tools necessary to give an outline of our algorithm for the computation of a geometric solution of the (sufficiently generic) sparse system $h_1 = 0, \ldots, h_n = 0$.

With notations as in the previous subsections, we assume that a fine-mixed subdivision of $\mathcal{A}$ induced by a lifting function ω is given. This means that we are given the set Γ of inner normals of the lower facets of the convex hull of $\widehat{\mathcal{A}}$, together with the corresponding cells of the convex hull of $\mathcal{A}$. In addition, we suppose that our input polynomials $h_1, \ldots, h_n \in \mathbb{Q}[X]$ satisfy conditions (H1) and (H2) and denote by $V_1 \subset \mathbb{A}^n$ the affine variety defined by $h_1, \ldots, h_n$.

First, we choose a *generic* linear form $u \in \mathbb{Q}[X]$ such that:

- u separates the points of the zero-dimensional varieties V_1 and $V_{0,\gamma}$ for every $\gamma \in \Gamma$. This condition is represented by the nonvanishing of a certain nonconstant polynomial of degree at most $4D^2$.
- An algorithm for the computation of the minimal polynomial of u in $V_{0,\gamma}$ described below can be extended to a computation of a geometric solution of $V_{0,\gamma}$ in the sense of Lemma 2.4 for every $\gamma \in \Gamma$. This condition is represented by the nonvanishing of a nonconstant polynomial of degree at most $4D_\gamma^3$ for each $\gamma \in \Gamma$.
- An algorithm for the computation of the minimal polynomial of u in $\widehat{V}$ described below can be extended to a computation of a geometric solution of $\widehat{V}$ in the sense of Lemma 2.4. This application of Lemma 2.4 requires that the coefficient vector of the linear form u does not annihilate a nonconstant polynomial of degree at most $4D^4$.

Fix $\rho \geq 2$. From Theorem 2.2 it follows that a linear form u satisfying these conditions can be obtained by randomly choosing its coefficients from the set $\{1, \ldots, 6\rho D^4\}$ with error probability at most $1/\rho$.

Next we compute the monic minimal polynomial $\widehat{m}_u \in \mathbb{Q}(T)[Y]$ of the linear form u in the curve $\widehat{V}$ introduced in (4.2). For this purpose, we approximate the Puiseux series expansions of the branches of $\widehat{V}$ lying above 0 by means of a symbolic (Newton–Hensel) "lifting" of the common zeros of the zero-dimensional varieties $V_{0,\gamma} \subset \mathbb{A}^n$ defined by the polynomials (4.4) for all $\gamma \in \Gamma$ (see Sect. 5).

This in turn requires the computation of a geometric solution of $V_{0,\gamma}$ for every $\gamma \in \Gamma$. By means of a change of variables we put the system $h_{1,\gamma}^{(0)} = 0, \ldots, h_{n,\gamma}^{(0)} = 0$

defining the variety $V_{0,\gamma}$ into a "diagonal" form (see Sect. 5.2 below), which allows us to compute the minimal polynomial $m_{u,\gamma}^{(0)}$ of u in $V_{0,\gamma}$. Since the linear form u satisfies condition (2) of the statement of Lemma 2.4, from this procedure we derive an algorithm computing a geometric solution of $V_{0,\gamma}$ according to Lemma 2.4.

Then we "lift" this geometric solution to a suitable (non-Archimedean) approximation $\widetilde{m}_\gamma$ of a factor m_γ (over $\overline{\mathbb{Q}(T)}$) of the desired minimal polynomial $\widehat{m}_u$ of u. In the next step we obtain the minimal polynomial $\widehat{m}_u = \prod_{\gamma\in\Gamma} m_\gamma$ from the approximate factors $\widetilde{m}_\gamma$, namely, we compute the dense representation of the coefficients (in $\mathbb{Q}(T)$) of $\widehat{m}_u$, using Padé approximation (see Sect. 5.3 below). Finally, we apply the proof of Lemma 2.4 to derive an algorithm for computing a geometric solution of the variety $\widehat{V}$.

In the last step we compute a geometric solution of the variety V_1 by substituting 1 for T in the polynomials that form the geometric solution of $\widehat{V}$.

The whole algorithm for solving the system $h_1 = 0, \ldots, h_n = 0$ may be briefly sketched as follows:

Algorithm 5.1

1. Choose the coefficients of a linear form $u \in \mathbb{Q}[X]$ at random from the set $\{1, \ldots, 6\rho D^4\}$.
2. For each $\gamma \in \Gamma$:
   - Find a geometric solution of the variety $V_{0,\gamma}$ defined in (4.5).
   - Obtain a straight-line program for the polynomials $h_{1,\gamma}, \ldots, h_{n,\gamma}$ defined in (4.6) from the coefficients of $h_1, \ldots, h_n$ and the entries of $\gamma \in \mathbb{Z}^{n+1}$.
   - "Lift" the computed geometric solution of $V_{0,\gamma}$ to an approximation $\widetilde{m}_\gamma$ of the factor m_γ of $\widehat{m}_u$ by means of a symbolic Newton–Hensel procedure.
3. Obtain a geometric solution of the curve $\widehat{V}$:
   - Compute the approximation $\widetilde{m}_u := \prod_{\gamma\in\Gamma} \widetilde{m}_\gamma$ of $\widehat{m}_u$.
   - Compute the dense representation of $\widehat{m}_u$ from $\widetilde{m}_u$ using Padé approximation.
   - Find a geometric solution of $\widehat{V}$ applying the proof of Lemma 2.4.
4. Substitute 1 for T in the polynomials which form the geometric solution of $\widehat{V}$ computed in the previous step to obtain a geometric solution of the variety V_1.

5.2 Geometric Solutions of the Starting Varieties

In this subsection we exhibit an algorithm that computes, for a given inner normal $\gamma \in \Gamma$, a geometric solution of the variety $V_{0,\gamma} \subset (\mathbb{C}^*)^n$ defined by the polynomials $h_{i,\gamma}^{(0)}$ $(1 \le i \le n)$ for polynomials $h_1, \ldots, h_n$ satisfying assumptions (H1) and (H2). This algorithm is based on the procedure presented in [26].

Fix a cell $C = (C^{(1)}, \ldots, C^{(s)})$ of type $(k_1, \ldots, k_s)$ of the given fine-mixed subdivision of $\mathcal{A}$ and let $\gamma \in \Gamma$ be its associated inner normal. For $1 \le \ell \le s$, we denote by $h_1^{(\ell)}, \ldots, h_{k_\ell}^{(\ell)}$ the polynomials in the set $\{h_{1,\gamma}^{(0)}, \ldots, h_{n,\gamma}^{(0)}\}$ that are supported in $C^{(\ell)}$. In the sequel, whenever there is no risk of confusion we will not write the subscript γ indicating which cell we are considering.

Our hypotheses imply that $h_1^{(\ell)}, \ldots, h_{k_\ell}^{(\ell)}$ are $\mathbb{Q}$-linear combinations of precisely $k_\ell + 1$ monomials in $\mathbb{Q}[X]$ and, up to a multiplication by a monomial, we may assume

one of them to be the constant term. Denote these monomials by $X^{\alpha_{\ell,0}}, \ldots, X^{\alpha_{\ell,k_\ell}}$, with $\alpha_{\ell,0} := 0 \in \mathbb{Z}^n$. Let $\widetilde{\mathcal{M}}^{(\ell)}$ be the matrix of $\mathbb{Q}^{k_\ell \times (k_\ell+1)}$ for which the following equality holds in $\mathbb{Q}[X, X^{-1}]^{k_\ell}$:

$$\widetilde{\mathcal{M}}^{(\ell)} \begin{pmatrix} X^{\alpha_{\ell,k_\ell}} \\ \vdots \\ X^{\alpha_{\ell,0}} \end{pmatrix} = \begin{pmatrix} h_1^{(\ell)} \\ \vdots \\ h_{k_\ell}^{(\ell)} \end{pmatrix}, \tag{5.1}$$

and let $\mathcal{M}^{(\ell)}$ denote the square $(k_\ell \times k_\ell)$-matrix obtained by deleting the last column from $\widetilde{\mathcal{M}}^{(\ell)}$. Set

$$\mathcal{M} := \begin{pmatrix} \mathcal{M}^{(1)} & 0 & \cdots & 0 \\ 0 & \mathcal{M}^{(2)} & \cdots & 0 \\ 0 & 0 & \ddots & 0 \\ 0 & 0 & \cdots & \mathcal{M}^{(s)} \end{pmatrix},$$

where 0 here represents different block matrices with all its entries equal to $0 \in \mathbb{Q}$. Then $\mathcal{M}$ is the matrix defined by the coefficients of the nonconstant terms of the (Laurent) polynomials $h_{1,\gamma}^{(0)}, \ldots, h_{n,\gamma}^{(0)}$, up to a translation.

Due to condition (H2) we have that the matrix $\mathcal{M}$ is invertible, which in turn implies that the square matrices $\mathcal{M}^{(\ell)}$ are invertible for $1 \le \ell \le s$. Following [26], we apply Gaussian elimination to the matrix $\widetilde{\mathcal{M}}^{(\ell)}$ for $1 \le \ell \le s$ and obtain a set of $k_\ell + 1$ binomials

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & -c_{\alpha_{\ell,k_\ell}} \\ 0 & 1 & 0 & \ldots & -c_{\alpha_{\ell,k_\ell-1}} \\ \vdots & & & \ddots & \\ 0 & 0 & \ldots & 1 & -c_{\alpha_{\ell,1}} \end{pmatrix} \begin{pmatrix} X^{\alpha_{\ell,k_\ell}} \\ X^{\alpha_{\ell,k_\ell-1}} \\ \vdots \\ X^{\alpha_{\ell,0}} \end{pmatrix} = \begin{pmatrix} X^{\alpha_{\ell,k_\ell}} - c_{\alpha_{\ell,k_\ell}} \\ X^{\alpha_{\ell,k_\ell-1}} - c_{\alpha_{\ell,k_\ell-1}} \\ \vdots \\ X^{\alpha_{\ell,1}} - c_{\alpha_{\ell,1}} \end{pmatrix}$$

that generate the same linear subspace of $\mathbb{Q}[X, X^{-1}]$ as the polynomials in (5.1). Therefore, for $1 \le \ell \le s$ the set of common zeros in $(\mathbb{C}^*)^n$ of the polynomials $h_1^{(\ell)}, \ldots, h_{k_\ell}^{(\ell)}$ is given by the system $X^{\alpha_{\ell,k_\ell}} = c_{\alpha_{\ell,k_\ell}}, \ldots, X^{\alpha_{\ell,1}} = c_{\alpha_{\ell,1}}$. Putting these s systems together, we obtain a binomial system defining $V_{0,\gamma}$ of the form

$$X^{\alpha_1} = p_1, \ldots, X^{\alpha_n} = p_n, \tag{5.2}$$

with $\alpha_i \in \mathbb{Z}^n$ and $p_i \in \mathbb{Q} \setminus \{0\}$ $(1 \le i \le n)$. Note that the second part of condition (H2) ensures the nonvanishing of the constants p_i for $1 \le i \le n$.

Now let $\mathcal{E}$ denote the $(n \times n)$-matrix whose columns are the exponent vectors $\alpha_1, \ldots, \alpha_n$. Using [54, Proposition 8.10], we obtain unimodular matrices $K = (k_{i,j})_{1 \le i,j \le n}$, $L = (l_{i,j})_{1 \le i,j \le n}$ of $\mathbb{Z}^{n \times n}$, and a diagonal matrix $\operatorname{diag}(r_1, \ldots, r_n) \in \mathbb{Z}^{n \times n}$ which give the Smith Normal Form for $\mathcal{E}$, i.e., matrices such that the identity

$$K \cdot \mathcal{E} \cdot L = \operatorname{diag}(r_1, \ldots, r_n) \tag{5.3}$$

holds in $\mathbb{Z}^{n \times n}$. We observe that the upper bound

$$\log \|K\| \le (4n + 5)\big(\log n + \log \|\mathcal{E}\|\big) \tag{5.4}$$

holds, where $\|A\|$ denotes the maximum of the absolute value of the entries of a given matrix A [54, Proposition 8.10].

Let $Z_1, \ldots, Z_n$ be new indeterminates, and write $Z := (Z_1, \ldots, Z_n)$. We introduce the change of coordinates given by $X_i := Z_1^{k_{1,i}} \cdots Z_n^{k_{n,i}}$ for $1 \le i \le n$. Making this change of coordinates in (5.2) we obtain the system

$$Z^{K\alpha_1} = p_1, \ldots, Z^{K\alpha_n} = p_n,$$

which is equivalent to the "diagonal" system

$$Z_j^{r_j} = \prod_{i=1}^{n} \left(Z^{K\alpha_i}\right)^{l_{i,j}} = \prod_{i=1}^{n} p_i^{l_{i,j}} =: q_j \quad (1 \le j \le n).$$

Inverting some of the coefficients q_j if necessary we may assume without loss of generality that the integers $r_1, \ldots, r_n$ are positive. We have thus a very convenient description of the variety $V_{0,\gamma}$ by a diagonal polynomial system in the coordinate system of $\mathbb{A}^n$ defined by $Z_1, \ldots, Z_n$. We shall compute a geometric solution of $V_{0,\gamma}$ in such a coordinate system, which will then be used to compute a geometric solution of $V_{0,\gamma}$ in the "standard" coordinate system defined by $X_1, \ldots, X_n$.

Example We illustrate the above procedure for the variety $V_{0,\gamma^{(3)}}$ of (4.12), namely,

$$\begin{cases} h^{(0)}_{1,\gamma^{(3)}} = 1 - X_1^2 X_2^2, \\ h^{(0)}_{2,\gamma^{(3)}} = X_1^2 X_2 + X_1 X_2^2, \end{cases} \qquad V_{0,\gamma^{(3)}} = \big\{(1,-1), (-1,1), (i,-i), (-i,i)\big\}. \quad (5.5)$$

Here the binomial system in (5.2) and the corresponding exponent vector matrix $\mathcal{E}$ are

$$\begin{cases} X_1^2 X_2^2 = 1, \\ X_1 X_2^{-1} = -1, \end{cases} \quad \text{and} \quad \mathcal{E} = \begin{pmatrix} 2 & 1 \\ 2 & -1 \end{pmatrix}.$$

Taking $K := \left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ and $L := \left(\begin{smallmatrix} 0 & 1 \\ 1 & -2 \end{smallmatrix}\right)$, we get $K \cdot \mathcal{E} \cdot L = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 4 \end{smallmatrix}\right)$ and, hence, making the change of coordinates $X_1 = Z_1 Z_2$, $X_2 = Z_2$ we obtain the equivalent diagonal system

$$\begin{cases} Z_1 = -1, \\ Z_2^4 = 1. \end{cases} \quad (5.6)$$

5.2.1 A Geometric Solution of $V_{0,\gamma}$ in the Coordinate System Defined by $Z_1, \ldots, Z_n$

The algorithm for computing a geometric solution of the variety $V_{0,\gamma}$ in the coordinate system defined by $Z_1, \ldots, Z_n$ takes as input the set of polynomials $Z_1^{r_1} - q_1, \ldots, Z_n^{r_n} - q_n \in \mathbb{Q}[Z_1, \ldots, Z_n]$ and outputs a linear form $\widetilde{u} \in \mathbb{Q}[Z_1, \ldots, Z_n]$ which separates the points of $V_{0,\gamma}$, the minimal polynomial $m_{\widetilde{u}} \in \mathbb{Q}[Y]$ of $\widetilde{u}$ in $V_{0,\gamma}$ and the parameterizations of $Z_1, \ldots, Z_n$ by the zeros of $m_{\widetilde{u}}$.

For this purpose, assume that we are given a linear form $\widetilde{u} := \widetilde{u}_1 Z_1 + \cdots + \widetilde{u}_n Z_n \in \mathbb{Q}[Z_1, \ldots, Z_n]$ which separates the points of $V_{0,\gamma}$. Observe that the fact that $\widetilde{u}$ is a separating linear form for $V_{0,\gamma}$ implies that $\widetilde{u}_i \neq 0$ holds for $i = 1, \ldots, n$. Let $Y, \widetilde{Y}$ be new indeterminates and let $m_1, \ldots, m_n \in \mathbb{Q}[Y]$ be the sequence of polynomials defined recursively by

$$m_1 := \widetilde{u}_1^{-r_1} Y^{r_1} - q_1, \qquad m_i := \mathrm{Res}_{\widetilde{Y}}\big(\widetilde{u}_i^{-r_i}\big(Y - \widetilde{Y}\big)^{r_i} - q_i, m_{i-1}\big(\widetilde{Y}\big)\big) \quad \text{for } 2 \leq i \leq n. \tag{5.7}$$

We claim that the polynomial m_n equals (up to scaling by a nonzero element of $\mathbb{Q}$) the minimal polynomial $m_{\widetilde{u}} \in \mathbb{Q}[Y]$ of the coordinate function induced by $\widetilde{u}$ in the $\mathbb{Q}$-algebra extension $\mathbb{Q} \hookrightarrow \mathbb{Q}[V_{0,\gamma}]$. Indeed, for every $2 \leq i \leq n$, the polynomial $m_i(Y)$ is a linear combination of $\widetilde{u}_i^{-r_i}(Y - \widetilde{Y})^{r_i} - q_i$ and $m_{i-1}(\widetilde{Y})$ over $\mathbb{Q}[Y, \widetilde{Y}]$. Let $u^{(i)} := \widetilde{u}_1 Z_1 + \cdots + \widetilde{u}_i Z_i$ for $1 \leq i \leq n$. Then the identity $\widetilde{u}_i^{-r_i}(u^{(i)} - u^{(i-1)})^{r_i} - q_i = 0$ holds in $\mathbb{Q}[V_{0,\gamma}]$. Thus, assuming inductively that $m_{i-1}(u^{(i-1)}) = 0$ in $\mathbb{Q}[V_{0,\gamma}]$, it follows that $m_i(u^{(i)}) = 0$ in $\mathbb{Q}[V_{0,\gamma}]$ as well. Taking into account that $\deg m_n \leq r_1 \cdots r_n$ and that $m_{\widetilde{u}}$ is a nonzero polynomial of degree $D_\gamma := r_1 \cdots r_n = \#(V_{0,\gamma})$, we conclude that our claim holds.

In order to compute the polynomial $m_{\widetilde{u}}$, we compute the resultants in (5.7). Since the resultant $\mathrm{Res}_{\widetilde{Y}}(\widetilde{u}_i^{-r_i}(Y - \widetilde{Y})^{r_i} - q_i, m_{i-1}(\widetilde{Y}))$ is a polynomial of $\mathbb{Q}[Y]$ of degree $r_1 \cdots r_i$, by univariate interpolation in the variable $\widetilde{Y}$ we reduce its computation to the computation of $r_1 \cdots r_i + 1$ resultants of univariate polynomials in $\mathbb{Q}[\widetilde{Y}]$. This interpolation step requires $O(\mathsf{M}(r_1^2 \cdots r_i^2))$ arithmetic operations in $\mathbb{Q}$ and does not require any division by a nonconstant polynomial in the coefficients $\widetilde{u}_1, \ldots, \widetilde{u}_n$ (see, e.g., [9, 10]). Each univariate resultant can be computed using the algorithms in, e.g., [6, 59] with $\mathsf{M}(r_1 \cdots r_i)$ arithmetic operations in $\mathbb{Q}$. Altogether, we obtain an algorithm for computing the minimal polynomial $m_{\widetilde{u}}$ which performs $O(\mathsf{M}(D_\gamma^2))$ arithmetic operations in $\mathbb{Q}$.

Example For the system (5.6) defining the variety $V_{0,\gamma^{(3)}}$ in the coordinate system Z_1, Z_2, taking the separating linear form $\widetilde{u} = Z_1 + Z_2$ we obtain:

- $m_1 := Y + 1$.
- $m_2 := \mathrm{Res}_{\widetilde{Y}}((Y - \widetilde{Y})^4 - 1, \widetilde{Y} + 1) = Y^4 + 4Y^3 + 6Y^2 + 4Y$.

Then, the minimal polynomial of $\widetilde{u}$ is $m_{\widetilde{u}} = Y^4 + 4Y^3 + 6Y^2 + 4Y$.

Next, we extend this algorithm to an algorithm for computing a geometric solution of $V_{0,\gamma}$ as explained in Sect. 2.3. We obtain the following result.

Proposition 5.2 *Suppose that the coefficients of the linear form $\widetilde{u}$ are randomly chosen in the set $\{1, \ldots, 4n\rho D_\gamma^3\}$, where ρ is a fixed positive integer. Then the algorithm described above computes a geometric solution of the variety $V_{0,\gamma}$ (in the coordinate system $Z_1, \ldots, Z_n$) with error probability at most $1/\rho$ using $O(n\mathsf{M}(D_\gamma^2))$ arithmetic operations in $\mathbb{Q}$.*

Proof Our previous arguments prove that the algorithm described above computes a geometric solution of $V_{0,\gamma}$ with the stated number of arithmetic operations in $\mathbb{Q}$. There remains to analyze its error probability.

The only probabilistic step of the algorithm is the choice of the coefficients of the linear form $\widetilde{u}$, which must satisfy two requirements. First, $\widetilde{u}$ must separate the points of the variety $V_{0,\gamma}$. Since $V_{0,\gamma}$ consists of D_γ distinct points of $\mathbb{A}^n$, from Theorem 2.2 it follows that for a random choice of the coefficients of $\widetilde{u}$ in the set $\{1,\ldots,4n\rho D_\gamma^3\}$, the linear form $\widetilde{u}$ separates the points of $V_{0,\gamma}$ with error probability at most $1/4n\rho D_\gamma \le 1/2\rho$.

The second requirement concerns the computation of the univariate resultants of the generic versions of the polynomials in (5.7). This is required in order to extend the algorithm for computing the minimal polynomial $m_{\widetilde{u}}$ to an algorithm for computing a geometric solution of the variety $V_{0,\gamma}$. We use a fast algorithm for computing resultants over $\mathbb{Q}(\Lambda)$ based on the Extended Euclidean Algorithm (EEA for short). We shall perform the EEA over the ring of power series $\mathbb{Q}[\![\Lambda-\widetilde{u}]\!]$, truncating all the intermediate results up to order 2. Therefore, the choice of the coefficients of $\widetilde{u}$ must guarantee that all the elements of $\mathbb{Q}[\Lambda]$ which have to be inverted during the execution of the EEA are invertible elements of the ring $\mathbb{Q}[\![\Lambda-\widetilde{u}]\!]$.

For this purpose, we observe that, similarly to the proof of [59, Theorem 6.52], one deduces that all the denominators of the elements of $\mathbb{Q}(\Lambda)$ arising during the application of the EEA to the generic version of the polynomials $\widetilde{u}_i^{-r_i}(\alpha-u^{(i-1)})^{r_i}-q_i$ and $m_{i-1}(u^{(i-1)})$ are divisors of at most $r_1\cdots r_{i-1}$ polynomials of $\mathbb{Q}[\Lambda]$ of degree $2r_1\cdots r_i$ for any $\alpha\in\mathbb{Q}$. This EEA step must be executed for $r_1\cdots r_i$ distinct values of $\alpha\in\mathbb{Q}$, in order to perform the interpolation step. Hence the product of the denominators arising during all the applications of the EEA has degree at most $2nD_\gamma^3$. Therefore, from Theorem 2.2 we conclude that for a random choice of its coefficients in the set $\{1,\ldots,4n\rho D_\gamma^3\}$, the linear form $\widetilde{u}$ satisfies our second requirement with error probability at most $1/2\rho$.

The lemma follows putting both error probability estimates together. □

5.2.2 *A Geometric Solution of $V_{0,\gamma}$ in the Coordinate System Defined by $X_1,\ldots,X_n$*

Now we compute a geometric solution of the variety $V_{0,\gamma}$ in the original coordinate system defined by $X_1,\ldots,X_n$.

For this purpose, we compute the minimal polynomial $m_u\in\mathbb{Q}[Y]$ of a linear form $u=u_1X_1+\cdots+u_nX_n\in\mathbb{Q}[X_1,\ldots,X_n]$ in $V_{0,\gamma}$. Let $V_{0,\gamma}:=\{\mathrm{x}_0^{(1,\gamma)},\ldots,\mathrm{x}_0^{(D_\gamma,\gamma)}\}$. Then we have $m_u(Y)=\prod_{j=1}^{D_\gamma}(Y-u(\mathrm{x}_0^{(j,\gamma)}))$. In order to compute m_u, we use the polynomials $m_{\widetilde{u}},\widetilde{w}_1,\ldots,\widetilde{w}_n$ which form the previously computed geometric solution of $V_{0,\gamma}$ in the variables $Z_1,\ldots,Z_n$: from the identities $X_i:=Z_1^{k_{1,i}^{(\gamma)}}\cdots Z_n^{k_{n,i}^{(\gamma)}}$ $(1\le i\le n)$ we deduce that m_u equals the minimal polynomial of the image of the projection $\eta_u:V_{0,\gamma}\to\mathbb{A}^1$ defined by $\eta_u^{(\gamma)}(z_1,\ldots,z_n):=\sum_{i=1}^n u_i z_1^{k_{1,i}^{(\gamma)}}\cdots z_n^{k_{n,i}^{(\gamma)}}$. Now the identities $Z_i=\widetilde{w}_i(\widetilde{u})$, which hold in $\mathbb{Q}[V_{0,\gamma}]$ for $1\le i\le n$, imply that

$$u=\sum_{i=1}^n u_i\big(\widetilde{w}_1(\widetilde{u})\big)^{k_{1,i}^{(\gamma)}}\cdots\big(\widetilde{w}_n(\widetilde{u})\big)^{k_{n,i}^{(\gamma)}} \tag{5.8}$$

holds in $\mathbb{Q}[V_{0,\gamma}]$, from which we easily conclude that m_u satisfies the following identity:

$$m_u(Y) = \mathrm{Res}_{\widetilde{Y}}\Big(Y - \sum_{i=1}^{n} u_i\big(\widetilde{w}_1\big(\widetilde{Y}\big)\big)^{k_{1,i}^{(\gamma)}} \cdots \big(\widetilde{w}_n\big(\widetilde{Y}\big)\big)^{k_{n,i}^{(\gamma)}}, m_{\widetilde{u}}\big(\widetilde{Y}\big)\Big). \tag{5.9}$$

Example We compute a geometric solution of $V_{0,\gamma^{(3)}}$ in the coordinate system X_1, X_2 for the linear form $u = X_1 - X_2$ from its geometric solution in the coordinates Z_1, Z_2 (see Sect. 5.2.1):

- $m_{\widetilde{u}} = Y^4 + 4Y^3 + 6Y^2 + 4Y$.
- $\widetilde{w}_1 = -1$.
- $\widetilde{w}_2 = Y + 1$.

From the change of coordinates $X_1 = Z_1 Z_2$, $X_2 = Z_2$ leading to system (5.6), we have $u = Z_1 Z_2 - Z_2$ and hence $u = -2(\widetilde{u} + 1)$. Therefore,

$$m_u = \mathrm{Res}_{\widetilde{Y}}\big(Y + 2\big(\widetilde{Y} + 1\big), \widetilde{Y}^4 + 4\widetilde{Y}^3 + 6\widetilde{Y}^2 + 4\widetilde{Y}\big) = Y^4 - 16.$$

Now we estimate the complexity of this step. We compute the monomials $(\widetilde{w}_1(\widetilde{u}))^{k_{1,i}^{(\gamma)}} \cdots (\widetilde{w}_n(\widetilde{u}))^{k_{n,i}^{(\gamma)}}$ $(1 \le i \le n)$ in the right-hand side of (5.8) modulo $m_{\widetilde{u}}(Y)$, with $O(n^2 \log(\max_{i,j} |k_{i,j}^{(\gamma)}|)\mathsf{M}(D_\gamma))$ arithmetic operations in $\mathbb{Q}$. From (5.4) it follows that

$$O\Big(n^2 \log\Big(\max_{i,j} \big|k_{i,j}^{(\gamma)}\big|\Big)\mathsf{M}(D_\gamma)\Big) = O\big(n^3 \log\big(n\|\mathcal{E}_\gamma\|\big)\mathsf{M}(D_\gamma)\big),$$

where $\mathcal{E}_\gamma$ is the matrix of the exponents of the cell corresponding to the inner normal γ. Observe that all these steps are independent of the coefficients of the linear form u we are considering and therefore do not introduce any division by a nonconstant polynomial in the coefficients $u_1, \ldots, u_n$.

In the next step we compute the right-hand side of (5.8) modulo $m_{\widetilde{u}}(Y)$, with $O(n D_\gamma)$ arithmetic operations in $\mathbb{Q}$. Then we compute the resultant (5.9) by a process which interpolates (5.9) in the variable Y to reduce the question to the computation of $D_\gamma + 1$ univariate resultants, in the same way as for the computation of the resultants in (5.7). This requires $O(\mathsf{M}(D_\gamma)^2)$ arithmetic operations in $\mathbb{Q}$.

If the linear form u separates the points of $V_{0,\gamma}$, then we can extend the algorithm for computing $m_u(Y)$ to an algorithm for computing a geometric solution of $V_{0,\gamma}$ with the algorithm underlying the proof of Lemma 2.4. This extension requires that the coefficients $u_1, \ldots, u_n$ of the linear form u do not annihilate the denominators in $\mathbb{Q}[\Lambda]$ which arise from the application of the algorithm described above to the generic version $\Lambda_1 X_1 + \cdots + \Lambda_n X_n$ of the linear form u. Such denominators arise only during the computation of the generic version of the resultant (5.9). Hence, with a similar analysis as in the proof of Proposition 5.2, we conclude that, if the coefficients of u are chosen randomly in the set $\{1, \ldots, 4\rho D_\gamma^3\}$, then the error probability of our algorithm is bounded by $1/\rho$. In conclusion, we have:

Proposition 5.3 *Suppose that we are given a geometric solution of $V_{0,\gamma}$ in the coordinate system $Z_1, \ldots, Z_n$, as provided by the algorithm underlying Proposition 5.2, and*

the coefficients of the linear form u are randomly chosen in the set $\{1,\dots,4\rho D_\gamma^3\}$, where ρ is a fixed positive integer. Then the algorithm described above computes a geometric solution of the variety $V_{0,\gamma}$ with error probability at most $1/\rho$ using $O(n^3\log(n\|\mathcal{E}_\gamma\|)\mathsf{M}(D_\gamma)^2)$ arithmetic operations in $\mathbb{Q}$.

Finally, from Propositions 5.2 and 5.3 and the fact that $\|E_\gamma\| \le 2\mathcal{Q}$ holds for $\mathcal{Q} := \max_{1\le i\le n}\{\|q\|;\, q\in\Delta_i\}$, we immediately deduce the following result.

Theorem 5.4 *Suppose that the coefficients of the linear forms $\widetilde{u}$ and u of the statement of Propositions 5.2 and 5.3 are chosen at random in the set $\{1,\dots,4n\rho D^3\}$, where ρ is a fixed positive integer. Then the algorithm underlying Propositions 5.2 and 5.3 computes a geometric solution of the varieties $V_{0,\gamma}$ for all $\gamma\in\Gamma$ with error probability at most $2/\rho$ using $O(n^3\log(n\mathcal{Q})\mathsf{M}(D)^2)$ arithmetic operations in $\mathbb{Q}$.*

Example For the polynomial system (4.7) we are considering and the linear form $u = X_1 - X_2$, the first step of Algorithm 5.1 computes the following geometric solutions of the varieties of (4.10), (4.11), and (4.12), respectively, as explained above:

$$\begin{aligned} V_{0,\gamma^{(1)}} &= \{(-1,-y-1)\in\mathbb{C}^2 : y^2+2y=0\},\\ V_{0,\gamma^{(2)}} &= \{(y-1,-1)\in\mathbb{C}^2 : y^2-2y=0\},\\ V_{0,\gamma^{(3)}} &= \{(\tfrac{1}{2}y,-\tfrac{1}{2}y)\in\mathbb{C}^2 : y^4-16=0\}. \end{aligned} \tag{5.10}$$

5.3 A Geometric Solution of the Curve $\widehat{V}$

The second step of our algorithm is devoted to the computation of a geometric solution of the curve $\widehat{V}$ of (4.2). This will be done by "lifting" the geometric solutions of the varieties $V_{0,\gamma}$ computed in the previous section for all $\gamma\in\Gamma$.

We recall the definition of the variety $\widehat{V}$. Let I denote the ideal of $\mathbb{Q}[X,T]$ generated by the polynomials $\widehat{h}_1,\dots,\widehat{h}_n$ of (4.1), which form the polyhedral deformation of the generic polynomials $h_1,\dots,h_n$, and let J denote the Jacobian determinant of $\widehat{h}_1,\dots,\widehat{h}_n$ with respect to the variables $X_1,\dots,X_n$. Let $V(I)$ be the set of common zeros in $\mathbb{A}^{n+1}$ of $\widehat{h}_1,\dots,\widehat{h}_n$. Then $\widehat{V} := V(I:J^\infty)$.

Alternatively, let $\pi : V(I)\to\mathbb{A}^1$ be the linear projection defined by $\pi(x,t)=t$. Consider the decomposition of $V(I)$ into its irreducible components $V(I)=\bigcup_{i=1}^{r+s}\mathcal{C}_i$. Suppose that the restriction $\pi|_{\mathcal{C}_i}:\mathcal{C}_i\to\mathbb{A}^1$ of the projection π is dominant for $1\le i\le r$ and is not dominant for $r+1\le i\le s$. We shall show that $\widehat{V} := \bigcup_{i=1}^{r}\mathcal{C}_i$ holds, i.e., $\widehat{V}$ is the union of all the irreducible components of $V(I)$ which project dominantly over $\mathbb{A}^1$. Furthermore, we shall show that $\widehat{V}\subset\mathbb{A}^{n+1}$ is a curve which constitutes a suitable deformation of the variety defined by the system $h_1=0,\dots,h_n=0$. For this purpose, we shall use the following technical lemma.

Lemma 5.5 *Let $F_1,\dots,F_n\in\mathbb{Q}[X,T]$ be polynomials which generate an ideal $I := (F_1,\dots,F_n)\subset\mathbb{Q}[X,T]$ and let J denote the Jacobian determinant of $F_1,\dots,F_n$ with respect to the variables X. Set $\mathcal{V} := \{(x,t)\in\mathbb{A}^{n+1} : F_1(x,t)=0,\dots,F_n(x,t)=0\}$ and consider the linear projection $\pi:\mathcal{V}\to\mathbb{A}^1$ defined by $\pi(x,t):=t$. Assume that $\#\pi^{-1}(t)\le D$ holds for generic values of $t\in\mathbb{A}^1$ and that there exists a point*

$t_0 \in \mathbb{A}^1$ such that the fiber $\pi^{-1}(t_0)$ is a zero-dimensional variety of degree D with $J(x, t_0) \neq 0$ for every $(x, t_0) \in \pi^{-1}(t_0)$.

Let $\mathcal{V}_{\mathrm{dom}}$ be the union of all the irreducible components $\mathcal{C}$ of $\mathcal{V}$ with $\overline{\pi(\mathcal{C})} = \mathbb{A}^1$. Then:

- *$\mathcal{V}_{\mathrm{dom}}$ is a nonempty equidimensional variety of dimension* 1.
- *$\mathcal{V}_{\mathrm{dom}}$ is the union of all the irreducible components of $\mathcal{V}$ having a nonempty intersection with $\pi^{-1}(t_0)$.*
- *$\mathcal{V}_{\mathrm{dom}} = V(I : J^\infty)$.*
- *The restriction $\pi|_{\mathcal{V}_{\mathrm{dom}}} : \mathcal{V}_{\mathrm{dom}} \to \mathbb{A}^1$ is a dominant map of degree D.*

Proof First we observe that $\dim(\mathcal{C}) \geq 1$ for each irreducible component $\mathcal{C}$ of $\mathcal{V}$, since $\mathcal{V}$ is defined by n polynomials in an $(n+1)$-dimensional space.

Let $\mathcal{C}$ be an irreducible component of $\mathcal{V}$ for which $\pi^{-1}(t_0) \cap \mathcal{C} \neq \emptyset$ holds. Consider the restriction $\pi|_{\mathcal{C}} : \mathcal{C} \to \mathbb{A}^1$ of the projection map π. Then we have that $\pi|_{\mathcal{C}}^{-1}(t_0)$ is a nonempty zero-dimensional variety, which implies that the generic fiber of $\pi|_{\mathcal{C}}$ is either zero-dimensional or empty. Since $\dim(\mathcal{C}) \geq 1$, the theorem on the Dimension of Fibers implies that $\dim(\mathcal{C}) = 1$ and that $\pi|_{\mathcal{C}} : \mathcal{C} \to \mathbb{A}^1$ is a dominant map with generically finite fibers. This shows that $\mathcal{C} \subset \mathcal{V}_{\mathrm{dom}}$ and, in particular, that $\mathcal{V}_{\mathrm{dom}}$ is nonempty.

Conversely, we have that $\pi^{-1}(t_0) \cap \mathcal{C} \neq \emptyset$ holds for any irreducible component $\mathcal{C}$ of $\mathcal{V}_{\mathrm{dom}}$. Indeed, assume on the contrary the existence of an irreducible component $\mathcal{C}_0$ not satisfying this condition. Then there is a point $t_1 \in \mathbb{A}^1$ having a finite fiber $\pi^{-1}(t_1)$ such that $\pi|_{\mathcal{C}_0}^{-1}(t_1)$ and $\pi|_{\mathcal{C}}^{-1}(t_1)$ have maximal cardinality for every $\mathcal{C}$ with $\mathcal{C} \cap \pi^{-1}(t_0) \neq \emptyset$. This implies that $\#\pi^{-1}(t_1) > \#\pi^{-1}(t_0) = D$, leading to a contradiction.

We conclude that $\mathcal{V}_{\mathrm{dom}}$ is the nonempty equidimensional variety of dimension 1 which consists of all the irreducible components $\mathcal{C}$ of $\mathcal{V}$ with $\pi^{-1}(t_0) \cap \mathcal{C} \neq \emptyset$. Furthermore, this shows that the restriction $\pi|_{\mathcal{V}_{\mathrm{dom}}} : \mathcal{V}_{\mathrm{dom}} \to \mathbb{A}^1$ is a dominant map of degree D.

Finally, we show that the identity $\mathcal{V}_{\mathrm{dom}} = V(I : J^\infty)$ holds. First, note that the irreducible components of $V(I : J^\infty)$ are all the irreducible components of $\mathcal{V}$ where the Jacobian J does not vanish identically. Thus, it is clear that $\mathcal{V}_{\mathrm{dom}} \subset V(I : J^\infty)$, since J does not vanish at the points of $\pi^{-1}(t_0) \cap \mathcal{C}$ for each irreducible component $\mathcal{C}$ of $\mathcal{V}_{\mathrm{dom}}$. On the other hand, if $\mathcal{C}$ is an irreducible component of $\mathcal{V}$ for which the projection $\pi|_{\mathcal{C}} : \mathcal{C} \to \mathbb{A}^1$ is not dominant, then $\mathcal{C}$ is the set of common zeros of the polynomials $F_1, \ldots, F_n, T - t_{\mathcal{C}}$ for some value $t_{\mathcal{C}}$. Since $\dim(\mathcal{C}) \geq 1$, we have that the Jacobian matrix $\partial(F_1, \ldots, F_n, T - t_{\mathcal{C}})/\partial(X_1, \ldots, X_n, T)$ is singular at every point $(x, t_{\mathcal{C}})$ of $\mathcal{C}$. Hence, its determinant, which equals J, vanishes over $\mathcal{C}$. □

Now we return to the study of the variety $\widehat{V}$ and show that the assumptions of Lemma 5.5 hold. Observe that $\pi^{-1}(t) = V_t \times \{t\}$ holds for every $t \in \mathbb{A}^1$, where $V_t := \{x \in \mathbb{A}^n : \widehat{h}_1(x, t) = 0, \ldots, \widehat{h}_n(x, t) = 0\}$. Furthermore, the polynomials $\widehat{h}_1(X, t), \ldots, \widehat{h}_n(X, t)$ are obtained by a suitable substitution of the variables Ω of the generic polynomials $H_1, \ldots, H_n \in \mathbb{Q}[\Omega, X]$ with supports $\Delta_1, \ldots, \Delta_n$ introduced in (4.16). Indeed, if $c = (c_1, \ldots, c_n)$ is the vector of coefficients of $h_1, \ldots, h_n$, the coefficient vector of $\widehat{h}_i(X, t)$ $(1 \leq i \leq n)$ is $(c_{i,q} t^{\omega_i(q)})_{q \in \Delta_i}$ for every

$t \in \mathbb{A}^1$. By Lemma 4.1, there exists a nonzero polynomial $P^{(0)} \in \mathbb{Q}[\Omega]$ such that, for any $c' = (c'_1, \ldots, c'_n)$ with $P^{(0)}(c') \neq 0$, the associated sparse system defines a zero-dimensional variety. In particular, the coefficients $c = (c_1, \ldots, c_n)$ of our input polynomials $h_1 := H_1(c_1, X), \ldots, h_n = H_n(c_n, X)$ satisfy $P^{(0)}(c) \neq 0$. This shows that the polynomial $P_T^{(0)} \in \mathbb{Q}[T]$ obtained by substituting $\Omega_{i,q} \mapsto c_{i,q} T^{\omega_i(q)}$ $(1 \leq i \leq n,\ q \in \Delta_i)$ in the polynomial $P^{(0)}$ is nonzero, since it does not vanish at $T = 1$. We conclude that V_t is a zero-dimensional variety for all but a finite number of $t \in \mathbb{A}^1$. Thus, $\pi^{-1}(t)$ is finite for generic values of $t \in \mathbb{A}^1$.

Finally, by condition (H1), the fiber $\pi^{-1}(1) = V(h_1, \ldots, h_n) \times \{1\}$ is a zero-dimensional variety of degree $D = \deg(\pi)$ and the Jacobian determinant $J := \det(\partial \widehat{h}_i / \partial X_j)_{1 \leq i,j \leq n}$ does not vanish at any of its points. On the other hand, the fact that $\#\pi^{-1}(t) \leq D$ holds for generic values $t \in \mathbb{A}^1$ follows from the BKK theorem.

This shows that the variety $V(I)$ and its defining polynomials $\widehat{h}_1, \ldots, \widehat{h}_n$ satisfy all the assumptions of Lemma 5.5. Thus, we have:

Lemma 5.6 *The variety $\widehat{V} \subset \mathbb{A}^{n+1}$ is a curve. Furthermore, every irreducible component of $\widehat{V}$ has a nonempty intersection with the fiber $\pi^{-1}(1)$ of the projection map $\pi : \widehat{V} \to \mathbb{A}^1$.*

5.3.1 Generic Linear Projections of $\widehat{V}$

In order to compute a geometric solution of the space curve $\widehat{V}$, we shall first exhibit a procedure for computing the minimal polynomial of a generic linear projection of $\widehat{V}$. Let $u \in \mathbb{Q}[X_1, \ldots, X_n]$ be a linear form which separates the points of the "initial varieties" $V_{0,\gamma}$ for all the inner normals $\gamma := (\gamma_1, \ldots, \gamma_{n+1})$ of the lower facets of the polyhedral deformation under consideration. Let $\pi_u : \widehat{V} \to \mathbb{A}^2$ be the morphism defined by $\pi_u(x, t) := (t, u(x))$. Since the projection map $\pi : \widehat{V} \to \mathbb{A}^1$ defined by $\pi(x, t) := t$ is dominant, it follows that the Zariski closure of the image of π_u is a $\mathbb{Q}$-definable hypersurface of $\mathbb{A}^2$. Denote by $M_u \in \mathbb{Q}[T, Y]$ a minimal defining polynomial for this hypersurface. For the sake of the argument, we shall assume further that the identity $\deg(\pi) = D$, and thus $\deg_Y M_u = D$, hold.

We can apply estimate (2.4) of Lemma 2.3 in order to estimate $\deg_T M_u$ in combinatorial terms (compare with [45, Theorem 1.1]). Indeed, let $\widehat{Q}_1, \ldots, \widehat{Q}_n \subset \mathbb{R}^{n+1}$ be the Newton polytopes of the polynomials $\widehat{h}_1, \ldots, \widehat{h}_n$ of (4.1), and let $\Delta \subset \mathbb{R}^{n+1}$ be the standard n-dimensional simplex in the hyperplane $\{T = 0\}$. Then the following estimate holds:

$$\deg_T M_u \leq E := \mathcal{M}\big(\Delta, \widehat{Q}_1, \ldots, \widehat{Q}_n\big). \tag{5.11}$$

Furthermore, equality holds in (5.11) for a generic choice of the coefficients of the polynomials $\widehat{h}_i$ and the linear form u.

Our purpose is to exhibit a procedure for computing the unique monic multiple $\widehat{m}_u$ in $\mathbb{Q}(T)[Y]$ of M_u of degree D. This polynomial can be alternatively defined in terms of the Puiseux series solutions to the polynomials $\widehat{h}_1, \ldots, \widehat{h}_n$ as we explain in what follows.

Since the projection map $\pi : \widehat{V} \to \mathbb{A}^1$ is dominant, it induces an extension $\mathbb{Q}[T] \hookrightarrow \mathbb{Q}[\widehat{V}]$, where $\mathbb{Q}[\widehat{V}]$ denotes the coordinate ring of $\widehat{V}$. This variety being

a curve, $\mathbb{Q}[\widehat{V}]$ turns out to be a finitely generated $\mathbb{Q}[T]$-module. Thus, tensoring with $\mathbb{Q}(T)$, we deduce that $\mathbb{Q}[\widehat{V}]\otimes\mathbb{Q}(T)$ is a $\mathbb{Q}(T)$-vector space of finite dimension. We claim that $\mathbb{Q}[\widehat{V}]\otimes\mathbb{Q}(T)=\mathbb{Q}[V(I)]\otimes\mathbb{Q}(T)$ holds. Indeed, since $\widehat{V}$ consists of the irreducible components of $V(I)$ which are mapped dominantly onto $\mathbb{A}^1$ by the projection π, for each of the remaining irreducible components $\mathcal{C}$ of $V(I)$, the set $\pi(\mathcal{C})\subset\mathbb{C}$ is a zero-dimensional $\mathbb{Q}$-definable variety. This implies that $I(\mathcal{C})\cap\mathbb{Q}[T]\neq\{0\}$ holds.

Let $\widehat{m}_u$ be the minimal polynomial of u in the extension $\mathbb{Q}(T)\hookrightarrow\mathbb{Q}[\widehat{V}]\otimes\mathbb{Q}(T)$. The fact that $\mathbb{Q}[\widehat{V}]\otimes\mathbb{Q}(T)$ is a finite-dimensional $\mathbb{Q}(T)$-vector space shows that the affine variety $\mathbb{V}:=\{\bar{x}\in\mathbb{A}^n(\overline{\mathbb{Q}}(T)^*):\widehat{h}_1(\bar{x})=0,\ldots,\widehat{h}_n(\bar{x})=0\}$ has dimension zero. Here $\overline{\mathbb{Q}}(T)^*:=\bigcup_{q\in\mathbb{N}}\overline{\mathbb{Q}}((T^{1/q}))$ denotes the field of Puiseux series in the variable T over $\overline{\mathbb{Q}}$ (see, e.g., [60]) and $\widehat{h}_1,\ldots,\widehat{h}_n$ are considered as elements of $\mathbb{Q}(T)[X]$. Our hypotheses imply that there exist D distinct n-tuples $x^{(\ell)}:=(x_1^{(\ell)},\ldots,x_n^{(\ell)})\in(\overline{\mathbb{Q}}(T)^*)^n$ of Puiseux series such that the following equalities hold in $\overline{\mathbb{Q}}(T)^*$, for $1\leq\ell\leq D$,

$$\widehat{h}_1\big(x^{(\ell)},T\big)=0,\ldots,\widehat{h}_n\big(x^{(\ell)},T\big)=0 \tag{5.12}$$

(see [26]). Since $\mathbb{Q}[\widehat{V}]\otimes\mathbb{Q}(T)$ is the coordinate ring of the $\mathbb{Q}(T)$-variety $\mathbb{V}$, from (5.12) we deduce that the dimension of $\mathbb{Q}[\widehat{V}]\otimes\mathbb{Q}(T)$ over $\mathbb{Q}(T)$ equals D. Moreover, since $\deg_Y\widehat{m}_u=D$ holds as a consequence of our assumptions, we conclude that

$$\widehat{m}_u=\prod_{\ell=1}^{D}\big(Y-u\big(x^{(\ell)}\big)\big). \tag{5.13}$$

Since $M_u(T,u(X))\in I(\widehat{V})$, it follows that $M_u(T,u(X))=0$ holds in $\mathbb{Q}[\widehat{V}]\otimes\mathbb{Q}(T)$, from which we conclude that M_u is a multiple of $\widehat{m}_u$ by a factor in $\mathbb{Q}(T)[Y]$. Taking into account that both are polynomials of degree D in the variable Y and that $\widehat{m}_u$ is monic in this variable, we deduce that $\widehat{m}_u$ is the quotient of M_u by its leading coefficient. We summarize our arguments in the following statement.

Lemma 5.7 *Let $\pi_u:\widehat{V}\to\mathbb{A}^2$ be the projection defined by $\pi_u(x,t):=(t,u(x))$. Assume that the identity $\deg(\pi)=D$ holds and let $M_u\in\mathbb{Q}[T,Y]$ be the minimal defining polynomial of the hypersurface $\overline{\pi_u(\mathbb{A}^2)}$. Denote by $\widehat{m}_u$ the only monic multiple of M_u in $\mathbb{Q}(T)[Y]$. Then $\widehat{m}_u(Y)=\prod_{\ell=1}^{D}(Y-u(x^{(\ell)}))$, where $x^{(1)},\ldots,x^{(D)}\in\mathbb{A}^n(\overline{\mathbb{Q}}(T)^*)$ are the solutions of* (5.12).

Next, we group the roots $u(x^{(\ell)})$ of the polynomial $\widehat{m}_u$ according to the facet from where they arise. With notations as in Sect. 4.1, let $\Gamma\subset\mathbb{Z}^{n+1}$ be the set of primitive integer vectors of the form $\gamma:=(\gamma_1,\ldots,\gamma_n,\gamma_{n+1})\in\mathbb{Z}^{n+1}$ with $\gamma_{n+1}>0$ for which there is a cell $C=(C^{(1)},\ldots,C^{(s)})$ of type $(k_1,\ldots,k_s)$ of the subdivision of $\mathcal{A}$ induced by ω such that $\widehat{C}$ has inner normal γ. As asserted in Sect. 4.1, if $\gamma\in\Gamma$ is the inner normal of the lifting $\widehat{C}$ of a cell C of type $(k_1,\ldots,k_s)$, there exist $D_\gamma:=k_1!\cdots k_s!\cdot\mathrm{Vol}(C)$ vectors of Puiseux series $x^{(j,\gamma)}:=(x_1^{(j,\gamma)},\ldots,x_n^{(j,\gamma)})\in\mathbb{A}^n(\mathbb{Q}(T)^*)$ $(1\leq j\leq D_\gamma)$ of the form

$$x_i^{(j,\gamma)}:=\sum_{m\geq0}x_{i,m}^{(j,\gamma)}T^{\frac{\gamma_i+m}{\gamma_{n+1}}}$$

satisfying (5.12). Considering the projection of the branches of $\widehat{V}$ parametrized by the D_γ vectors of Puiseux series $x^{(j,\gamma)}$ for each $\gamma \in \Gamma$, we obtain the following element m_γ of $\mathbb{Q}((T^{1/\gamma_{n+1}}))[Y]$:

$$m_\gamma := \prod_{j=1}^{D_\gamma} \big(Y - u\big(x^{(j,\gamma)}\big)\big). \tag{5.14}$$

From (2.2) we conclude that (5.13) may be expressed in the following way:

$$\widehat{m}_u = \prod_{\gamma\in\Gamma} m_\gamma. \tag{5.15}$$

Since $\widehat{m}_u$ belongs to $\mathbb{Q}(T)[Y]$ and its primitive multiple $M_u \in \mathbb{Q}[T, Y]$ satisfies the degree estimate $\deg_T M_u \le E$, in order to compute the dense representation of $\widehat{m}_u$ we shall compute the Puiseux expansions of the coefficients of the factors $m_\gamma \in \mathbb{Q}((T^{1/\gamma_{n+1}}))[Y]$ of $\widehat{m}_u$ truncated up to order $2E$. Using Padé approximation it is possible to recover the dense representation of $\widehat{m}_u$ from this data.

Fix $\gamma \in \Gamma$ and set $\mathbf{x}_m^{(j,\gamma)} := (x_{1,m}^{(j,\gamma)}, \ldots, x_{n,m}^{(j,\gamma)})$ for every $m \ge 0$ and $1 \le j \le D_\gamma$. Since

$$\widehat{h}_i\Bigg(\sum_{m\ge0} x_{1,m}^{(j,\gamma)} T^{\frac{\gamma_1+m}{\gamma_{n+1}}}, \ldots, \sum_{m\ge0} x_{n,m}^{(j,\gamma)} T^{\frac{\gamma_n+m}{\gamma_{n+1}}}, T\Bigg) = 0$$

holds for $1 \le j \le D_\gamma$ and $1 \le i \le n$, we have

$$\begin{aligned}
0 &= T^{-m_i}\widehat{h}_i\Bigg(\sum_{m\ge0} x_{1,m}^{(j,\gamma)} T^{\gamma_1+m}, \ldots, \sum_{m\ge0} x_{n,m}^{(j,\gamma)} T^{\gamma_n+m}, T^{\gamma_{n+1}}\Bigg) \\
&= T^{-m_i}\widehat{h}_i\Bigg(T^{\gamma_1}\sum_{m\ge0} x_{1,m}^{(j,\gamma)} T^{m}, \ldots, T^{\gamma_n}\sum_{m\ge0} x_{n,m}^{(j,\gamma)} T^{m}, T^{\gamma_{n+1}}\Bigg) \\
&= h_{i,\gamma}\Bigg(\sum_{m\ge0} \mathbf{x}_m^{(j,\gamma)} T^m, T\Bigg),
\end{aligned}$$

according to (4.6). Therefore the polynomial $m_\gamma(T^{\gamma_{n+1}}, Y) \in \mathbb{Q}((T))[Y]$ can be expressed in terms of the power series solutions

$$\sigma^{(j,\gamma)} := \big(\sigma_1^{(j,\gamma)}, \ldots, \sigma_n^{(j,\gamma)}\big) := \sum_{m\ge0} \mathbf{x}_m^{(j,\gamma)} T^m \quad (1 \le j \le D_\gamma) \tag{5.16}$$

of $h_{1,\gamma}, \ldots, h_{n,\gamma}$. Indeed, from (5.14) it follows that

$$\begin{aligned}
m_\gamma(T^{\gamma_{n+1}}, Y) &= \prod_{j=1}^{D_\gamma}\Bigg(Y - \sum_{i=1}^{n} u_i \sum_{m\ge0} x_{i,m}^{(j,\gamma)} T^{\gamma_i+m}\Bigg) \\
&= \prod_{j=1}^{D_\gamma}\Bigg(Y - \sum_{m\ge0}\sum_{i=1}^{n} u_i x_{i,m}^{(j,\gamma)} T^{\gamma_i} T^{m}\Bigg)
\end{aligned}$$

$$= \prod_{j=1}^{D_\gamma} \left(Y - \sum_{m\geq 0} u_\gamma\big(\mathbf{x}_m^{(j,\gamma)}\big) T^m \right)$$

$$= \prod_{j=1}^{D_\gamma} \left(Y - u_\gamma\left(\sum_{m\geq 0} \mathbf{x}_m^{(j,\gamma)} T^m \right) \right) =: m_{u_\gamma}(T, Y),$$

where $u_\gamma := \sum_{i=1}^n u_i T^{\gamma_i} X_i$. In conclusion, we have:

Lemma 5.8 *Fix $\gamma := (\gamma_1, \ldots, \gamma_{n+1}) \in \Gamma$ and let m_γ be as in (5.14). Then the Laurent polynomial $m_\gamma(T^{\gamma_{n+1}}, Y) \in \mathbb{Q}((T))[Y]$ equals the minimal polynomial $m_{u_\gamma}(T, Y)$ of the projection induced by $u_\gamma := \sum_{i=1}^n u_i T^{\gamma_i} X_i$ on the subvariety V_γ of $\mathbb{A}^n(\overline{\mathbb{Q}}(T)^*)$ consisting of the set of power series $\{\sigma^{(1,\gamma)}, \ldots, \sigma^{(D_\gamma,\gamma)}\}$ of (5.16).*

This lemma will be critical in order to obtain suitable approximations to the Laurent polynomials $m_\gamma(T^{\gamma_{n+1}}, Y)$ in $\mathbb{Q}((T))[Y]$.

5.3.2 A Procedure for Computing $\widehat{m}_u$

Now we exhibit a procedure for computing the minimal polynomial $\widehat{m}_u$, which is based on the computation of the Laurent polynomials m_γ arising in the factorization of $\widehat{m}_u = \prod_{\gamma\in\Gamma} m_\gamma$ in terms of Puiseux expansions according to Lemmas 5.7 and 5.8. Then we will apply Lemma 2.4 to this procedure in order to obtain an algorithm for computing a geometric solution of the curve $\widehat{V}$.

In order to describe this approximation, we introduce the following terminology: for $G, \widetilde{G} \in \overline{\mathbb{Q}}((T))$ and $s \in \mathbb{Z}$, we say that $\widetilde{G}$ approximates G with precision s in $\overline{\mathbb{Q}}((T))$ if the Laurent series $G - \widetilde{G}$ has order at least $s+1$ in T. We shall use the notation $G \equiv \widetilde{G} \bmod (T^{s+1})$. Furthermore, if $G, \widetilde{G}$ are two elements of a polynomial ring $\overline{\mathbb{Q}}((T))[Y]$, we say that $\widetilde{G}$ approximates G with precision s if every coefficient $\widetilde{a} \in \overline{\mathbb{Q}}((T))$ of $\widetilde{G}$ approximates the corresponding coefficient $a \in \overline{\mathbb{Q}}((T))$ of G with precision s (in the sense of the previous definition).

Fix $\gamma := (\gamma_1, \ldots, \gamma_n) \in \Gamma$. In order to compute the required approximation of the polynomial m_{u_γ} of the statement of Lemma 5.8, we first compute a corresponding approximation of the polynomials that form a geometric solution of the variety $V_\gamma := \{\sigma^{(j,\gamma)} : 1 \leq j \leq D_\gamma\}$. Observe that

$$\begin{aligned}\big\{\sigma^{(j,\gamma)}(0) : 1 \leq j \leq D_\gamma\big\} &= \big\{\mathrm{x}_0^{(j,\gamma)} : 1 \leq j \leq D_\gamma\big\} \\ &= V\big(h_{1,\gamma}^{(0)}, \ldots, h_{n,\gamma}^{(0)}\big) \cap \big(\mathbb{C}^*\big)^n \\ &= V\big(h_{1,\gamma}(X, 0), \ldots, h_{n,\gamma}(X, 0)\big) \cap \big(\mathbb{C}^*\big)^n = V_{0,\gamma}\end{aligned}$$

holds. Since $\det(\partial h_{i,\gamma}(X, 0)/\partial X_k)_{1\leq i,k\leq n}(\mathrm{x}_0^{(j,\gamma)}) \neq 0$ holds for $1 \leq j \leq D_\gamma$, we may apply the global Newton iterator of [22] (see also [52]) in order to "lift" the given geometric solution of $V_{0,\gamma}$ to the geometric solution of the variety V_γ associated to the linear form $u \in \mathbb{Q}[X]$ with any prescribed precision.

Suppose that we are given polynomials $m_{u,\gamma}^{(0)}, w_{u,1,\gamma}^{(0)}, \ldots, w_{u,n,\gamma}^{(0)} \in \mathbb{Q}[Y]$ which form a geometric solution of $V_{0,\gamma}$, as provided by the algorithm underlying Theorem 5.4. Recall that $m_{u,\gamma}^{(0)}(u(\mathrm{x}_0^{(j,\gamma)})) = 0$ and $(\mathrm{x}_0^{(j,\gamma)})_i = w_{u,i,\gamma}^{(0)}(u(\mathrm{x}_0^{(j,\gamma)}))$ hold for $1 \le i \le n$ and $1 \le j \le D_\gamma$. The global Newton iterator is a recursive procedure whose kth step computes approximations $m_{u,\gamma}^{(k)}, w_{u,1,\gamma}^{(k)}, \ldots, w_{u,n,\gamma}^{(k)} \in \mathbb{Q}[T, Y]$ of the polynomials $m_{u,\gamma}, w_{u,1,\gamma}, \ldots, w_{u,n,\gamma}$ which form the geometric solution of V_γ associated with the linear form u with precision 2^k for any $k \ge 0$.

We may assume without loss of generality that $\gamma_i \ge 0$ and $0 = \min\{\gamma_1, \ldots, \gamma_n\}$ hold for $1 \le i \le n$. Indeed, if there exists $\gamma_i < 0$, setting $\gamma_{i_0} := \min\{\gamma_1, \ldots, \gamma_n\}$ we have

$$\begin{aligned} T^{-\gamma_{i_0} D_\gamma} m_\gamma\big(T^{\gamma_{n+1}}, T^{\gamma_{i_0}} Y\big) &= \prod_{j=1}^{D_\gamma} T^{-\gamma_{i_0}} \left(T^{\gamma_{i_0}} Y - \sum_{i=1}^{n} u_i \sum_{m \ge 0} x_{i,m}^{(j,\gamma)} T^{\gamma_i + m} \right) \\ &= \prod_{j=1}^{D_\gamma} \left(Y - T^{-\gamma_{i_0}} \sum_{i=1}^{n} u_i \sum_{m \ge 0} x_{i,m}^{(j,\gamma)} T^{\gamma_i + m} \right) \\ &= \prod_{j=1}^{D_\gamma} \left(Y - \sum_{i=1}^{n} u_i \sum_{m \ge 0} x_{i,m}^{(j,\gamma)} T^{\gamma_i - \gamma_{i_0} + m} \right). \end{aligned} \tag{5.17}$$

Since $\gamma_i - \gamma_{i_0} \ge 0$ holds for $1 \le i \le n$, this shows that the computation of an approximation $m_{u_\gamma} := m_\gamma(T^{\gamma_{n+1}}, Y)$ can easily be reduced to a situation in which $\gamma_i \ge 0$ holds for $1 \le i \le n$.

Note that the global Newton iterator cannot be directly applied in order to compute the geometric solution of $\{\sigma^{(j,\gamma)}; 1 \le j \le D_\gamma\}$ associated with the linear form $u_\gamma \in \mathbb{Q}[T][X]$, because the coefficients of u_γ are nonconstant polynomials of $\mathbb{Q}[T]$. Indeed, two critical problems arise:

(1) Although by hypothesis u_γ separates the points of V_γ, it might not separate the points of $V_{0,\gamma}$ and it is not clear from which precision on, the corresponding approximations of the points of V_γ are separated by u_γ. Requiring u_γ to be a separating form for all the approximations of the points of V_γ is an essential hypothesis for the iterator of [22] which cannot be suppressed without causing a significant growth of the complexity of the procedure (see [31, 32]).
(2) The iterator of [22] makes critical use of the fact that the coefficients of the linear form under consideration are elements of $\mathbb{Q}$ in order to determine how a given precision can be achieved.

Nevertheless, we shall exhibit a modification of the procedure which computes an approximation of $m_{u_\gamma}(T, Y)$ with precision $2\gamma_{n+1}E$ without changing the asymptotic number of arithmetic operations performed.

In order to circumvent (1) we require an additional generic condition to be satisfied by the coefficients $u_1, \ldots, u_n$ defining $u_\gamma := \sum_{i=1}^n u_i T^{\gamma_i} X_i$, namely, that u_γ separates the first M_γ terms of the series $\sigma^{(j,\gamma)}$. Our next result asserts that for a random choice of the coefficients u_γ, this condition is likely to happen.

Lemma 5.9 *For a random choice of values $u_1, \ldots, u_n$ in the set $\{1, \ldots, \rho D_\gamma^2\}$, the linear form $u_\gamma := \sum_{i=1}^n u_i T^{\gamma_i} X_i$ separates the initial terms $\sum_{m=0}^{M_\gamma} \mathrm{x}_m^{(j,\gamma)} T^m$ of the power series $\sigma^{(j,\gamma)}$ $(1 \le j \le D_\gamma)$ with probability at least $1 - 1/\rho$.*

Proof For a given linear form $u_\gamma := \sum_{i=1}^n u_i T^{\gamma_i} X_i$ as in the statement of the lemma, we have $u_\gamma(\sigma^{(j,\gamma)}) = \sum_{m \ge 0} (\sum_{i=1}^n u_i x_{i,m-\gamma_i}^{(j,\gamma)}) T^m$ for every $1 \le j \le D_\gamma$, where $x_{i,m-\gamma_i}^{(j,\gamma)} := 0$ for $m < \gamma_i$. We make the following claim.

Claim *Set $M_\gamma := \max\{\gamma_1, \ldots, \gamma_n\}$ and let $\Lambda_1, \ldots, \Lambda_n$ be indeterminates over $\mathbb{C}[T, X]$. Then the following inequality holds, for every $1 \le j, h \le D_\gamma$ with $j \ne h$,*

$$\sum_{m=0}^{M_\gamma} \left(\sum_{i=1}^n \Lambda_i \, x_{i,m-\gamma_i}^{(j,\gamma)} \right) T^m \ne \sum_{m=0}^{M_\gamma} \left(\sum_{i=1}^n \Lambda_i \, x_{i,m-\gamma_i}^{(h,\gamma)} \right) T^m.$$

Proof of Claim Suppose on the contrary that there exist $j \ne h$ such that $\sum_{m=0}^{M_\gamma} (\sum_{i=1}^n \Lambda_i \, x_{i,m-\gamma_i}^{(j,\gamma)}) T^m = \sum_{m=0}^{M_\gamma} (\sum_{i=1}^n \Lambda_i \, x_{i,m-\gamma_i}^{(h,\gamma)}) T^m$. Substituting $T^{-\gamma_i} \Lambda_i$ for Λ_i in this identity for $i = 1, \ldots, n$, we have $\sum_{m=0}^{M_\gamma} \sum_{i=1}^n \Lambda_i \, x_{i,m-\gamma_i}^{(j,\gamma)} T^{m-\gamma_i} = \sum_{m=0}^{M_\gamma} \sum_{i=1}^n \Lambda_i \, x_{i,m-\gamma_i}^{(h,\gamma)} T^{m-\gamma_i}$, that is,

$$\sum_{i=1}^n \sum_{m=0}^{M_\gamma - \gamma_i} \Lambda_i x_{i,m}^{(j,\gamma)} T^m = \sum_{i=1}^n \sum_{m=0}^{M_\gamma - \gamma_i} \Lambda_i x_{i,m}^{(h,\gamma)} T^m.$$

Substituting 0 for T in this identity, we deduce that

$$\sum_{i=1}^n \Lambda_i x_{i,0}^{(j,\gamma)} = \sum_{i=1}^n \Lambda_i x_{i,0}^{(h,\gamma)},$$

which contradicts the fact that the vectors $\mathbf{x}_0^{(j,\gamma)} = (x_{1,0}^{(j,\gamma)}, \ldots, x_{n,0}^{(j,\gamma)})$ $(1 \le j \le D_\gamma)$ are all distinct. This finishes the proof of the claim.

By the claim we see that the polynomial $\sum_{m=0}^{M_\gamma} (\sum_{i=1}^n \Lambda_i \, (x_{i,m-\gamma_i}^{(j,\gamma)} - x_{i,m-\gamma_i}^{(h,\gamma)})) T^m$ of $\mathbb{Q}[\Lambda][T]$ is nonzero, and therefore has a nonzero coefficient $a_{j,h} \in \mathbb{C}[\Lambda]$ for every $1 \le j < h \le D_\gamma$. Consider the polynomial $A_\gamma(\Lambda) := \prod_{1 \le j < h \le D_\gamma} a_{j,h} \in \mathbb{C}[\Lambda]$. Since $a_{j,h}$ has degree 1 for every $1 \le j < h \le D_\gamma$, it follows that A_γ has degree $\binom{D_\gamma}{2}$. Furthermore, for every $(u_1, \ldots, u_n) \in \mathbb{C}^n$ with $A_\gamma(u_1, \ldots, u_n) \ne 0$, the corresponding polynomial $u_\gamma := \sum_{i=1}^n u_i T^{\gamma_i} X_i$ separates the initial terms $\sum_{m=0}^{M_\gamma} \mathrm{x}_m^{(j,\gamma)} T^m$ of the power series $\sigma^{(j,\gamma)}$ $(1 \le j \le D_\gamma)$. Therefore, by Theorem 2.2 we see that, for a random choice of the coefficients $u_1, \ldots, u_n$ in the set $\{1, \ldots, \rho D_\gamma^2\}$, the linear form u_γ separates the first M_γ terms of the points of V_γ with probability at least $1 - 1/\rho$. □

Assume that the coefficients $u_1, \ldots, u_n$ satisfy the statement of the lemma. The algorithm computing an approximation of m_{u_γ} consists of the following three steps:

(Step I) We compute a suitable approximation to the geometric solution of V_γ associated to the linear form $u := \sum_{i=1}^n u_i X_i$ by means of $\kappa_0 := \lceil \log(M_\gamma + 1) \rceil$ steps of the global Newton iterator of [22].

(Step II) We use the approximation of the previous step in order to obtain a corresponding approximation $m_{u_\gamma}^{(\kappa_0)}, w_{u_\gamma,1}^{(\kappa_0)}, \ldots, w_{u_\gamma,n}^{(\kappa_0)}$ of the polynomials that form the geometric solution of V_γ associated with u_γ.

(Step III) We apply an adaptation of the global Newton iterator which takes as input the polynomials of the previous step $m_{u_\gamma}^{(\kappa_0)}, w_{u_\gamma,1}^{(\kappa_0)}, \ldots, w_{u_\gamma,n}^{(\kappa_0)}$ and outputs the required approximation to the polynomials $m_{u_\gamma}, w_{u_\gamma,1}, \ldots, w_{u_\gamma,n}$ that form the geometric solution of V_γ associated with u_γ.

Proposition 5.10 *Fix $\gamma := (\gamma_1, \ldots, \gamma_n) \in \Gamma$ and assume that a geometric solution of the variety $V_{0,\gamma}$ is given, as provided by Theorem 5.4. Assume further that the coefficients of the linear form u of the given geometric solution of $V_{0,\gamma}$ are randomly chosen in the set $\{1, \ldots, 4\rho D_\gamma^3\}$ for a given $\rho \in \mathbb{N}$. Then the algorithm above computes an approximation to the polynomial $m_{u_\gamma} \in \mathbb{Q}((T))[Y]$ with precision $2E\gamma_{n+1}$. The procedure requires $O((nL_\gamma + n^\Omega)\mathsf{M}(D_\gamma)(\mathsf{M}(M_\gamma)\mathsf{M}(D_\gamma)/\log(M_\gamma) + \mathsf{M}(E\gamma_{n+1})))$ arithmetic operations in $\mathbb{Q}$, where $M_\gamma := \max\{\gamma_1, \ldots, \gamma_n\}$ and L_γ is the number of arithmetic operations required to evaluate the polynomials $h_{i,\gamma}$ of (4.6), and has error probability at most $2/\rho$.*

Proof We consider Steps I, II, and III in detail. Step I takes as input the given geometric solution $m_{u,\gamma}^{(0)}, w_{u,1,\gamma}^{(0)}, \ldots, w_{u,n,\gamma}^{(0)}$ of $V_{0,\gamma}$, and performs $\kappa_0 := \lceil \log(M_\gamma + 1) \rceil$ times the global Newton iterator of [22] to obtain polynomials $m_{u,\gamma}^{(\kappa_0)}, w_{u,1,\gamma}^{(\kappa_0)}, \ldots, w_{u,n,\gamma}^{(\kappa_0)} \in \mathbb{Q}[T, Y]$ such that the following conditions hold:

$(\mathrm{i})_{u,\kappa_0}$ $\deg_Y m_{u,\gamma}^{(\kappa_0)} = D_\gamma$ and $\deg_T m_{u,\gamma}^{(\kappa_0)} \le M_\gamma$.

$(\mathrm{ii})_{u,\kappa_0}$ $\deg_Y w_{u,i,\gamma}^{(\kappa_0)} < D_\gamma$ and $\deg_T w_{u,i,\gamma}^{(\kappa_0)} \le M_\gamma$ for $1 \le i \le n$.

$(\mathrm{iii})_{u,\kappa_0}$ $m_{u,\gamma}^{(\kappa_0)} \equiv \prod_{j=1}^{D_\gamma} (Y - \varphi_{\kappa_0}^{(j,\gamma)}) \bmod (T^{M_\gamma+1})$.

$(\mathrm{iv})_{u,\kappa_0}$ $\sigma_i^{(j,\gamma)} \equiv w_{u,i,\gamma}^{(\kappa_0)}(T, \varphi_{\kappa_0}^{(j,\gamma)}) \bmod (T^{M_\gamma+1})$ for $1 \le i \le n$.

Here $\varphi_{\kappa_0}^{(j,\gamma)}$ is the Taylor expansion of order 2^{κ_0} of the power series $u(\sigma^{(j,\gamma)})$, that is, $\varphi_{\kappa_0}^{(j,\gamma)} := \sum_{m=0}^{2^{\kappa_0}} u(\mathrm{x}_m^{(j,\gamma)}) T^m$ for $1 \le j \le D_\gamma$.

According to [22, Proposition 7], it follows that this step requires performing $O((nL_\gamma + n^\Omega)\mathsf{M}(D_\gamma)\mathsf{M}(M_\gamma)/\log(M_\gamma))$ arithmetic operations in $\mathbb{Q}$, where L_γ denotes the number of arithmetic operations in $\mathbb{Q}$ required to evaluate the polynomials $h_{i,\gamma}$ of (4.6). Furthermore, in view of the application of Lemma 2.4 it is important to remark that this step does not involve any division by a nonconstant polynomial in the coefficients $u_1, \ldots, u_n$.

Next we discuss Step II. Here we obtain approximations $m_{u_\gamma}^{(\kappa_0)}, w_{u_\gamma,1}^{(\kappa_0)}, \ldots, w_{u_\gamma,n}^{(\kappa_0)}$ of the polynomials that form the geometric solution of V_γ associated with u_γ with precision $2^{\kappa_0} \ge M_\gamma$, namely:

- $\deg_Y m_{u_\gamma}^{(\kappa_0)} = D_\gamma$ and $\deg_T m_{u_\gamma}^{(\kappa_0)} \le 2^{\kappa_0}$.

- $\deg_Y w_{u_\gamma,i}^{(\kappa_0)} < D_\gamma$ and $\deg_T w_{u_\gamma,i}^{(\kappa_0)} \le 2^{\kappa_0}$ for $1 \le i \le n$.
- $m_{u_\gamma}^{(\kappa_0)} \equiv \prod_{j=1}^{D_\gamma}(Y - \phi_{\kappa_0}^{(j,\gamma)}) \bmod (T^{2^{\kappa_0}+1})$.
- $\sigma_i^{(j,\gamma)} \equiv w_{u_\gamma,i}^{(\kappa_0)}(T, \phi_{\kappa_0}^{(j,\gamma)}) \bmod (T^{2^{\kappa_0}+1})$ for $1 \le i \le n$.

Here $\phi_{\kappa_0}^{(j,\gamma)}$ is the Taylor expansion of $\phi^{(j,\gamma)} := u_\gamma(\sigma^{(j,\gamma)})$ of order 2^{κ_0} for $1 \le j \le D_\gamma$.

From conditions $(\mathrm{i})_{u,\kappa_0}$–$(\mathrm{iv})_{u,\kappa_0}$ and elementary properties of the resultant it is easy to see that $m_{u_\gamma}^{(\kappa_0)}$ satisfies the following identity:

$$m_{u_\gamma}^{(\kappa_0)}(Y) = \mathrm{Res}_{\widetilde{Y}}\left(Y - \sum_{i=1}^{n} u_i T^{\gamma_i} w_{u,i,\gamma}^{(\kappa_0)}\big(\widetilde{Y}\big), m_{u,\gamma}^{(\kappa_0)}\big(\widetilde{Y}\big)\right). \tag{5.18}$$

The resultant of the right-hand side is computed $\bmod (T^{M_\gamma+1})$ by interpolation in the variable Y to reduce the problem to the computation of D_γ resultants, as explained in the computation of the resultant in (5.9). These D_γ resultants involve two polynomials of $\mathbb{Q}[T, \widetilde{Y}]$ of degree in $\widetilde{Y}$ bounded by D_γ and are computed $\bmod (T^{M_\gamma+1})$. Hence we deduce that this step requires $O(\mathsf{M}(D_\gamma)D_\gamma\mathsf{M}(M_\gamma)/\log(M_\gamma))$ arithmetic operations in $\mathbb{Q}$.

We apply Lemma 2.4 in order to extend this procedure to an algorithm computing $m_{u_\gamma}^{(\kappa_0)}, w_{u_\gamma,1}^{(\kappa_0)}, \ldots, w_{u_\gamma,n}^{(\kappa_0)}$. For this purpose, we observe that a similar argument as in the proof of Proposition 5.2 proves that the denominators in $\mathbb{Q}[\Lambda]$, which arise during the computation of the D_γ resultants required to compute the minimal polynomial of the generic version $\sum_{i=1}^{n} \Lambda_i T^{\gamma_i} X_i$ of the linear form u_γ, are divisors of a polynomial of $\mathbb{Q}[\Lambda]$ of degree at most $4D_\gamma^3$. Applying Theorem 2.2 we see that for a random choice of the coefficients $u_1, \ldots, u_n$ in the set $\{1, \ldots, 4\rho D_\gamma^3\}$ none of these denominators are annihilated with probability at least $1 - 1/\rho$.

Finally, we consider Step III. For $\kappa_1 := \lceil \log(2\gamma_{n+1}E + 1) \rceil$, we apply $\kappa_1 - \kappa_0$ times an adaptation of the global Newton iterator of [22] to the polynomials $m_{u_\gamma}^{(\kappa_0)}, w_{u_\gamma,1}^{(\kappa_0)}, \ldots, w_{u_\gamma,n}^{(\kappa_0)}$ computed in the previous step. In the kth iteration step, we compute polynomials $m_{u_\gamma}^{(k)}, w_{u_\gamma,1}^{(k)}, \ldots, w_{u_\gamma,n}^{(k)}$ satisfying:

- $\deg_Y m_{u_\gamma}^{(k)} = D$ and $\deg_T m_{u_\gamma}^{(k)} \le 2^k$.
- $m_{u_\gamma}^{(k)} = \prod_{j=1}^{D_\gamma}(Y - \phi_k^{(j,\gamma)})$.
- $\deg_Y w_{u_\gamma,i}^{(k)} < D$ and $\deg_T w_{u_\gamma,1}^{(k)} \le 2^k$ for $1 \le i \le n$.
- $\sigma_i^{(j,\gamma)} \equiv w_{u_\gamma,i}^{(k)}(T, \phi_k^{(j,\gamma)}) \bmod (T^{2^k+1})$ for $1 \le i \le n$.

Here $\phi_k^{(j,\gamma)}$ is the Taylor expansion of $\phi^{(j,\gamma)} := u_\gamma(\sigma^{(j,\gamma)})$ of order 2^k for $1 \le j \le D_\gamma$. In particular, it follows that $m_{u_\gamma}^{(\kappa_1)}$ is the required approximation to m_{u_γ} with precision $2\gamma_{n+1}E$.

Fix $\kappa_0 < k \le \kappa_1$. We briefly describe how we can obtain an approximation with precision 2^k of the polynomials that form the geometric solution of V_γ associated to the linear form u_γ from an approximation with precision 2^{k-1}. Similarly to [22], set $\Delta_k(T, Y) := u_\gamma(\widetilde{w}_{u_\gamma}^{(k)}) - u_\gamma(w_{u_\gamma}^{(k-1)}) = u_\gamma(\widetilde{w}_{u_\gamma}^{(k)}) - Y$, where $\widetilde{w}_{u_\gamma}^{(k)}$ is

the result of applying a "classical Newton step" to $w_{u_\gamma}^{(k-1)}$, as described in [22]. Furthermore, write $\Delta_m(T,Y) := T^{-1-2^{k-1}}(m_{u_\gamma}^{(k)} - m_{u_\gamma}^{(k-1)})$. Since $m_{u_\gamma}^{(k)}(Y+\Delta_k) \equiv 0 \mod (T^{2^k+1}, m_{u_\gamma}^{(k-1)})$ holds (see [16, §4.2]), it follows that

$$\begin{aligned} 0 \equiv m_{u_\gamma}^{(k)}(Y+\Delta_k) &\equiv m_{u_\gamma}^{(k-1)}(Y+\Delta_k) + T^{2^{k-1}+1}\Delta_m(Y+\Delta_k) \mod \bigl(T^{2^k+1}, m_{u_\gamma}^{(k-1)}\bigr) \\ &\equiv \Delta_k \frac{\partial m_{u_\gamma}^{(k-1)}}{\partial Y}(Y) + T^{2^{k-1}+1}\Delta_m(Y) \mod \bigl(T^{2^k+1}, m_{u_\gamma}^{(k-1)}\bigr). \end{aligned}$$

We conclude that the following congruence relation holds:

$$m_{u_\gamma}^{(k)} \equiv m_{u_\gamma}^{(k-1)} - \left(\Delta_k \frac{\partial m_{u_\gamma}^{(k-1)}}{\partial Y} \bmod m_{u_\gamma}^{(k-1)}\right) \mod \bigl(T^{2^k+1}\bigr). \tag{5.19}$$

A similar argument proves the following congruence relation:

$$\begin{aligned} w_{u_\gamma,i}^{(k)} \equiv \widetilde{w}_{u_\gamma,i}^{(k-1)} - \left(\Delta_k \frac{\partial \widetilde{w}_{u_\gamma,i}^{(k-1)}}{\partial Y} \bmod m_{u_\gamma}^{(k-1)}\right) &\mod \bigl(T^{2^k+1}\bigr) \\ \text{for } 1 \le i \le n. & \end{aligned} \tag{5.20}$$

Each iteration of our adaptation of the global Newton iteration is based on (5.19) and (5.20), which are extensions of the corresponding congruence relations of [22]. We first compute $\widetilde{w}_{u_\gamma}^{(k)}$ by a standard Newton–Hensel lifting, and then evaluate the expressions (5.19) and (5.20). With a similar analysis as in [22, Proposition 7] we conclude that the whole procedure requires $O((nL_\gamma + n^\Omega)\mathsf{M}(D_\gamma)E\gamma_{n+1})$ arithmetic operations in $\mathbb{Q}$.

Finally, combining the complexity estimates of Steps I, II, and III and the probability of achievement of the two generic conditions imposed to the coefficients $u_1,\ldots,u_n$ (the condition underlying Lemma 5.9 and the application of Lemma 2.4 in Step II), we deduce the statement of the proposition. □

Example Consider the sparse polynomial system defined in (4.7) and their associated inner normals $\gamma^{(1)} = (2,-1,2)$, $\gamma^{(2)} = (-1,2,2)$ and $\gamma^{(3)} = (-1,-1,4)$. In (5.10) we have computed the geometric solutions for the varieties $V_{0,\gamma^{(i)}}$ $(i=1,2,3)$ associated to the linear form $u := X_1 - X_2$.

From these geometric solutions, in the second step of Algorithm 5.1 we obtain approximations to the polynomials $m_{u_{\gamma^{(i)}}}$ $(i=1,2,3)$. In order to compute in the next step a complete geometric solution of the variety associated to the linear form $u := X_1 - X_2$, we will deal with the first-order Taylor approximations of the minimal polynomials of the generic linear form $U := \Lambda_1 X_1 + \Lambda_2 X_2$ centered at $(\Lambda_1,\Lambda_2) = (1,-1)$. Recall that, in this case, $E = 3$ (see (2.10)):

- For $i=1$, we have $\gamma^{(1)} = (2,-1,2)$, $D_{\gamma^{(1)}} = 2$. Following (5.17), we compute an approximation of $T^2 m_{\gamma^{(1)}}(T^2, T^{-1}Y)$ with precision 12 by applying our modified Newton–Hensel lifting to the geometric solution of $V_{0,\gamma^{(1)}}$ previously computed, thus obtaining

$$\begin{aligned} m_1 = {} & Y^2 + \big(-4T^{11} + 4T^9 + 2T^3 + \big(4T^{11} + 6T^9 + 2T^7 + 2T^3\big)(\Lambda_1 - 1) \\ & + \big(8T^{11} + 2T^9 + 2T^7\big)(\Lambda_2 + 1)\big)Y \\ & - 6T^{12} + T^8 + T^4 - 1 + \big(-10T^{12} - 6T^{10}\big)(\Lambda_1 - 1) \\ & + \big(2T^{12} - 6T^{10} - 2T^8 - 2T^4 + 2\big)(\Lambda_2 + 1). \end{aligned}$$

- For $i = 2$, we have $\gamma^{(2)} = (-1, 2, 2)$, $D_{\gamma^{(2)}} = 2$. Following (5.17), we compute an approximation of $T^2 m_{\gamma^{(2)}}(T^2, T^{-1}Y)$ with precision 12 by applying our modified Newton–Hensel lifting to the geometric solution of $V_{0,\gamma^{(2)}}$, thus obtaining

$$\begin{aligned} m_2 = {} & Y^2 + \big(4T^{11} - 4T^9 - 2T^3 + \big(8T^{11} + 2T^9 + 2T^7\big)(\Lambda_1 - 1) \\ & + \big(4T^{11} + 6T^9 + 2T^7 + 2T^3\big)(\Lambda_2 + 1)\big)Y \\ & - 6T^{12} + T^8 + T^4 - 1 + \big(-2T^{12} + 6T^{10} + 2T^8 + 2T^4 - 2\big)(\Lambda_1 - 1) \\ & + \big(10T^{12} + 6T^{10}\big)(\Lambda_2 + 1). \end{aligned}$$

- For $i = 3$, we have $\gamma^{(3)} = (-1, -1, 4)$, $D_{\gamma^{(3)}} = 4$. Following (5.17), we first compute an approximation of $T^4 m_{\gamma^{(3)}}(T^4, T^{-1}Y)$ with precision 24 by applying our modified Newton–Hensel lifting to the geometric solution of $V_{0,\gamma^{(3)}}$, thus obtaining

$$\begin{aligned} m_3 = {} & Y^4 + \big(\big(-12T^{21} - 8T^{17} - 4T^{13} - 2T^5\big)(\Lambda_1 - 1) \\ & + \big(-12T^{21} - 8T^{17} - 4T^{13} - 2T^5\big)(\Lambda_2 + 1)\big)Y^3 \\ & + \big(28T^{22} - 2T^{14} + 4T^{10} - 2T^6 + 8T^2 \\ & + \big(-28T^{22} + 2T^{14} - 4T^{10} + 2T^6 - 8T^2\big)(\Lambda_2 + 1) \\ & + \big(28T^{22} - 2T^{14} + 4T^{10} - 2T^6 + 8T^2\big)(\Lambda_1 - 1)\big)Y^2 \\ & + \big(\big(-192T^{23} - 70T^{19} - 48T^{15} - 2T^{11} - 16T^7 - 8T^3\big)(\Lambda_1 - 1) \\ & + \big(-192T^{23} - 70T^{19} - 48T^{15} - 2T^{11} - 16T^7 - 8T^3\big)(\Lambda_2 + 1)\big)Y \\ & + 152T^{24} + 66T^{20} - 32T^{16} + 33T^{12} - 16 - 8T^8 \\ & + \big(-304T^{24} - 132T^{20} + 64T^{16} - 66T^{12} + 16T^8 + 32\big)(\Lambda_2 + 1) \\ & + \big(304T^{24} + 132T^{20} - 64T^{16} + 66T^{12} - 16T^8 - 32\big)(\Lambda_1 - 1). \end{aligned}$$

Using the algorithm of the statement of Proposition 5.10 for all $\gamma \in \Gamma$ we obtain approximations of the factors m_γ which allow us to compute the minimal polynomial m_u and hence a geometric solution of $\widehat{V}$. Our next result outlines this procedure and estimates its complexity and error probability.

Proposition 5.11 *Suppose that we are given a geometric solution of the variety $V_{0,\gamma}$ for all $\gamma \in \Gamma$, as provided by Theorem 5.4, with a linear form $u \in \mathbb{Q}[X_1, \ldots, X_n]$*

whose coefficients are randomly chosen in the set $\{1,\dots,4\rho D^4\}$, *where* ρ *is a fixed positive integer. Then we can compute a geometric solution of the curve* $\widehat{V}$ *with* $O((n^3N\log\mathcal{Q}+n^{1+\Omega})\mathsf{M}(\mathcal{M}_\Gamma)\mathsf{M}(D)(\mathsf{M}(D)+\mathsf{M}(E)))$ *arithmetic operations in* $\mathbb{Q}$ *and error probability bounded by* $1/\rho$. *Here* $N:=\sum_{i=1}^n \#\Delta_i$, $\mathcal{Q}:=\max_{1\le i\le n}\{\|q\|;\, q\in\Delta_i\}$, *and* $\mathcal{M}_\Gamma:=\max_{\gamma\in\Gamma}\max\{\gamma_1,\dots,\gamma_{n+1}\}$.

Proof For each $\gamma\in\Gamma$, we apply the algorithm underlying the proof of Proposition 5.10 in order to obtain an approximation of m_{u_γ} with precision $2\gamma_{n+1}E$. Due to Lemma 5.8, this polynomial immediately yields an approximation with precision $2E$ of $m_\gamma(T,Y)$ in $\mathbb{Q}((T^{1/\gamma_{n+1}}))[Y]$.

Multiplying all these approximations, we obtain an approximation with precision $2E$ of the polynomial $\widehat{m}_u=\prod_{\gamma\in\Gamma}m_\gamma$ of (5.15). Since every coefficient $a_j(T)$ of $\widehat{m}_u\in\mathbb{Q}(T)[Y]$ is a rational function of $\mathbb{Q}(T)$ having a reduced representation with numerator and denominator of degree at most E, such a representation of $a_j(T)$ can be computed from its approximation with precision $2E$ using Padé approximation with $O(\mathsf{M}(E))$ arithmetic operations in $\mathbb{Q}$.

In order to estimate the complexity of the whole procedure, we estimate the complexity of its three main steps:

(i) The computation of the polynomials m_γ with precision $2E$ for all $\gamma\in\Gamma$, which requires $O(\sum_{\gamma\in\Gamma}(nL_\gamma+n^{\Omega})\mathsf{M}(D_\gamma)(\mathsf{M}(M_\gamma)\mathsf{M}(D_\gamma)/\log(M_\gamma)+\mathsf{M}(E\gamma_{n+1})))$ arithmetic operations in $\mathbb{Q}$.

(ii) The computation of the product $\prod_{\gamma\in\Gamma}m_\gamma$ with precision $2E$, which requires $O(\mathsf{M}(D)\mathsf{M}(E))$ arithmetic operations in $\mathbb{Q}$.

(iii) The computation of a reduced representation of all the coefficients of $\widehat{m}_u\in\mathbb{Q}(T)[Y]$, which requires $O(\mathsf{M}(E)D)$ arithmetic operations in $\mathbb{Q}$.

Observe that, from the sparse representation of the polynomials $h_1,\dots,h_n$, we easily obtain a straight-line program computing the polynomials $h_{i,\gamma}$ of (4.6) with $O(nN\log(\mathcal{Q}M_\gamma))$ arithmetic operations in $\mathbb{Q}$ for every $\gamma\in\Gamma$, where $N:=\sum_{i=1}^n\#\Delta_i$ and $\mathcal{Q}:=\max_{1\le i\le n}\{\|q\|;\, q\in\Delta_i\}$. Therefore, the algorithm performs $O((n^2N\log\mathcal{Q}+n^{\Omega})\mathsf{M}(\mathcal{M}_\Gamma)\mathsf{M}(D)(\mathsf{M}(D)+\mathsf{M}(E)))$ arithmetic operations in $\mathbb{Q}$, where $\mathcal{M}_\Gamma:=\max_{\gamma\in\Gamma}\{M_\gamma,\gamma_{n+1}\}$.

Next we discuss how this procedure can be extended to the computation of a geometric solution of $\widehat{V}$ in the sense of Sect. 2.3. Two computations of the above procedure involve divisions by the coefficients u_i of the linear form u: the computation of the resultant of (5.18) for all $\gamma\in\Gamma$ and the Padé approximations of (iii). Both computations are reduced to D applications of the EEA, which is performed in a ring $\mathbb{Q}(\Lambda)$. A similar analysis as in Proposition 5.2 shows that all the denominators in $\mathbb{Q}[\Lambda]$ arising during such application of the EEA are divisors of a polynomial of degree $4D^4$. Therefore, according to Lemma 2.4, we conclude that a geometric solution of $\widehat{V}$ can be computed with $O((n^3N\log\mathcal{Q}+n^{1+\Omega})\mathsf{M}(\mathcal{M}_\Gamma)\mathsf{M}(D)(\mathsf{M}(D)+\mathsf{M}(E)))$ arithmetic operations in $\mathbb{Q}$, with an algorithm with error probability at most $1/\rho$, provided that the coefficients of u are randomly chosen in the set $\{1,\dots,4\rho D^4\}$. □

Example We continue with our previous example.

- For $i = 1$, the algorithm obtains an approximation $\widetilde{m}_{\gamma^{(1)}}$ of $m_{\gamma^{(1)}}$ by substituting $Y = TY$ in the polynomial m_1 previously computed, multiplying it by T^{-2} and replacing T^2 with T, which yields

$$\begin{aligned}\widetilde{m}_{\gamma^{(1)}} = {} & Y^2 + \big(-4T^5 + 4T^4 + 2T + \big(8T^5 + 2T^4 + 2T^3\big)(\Lambda_2 + 1) \\ & + \big(4T^5 + 6T^4 + 2T^3 + 2T\big)(\Lambda_1 - 1)\big)Y \\ & - 6T^5 + T^3 + T - \frac{1}{T} + \left(2T^5 - 6T^4 - 2T^3 - 2T + \frac{2}{T}\right)(\Lambda_2 + 1) \\ & + \big(-10T^5 - 6T^4\big)(\Lambda_1 - 1).\end{aligned}$$

- For $i = 2$, the algorithm obtains an approximation $\widetilde{m}_{\gamma^{(2)}}$ of $m_{\gamma^{(2)}}$ by substituting $Y = TY$ in the polynomial m_2, multiplying it by T^{-2} and replacing T^2 with T, which yields

$$\begin{aligned}\widetilde{m}_{\gamma^{(2)}} = {} & Y^2 + \big(4T^5 - 4T^4 - 2T + \big(8T^5 + 2T^4 + 2T^3\big)(\Lambda_1 - 1) \\ & + \big(4T^5 + 6T^4 + 2T^3 + 2T\big)(\Lambda_2 + 1)\big)Y \\ & - 6T^5 + T^3 + T - \frac{1}{T} + \left(-2T^5 + 6T^4 + 2T^3 + 2T - \frac{2}{T}\right)(\Lambda_1 - 1) \\ & + \big(10T^5 + 6T^4\big)(\Lambda_2 + 1).\end{aligned}$$

- For $i = 3$, the algorithm obtains an approximation $\widetilde{m}_{\gamma^{(3)}}$ of $m_{\gamma^{(3)}}$ by substituting $Y = TY$ in the polynomial m_3, multiplying it by T^{-4} and replacing T^4 with T, which yields

$$\begin{aligned}\widetilde{m}_{\gamma^{(3)}} = {} & Y^4 + \big(\big(-12T^5 - 8T^4 - 4T^3 - 2T\big)(\Lambda_1 - 1) \\ & + \big(-12T^5 - 8T^4 - 4T^3 - 2T\big)(\Lambda_2 + 1)\big)Y^3 \\ & + \big(28T^5 - 2T^3 + 4T^2 - 2T + 8 \\ & + \big(28T^5 - 2T^3 + 4T^2 - 2T + 8\big)(\Lambda_1 - 1) \\ & + \big(-28T^5 - 2T^3 - 4T^2 + 2T - 8\big)(\Lambda_2 + 1)\big)Y^2 \\ & + \big(\big(-192T^5 - 70T^4 - 48T^3 - 2T^2 - 16T - 8\big)(\Lambda_1 - 1) \\ & + \big(-192T^5 - 70T^4 - 48T^3 - 2T^2 - 16T - 8\big)(\Lambda_2 + 1)\big)Y \\ & + 152T^5 + 66T^4 - 32T^3 + 33T^2 - 8T - \frac{16}{T} \\ & + \left(304T^5 + 132T^4 - 64T^3 + 66T^2 - 16T - \frac{32}{T}\right)(\Lambda_1 - 1) \\ & + \left(-304T^5 - 132T^4 + 64T^3 - 66T^2 + 16T + \frac{32}{T}\right)(\Lambda_2 + 1).\end{aligned}$$

Computing the first-order Taylor approximation centered at $(\Lambda_1, \Lambda_2) = (1, -1)$ of the product $\widetilde{m}_{\gamma^{(1)}}\widetilde{m}_{\gamma^{(2)}}\widetilde{m}_{\gamma^{(3)}}$ with precision $2E = 6$ in the variable T, and applying a Padé approximation algorithm, we obtain the polynomial

$$\begin{aligned}
M := {} & Y^8 + \frac{8T-2}{T}Y^6 + \frac{2T^2-32T+1}{T^2}Y^4 + \frac{-28T^2-2T+40}{T^2}Y^2 \\
& + \frac{33T^3+24T^2-16}{T^3} + \left(\frac{8T-2}{T}Y^6 - 10Y^5 + \frac{4T^2-64T+2}{T^2}Y^4\right. \\
& + \frac{-48T+14}{T}Y^3 + \frac{-84T^2-6T+120}{T^2}Y^2 \\
& \left. + \frac{14T^2+80T-8}{T^2}Y + \frac{132T^3+96T^2-64}{T^3}\right)(\Lambda_1 - 1) \\
& + \left(\frac{-8T+2}{T}Y^6 - 10Y^5 + \frac{-4T^2+64T-2}{T^2}Y^4 + \frac{-48T+14}{T}Y^3\right. \\
& + \frac{84T^2+6T-120}{T^2}Y^2 + \frac{14T^2+80T-8}{T^2}Y \\
& \left. + \frac{-132T^3-96T^2+64}{T^3}\right)(\Lambda_2 + 1).
\end{aligned}$$

This polynomial is the first-order Taylor approximation centered at $(\Lambda_1, \Lambda_2) = (1, -1)$ of the minimal polynomial of the generic linear form $U := \Lambda_1 X_1 + \Lambda_2 X_2$.

Therefore, a geometric solution of the curve $\widehat{V}$ defined in (4.9) is given by the polynomials

$$\widehat{m}_u(Y), \qquad \frac{\partial \widehat{m}_u}{\partial Y}X_1 + \widehat{v}_1(Y), \qquad \frac{\partial \widehat{m}_u}{\partial Y}X_2 + \widehat{v}_2(Y),$$

where

$$\begin{aligned}
\widehat{m}_u = {} & Y^8 + \frac{8T-2}{T}Y^6 + \frac{2T^2-32T+1}{T^2}Y^4 \\
& + \frac{-28T^2-2T+40}{T^2}Y^2 + \frac{24T^2+33T^3-16}{T^3}
\end{aligned}$$

is the polynomial obtained substituting $\Lambda_1 = 1$, $\Lambda_2 = -1$ in M,

$$\begin{aligned}
\widehat{v}_1 = {} & \frac{8T-2}{T}Y^6 - 10Y^5 + \frac{4T^2-64T+2}{T^2}Y^4 + \frac{-48T+14}{T}Y^3 \\
& + \frac{-84T^2-6T+120}{T^2}Y^2 + \frac{14T^2+80T-8}{T^2}Y + \frac{132T^3+96T^2-64}{T^3}
\end{aligned}$$

is the partial derivative $\partial M/\partial \Lambda_1$,

$$\widehat{v}_2 = \frac{-8T+2}{T}Y^6 - 10Y^5 + \frac{-4T^2+64T-2}{T^2}Y^4 + \frac{-48T+14}{T}Y^3 + \frac{84T^2+6T-120}{T^2}Y^2 + \frac{14T^2+80T-8}{T^2}Y + \frac{-132T^3-96T^2+64}{T^3}$$

is the partial derivative $\partial M/\partial \Lambda_2$.

Putting together Theorem 5.4 and Proposition 5.11 we obtain the main result of this section.

Theorem 5.12 *Let ρ be a fixed positive integer. Suppose that the coefficients of the linear form $\widetilde{u}$ of the statement of Theorem 5.4 and of the linear form u are randomly chosen in the set $\{1,\ldots,4n\rho D^4\}$. Then the algorithm underlying Theorem 5.4 and Proposition 5.11 computes a geometric solution of the curve $\widehat{V}$ with error probability $3/\rho$ performing $O((n^3N\log\mathcal{Q}+n^{1+\Omega})\mathsf{M}(\mathcal{M}_\Gamma)\mathsf{M}(D)(\mathsf{M}(D)+\mathsf{M}(E)))$ arithmetic operations in $\mathbb{Q}$. Here $N:=\sum_{i=1}^n \#\Delta_i$, $\mathcal{Q}:=\max_{1\le i\le n}\{\|q\|; q\in\Delta_i\}$, and $\mathcal{M}_\Gamma:=\max_{\gamma\in\Gamma}\|\gamma\|$.*

5.4 Solving a Sufficiently Generic Sparse System

Now we obtain a geometric solution of the zero-dimensional variety $V_1:=\{x\in\mathbb{C}^n : h_1(x)=0,\ldots,h_n(x)=0\}$ from a geometric solution of the curve $\widehat{V}$.

With notations as in the previous section, we have that $V_1=\pi^{-1}(1)$, where $\pi:\widehat{V}\to\mathbb{A}^1$ is the linear projection defined by $\pi(x,t):=t$. Moreover, due to Lemma 5.6, the equality $V_1=\pi^{-1}(1)\cap\widehat{V}$ holds.

This enables us to easily obtain a geometric solution of V_1 from a geometric solution of the curve $\widehat{V}$. Indeed, let $\widehat{m}_u(T,Y),\widehat{v}_1(T,Y),\ldots,\widehat{v}_n(T,Y)$ be the polynomials which form a geometric solution of $\widehat{V}$ associated to a linear form $u\in\mathbb{Q}[X]$. Suppose further that the linear form u separates the points of V_1. Making the substitution $T=1$, we obtain new polynomials $\widehat{m}_u(1,Y),\widehat{v}_1(1,Y),\ldots,\widehat{v}_n(1,Y)\in\mathbb{Q}[Y]$ such that $\widehat{m}_u(1,u(X))$ and $\frac{\partial\widehat{m}_u}{\partial Y}(1,u(X))X_i-\widehat{v}_i(1,u(X))$ $(1\le i\le n)$ vanish over V_1. Taking into account that $\deg_Y(\widehat{m}_u)=D=\#V_1$ and that u separates the points of V_1, it follows that the polynomials $\widehat{m}_u(1,Y),\widehat{v}_1(1,Y),\ldots,\widehat{v}_n(1,Y)\in\mathbb{Q}[Y]$ form a geometric solution of V_1.

Proposition 5.13 *Let ρ be a fixed positive integer. With assumptions and notations as in Theorem 5.12, the algorithm described above computes a geometric solution of the zero-dimensional variety V_1 with error probability $4/\rho$ using $O((n^3N\log\mathcal{Q}+n^{1+\Omega})\mathsf{M}(\mathcal{M}_\Gamma)\mathsf{M}(D)(\mathsf{M}(D)+\mathsf{M}(E)))$ arithmetic operations in $\mathbb{Q}$.*

Example By substituting 1 for T in the geometric solution of the curve $\widehat{V}$ defined in (4.9) computed in the previous section, we obtain a geometric solution of the zero-dimensional variety $V_1=\{(x_1,x_2)\in\mathbb{C}^2 : 1-x_1^2-x_2^2-x_1^2x_2^2=0,$

$1 + x_1^2 x_2 + x_1 x_2^2 = 0\}$ defined by the system (4.7), namely,

$$m_u(Y), \qquad \frac{\partial m_u}{\partial Y}(Y)X_1 + v_1(Y), \qquad \frac{\partial m_u}{\partial Y}(Y)X_2 + v_2(Y),$$

where

- $m_u(Y) := \widehat{m}_u(1, Y) = Y^8 + 6Y^6 - 29Y^4 + 10Y^2 + 41$.
- $v_1(Y) := \widehat{v}_1(1, Y) = 6Y^6 - 10Y^5 - 58Y^4 - 34Y^3 + 30Y^2 + 86Y + 164$.
- $v_2(Y) := \widehat{v}_2(1, Y) = -6Y^6 - 10Y^5 + 58Y^4 - 34Y^3 - 30Y^2 + 86Y - 164$.

6 The Solution of the Input System

Let notations and assumptions be as in the previous sections. Assume that we are given a geometric solution $m_u(Y), v_1(Y), \ldots, v_n(Y)$ of the zero-dimensional variety V_1 defined by the polynomials $h_1 := f_1 + g_1, \ldots, h_n := f_n + g_n$. Assume further that the linear form u of such a geometric solution separates the points of the zero-dimensional variety $f_1 = 0, \ldots, f_n = 0$. In this section we describe a procedure for computing a geometric solution of the input system $f_1 = 0, \ldots, f_n = 0$.

For this purpose, we introduce an indeterminate T over $\mathbb{Q}[X]$ and consider the "deformation" $F_1, \ldots, F_n \in \mathbb{Q}[X, T]$ of the polynomials $f_1, \ldots, f_n$ defined in the following way:

$$F_i(X, T) := f_i(X) + (1 - T)g_i(X) \quad (1 \le i \le n). \tag{6.1}$$

Set $\mathcal{V} := \{(x, t) \in \mathbb{A}^{n+1} : F_1(x, t) = 0, \ldots, F_n(x, t) = 0\}$ and denote by $\pi : \mathcal{V} \to \mathbb{A}^1$ the projection map defined by $\pi(x, t) := t$. As in Sect. 5.3, we introduce the variety $\mathcal{V}_{\mathrm{dom}} \subset \mathbb{A}^{n+1}$ defined as the union of all the irreducible components of $\mathcal{V}$ whose projection over $\mathbb{A}^1$ is dominant.

6.1 Solution of the Second Deformation

In this subsection we describe an efficient procedure for computing a geometric solution of $\mathcal{V}_{\mathrm{dom}}$ from the geometric solution of $\pi^{-1}(0)$ provided by Proposition 5.13.

Since $\pi^{-1}(0)$ is the variety defined by the "sufficiently generic" sparse system $h_1(X) = F_1(X, 0) = 0, \ldots, h_n(X) = F_n(X, 0) = 0$, with similar arguments to those leading to the proof of Lemma 5.6, it is not difficult to see that the polynomials $F_1, \ldots, F_n$, the variety $\mathcal{V}$, the projection $\pi : \mathcal{V} \to \mathbb{A}^1$, and the fiber $\pi^{-1}(0)$ satisfy all the assumptions of Lemma 5.5. We conclude that $\mathcal{V}_{\mathrm{dom}}$ is a curve and that the identity $\mathcal{V} \cap \pi^{-1}(0) = \mathcal{V}_{\mathrm{dom}} \cap \pi^{-1}(0)$ holds. Furthermore, Lemma 5.5 implies that all the hypotheses of [52, Theorem 2] are satisfied.

Therefore, applying the "formal Newton lifting process" underlying the proof of [52, Theorem 2], we compute polynomials $\widetilde{m}_u(T, Y), \widetilde{v}_1(T, Y), \ldots, \widetilde{v}_n(T, Y) \in \mathbb{Q}[T, Y]$ which form a geometric solution of $\mathcal{V}_{\mathrm{dom}}$. The formal Newton lifting process requires $O((nL' + n^{\Omega+1})\mathsf{M}(D)\mathsf{M}(E'))$ arithmetic operations in $\mathbb{Q}$, where L' denotes the number of arithmetic operations required to evaluate $F_1, \ldots, F_n$ and E' is any upper bound of the degree of $\widetilde{m}_u$ in the variable T.

In order to estimate the quantity L', we observe that from the sparse representation of the polynomials $f_1, \ldots, f_n, h_1, \ldots, h_n$ we easily obtain a straight-line program of length at most $O(nN \log \mathcal{Q})$ which evaluates $f_1, \ldots, f_n, h_1, \ldots, h_n$. Therefore, the polynomials $F_1, \ldots, F_n$ can also be represented by a straight-line program of length at most $O(nN \log \mathcal{Q})$.

Furthermore, we can apply Lemma 2.3 in order to estimate $\deg_T \widetilde{m}_u$ in combinatorial terms. Indeed, let $\widetilde{Q}_1, \ldots, \widetilde{Q}_n \subset \mathbb{R}^{n+1}$ be the Newton polytopes of $F_1, \ldots, F_n$ and let $\Delta \subset \mathbb{R}^{n+1}$ be the standard n-dimensional simplex in the hyperplane $\{T = 0\}$. Since $\widetilde{Q}_i \subset Q_i \times [0, 1]$ holds for $1 \le i \le n$, where $Q_i \subset \mathbb{R}^n$ is the Newton polytope of h_i, by (2.5) of Lemma 2.3 we deduce the following estimate:

$$\deg_T \widetilde{m}_u \le E' := \sum_{i=1}^{n} \mathcal{M}(\Delta, Q_1, \ldots, Q_{i-1}, Q_{i+1}, \ldots, Q_n). \tag{6.2}$$

With this estimate for L' and this definition of E', we have:

Proposition 6.1 *Suppose that we are given a geometric solution of the variety V_1, as provided by Proposition 5.13. A geometric solution of $\mathcal{V}_{\mathrm{dom}}$ can be deterministically computed with $O((n^2 N \log \mathcal{Q} + n^{\Omega+1})\mathsf{M}(D)\mathsf{M}(E'))$ arithmetic operations in $\mathbb{Q}$.*

6.2 Solving the Input System

Making the substitution $T = 1$ in the polynomials $\widetilde{m}_u(T, Y), \widetilde{v}_i(T, Y)$ $(1 \le i \le n)$ which form the geometric solution of $\mathcal{V}_{\mathrm{dom}}$ computed by the algorithm of Proposition 6.1 we obtain polynomials $\widetilde{m}_u(1, Y), \widetilde{v}_1(1, Y), \ldots, \widetilde{v}_n(1, Y) \in \mathbb{Q}[Y]$ which represent a complete description of our input system $f_1(X) = 0, \ldots, f_n(X) = 0$, eventually including multiplicities. Such multiplicities are represented by multiple factors of $\widetilde{m}_u(1, Y)$, which are also factors of $\widetilde{v}_1(1, Y), \ldots, \widetilde{v}_n(1, Y)$ (see, e.g., [22, §6.5]). In order to remove them, we compute $a(Y) := \gcd(\widetilde{m}_u(1, Y), (\partial \widetilde{m}_u / \partial Y)(1, Y))$, and the polynomials $m(Y) := \widetilde{m}_u(1, Y)/a(Y)$, $b(Y) := ((\partial \widetilde{m}_u / \partial Y)(1, Y)/a(Y))^{-1} \bmod m(Y)$, and $w_i(Y) := b(Y)(\widetilde{v}_i(1, Y)/a(Y)) \bmod m(Y)$ $(1 \le i \le n)$. Then $m, w_1, \ldots, w_n$ form a geometric solution of our input system and can be computed with $O(n\mathsf{M}(D)E')$ additional arithmetic operations in $\mathbb{Q}$.

Summarizing, we sketch the whole procedure computing a geometric solution of the input system $f_1 = 0, \ldots, f_n = 0$. Fix $\rho \ge 4$. We randomly choose the coefficients of the polynomials $g_1, \ldots, g_n$ in the set $\{1, \ldots, 4\rho(nd)^{2n+1} + 2\rho n^2 2^{\mathcal{N}_1 + \cdots + \mathcal{N}_s}\}$ and coefficients of linear forms $u, \widetilde{u}$ in the set $\{1, \ldots, 16n\rho D^4\}$. By Theorem 2.2 it follows that the polynomials $g_1, \ldots, g_n$ and the linear forms $u, \widetilde{u}$ satisfy all the conditions required with probability at least $1 - 1/\rho$. Then we apply the algorithms underlying Propositions 5.13 and 6.1 in order to obtain a geometric solution of the variety $\mathcal{V}_{\mathrm{dom}}$. Finally, we use the procedure above to compute a geometric solution of the input system $f_1 = 0, \ldots, f_n = 0$. This yields the following result.

Theorem 6.2 *The algorithm sketched above computes a geometric solution of the input system $f_1 = 0, \ldots, f_n = 0$ with error probability at most $1/\rho$ using*

$$O\big(\big(n^3 N \log \mathcal{Q} + n^{1+\Omega}\big)\mathsf{M}(D)\big(\mathsf{M}(\mathcal{M}_\Gamma)\big(\mathsf{M}(D) + \mathsf{M}(E)\big) + \mathsf{M}\big(E'\big)\big)\big)$$

arithmetic operations in $\mathbb{Q}$. *Here* $N := \sum_{i=1}^{n} \#\Delta_i$, $\mathcal{M}_\Gamma := \max_{\gamma\in\Gamma} \|\gamma\|$, $\mathcal{Q} := \max_{1\le i\le n}\{\|q\|; q \in \Delta_i\}$ *and* E, E' *are defined in* (5.11) *and* (6.2), *respectively.*

We remark that our algorithm can be applied *mutatis mutandis* in order to compute the isolated points of an input system having a solution set with positive-dimensional components. Indeed, since the first deformation is not determined by the input system but by its monomial structure, it computes a geometric solution of a generic sparse system as described in Sect. 5. Then we execute our second deformation on the polynomials $F_1, \ldots, F_n$ of (6.1), considering the saturation $(I : J^\infty)$, where $I := (F_1, \ldots, F_n) \subset \mathbb{Q}[X, T]$ and J denotes the Jacobian determinant of $F_1, \ldots, F_n$ with respect to the variables X. From Lemma 5.5 it follows that positive-dimensional components of $f_1 = 0, , \ldots, f_n = 0$ are "cleaned" by the saturation $(I : J^\infty)$. Hence, our algorithm properly outputs the isolated points of $f_1 = 0, , \ldots, f_n = 0$, as stated.

Acknowledgements The authors wish to thank Martín Sombra and Ioannis Emiris for helpful discussions and comments. They also thank an anonymous referee for several useful remarks, which helped to improve the presentation of the results of this paper.

References

1. E.L. Allgower, K. Georg, *Numerical Continuation Methods: An Introduction*. Springer Ser. Comput. Math., vol. 13 (Springer, New York, 1990).
2. M.E. Alonso, E. Becker, M.-F. Roy, T. Wörmann, Zeros, multiplicities and idempotents for zero-dimensional systems, in *Algorithms in Algebraic Geometry and Applications, Proceedings of MEGA'94*. Prog. Math., vol. 143 (Birkhäuser, Boston, 1996), pp. 1–15.
3. J.L. Balcázar, J. Díaz, J. Gabarró, *Structural Complexity I*. Monogr. Theor. Comput. Sci. EATCS Ser., vol. 11 (Springer, Berlin, 1988).
4. W. Baur, V. Strassen, The complexity of partial derivatives, *Theor. Comput. Sci.* **22**, 317–330 (1983).
5. D.N. Bernstein, The number of roots of a system of equations, *Funct. Anal. Appl.* **9**, 183–185 (1975).
6. D. Bini, V. Pan, *Polynomial and Matrix Computations*. Progress in Theoretical Computer Science (Birkhäuser, Boston, 1994).
7. L. Blum, F. Cucker, M. Shub, S. Smale, *Complexity and Real Computation* (Springer, New York, 1998).
8. A. Bompadre, G. Matera, R. Wachenchauzer, A. Waissbein, Polynomial equation solving by lifting procedures for ramified fibers, *Theoret. Comput. Sci.* **315**(2–3), 335–369 (2004).
9. A. Bostan, G. Lecerf, E. Schost, Tellegen's principle into practice, in *Proceedings of the International Symposium on Symbolic and Algebraic Computation (ISSAC'03)*, Philadelphia, PA, 3–6 August 2003, ed. by J.R. Sendra (ACM Press, New York, 2003), pp. 37–44.
10. A. Bostan, E. Schost, Polynomial evaluation and interpolation on special sets of points, *J. Complexity* **21**(4), 420–446 (2005).
11. P. Bürgisser, M. Clausen, M.A. Shokrollahi, *Algebraic Complexity Theory*. Grundlehren Math. Wiss., vol. 315 (Springer, Berlin, 1997).
12. A. Cafure, G. Matera, A. Waissbein, Inverting bijective polynomial maps over finite fields, in *Proceedings of the 2006 Information Theory Workshop, ITW2006*, Punta del Este, Uruguay, 13–17 March 2006, ed. by G. Seroussi, A. Viola (IEEE Information Theory Society, New York, 2006), pp. 27–31.
13. D. Castro, M. Giusti, J. Heintz, G. Matera, L.M. Pardo, The hardness of polynomial equation solving, *Found. Comput. Math.* **3**(4), 347–420 (2003).
14. D. Cox, J. Little, D. O'Shea, *Using Algebraic Geometry*. Grad. Texts in Math., vol. 185 (Springer, New York, 1998).
15. J.-P. Dedieu, Condition number analysis for sparse polynomial systems, in *Foundations of Computational Mathematics*, Rio de Janeiro, 1997, ed. by F. Cucker, M. Shub (Springer, Berlin, 1997), pp. 267–276.

16. C. Durvye, G. Lecerf, A concise proof of the Kronecker polynomial system solver from scratch, *Exp. Math.* (2006, in press). doi:10.1016/j.expmath.2007.07.001.
17. I.Z. Emiris, J. Canny, Efficient incremental algorithms for the sparse resultant and the mixed volume, *J. Symb. Comput.* **20**, 117–149 (1995).
18. G. Ewald, *Combinatorial Convexity and Algebraic Geometry*. Grad. Texts in Math., vol. 168 (Springer, New York, 1996).
19. I.M. Gelfand, M.M. Kapranov, A.V. Zelevinsky, *Discriminants, Resultants, and Multidimensional Determinants* (Birkhäuser, Boston, 1994).
20. M. Giusti, K. Hägele, J. Heintz, J.E. Morais, J.L. Montaña, L.M. Pardo, Lower bounds for Diophantine approximation, *J. Pure Appl. Algebra* **117–118**, 277–317 (1997).
21. M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L.M. Pardo, Straight-line programs in geometric elimination theory, *J. Pure Appl. Algebra* **124**, 101–146 (1998).
22. M. Giusti, G. Lecerf, B. Salvy, A Gröbner free alternative for polynomial system solving, *J. Complex.* **17**(1), 154–211 (2001).
23. J. Heintz, On the computational complexity of polynomials and bilinear maps, in *Proceedings of the 5th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-5*, Menorca, Spain, 15–19 June 1987, ed. by L. Huguet, A. Poli. Lecture Notes in Comput. Sci., vol. 356 (Springer, Berlin, 1989), pp. 269–300.
24. J. Heintz, G. Jeronimo, J. Sabia, P. Solernó, Intersection theory and deformation algorithms. The multihomogeneous case, Manuscript, Universidad de Buenos Aires, 2002.
25. J. Heintz, T. Krick, S. Puddu, J. Sabia, A. Waissbein, Deformation techniques for efficient polynomial equation solving, *J. Complex.* **16**(1), 70–109 (2000).
26. B. Huber, B. Sturmfels, A polyhedral method for solving sparse polynomial systems, *Math. Comput.* **64**(212), 1541–1555 (1995).
27. B. Huber, B. Sturmfels, Bernstein's theorem in affine space, *Discrete Comput. Geom.* **17**, 137–141 (1997).
28. G. Jeronimo, T. Krick, J. Sabia, M. Sombra, The computational complexity of the Chow form, *Found. Comput. Math.* **4**(1), 41–117 (2004).
29. A.G. Khovanski, Newton polyhedra and the genus of complete intersections, *Funct. Anal. Appl.* **12**, 38–46 (1978).
30. A.G. Kushnirenko, Newton polytopes and the Bézout theorem, *Funct. Anal. Appl.* **10**, 233–235 (1976).
31. G. Lecerf, Quadratic Newton iteration for systems with multiplicity, *Found. Comput. Math.* **2**(3), 247–293 (2002).
32. G. Lecerf, Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers, *J. Complex.* **19**(4), 564–596 (2003).
33. T.-Y. Li, X. Li, Finding mixed cells in the mixed volume computation, *Found. Comput. Math.* **1**(2), 161–181 (2001).
34. T.Y. Li, Numerical solution of multivariate polynomial systems by homotopy continuation methods, *Acta Numer.* **6**, 399–436 (1997).
35. T.Y. Li, X. Wang, The BKK root count in $\mathbb{C}^n$, *Math. Comput.* **65**(216), 1477–1484 (1996).
36. G. Malajovich, J.M. Rojas, High probability analysis of the condition number of sparse polynomial systems, *Theor. Comput. Sci.* **315**(2–3), 525–555 (2004).
37. A. Morgan, *Solving Polynomial Systems Using Continuation for Engineering and Scientific Problems* (Prentice-Hall, Englewood Cliffs, 1987).
38. A. Morgan, A. Sommese, C. Wampler, A generic product–decomposition formula for Bézout numbers, *SIAM J. Numer. Anal.* **32**, 1308–1325 (1995).
39. M. Oka, *Non-Degenerate Complete Intersection Singularity* (Hermann, Paris, 1997).
40. L.M. Pardo, How lower and upper complexity bounds meet in elimination theory, in *Applied Algebra, Algebraic Algorithms and Error Correcting Codes, Proceedings of AAECC-11*, ed. by G. Cohen, M. Giusti, T. Mora. Lecture Notes in Comput. Sci., vol. 948 (Springer, Berlin, 1995), pp. 33–69.
41. L.M. Pardo, J. San Martín, Deformation techniques to solve generalized Pham systems, *Theoret. Comput. Sci.* **315**(2–3), 593–625 (2004).
42. P. Pedersen, B. Sturmfels, Product formulas for resultants and Chow forms, *Math. Z.* **214**(3), 377–396 (1993).
43. P. Philippon, M. Sombra, Hauteur normalisée des variétés toriques projectives, *J. Inst. Math. Jussieu* (2003, in press). doi:10.1017/S1474748007000138, 35pp., eprint math.NT/0406476.
44. P. Philippon, M. Sombra, Géométrie Diophantienne et variétés toriques, *C. R. Math. Acad. Sci. Paris* **340**, 507–512 (2005).

45. P. Philippon, M. Sombra, A refinement of the Kušnirenko–Bernštein estimate, Manuscript, 2006. arXiv:0709.3306.
46. J.M. Rojas, Solving degenerate sparse polynomial systems faster, *J. Symbolic Comput.* **28**(1/2), 155–186 (1999).
47. J.M. Rojas, Algebraic geometry over four rings and the frontier of tractability, in *Proceedings of a Conference on Hilbert's Tenth Problem and Related Subjects*, University of Gent, 1–5 November 1999, ed. by J. Denef et al. Contemp. Math., vol. 270 (AMS, Providence, 2000), pp. 275–321
48. J.M. Rojas, Why polyhedra matter in non-linear equation solving, in *Proceedings of the Conference on Algebraic Geometry and Geometric Modelling*, Vilnius, Lithuania, 29 July–2 August 2002. Contemp. Math., vol. 334 (AMS, Providence, 2003), pp. 293–320.
49. J.M. Rojas, X. Wang, Counting affine roots of polynomial systems via pointed Newton polytopes, *J. Complex.* **12**(2), 116–133 (1996).
50. J. Sabia, P. Solernó, Bounds for traces in complete intersections and degrees in the Nullstellensatz, *Appl. Algebra Eng. Commun. Comput.* **6**(6), 353–376 (1996).
51. J.E. Savage, *Models of Computation. Exploring the Power of Computing* (Addison-Wesley, Reading, 1998).
52. E. Schost, Computing parametric geometric resolutions, *Appl. Algebra Eng. Commun. Comput.* **13**, 349–393 (2003).
53. A. Sommese, C. Wampler, *The Numerical Solution of Systems of Polynomials Arising in Engineering and Science* (World Scientific, Singapore, 2005).
54. A. Storjohann, Algorithms for matrix canonical forms, Ph.D. thesis, ETH, Zürich, Switzerland, 2000.
55. V. Strassen, Algebraic complexity theory, in *Handbook of Theoretical Computer Science*, ed. by J. van Leeuwen (Elsevier, Amsterdam, 1990), pp. 634–671.
56. J. Verschelde, K. Gatermann, R. Cools, Mixed volume computation by dynamic lifting applied to polynomial system solving, *Discrete Comput. Geom.* **16**(1), 69–112 (1996).
57. J. Verschelde, P. Verlinden, R. Cools, Homotopies exploiting Newton polytopes for solving sparse polynomial systems, *SIAM J. Numer. Anal.* **31**(3), 915–930 (1994).
58. J. von zur Gathen, Parallel arithmetic computations: a survey, in *Proceedings of the 12th International Symposium on Mathematical Foundations of Computer Science*, Bratislava, Czechoslovakia, 25–29 August 1986, ed. by J. Gruska, B. Rovan, J. Wiedermann. Lecture Notes in Comput. Sci., vol. 233 (Springer, Berlin, 1986), pp. 93–112.
59. J. von zur Gathen, J. Gerhard, *Modern Computer Algebra* (Cambridge University Press, Cambridge, 1999).
60. R.J. Walker, *Algebraic Curves* (Dover, New York, 1950).
61. R. Zippel, *Effective Polynomial Computation*. Kluwer Int. Ser. Eng. Comput. Sci., vol. 241 (Kluwer, Dordrecht, 1993).