Discrete Comput Geom (2014) 51:578–599
DOI 10.1007/s00454-014-9571-z

Elimination for Generic Sparse Polynomial Systems

María Isabel Herrero · Gabriela Jeronimo ·
Juan Sabia

Received: 28 February 2013 / Revised: 27 December 2013 / Accepted: 6 January 2014 /
Published online: 22 January 2014

Abstract We present a new probabilistic symbolic algorithm that, given a variety defined in an n-dimensional affine space by a generic sparse system with fixed supports, computes the Zariski closure of its projection to an ℓ-dimensional coordinate affine space with $\ell < n$. The complexity of the algorithm depends polynomially on some combinatorial invariants associated to the supports.

Keywords Projection of algebraic varieties · Sparse polynomial systems ·
Algorithms and complexity

1 Introduction

Let $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_r)$ be a family of finite subsets of $(\mathbb{Z}_{\geq 0})^n$ and $\mathbf{f} = (f_1, \ldots, f_r)$ a system of polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ supported on $\mathcal{A}$. If $V(\mathbf{f}) \subset \mathbb{C}^n$ denotes the affine variety of the common zeros of the polynomials in $\mathbf{f}$ and, for a given $\ell < n$,

M.I. Herrero · G. Jeronimo
Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, 1428 Buenos Aires, Argentina
e-mail: jeronimo@dm.uba.ar

M.I. Herrero
e-mail: iherrero@dm.uba.ar

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

J. Sabia
e-mail: jsabia@dm.uba.ar

G. Jeronimo · J. Sabia
IMAS, CONICET–UBA, Buenos Aires, Argentina

$\pi : \mathbb{C}^n \to \mathbb{C}^\ell$ is the projection $\pi(x_1, \dots, x_n) = (x_1, \dots, x_\ell)$, we consider the problem of computing algorithmically a description of the Zariski closure $\overline{\pi(V(\mathbf{f}))} \subset \mathbb{C}^\ell$ within a complexity depending on combinatorial invariants associated to the input supports.

The computation of (Zariski closures of) linear projections of varieties is the basic task in elimination theory. A more general formulation of this problem is algorithmic quantifier elimination over algebraically closed fields (see, for instance, [9, 18, 23, 36, 44] for algorithms with complexities depending on the number and degrees of the polynomials and the number of variables involved). Particular instances of the computation of Zariski closures of projections are the computation of Chow forms (see, for instance, [7, 21, 29]), classical resultants (see [13] and the references therein) and sparse resultants (see, for example, [8, 12, 28, 43]).

The foundations of the study of sparse polynomial systems can be traced back to [4, 31] and [32], which prove that the number of isolated roots in $(\mathbb{C}^*)^n$ of a system of n polynomial equations in n unknowns is bounded by the mixed volume of the family of their supports.

This result led to the construction of algorithms for the computation of these isolated solutions, particularly designed to deal with sparse systems (see, for instance, [26, 30, 38, 46]), which run faster than the known general procedures solving this task. Later on, upper bounds for the number of isolated *affine* solutions of sparse systems were obtained and new efficient algorithms to compute them were designed (see, for instance, [17, 20, 24, 27, 34, 37, 39]). More recently, positive dimensional components of affine varieties defined by sparse systems were also considered: in [45], certificates for the existence of 1-dimensional components were given and, in [1] and [2], under certain assumptions on the equations, algorithmic methods to describe Puiseux series expansions of curves and arbitrary positive dimensional components, respectively, were presented. Also, in [25], an upper bound in terms of mixed volumes for the degree of the affine variety defined by a sparse polynomial system of n equations in n unknowns was proved and algorithms for characterizing the equidimensional decomposition of affine varieties defined by sparse systems were designed. The good performance of the most efficient algorithms dealing with sparse systems relies on the use of polyhedral deformations introduced in [26], because these deformations essentially preserve the monomial structure of the system involved.

In this paper, we present a probabilistic symbolic algorithm which computes the Zariski closure $\overline{\pi(V(\mathbf{f}))} \subset \mathbb{C}^\ell$ for a sparse system $\mathbf{f}$ with fixed supports and *generic* coefficients. We use the decomposition of the variety $V(\mathbf{f})$ into equidimensional subvarieties contained in coordinate subspaces proved in [25] to reduce the problem to the case of a variety such that each of its components intersects the torus. In this case we compute a *geometric resolution* of the variety with respect to a suitably chosen set of free variables and, from this resolution, we show how to obtain a geometric resolution of the Zariski closure of the required projection. The complexity of our algorithm is polynomial in some combinatorial invariants associated to the supports of the input polynomials. Our main result is the following.

Theorem 1 *Let* $\mathbf{f} = (f_1, \dots, f_r)$ *be a system of polynomials in* $\mathbb{Q}[X_1, \dots, X_n]$ *with generic coefficients supported on a family* $\mathcal{A} = (\mathcal{A}_1, \dots, \mathcal{A}_r)$ *of finite subsets of* $(\mathbb{Z}_{\geq 0})^n$ *such that* $\dim(\sum_{j \in J} \mathcal{A}_j) \geq \#J$ *for every* $J \subset \{1, \dots, r\}$, *and let* $V^*(\mathbf{f}) \subset \mathbb{C}^n$

be the Zariski closure of

$$\{x \in (\mathbb{C}^*)^n \mid f_j(x) = 0 \textit{ for every } 1 \le j \le r\}.$$

There is a probabilistic algorithm that computes a geometric resolution of $\overline{\pi(V^*(\mathbf{f}))}$, *where* $\pi : \mathbb{C}^n \to \mathbb{C}^\ell$ *is the projection to the first* ℓ *coordinates, within*

$$O\big(r\mathcal{D}\big(n^2 N \log(d)\big(\mathcal{D}^2 + \mathcal{E}\big) + \mathcal{D}^5\big)\big)$$

operations in $\mathbb{Q}$ *up to logarithmic factors, where*

$$\mathcal{D} = MV\big(\mathcal{A}, \Delta^{(n-r)}\big), \qquad N = \sum_{1\le j\le r} \#\mathcal{A}_j, \qquad d := \max_j\big\{\deg(f_j)\big\} \quad \textit{and}$$

$$\mathcal{E} = \sum_{1\le h\le r} MV\big(((\mathcal{A}_j)_{j\ne h}), \Delta^{(n-r+1)}\big).$$

Here, MV denotes the mixed volume, Δ *is the vertex set of the standard simplex in* $\mathbb{R}^n$ *and the superscript indicates the number of repetitions.*

The stated complexity is due to a polyhedral deformation-based algorithm to solve generic sparse zero-dimensional systems [30], an algorithmic Newton–Hensel lifting [40] and codification of multivariate polynomials as straight-line programs [6]. As in [30], we do not take into account the cost of mixed-volume related computations (see Sect. 2.2 for more details on this point). Furthermore, in the complexity of Theorem 1 we have ignored terms depending on the size of certain combinatorial objects associated to polyhedral deformations involved; for a more precise complexity estimate, see Theorem 10.

The paper is organized as follows. In Sect. 2, the notation and the basic theoretical and algorithmic notions used throughout are introduced. Section 3 is devoted to proving the main theoretical results on which our algorithms rely. Finally, Sect. 4 contains the descriptions, proof of correctness, and complexity estimates of our algorithms, and examples illustrating how they work.

2 Preliminaries

2.1 Basic Definitions and Notation

Let k be a field of characteristic zero and $\overline{k}$ be an algebraic closure of k. Given polynomials $f_1, \dots, f_r \in k[X_1, \dots, X_n]$, we write $V(\mathbf{f}) = V(f_1, \dots, f_r)$ for the affine variety which is the set of the common zeros of $\mathbf{f} = (f_1, \dots, f_r)$ in $\overline{k}^n$, and

$$V^*(\mathbf{f}) = V^*(f_1, \dots, f_r) := \overline{V(f_1, \dots, f_r) \cap \big(\overline{k}^*\big)^n}$$

for the union of the irreducible components of $V(f_1, \dots, f_r)$ containing points with all their coordinates in $\overline{k}^* := \overline{k} - \{0\}$.

For a variety $V \subset \overline{k}^n$ definable over k, we denote $k[V] = k[X_1, \dots, X_n]/I(V)$ its coordinate ring (where $I(V) \subset k[X_1, \dots, X_n]$ is the ideal of the polynomials vanishing identically on V). If V is irreducible, we write $k(V)$ for the fraction field of $k[V]$.

To describe zero-dimensional affine varieties we use the notion of a *geometric resolution* (see, for instance, [22] and the references therein): Let $V = \{\xi^{(1)}, \dots, \xi^{(D)}\} \subset \overline{k}^n$ be a zero-dimensional variety defined by polynomials in $k[X_1, \dots, X_n]$. Given a linear form $\lambda = \lambda_1 X_1 + \dots + \lambda_n X_n$ in $k[X_1, \dots, X_n]$ such that $\lambda(\xi^{(i)}) \neq \lambda(\xi^{(j)})$ if $i \neq j$, the following polynomials completely characterize V:

- the minimal polynomial $q_\lambda = \prod_{1 \le i \le D}(Y - \lambda(\xi^{(i)})) \in k[Y]$ of λ over the variety V (where Y is a new variable),
- polynomials $v_1, \dots, v_n \in k[Y]$ with $\deg(v_j) < D$ for every $1 \le j \le n$ satisfying $V = \{(v_1(\eta), \dots, v_n(\eta)) \in \mathbb{C}^n \mid \eta \in \overline{k}, q_\lambda(\eta) = 0\}$.

The family of univariate polynomials $(q_\lambda, v_1, \dots, v_n) \in k[Y]^{n+1}$ is called the geometric resolution of V (or a geometric resolution of $k[V]$) associated with the linear form λ.

The notion of geometric resolution can be extended to any equidimensional variety: Let $V \subset \overline{k}^n$ be an equidimensional variety of dimension t defined by polynomials in $k[X_1, \dots, X_n]$. Assume that, for each irreducible component W of V, the identity $I(W) \cap k[X_1, \dots, X_t] = \{0\}$ holds. By considering $k(X_1, \dots, X_t) \otimes k[V]$, we are in a zero-dimensional situation, and we call a *geometric resolution of V with free variables* $X_1, \dots, X_t$ to a geometric resolution $(q_\lambda, v_{t+1}, \dots, v_n) \in k(X_1, \dots, X_t)[Y]^{n-t+1}$ of $k(X_1, \dots, X_t) \otimes k[V]$ associated to a linear form $\lambda \in k[X_{t+1}, \dots, X_n]$. If $\hat{q}_\lambda \in k[X_1, \dots, X_t, Y]$ is obtained from q_λ by clearing denominators, a geometric resolution of V gives a birational map between the hypersurface $\{(x_1, \dots, x_t, y) \in \overline{k}^{n-t+1} \mid \hat{q}_\lambda(x_1, \dots, x_t, y) = 0\}$ and V.

When dealing with varieties defined by sparse polynomial systems, an important combinatorial invariant associated to the system is the mixed volume of their supports. For a family $\mathcal{A} = (\mathcal{A}_1, \dots, \mathcal{A}_n)$ of n finite subsets of $(\mathbb{Z}_{\ge 0})^n$, $MV_n(\mathcal{A})$ (or $MV(\mathcal{A})$ if n is clear from the context) denotes the n-dimensional mixed volume of the convex hulls in $\mathbb{R}^n$ of $\mathcal{A}_1, \dots, \mathcal{A}_n$ (see, for instance, [10, Chap. 7] for the definition and basic properties). In this context, we write Δ for the vertex set $\{0, e_1, \dots, e_n\}$ of the standard simplex of $\mathbb{R}^n$, which is the support of an affine linear form with non-zero coefficients, and $\Delta^{(t)}$ for the family of t copies of Δ.

2.2 Algorithms and Codification

Although we work with polynomials, our algorithms only deal with elements in a base field k. The notion of *complexity* of an algorithm we consider is the number of operations and comparisons in k it performs. We will encode multivariate polynomials in different ways:

- in sparse form, that is, by means of the list of pairs (a, c_a) where a runs over a fixed set including the exponents of the monomials appearing in the polynomial with non-zero coefficients and c_a is the corresponding coefficient,
- in the standard dense form, which encodes a polynomial of degree bounded by d as the vector of the coefficients of all the monomials of degree at most d including zeros (we use this encoding only for univariate polynomials),

- in the *straight-line program* (slp for short) encoding. A straight-line program is an algorithm without branchings which allows the evaluation of the polynomial at a generic value (for a precise definition and properties of slp's, see [6]).

In our complexity estimates, we use the usual O notation: for $f, g\colon \mathbb{Z}_{\geq 0} \to \mathbb{R}$, $f(d) = O(g(d))$ if $|f(d)| \leq c|g(d)|$ for a positive constant c. We also use the notation $M(d) = d\log^2(d)\log(\log(d))$, where log denotes logarithm to base 2. We recall that multipoint evaluation and interpolation of univariate polynomials of degree d with coefficients in a commutative ring R of characteristic 0 can be performed with $O(M(d))$ operations and that multiplication and division with remainder of such polynomials can be done with $O(M(d)/\log(d))$ arithmetic operations in R. We write Ω for the exponent ($\Omega < 4$) in the complexity $O(d^{\Omega})$ of operations (determinant and adjoint computations) on $d \times d$ matrices with entries in a commutative ring R [3]. We use Padé approximation in order to compute the dense representation of the numerator and denominator of a rational function $f = \frac{p}{q} \in k(Y)$ with $\max\{\deg p, \deg q\} \leq d$ from its Taylor series expansion up to order $2d$, which we do by means of subresultant computations within $O(d^{\Omega+1})$ arithmetic operations in k (see [48, Corollaries 5.21 and 6.48]).

Our algorithms are probabilistic in the sense that they make random choices of points (which we consider cost-free in our complexity estimates) which lead to a correct computation provided the points lie outside certain proper Zariski closed sets of suitable affine spaces. Using the Schwartz–Zippel Lemma [41, 49], the error probability of our algorithms can be controlled by making these random choices within sufficiently large sets of integer numbers whose size depend on the degrees of the polynomials defining the previously mentioned Zariski closed sets.

We use two previous algorithms as subroutines:

- a probabilistic algorithm that, given n generic sparse polynomials in n variables with coefficients in k, computes a geometric resolution of the set of their common zeros in $\overline{k}^n$ (see [30, Sect. 5]),
- a Newton–Hensel-based procedure that, given a system $\mathbf{f}$ of n polynomials in n variables and t parameters, a specialization point $\xi \in \mathbb{Q}^t$ for the parameters and a geometric resolution of the set of simple common zeros of $\mathbf{f}(\xi, \cdot)$, computes an approximation up to a given precision of the geometric resolution of the components of $V(\mathbf{f})$ where the Jacobian determinant of the system with respect to its n variables does not vanish identically (see [40, Sect. 4.2]).

The algorithm in [30] assumes that the mixed cells in a fine mixed subdivision of the family of the input supports are given (see [26] for the definition of a fine mixed subdivision), that is to say, the computation of mixed cells is considered as a pre-processing. In this paper, our algorithms also require deciding whether a mixed volume is zero or not, and computing mixed volumes.

While the non-vanishing of a mixed volume can be decided algorithmically in polynomial time, the problem of computing mixed volumes is known to be #P-hard (see [14, 16]). The mixed cells in a fine mixed subdivision of a family of finite sets of $\mathbb{Z}^n$ (and, therefore, the mixed volume) can be obtained algorithmically by means of *lifting* (see [26]) and linear programming-based procedures. In [16], an algorithm following this approach is presented with a worst-case complexity single exponential in n. Successive algorithms that run faster according to numerical results can be found in [33] and [19]. A dynamic approach which does not use a random lifting function is given in [47]. The dynamic enumeration procedure from [35], which proved to be efficient even for large systems, seems to be the fastest known up until now. However, there are no explicit complexity upper bounds for these more efficient procedures, neither depending on the input nor the output size (namely, the mixed volume).

As in [30], we consider the computation of mixed cells as a pre-processing and do not include its cost in our complexity estimates. Note that if our algorithm needs to be applied to several systems with the same supports, this pre-processing only has to be carried out once.

3 Theoretical Results

Let n, r be positive integers and $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_r)$ a family of r finite subsets of $(\mathbb{Z}_{\geq 0})^n$. Consider r polynomials in n variables $X = (X_1, \ldots, X_n)$ supported on $\mathcal{A}$ with indeterminate coefficients: for every $1 \leq j \leq r$, let

$$f_j(C_j, X) = \sum_{a \in \mathcal{A}_j} C_{j,a} X^a, \tag{1}$$

where $C_j := (C_{j,a})_{a \in \mathcal{A}_j}$ is a set of $N_j := \#\mathcal{A}_j$ new indeterminates. Let $\mathbf{f} := (f_1, \ldots, f_r)$ and $K := \mathbb{Q}(C_1, \ldots, C_r)$.

3.1 Reduction to the Toric Case

Consider the family $\mathbf{f} = (f_1, \ldots, f_r)$ of polynomials in $K[X_1, \ldots, X_n]$ supported on $\mathcal{A}$ with indeterminate coefficients introduced in (1). Since $\mathbf{f}$ is a generic system supported on $\mathcal{A}$, the equidimensional decomposition of the affine variety $V(\mathbf{f}) \subset \overline{K}^n$ depends only on the combinatorial structure of $\mathcal{A}$ (see [25]). Moreover, its equidimensional components can be defined from certain smaller polynomial families $\mathbf{f}_I$ in fewer variables associated to $\mathbf{f}$. This decomposition, which we explain below, enables us to reduce the problem of computing a projection of the affine variety $V(\mathbf{f})$ to the computation of finitely many projections of varieties having a non-empty intersection with the torus.

For $I \subset \{1, \ldots, n\}$, given a polynomial $f \in K[X_1, \ldots, X_n]$, we write f_I to denote the polynomial in $K[(X_i)_{i \notin I}]$ obtained from f by specializing $X_i = 0$ for every $i \in I$. We define $J_I = \{j \in \{1, \ldots, r\} \mid \exists a \in \mathcal{A}_j : a_i = 0 \, \forall i \in I\}$ and $\mathbf{f}_I = ((f_j)_I)_{j \in J_I}$ (note that J_I is the set of indices of those polynomials f_j that do not vanish identically when specializing $X_i = 0$ for every $i \in I$). Let

$$\Gamma = \Big\{ I \subset \{1, \ldots, n\} \mid \forall J \subset J_I,\ \dim\Big(\sum_{j \in J} \mathcal{A}_j^I\Big) \geq \#J; \forall \widetilde{I} \subset I,\ \#J_{\widetilde{I}} + \#\widetilde{I} \geq \#J_I + \#I \Big\},$$

where, for every $1 \leq j \leq r$, $\mathcal{A}_j^I \subset (\mathbb{Z}_{\geq 0})^{n - \#I}$ denotes the support of $(f_j)_I$. Finally, let $\varphi_I : \overline{K}^{n-\#I} \to \overline{K}^n$ be the map that inserts zeros in the coordinates indexed by I.

Using the previous notation, according to [25, Theorem 7], we have

$$V(\mathbf{f}) = \bigcup_{I\in\Gamma} \varphi_I\big(V^*(\mathbf{f}_I)\big).$$

Let $\pi : \overline{K}^n \to \overline{K}^\ell$ be the projection $\pi(x_1,\dots,x_n) = (x_1,\dots,x_\ell)$. For $I \subset \{1,\dots,n\}$, let $\ell_I = \ell - \#(I\cap\{1,\dots,\ell\})$, $\pi_{\ell_I} : \overline{K}^{n-\#I} \to \overline{K}^{\ell_I}$ the projection to the first coordinates and $\varphi_{I\cap\{1,\dots,\ell\}} : \overline{K}^{\ell_I} \to \overline{K}^\ell$ the map that inserts zeros in the coordinates indexed by $I\cap\{1,\dots,\ell\}$. As $\pi(\varphi_I(V^*(\mathbf{f}_I))) = \varphi_{I\cap\{1,\dots,\ell\}}(\pi_{\ell_I}(V^*(\mathbf{f}_I)))$ holds for every I, we conclude that

$$\pi\big(V(\mathbf{f})\big) = \bigcup_{I\in\Gamma} \varphi_{I\cap\{1,\dots,\ell\}}\big(\pi_{\ell_I}\big(V^*(\mathbf{f}_I)\big)\big).$$

Therefore, the computation of $\overline{\pi(V(\mathbf{f}))}$ amounts to obtaining the Zariski closures of the projections by π_{ℓ_I} of the affine varieties $V^*(\mathbf{f}_I) = \{x\in(\overline{K}^*)^{n-\#I} \mid \mathbf{f}_I(x)=0\}$. For this reason, in the sequel we will deal with this problem.

3.2 The Vanishing Ideal of the Projection

We consider a generic polynomial system $\mathbf{f} := (f_1,\dots,f_r)$ supported on $\mathcal{A} := (\mathcal{A}_1,\dots,\mathcal{A}_r)$ with indeterminate coefficients $C_j := (C_{j,a})_{a\in\mathcal{A}_j}$ for every $1\le j\le r$ as in Eq. (1). We assume that $r\le n$ and that, for every $J\subset\{1,\dots,r\}$, $\dim(\sum_{j\in J}\mathcal{A}_j)\ge \#J$ (or, equivalently, $MV(\mathcal{A},\Delta^{(n-r)})>0$) so that $V^*(\mathbf{f})$ is not empty.

Our aim is to obtain a geometric resolution of the Zariski closure $\overline{\pi(V^*(\mathbf{f}))}$, where $\pi : \overline{K}^n \to \overline{K}^\ell$ ($\ell\le n$) is the projection defined by $\pi(x_1,\dots,x_n) = (x_1,\dots,x_\ell)$. We begin by proving some basic results on the vanishing ideals of the varieties $V^*(\mathbf{f})$ and $\overline{\pi(V^*(\mathbf{f}))}$.

Lemma 2 *Under the previous assumptions,* $(f_1,\dots,f_r) : (X_1\cdots X_n)^\infty$ *is a prime ideal in* $K[X_1,\dots,X_n]$ *of dimension* $n-r$. *Moreover,* $I(V^*(\mathbf{f})) = (f_1,\dots,f_r) : (X_1\cdots X_n)^\infty$.

Proof For every $1\le j\le r$, fix $a_{j0}\in\mathcal{A}_j$ and let $\mathcal{A}'_j := \mathcal{A}_j - \{a_{j0}\}$ and $C'_j := C_j - \{C_{j,a_{j0}}\}$. We denote $C := (C_1,\dots,C_r)$ and $C' := (C'_1,\dots,C'_r)$. Consider the ring morphism $\psi : \mathbb{Q}[C,X] \to \mathbb{Q}[C',X]_{X_1\cdots X_n}$ (where $\mathbb{Q}[C',X]_{X_1\cdots X_n}$ is the localization of $\mathbb{Q}[C',X]$ at the multiplicative set $\{(X_1\cdots X_n)^m \mid m\in\mathbb{Z}_{\ge 0}\}$) defined by $\psi(X_i) = X_i$ for $1\le i\le n$, $\psi(C_{j,a}) = C_{j,a}$ for $1\le j\le r$, $a\in\mathcal{A}'_j$, and $\psi(C_{j,a_{j0}}) = -X^{-a_{j0}}(\sum_{a\in\mathcal{A}'_j} C_{j,a}X^a)$ for $1\le j\le r$.

We claim that $\ker(\psi) = (f_1,\dots,f_r) : (X_1\cdots X_n)^\infty$. It is clear that for a polynomial $g\in(f_1,\dots,f_r) : (X_1\cdots X_n)^\infty$, $\psi(g)=0$. Assume now that for a polynomial $g\in\mathbb{Q}[C,X]$ we have $\psi(g)=0$. Let $C_0 := (C_{1,a_{10}},\dots,C_{r,a_{r0}})$ and let $\widehat{C}_0 := (\widehat{C}_{10},\dots,\widehat{C}_{r0})$ be new variables. By Taylor expansion, $g(\widehat{C}_0,C',X) = g(C_0,C',X) + \sum_{1\le j\le r}(\widehat{C}_{j0} - C_{j,a_{j0}})\cdot G_j$ for certain polynomials $G_j\in\mathbb{Q}[\widehat{C}_0,C,X]$.

Specializing $\widehat{C}_{j0} = -X^{-a_{j0}}(\sum_{a\in\mathcal{A}'_j} C_{j,a}X^a)$ for every $1 \le j \le r$, it follows that $\psi(g) = g(C_0, C', X) - \sum_{1\le j\le r} X^{-a_{j0}} f_j \cdot \widetilde{G}_j$ with $\widetilde{G}_j \in \mathbb{Q}[C, X]_{X_1\cdots X_n}$; therefore, $g(C, X) = \sum_{1\le j\le r} X^{-a_{j0}} f_j \cdot \widetilde{G}_j$. Multiplying by $(X_1 \cdots X_n)^m$ for a sufficiently large m, we conclude that $(X_1 \cdots X_n)^m g(C, X) \in (f_1, \ldots, f_r)$.

Then, $(f_1, \ldots, f_r) : (X_1 \cdots X_n)^\infty$ is a prime ideal of $\mathbb{Q}[C, X]$. The first statement of the lemma follows by localizing at $\mathbb{Q}[C] - \{0\}$.

In order to prove the second part of the lemma, consider first a polynomial $g \in (f_1, \ldots, f_r) : (X_1 \cdots X_n)^\infty$, and let $m \in \mathbb{Z}_{\ge 0}$ be such that $(X_1 \cdots X_n)^m g \in (f_1, \ldots, f_r)$. Then, $(X_1 \cdots X_n)^m g$ vanishes over $V(\mathbf{f})$ and so, g vanishes over $V(\mathbf{f}) \cap (\overline{K}^*)^n$; therefore, $g \in I(V^*(\mathbf{f}))$. Conversely, if $g \in I(V^*(\mathbf{f}))$, then it vanishes over each irreducible component of $V(\mathbf{f})$ intersecting $(\overline{K}^*)^n$ properly. Then, $(X_1 \cdots X_n)g$ vanishes over $V(f_1, \ldots, f_r)$, which implies that there exists $m \in \mathbb{Z}_{\ge 0}$ with $(X_1 \cdots X_n)^m g^m \in (f_1, \ldots, f_r)$. Therefore, $g^m \in (f_1, \ldots, f_r) : (X_1 \cdots X_n)^\infty$ and, since this is a prime ideal, it follows that $g \in (f_1, \ldots, f_r) : (X_1 \cdots X_n)^\infty$. □

Corollary 3 *The affine variety $V^*(\mathbf{f}) \subset \overline{K}^n$ is an irreducible K-variety of dimension $n - r$.*

Taking into account that for any K-variety $V \subset \overline{K}^n$, the identity $I(\overline{\pi(V)}) = I(V) \cap K[X_1, \ldots, X_\ell]$ holds, Lemma 2 also enables us to characterize the vanishing ideal of the projection we want to compute:

Corollary 4 *With the previous assumptions and notation*,

$$I\big(\overline{\pi\big(V^*(\mathbf{f})\big)}\big) = \big((f_1, \ldots, f_r) : (X_1 \cdots X_n)^\infty\big) \cap K[X_1, \ldots, X_\ell].$$

Let $t := \dim(\overline{\pi(V^*(\mathbf{f}))})$. Without loss of generality, by renaming variables, we may assume that $\{X_1, \ldots, X_t\} \subset \{X_1, \ldots, X_\ell\}$ is a transcendence basis of $K(\overline{\pi(V^*(\mathbf{f}))})$ over K and $\{X_{t+r+1}, \ldots, X_n\}$ are such that $\{X_1, \ldots, X_t, X_{t+r+1}, \ldots, X_n\}$ is a transcendence basis of $K(V^*(\mathbf{f}))$ over K. The following proposition generically allows us to deal with projections with 0-dimensional generic fibers.

Proposition 5 *There is a Zariski dense open set $\mathcal{O} \subseteq \overline{K}^{n-t-r}$ such that, for every $b \in K^{n-t-r} \cap \mathcal{O}$, the identity $I(\overline{\pi(V^*(\mathbf{f}))}) = ((f_1(X_1, \ldots, X_{t+r}, b), \ldots, f_r(X_1, \ldots, X_{t+r}, b)) : (X_1 \cdots X_{t+r})^\infty) \cap K[X_1, \ldots, X_\ell]$ holds.*

Proof Let $\widehat{X} := (X_1, \ldots, X_{t+r})$. From Corollary 4, it is clear that $I(\overline{\pi(V^*(\mathbf{f}))}) \subset ((f_1(\widehat{X}, b), \ldots, f_r(\widehat{X}, b)) : (X_1 \cdots X_{t+r})^\infty) \cap K[X_1, \ldots, X_\ell]$ for every $b = (b_{t+r+1}, \ldots, b_n)$ such that $b_i \ne 0$ for every $t + r + 1 \le i \le n$.

For the converse inclusion, first note that, for every $1 \le j \le r$,

$$\begin{aligned} &K[X_1, \ldots, X_n]/(f_1, \ldots, f_j) : (X_1 \cdots X_n)^\infty \\ &\quad\simeq K[X_1, \ldots, X_n]_{(X_1\cdots X_n)}/(f_1, \ldots, f_j) \\ &\quad\simeq K[Y, X_1, \ldots, X_n]/(YX_1 \cdots X_n - 1, f_1, \ldots, f_j). \end{aligned}$$

As in the first part of the proof of Lemma 2, it follows that $(f_1,\dots,f_j):(X_1\cdots X_n)^\infty$ is a prime ideal of dimension $n-j$ for every $1\le j\le r$; therefore, $YX_1\cdots X_n-1$, $f_1,\dots,f_r$ is a reduced regular sequence in $K[Y,X_1,\dots,X_n]$. Moreover, the set $\{X_1,\dots,X_t,X_{t+r+1},\dots,X_n\}$ is algebraically independent modulo $(YX_1\cdots X_n-1$, $f_1,\dots,f_r)$. Then, by [11, Corollary 17 and Theorem 19], there exists a K-definable Zariski dense open set $\mathcal{O}\subset\overline{K}^{n-t-r}$ containing $\{x_i\neq 0\ \forall\, 1\le i\le t+r\}$ such that for every $b\in\mathcal{O}\cap K^{n-t-r}$, $c_bYX_1\cdots X_{t+r}-1$, $f_1(\widehat{X},b),\dots,f_r(\widehat{X},b)$ (where $c_b:=b_{t+r+1}\cdots b_n$) is a reduced regular sequence in $K[\widehat{X}]$ and $\{X_1,\dots,X_t\}$ is algebraically independent modulo each of the associated primes of the ideal this regular sequence generates. By noticing that

$$\begin{aligned}K[\widehat{X}]/\big(f_1(\widehat{X},b),\dots,f_r(\widehat{X},b)\big):(X_1\cdots X_{t+r})^\infty\\ \simeq K[\widehat{X}]/\big(c_bYX_1\cdots X_{t+r}-1,f_1(\widehat{X},b),\dots,f_r(\widehat{X},b)\big),\end{aligned}$$

we conclude that $(f_1(\widehat{X},b),\dots,f_r(\widehat{X},b)):(X_1\cdots X_{t+r})^\infty$ is a radical equidimensional ideal of dimension t and $\{X_1,\dots,X_t\}$ is algebraically independent modulo each of its associated primes. Then, the same holds for the ideal $((f_1(\widehat{X},b),\dots,f_r(\widehat{X},b)):(X_1\cdots X_{t+r})^\infty)\cap K[X_1,\dots,X_\ell]$. As this ideal includes the t-dimensional prime ideal $I(\overline{\pi(V^*(\mathbf{f}))})$, the equality in the statement of the proposition holds. □

3.3 Free Variables

The following result gives a combinatorial condition for the algebraic independence of a subset of variables modulo the vanishing ideal of $V^*(\mathbf{f})$ that we will use in our algorithm to compute a suitable transcendence basis of the rational fraction field of this variety.

Lemma 6 *Let $f_1,\dots,f_r\in K[X_1,\dots,X_n]$ be sparse polynomials supported on a family $\mathcal{A}=(\mathcal{A}_1,\dots,\mathcal{A}_r)$ of finite subsets of $(\mathbb{Z}_{\ge 0})^n$ as introduced in (1), and let $\mathcal{I}=(f_1,\dots,f_r):(X_1\cdots X_n)^\infty\subset K[X_1,\dots,X_n]$. Let $\{e_1,\dots,e_n\}$ be the canonical basis of $\mathbb{Q}^n$.*

Then, the set $\{X_{i_1},\dots,X_{i_k}\}\subset\{X_1,\dots,X_n\}$ for $1\le i_1<\cdots<i_k\le n$ is algebraically independent modulo $\mathcal{I}$ if and only if $MV(\mathcal{A}_1,\dots,\mathcal{A}_r,\{0,e_{i_1}\},\dots,\{0,e_{i_k}\},\Delta^{(n-r-k)})>0$.

Proof First, assume that $MV(\mathcal{A}_1,\dots,\mathcal{A}_r,\{0,e_{i_1}\},\dots,\{0,e_{i_k}\},\Delta^{(n-r-k)})>0$. Let Q be a non-zero polynomial in the coefficients of a system supported on $(\mathcal{A},\{0,e_{i_1}\},\dots,\{0,e_{i_k}\},\Delta^{(n-r-k)})$ such that for each coefficient vector $(c,\eta)=(c_1,\dots,c_r,\eta_{r+1},\dots,\eta_n)$ with coordinates in $\mathbb{Q}^*$ and $Q(c,\eta)\neq 0$, the corresponding sparse system has as many isolated solutions in $(\mathbb{C}^*)^n$ as the mixed volume.

Let $p\in\mathcal{I}\cap K[X_{i_1},\dots,X_{i_k}]$. Without loss of generality, we may assume that $p\in\mathbb{Q}[C,X_{i_1},\dots,X_{i_k}]$. Then there exist $m\in\mathbb{Z}_{\ge 0}$ and a non-zero polynomial $p_0\in\mathbb{Q}[C]$ such that

$$p_0(C)(X_1\cdots X_n)^m p(C,X_{i_1},\dots,X_{i_k})=g_1f_1+\cdots+g_rf_r \tag{2}$$

with $g_1,\dots,g_r\in\mathbb{Q}[C,X_1,\dots,X_n]$.

For each (c,η) with coordinates in $\mathbb{Q}^*$ such that $p_0(c)Q(c,\eta)\neq 0$, considering a solution $\xi \in (\mathbb{C}^*)^n$ of the system

$$
\begin{aligned}
&f_1(c_1,X)=0, \quad \dots, \quad f_r(c_r,X)=0,\\
&\eta_{r+1,1}+\eta_{r+1,2}X_{i_1}=0, \quad \dots, \quad \eta_{r+k,1}+\eta_{r+k,2}X_{i_k}=0,\\
&\eta_{r+k+1,0}+\sum_{1\le i\le n}\eta_{r+k+1,i}X_i=0, \quad \dots, \quad \eta_{n,0}+\sum_{1\le i\le n}\eta_{n,i}X_i=0
\end{aligned}
$$

and specializing identity (2) in (c,η,ξ) we obtain $p(c,-\eta_{r+1,1}/\eta_{r+1,2},\dots,-\eta_{r+k,1}/\eta_{r+k,2})=0$. We conclude that $p\equiv 0$.

Assume now that $\{X_{i_1},\dots,X_{i_k}\}$ is algebraically independent modulo $\mathcal{I}=I(V^*(\mathbf{f}))$. Let $l_1,\dots,l_{n-r-k}$ be linear forms in the variables $X_1,\dots,X_n$ with coefficients in K^* such that $\{X_{i_1},\dots,X_{i_k},l_1,\dots,l_{n-r-k}\}$ is a transcendence basis of $K(V^*(\mathbf{f}))$. Since $V^*(\mathbf{f})\cap(\overline{K}^*)^n$ is a dense open subset of $V^*(\mathbf{f})$, for a generic $(\zeta_1,\dots,\zeta_{n-r})\in(\overline{K}^*)^{n-r}$, the set

$$V^*(\mathbf{f})\cap\{x_{i_j}=\zeta_j\ \forall\, 1\le j\le k\}\cap\big\{l_j(x)=\zeta_{k+j}\ \forall\, 1\le j\le n-r-k\big\}$$

is not empty and consists of finitely many points in $(\overline{K}^*)^n$. These points are the common solutions in $(\overline{K}^*)^n$ of the system

$$
\begin{aligned}
&f_1(X)=0, \quad \dots, \quad f_r(X)=0, \qquad X_{i_1}-\zeta_1=0, \quad \dots, \quad X_{i_k}-\zeta_k=0,\\
&l_1(X)-\zeta_{k+1}=0, \quad \dots, \quad l_{n-r-k}(X)-\zeta_{n-r}=0,
\end{aligned}
$$

which is supported on $(\mathcal{A}_1,\dots,\mathcal{A}_r,\{0,e_{i_1}\},\dots,\{0,e_{i_k}\},\Delta^{(n-r-k)})$. By Bernstein's Theorem, we conclude that $MV(\mathcal{A}_1,\dots,\mathcal{A}_r,\{0,e_{i_1}\},\dots,\{0,e_{i_k}\},\Delta^{(n-r-k)})>0$. □

Remark 7 For $1\le i_1<\dots<i_k\le n$, we have

$$
\begin{aligned}
&MV_n\big(\mathcal{A}_1,\dots,\mathcal{A}_r,\{0,e_{i_1}\},\dots,\{0,e_{i_k}\},\Delta^{(n-r-k)}\big)\\
&\quad=MV_{n-k}\big(\varpi(\mathcal{A}_1),\dots,\varpi(\mathcal{A}_r),\varpi(\Delta)^{(n-r-k)}\big)
\end{aligned}
$$

(see [42, Lemma 6]), where $\varpi:\mathbb{R}^n\to\mathbb{R}^{n-k}$ is the projection to the coordinates indexed by $\{1,\dots,n\}-\{i_1,\dots,i_k\}$. This implies that, in order to determine whether a set of k variables is algebraically independent or not, it suffices to determine whether an $(n-k)$-dimensional mixed volume is zero or not.

4 Algorithms

In this section we will present an algorithm to compute the Zariski closure of the projection of $V^*(\mathbf{f})$ to the first ℓ coordinates, where $\mathbf{f}$ is a generic polynomial system with given supports. First, we describe some subroutines.

4.1 Subroutines

The first subroutine we will use, which follows from Lemma 6, computes a transcendence basis of $K(V^*(\mathbf{f}))$ containing a transcendence basis of $K(\overline{\pi(V^*(\mathbf{f}))})$.

Algorithm `TransBasis`

INPUT: A family $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_r)$ of finite subsets of $(\mathbb{Z}_{\geq 0})^n$ such that $\dim(\sum_{j \in J} \mathcal{A}_j) \geq \#J$ for every $J \subset \{1, \ldots, r\}$.

1. $TB := \emptyset$
2. $k := 1$
3. while $\#TB < n - r$ do
   (a) If $MV(\mathcal{A}_1, \ldots, \mathcal{A}_r, (\{0, e_{i_j}\})_{i_j \in TB}, \{0, e_k\}, \Delta^{(n-r-\#TB-1)}) > 0$,
   $TB := TB \cup \{k\}$.
   (b) $k := k + 1$

OUTPUT: The set $TB = \{i_1, \ldots, i_{n-r}\}$ with $i_1 < \cdots < i_{n-r}$ such that $\{X_{i_1}, \ldots, X_{i_{n-r}}\}$ is a transcendence basis of $K(V^*(\mathbf{f}))$ over K and, for each $1 \leq j \leq n - r$, $\{X_{i_1}, \ldots, X_{i_j}\}$ is a maximal algebraically independent subset of $\{X_1, \ldots, X_{i_j}\}$.

Note that the above algorithm requires to decide whether the mixed volume of a family of finite sets is non-zero for at most n families. Following [14, Theorem 8], there is a polynomial time algorithm to achieve this task based on the matroid intersection algorithm from [15]. Therefore, Algorithm `TransBasis` runs in polynomial time.

Without loss of generality, by renaming variables, we may assume that the transcendence basis of $K(V^*(\mathbf{f}))$ obtained by applying algorithm `TransBasis` is $\{X_1, \ldots, X_t, X_{t+r+1}, \ldots, X_n\}$ with $t \leq \ell$ and $\ell \leq t + r$. Then, $\{X_1, \ldots, X_t\}$ is a transcendence basis of $K(\overline{\pi(V^*(\mathbf{f}))})$. Let $\mathbf{f}_b$ be the polynomial system obtained by evaluating $X_{t+r+1}, \ldots, X_n$ in a generic point b. By Proposition 5, we may obtain $\overline{\pi(V^*(\mathbf{f}))}$ using the system $\mathbf{f}_b$. In order to do this, we will compute first a geometric resolution of $V^*(\mathbf{f}_b)$ by means of the subroutine we introduce below.

Let k be a field of characteristic 0. Algorithm `ParametricToricGeomRes` computes a geometric resolution of the variety $V^*(\mathbf{g})$ defined from a generic sparse system $\mathbf{g} := (g_1, \ldots, g_r)$ in $k[X_1, \ldots, X_{t+r}]$ with given supports $\mathcal{S} := (\mathcal{S}_1, \ldots, \mathcal{S}_r)$, provided that $\{X_1, \ldots, X_t\}$ is a set of independent variables for all its components. This subroutine is obtained by following the parametric geometric resolution algorithm from [40, Theorem 2] taking $X_1, \ldots, X_t$ as the parameters.

Algorithm `ParametricToricGeomRes`

INPUT: A generic sparse system $\mathbf{g} := (g_1, \ldots, g_r)$ in $k[X_1, \ldots, X_{t+r}]$ with given supports $\mathcal{S} := (\mathcal{S}_1, \ldots, \mathcal{S}_r)$ such that $\{X_1, \ldots, X_t\}$ is algebraically independent modulo each associated prime of $(g_1, \ldots, g_r) : (X_1 \cdots X_{t+r})^\infty$.

1. Choose $\xi = (\xi_1, \dots, \xi_t)$ at random with $\xi_i \in \mathbb{Z} - \{0\}$ for every $1 \le i \le t$.
2. Compute a geometric resolution of the common solutions of $\mathbf{g}(\xi, X_{t+1}, \dots, X_{t+r})$ in $(\overline{k}^*)^r$.
3. Obtain an slp encoding the polynomials in $\mathbf{g}$.
4. Apply a symbolic Newton–Hensel lifting (in the parameters $X_1, \dots, X_t$) to the geometric resolution obtained in step 2 with precision $2MV(\mathcal{S}, \Delta^{(t)})$.
5. Applying Padé approximation to the output of the previous step, recover numerators and denominators in $k[X_1, \dots, X_t]$ for the coefficients of the polynomials in the geometric resolution of $V^*(\mathbf{g})$.

OUTPUT: A geometric resolution of $V^*(\mathbf{g})$ with free variables $X_1, \dots, X_t$.

Before estimating the complexity of the previous algorithm, we present a simple example to illustrate how the algorithm works.

Example Let $\mathbf{g}$ be the following sparse system supported on $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$, where $\mathcal{S}_1 = \{(0,0,0), (1,1,0), (0,1,1)\}$ and $\mathcal{S}_2 = \{(0,0,0), (2,1,1), (0,2,0), (1,1,1)\}$:

$$\mathbf{g} := \begin{cases} g_1 = 2 + 3X_1X_2 - X_2X_3, \\ g_2 = -1 + 2X_1^2X_2X_3 + 2X_2^2 + X_1X_2X_3. \end{cases}$$

Here, $\{X_1\}$ is algebraically independent modulo $(g_1, g_2) : (X_1X_2X_3)^\infty$.

In step 1, the algorithm chooses a value $\xi_1 \in \mathbb{Z} - \{0\}$ at random and specializes $X_1 = \xi_1$. Setting $\xi_1 = 1$, we obtain the system

$$\mathbf{g}_1 := \begin{cases} g_{11} = 2 + 3X_2 - X_2X_3, \\ g_{21} = -1 + 3X_2X_3 + 2X_2^2. \end{cases}$$

Now, the algorithm computes a geometric resolution of the common zeros of $\mathbf{g}_1$ in $(\mathbb{C}^*)^2$. This is a generic system supported on $(\{(0,0), (1,0), (1,1)\}, \{(0,0), (1,1), (2,0)\})$. Then, in order to solve it, we can apply the algorithm from [30, Sect. 5]. Choosing X_3 as separating linear form, we obtain

- $q_{X_3}(Y) = Y^2 - \frac{12}{5}Y - \frac{1}{5}$
- $w_2(Y) = -\frac{5}{4}Y - \frac{3}{4}$
- $w_3(Y) = Y$

From this geometric resolution, the algorithm computes a sufficiently good approximation of a geometric resolution of $V^*(\mathbf{g})$.

A geometric resolution of $V^*(\mathbf{g})$ consists of univariate polynomials with coefficients that are rational functions in the parameter X_1 with numerators and denominators of degrees bounded by $\deg V^*(\mathbf{g})$ (see [40, Theorem 1]). These rational functions can be regarded as power series in the variable X_1 centered at $\xi_1 = 1$, and therefore, they can be recovered by means of Padé approximation from sufficiently many terms of their expansions. The precision required to do this equals $2\deg V^*(\mathbf{g}) = 2MV(\mathcal{S}, \Delta)$. Since $MV(\mathcal{S}, \Delta) = 6$, in step 4, the algorithm applies a Newton–Hensel lifting (in the parameter X_1), as explained in [40, Sect. 4.2], to the geometric resolution (q_{X_3}, w_2, w_3) with precision 12, obtaining

- $\widehat{q}_{X_3}(Y) = Y^2 + q_1 Y + q_0$
- $\widehat{w}_2(Y) = w_{21} Y + w_{20}$
- $\widehat{w}_3(Y) = w_{31} Y + w_{30}$

where

- $q_1 = -\frac{12}{5} - \frac{18}{5}(X_1 - 1) + \frac{18}{25}(X_1 - 1)^2 - \frac{24}{25}(X_1 - 1)^3 + \frac{168}{125}(X_1 - 1)^4 - \frac{48}{25}(X_1 - 1)^5 + \frac{1728}{625}(X_1 - 1)^6 - \frac{2496}{625}(X_1 - 1)^7 + \frac{18048}{3125}(X_1 - 1)^8 - \frac{26112}{3125}(X_1 - 1)^9 + \frac{188928}{15625}(X_1 - 1)^{10} - \frac{273408}{15625}(X_1 - 1)^{11} + \frac{1978368}{78125}(X_1 - 1)^{12}$
- $q_0 = -\frac{1}{5} - \frac{16}{5}(X_1 - 1) + \frac{119}{25}(X_1 - 1)^2 - \frac{174}{25}(X_1 - 1)^3 + \frac{1264}{125}(X_1 - 1)^4 - \frac{1832}{125}(X_1 - 1)^5 + \frac{13264}{625}(X_1 - 1)^6 - \frac{768}{25}(X_1 - 1)^7 + \frac{138944}{3125}(X_1 - 1)^8 - \frac{201088}{3125}(X_1 - 1)^9 + \frac{1455104}{15625}(X_1 - 1)^{10} - \frac{2105856}{15625}(X_1 - 1)^{11} + \frac{15238144}{78125}(X_1 - 1)^{12}$
- $w_{21} = -\frac{5}{4} - \frac{5}{2}(X_1 - 1) - (X_1 - 1)^2$
- $w_{20} = -\frac{3}{4} - \frac{3}{4}(X_1 - 1)$
- $w_{31} = 1$
- $w_{30} = 0$

Finally, Padé approximation is applied, following [48, Corollaries 5.21 and 6.48], to each of the coefficients previously computed in order to obtain the numerators and denominators of the coefficients in the geometric resolution of $V^*(\mathbf{g})$ associated to the linear form X_3:

- $Q_{X_3}(Y) = Y^2 + \frac{-12X_1^3 - 6X_1^2 + 6X_1}{4X_1^2 + 2X_1 - 1} Y + \frac{-9X_1^2 + 8}{4X_1^2 + 2X_1 - 1}$
- $W_2(Y) = (-X_1^2 - \frac{1}{2}X_1 + \frac{1}{4})Y - \frac{3}{4}X_1$
- $W_3(Y) = Y$

Now we explain how the different steps of the algorithm are carried out in general and estimate the number of operations in k it performs. We will use the notation $N = \sum_{1 \le j \le r} \#\mathcal{S}_j$ and $d = \max_{1 \le j \le r} \deg(g_j)$.

In Step 2, the algorithm computes the sparse encoding of $\mathbf{g}(\xi, X_{t+1}, \ldots, X_{t+r})$ within $O(r(t+r)N\log(d))$ operations. Then, this system is solved using the procedure from [30, Sect. 5] within complexity $O(r^3 N \log(d) M(\mathcal{M}) M(MV(\varpi(\mathcal{S}))) \times (M(MV(\varpi(\mathcal{S}))) + M(\omega_{\max} \sum_{1 \le h \le r} MV(\varpi(\mathcal{S}_j)_{j \ne h}, \Delta))))$, where ϖ is the projection to the last r coordinates, $\omega_{\max}$ is the maximum of the values taken by a generic lifting function ω for $\varpi(\mathcal{S}) := (\varpi(\mathcal{S}_1), \ldots, \varpi(\mathcal{S}_r))$, and $\mathcal{M} := \max\{\|\mu\|\}$, the maximum ranging over all primitive normal vectors to the mixed cells in the fine mixed subdivision of $\varpi(\mathcal{S})$ induced by ω.

In Step 3, an slp of length $O((t+r)N\log(d))$ encoding the polynomials $\mathbf{g}$ is obtained from their sparse representation.

The next step is performed modifying the procedure in [40, Sect. 4.2] in order to use straight-line programs for computations with truncated multivariate power series. We represent each of these series as the vector of its homogeneous components and these components by means of straight-line programs. The required precision is $2\deg(V^*(\mathbf{g})) = 2MV(\mathcal{S}, \Delta^{(t)})$ (see [40, Theorem 1] and [25, Lemma 1]). Therefore, this step is done within complexity $O((r(t+r)N\log(d) + r^4) M(MV(\varpi(\mathcal{S}))) MV(\mathcal{S}, \Delta^{(t)})^2)$ and produces an slp of the same order encoding the homogeneous components of the coefficients of the output.

Finally, the Padé approximation to obtain the coefficients of the geometric resolution is done by reducing it to a univariate problem and solving it by means of subresultant computations following [48, Corollaries 5.21 and 6.48]. This step adds $O(rMV(\mathcal{S},\Delta^{(t)})^{\Omega+2})$ operations to the previous complexity and $O(rMV(\mathcal{S},\Delta^{(t)})^{\Omega+1})$ to the slp length.

Therefore, we have the following complexity result:

Lemma 8 *Let* $\mathbf{g} := (g_1,\dots,g_r)$ *in* $k[X_1,\dots,X_{t+r}]$ *be a generic sparse system with supports* $\mathcal{S} := (\mathcal{S}_1,\dots,\mathcal{S}_r)$ *such that* $\{X_1,\dots,X_t\}$ *is algebraically independent modulo each associated prime of* $(g_1,\dots,g_r):(X_1\cdots X_{t+r})^\infty$. *Algorithm* `ParametricToricGeomRes` *computes a geometric resolution of* $V^*(\mathbf{g})$. *With the previous notation, the total number of operations in* k *performed by the algorithm is of order*

$$O\Big(\big(r^3+rt\big)N\log(d)M(\mathcal{M})M\big(MV\big(\varpi(\mathcal{S})\big)\big)\Big(MV\big(\mathcal{S},\Delta^{(t)}\big)^2 + M\Big(\omega_{\max}\sum_{1\le h\le r} MV\big(\varpi\big((\mathcal{S}_j)_{j\neq h}\big),\Delta\big)\Big)\Big)+rMV\big(\mathcal{S},\Delta^{(t)}\big)^{\Omega+2}\Big).$$

The algorithm produces an slp of length

$$O\big(rMV\big(\mathcal{S},\Delta^{(t)}\big)^2\big((t+r)N\log(d)+r^3\big)M\big(MV\big(\varpi(\mathcal{S})\big)\big)+MV\big(\mathcal{S},\Delta^{(t)}\big)^{\Omega-1}\big)$$

for the coefficients of the output.

The last step of our main algorithm consists in describing the projection to a coordinate subspace of an equidimensional variety of dimension t given by a geometric resolution in the case that the projection has the same dimension t. To do this, we apply the subroutine described below.

Let $V\subset \overline{k}^{t+r}$ be an equidimensional variety of dimension t definable over k and such that for each irreducible component W of V, $I(W)\cap k[X_1,\dots,X_t]=\{0\}$ holds. Consider the projection $\pi:\overline{k}^{t+r}\to\overline{k}^{\ell}$ where $\ell>t$, $\pi(x_1,\dots,x_{t+r})=(x_1,\dots,x_\ell)$. Note that $\{X_1,\dots,X_t\}$ are free variables with respect to each irreducible component of $\overline{\pi(V)}$. Let $\mathbb{K}:=k(X_1,\dots,X_t)$. Suppose $\lambda\in k[X_{t+1},\dots,X_{t+r}]$ is a primitive element for $\mathbb{K}\otimes k[V]$ and let $(q_\lambda,w_{t+1},\dots,w_{t+r})\in\mathbb{K}[Y]^{r+1}$ be the associated geometric resolution. Let D be the dimension of $\mathbb{K}\otimes k[V]$ as $\mathbb{K}$-vector space.

Let $\mu=\mu_{t+1}X_{t+1}+\cdots+\mu_\ell X_\ell$ be a primitive element for $\mathbb{K}\otimes k[\overline{\pi(V)}]$. As $I(\overline{\pi(V)})=I(V)\cap k[X_1,\dots,X_\ell]$, to find the minimal polynomial of μ with respect to $\overline{\pi(V)}$, it suffices to find a polynomial $q_\mu\in\mathbb{K}[Y]$ of minimal degree such that $q_\mu(\mu)\in\mathbb{K}\otimes I(V)$. Then, $\delta:=\deg_Y(q_\mu)$ is the dimension of $\mathbb{K}\otimes k[\overline{\pi(V)}]$ as a $\mathbb{K}$-vector space and so, for each $t+1\le j\le\ell$, in order to obtain a polynomial v_j such that $X_j=v_j(\mu)$ in $\mathbb{K}\otimes k[\overline{\pi(V)}]$ it suffices to find a linear combination $X_j=\sum_{i=0}^{\delta-1}v_{ji}\mu^i$ of $\{1,\mu,\dots,\mu^{\delta-1}\}$ in $\mathbb{K}\otimes k[V]$. To do this, we use the basis $B_\lambda:=\{1,\lambda,\dots,\lambda^{D-1}\}$ of $\mathbb{K}\otimes k[V]$.

In order to compute the geometric resolution of $\overline{\pi(V)}$ associated with μ, we first look for the minimal power μ^δ which is a $\mathbb{K}$-linear combination of $\{1, \mu, \dots, \mu^{\delta-1}\}$ in $\mathbb{K} \otimes k[V]$. Since $X_j = w_j(\lambda)$ for every $t+1 \le j \le t+r$, we have $\mu = \sum_{j=t+1}^{\ell} \mu_j w_j(\lambda) = p_\mu(\lambda)$, where $p_\mu(Y) := \sum_{j=t+1}^{\ell} \mu_j w_j(Y)$ and, for every $i \in \mathbb{N}$, $\mu^i = p_\mu(\lambda)^i = (p_\mu(Y)^i \mod q_\lambda(Y))|_{Y=\lambda}$. Therefore, δ equals the rank of the $D \times D$ matrix whose columns are the coefficients of the polynomials $(p_\mu(Y)^i \mod q_\lambda(Y))$ for $i = 0, \dots, D-1$.

Then, we obtain the minimal polynomial $q_\mu(Y) := Y^\delta + \sum_{i=0}^{\delta-1} q_{\mu,i} Y^i$ of μ and the polynomials $v_j(Y) = \sum_{i=0}^{\delta-1} v_{ji} Y^i$, $t+1 \le j \le \ell$, which form the geometric resolution of $\overline{\pi(V)}$, by solving the linear systems obtained by equating the coefficients of the different powers of λ in the identities

$$p_{\mu^\delta}(\lambda) = \sum_{i=0}^{\delta-1} (-q_{\mu,i}) p_{\mu^i}(\lambda) \quad \text{and} \quad w_j(\lambda) = \sum_{i=0}^{\delta-1} v_{ji}\, p_{\mu^i}(\lambda), \quad t+1 \le j \le \ell.$$

Summarizing, with the previous notation and hypothesis, we have the following.

Algorithm `GeomResProj`

INPUT: A geometric resolution $(q_\lambda, w_{t+1}, \dots, w_{t+r})$ of V with free variables $X_1, \dots, X_t$, and a linear form $\mu = \sum_{j=1}^{\ell-t} \mu_{t+j} X_{t+j} \in k[X_{t+1}, \dots, X_\ell]$ which is a primitive element for $\mathbb{K} \otimes k[\overline{\pi(V)}]$.

1. Set $p_{\mu^0}(Y) := 1$ and $p_\mu(Y) := \sum_{h=0}^{D-1} (\sum_{j=t+1}^{\ell} \mu_j w_{j,h}) Y^h$, where $(w_{j,0}, \dots, w_{j,D-1}) =: \mathbf{w}_j$ is the vector of coefficients of $w_j(Y)$ for $j = t+1, \dots, t+r$.
2. For $i = 2, \dots, D$, compute $p_{\mu^i}(Y) := (p_\mu(Y) \cdot p_{\mu^{i-1}}(Y) \mod q_\lambda(Y))$.
3. Compute $\delta := \text{rank}(\mathbf{p}_{\mu^0}, \mathbf{p}_\mu, \dots, \mathbf{p}_{\mu^{D-1}})$, where $\mathbf{p}_{\mu^i} \in \mathbb{K}^{D \times 1}$ denotes the vector of coefficients of p_{μ^i}.
4. Set $\mathbf{P} := (\mathbf{p}_{\mu^0}, \mathbf{p}_\mu, \dots, \mathbf{p}_{\mu^{\delta-1}}) \in \mathbb{K}^{D \times \delta}$.
5. Solve the linear systems $\mathbf{P} \cdot \mathbf{q} = \mathbf{p}_{\mu^\delta}$ and $\mathbf{P} \cdot \mathbf{v}_j = \mathbf{w}_j$, $t+1 \le j \le \ell$, to obtain $\mathbf{q} := (q_0, \dots, q_{\delta-1})$ and $\mathbf{v}_j := (v_{j,0}, \dots, v_{j,\delta-1})$.
6. Set $q_\mu(Y) := Y^\delta - \sum_{i=0}^{\delta-1} q_i Y^i$ and $v_j(Y) := \sum_{i=0}^{\delta-1} v_{ji} Y^i$ for every $t+1 \le j \le \ell$.

OUTPUT: The geometric resolution $(q_\mu, v_{t+1}, \dots, v_\ell)$ of the projection $\overline{\pi(V)} \subset \overline{k}^\ell$ with free variables $X_1, \dots, X_t$ associated to the linear form μ.

The correctness of the procedure follows from our previous arguments. Now we estimate its complexity. Assume that the input polynomials are encoded in dense form as degree D univariate polynomials in $k(X_1, \dots, X_t)[Y]$ and their coefficients are encoded by an slp over k of length L.

In Step 1, the algorithm computes an slp encoding the coefficients of p_μ of length bounded by $L + 2D(\ell - t)$.

In order to fulfill Step 2, we first compute recursively the powers Y^h for $h = D, \dots, 2D-2$ modulo $q_\lambda(Y)$ from the coefficients of q_λ and then, we obtain an slp of length $O(L + D(\ell - t) + D^3)$ for the coefficients of p_{μ^i} for $i = 2, \dots, D$ by expanding the product $p_\mu(Y) \cdot p_{\mu^{i-1}}(Y)$ and substituting the powers of Y by their previously computed expressions.

Step 3 is done probabilistically by choosing a point $x = (x_1, \dots, x_t)$ at random, evaluating the involved rational functions at this point within $O(L + D(\ell - t) + D^3)$ operations in k and finally computing the rank δ of $(\mathbf{p}_{\mu^0}(x), \mathbf{p}_\mu(x), \dots, \mathbf{p}_{\mu^{D-1}}(x))$ within $O(D^\omega)$ operations in k, with $\omega < 3$ (see [5, Chap. 2, Sect. 2]).

To solve the linear systems involved in Step 5, the algorithm computes the invertible matrix $\mathbf{P}^t\mathbf{P}$ within $O(D\delta^2)$ operations in k, its adjoint matrix and determinant within $O(\delta^\Omega)$ additional operations, and the products $\mathrm{adj}(\mathbf{P}^t\mathbf{P})\mathbf{p}_{\mu^\delta}$ and $\mathrm{adj}(\mathbf{P}^t\mathbf{P})\mathbf{w}_j$ for $t + 1 \le j \le \ell$ with $O(\delta^2(\ell - t))$.

Adding the previous estimates, we conclude that the algorithm produces an slp of length $O(L + D^3 + D\delta(\ell - t) + \delta^\Omega)$ over k within a complexity of the same order. Taking into account that $\delta \le D$, we have the following.

Lemma 9 *Let $V \subset \overline{k}^{t+r}$ be an equidimensional variety of dimension t definable over k and such that for each irreducible component W of V, $I(W) \cap k[X_1, \dots, X_t] = \{0\}$ holds. With the previous notation, given a geometric resolution of V with free variables $X_1, \dots, X_t$, and a linear form μ which is a primitive element for $\mathbb{K} \otimes k[\overline{\pi(V)}]$, Algorithm* `GeomResProj` *computes the geometric resolution of the projection $\overline{\pi(V)} \subset \overline{k}^\ell$ with free variables $X_1, \dots, X_t$ associated to the linear form μ within $O(L + D^\Omega + D^2(\ell - t))$ operations in k. The output of the algorithm is encoded by an slp of length of the same order.*

4.2 An Algorithm to Find the Projection

Here we present a probabilistic algorithm that, from a fixed family $\mathcal{A} = (\mathcal{A}_1, \dots, \mathcal{A}_r)$ of finite sets $(\mathbb{Z}_{\ge 0})^n$ and a fixed family of variables $X_1, \dots, X_\ell$, obtains a geometric resolution of $\overline{\pi(V^*(\mathbf{f}))} \subset \overline{K}^\ell$, where $\mathbf{f} = (f_1, \dots, f_r)$ is defined in Eq. (1) and $\pi : \overline{K}^n \to \overline{K}^\ell$ is the projection $\pi(x_1, \dots, x_n) = (x_1, \dots, x_\ell)$.

Algorithm K-`Projection`

INPUT: A family $\mathcal{A} = (\mathcal{A}_1, \dots, \mathcal{A}_r)$ of finite subsets of $(\mathbb{Z}_{\ge 0})^n$ such that $\dim(\sum_{j \in J} \mathcal{A}_j) \ge \#J$ for every $J \subset \{1, \dots, r\}$ and a set of variables $\{X_1, \dots, X_\ell\} \subset \{X_1, \dots, X_n\}$.

1. Apply Algorithm `TransBasis` to the family $\mathcal{A}$. Without loss of generality, we suppose the transcendence basis obtained is $\{X_1, \dots, X_t, X_{t+r+1}, \dots, X_n\}$ with $t \le \ell$ and $t + r + 1 > \ell$.
2. Choose randomly in $\mathbb{Z}$ the entries of a vector $b = (b_{t+r+1}, \dots, b_n)$ and of a vector $(\lambda_{t+1}, \dots, \lambda_{t+r})$.
3. Obtain the sparse representation of the system of polynomials
   $\mathbf{f}_b = (f_1(X_1, \dots, X_{t+r}, b), \dots, f_r(X_1, \dots, X_{t+r}, b))$ in $K[X_1, \dots, X_{t+r}]$.

4. Apply Algorithm `ParametricToricGeomRes` to the system $\mathbf{f}_b$ and the variables $X_1, \dots, X_t$ to obtain the geometric resolution $(q_\lambda, w_{t+1}, \dots, w_{t+r})$ of the variety $V^*(\mathbf{f}_b)$ with free variables $X_1, \dots, X_t$ associated to the linear form $\lambda = \lambda_{t+1}X_{t+1} + \cdots + \lambda_{t+r}X_{t+r}$.
5. Choose randomly in $\mathbb{Z}$ the entries of a vector $(\mu_{t+1}, \dots, \mu_\ell)$.
6. Apply Algorithm `GeomResProj` to $(q_\lambda, w_{t+1}, \dots, w_{t+r})$ and $\mu = \mu_{t+1}X_{t+1} + \cdots + \mu_\ell X_\ell$.

OUTPUT: A geometric resolution $(q_\mu, v_{t+1}, \dots, v_\ell)$ of $\overline{\pi(V^*(\mathbf{f}))} \subset \overline{K}^\ell$, where $\pi : \overline{K}^n \to \overline{K}^\ell$ is the projection to the first coordinates.

Theorem 10 *Given a family $\mathcal{A} = (\mathcal{A}_1, \dots, \mathcal{A}_r)$ of finite subsets of $(\mathbb{Z}_{\geq 0})^n$ such that $\dim(\sum_{j \in J} \mathcal{A}_j) \geq \#J$ for every $J \subset \{1, \dots, r\}$ and the projection $\pi : \overline{K}^n \to \overline{K}^\ell$ to the first coordinates, Algorithm K-`Projection` is a probabilistic procedure that computes a geometric resolution of $\overline{\pi(V^*(\mathbf{f}))}$ for the sparse system $\mathbf{f}$ supported on $\mathcal{A}$ with indeterminate coefficients within*

$$O\big((n^2 + r^3)N \log(d) M(\mathcal{D}) \varXi \left(\mathcal{D}^2 + M(\mathcal{E})\right) + r\mathcal{D}^{\Omega+2}\big)$$

operations in K, where $N = \sum_{1 \leq j \leq r} \#\mathcal{A}_j$, $d := \max_{1 \leq j \leq r}\{\deg_X(f_j)\}$, $\mathcal{D} = MV(\mathcal{A}, \Delta^{(n-r)})$, $\mathcal{E} = \sum_{1 \leq h \leq r} MV(((\mathcal{A}_j)_{j \neq h}), \Delta^{(n-r+1)})$, and $\varXi$ is a constant measuring the size of certain combinatorial objects involved at intermediate computations and associated to the family of supports $\mathcal{A}$.

Proof Since in our complexity estimates we only take into account the number of operations in K (and not mixed volume or mixed subdivision computations), to obtain the overall complexity of the algorithm it suffices to add the complexities of steps 3, 4 and 6.

Step 3 can be done within $O(n^2 N \log(d))$ operations in K.

The complexity of Step 4 is the already stated for Algorithm `ParametricToricGeomRes` in Lemma 8. Note that for generic b, the system $\mathbf{f}_b$ is a generic polynomial system supported on $\mathcal{S} := (\mathcal{S}_1, \dots, \mathcal{S}_r)$, where $\mathcal{S}_j \subset (\mathbb{Z}_{\geq 0})^{t+r}$ is the projection of $\mathcal{A}_j$ to the first $t + r$ coordinates for every $1 \leq j \leq r$. Moreover, by Bernstein's Theorem, $MV(\mathcal{S}, \Delta^{(t)}) \leq MV(\mathcal{A}, \Delta^{(n-r)})$, $MV(\varpi(\mathcal{S})) \leq MV(\mathcal{A}, \Delta^{(n-r)})$ and, for every $1 \leq h \leq r$, $MV(\varpi((\mathcal{S}_j)_{j \neq h}), \Delta) \leq MV(((\mathcal{A}_j)_{j \neq h}), \Delta^{(n-r+1)})$. We take $\varXi$ such that $M(\mathcal{M})M(\omega_{\max}) \leq \varXi$.

Finally, the complexity of Step 6 follows from Lemma 9. Note that, here, $D \leq MV(\mathcal{A}, \Delta^{(n-r)})$ and L is the length of the slp computed in Step 4 according to Lemma 8. □

4.3 Example

Consider a sparse system of two polynomials in five variables supported on $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$, where $\mathcal{A}_1 = \{(0, 0, 0, 0, 0), (1, 1, 1, 0, 0), (2, 0, 0, 4, 2), (0, 0, 0, 8, 4)\}$ and

$\mathcal{A}_2 = \{(1,0,1,1,2), (0,1,2,5,4), (1,3,0,5,4)\}$, with indeterminate coefficients:

$$\mathbf{f} := \begin{cases} f_1 = C_{11} + C_{12}X_1X_2X_3 + C_{13}X_1^2X_4^4X_5^2 + C_{14}X_4^8X_5^4, \\ f_2 = C_{21}X_1X_3X_4X_5^2 + C_{22}X_2X_3^2X_4^5X_5^4 + C_{23}X_1X_2^3X_4^5X_5^4 \end{cases}$$

and the projection $\pi : \mathbb{A}^5 \to \mathbb{A}^3$, $\pi(x_1, x_2, x_3, x_4, x_5) = (x_1, x_2, x_3)$. We are going to show a geometric resolution of $\overline{\pi(V^*(\mathbf{f}))}$ following Algorithm K-`Projection`.

First, we apply Algorithm `TransBasis` and we find that $\{X_1, X_2, X_4\}$ is a transcendence basis of $K(V^*(\mathbf{f}))$, and so, $\{X_1, X_2\}$ is a transcendence basis of $K(\overline{\pi(V^*(\mathbf{f}))})$.

Now, the algorithm chooses a value b at random and specializes $X_4 = b$. Set $b = 1$. The specialized system is

$$\mathbf{f}_1 := \begin{cases} f_{11} = C_{11} + C_{12}X_1X_2X_3 + C_{13}X_1^2X_5^2 + C_{14}X_5^4, \\ f_{21} = C_{21}X_1X_3X_5^2 + C_{22}X_2X_3^2X_5^4 + C_{23}X_1X_2^3X_5^4. \end{cases}$$

The next step is to apply Algorithm `ParametricToricGeomRes` with free variables X_1, X_2. We choose $\lambda = X_5$ as the primitive element to obtain the geometric resolution:

- $q_{X_5}(Y) = Y^{10} + \frac{2C_{13}X_1^2}{C_{14}}Y^8 + \frac{C_{13}^2X_1^4+2C_{11}C_{14}}{C_{14}^2}Y^6 + \frac{(-C_{12}C_{21}C_{14}+2C_{11}C_{22}C_{13})X_1^2}{C_{22}C_{14}^2}Y^4 + \frac{-C_{12}C_{21}C_{13}X_1^4+C_{11}^2C_{22}+C_{12}^2C_{23}X_1^3X_2^4}{C_{22}C_{14}^2}Y^2 - \frac{C_{12}C_{21}C_{11}X_1^2}{C_{22}C_{14}^2}$
- $w_3(Y) = -\frac{C_{14}}{C_{12}X_1X_2}Y^4 - \frac{C_{13}X_1}{C_{12}X_2}Y^2 - \frac{C_{11}}{C_{12}X_1X_2}$
- $w_5(Y) = Y$

Finally, Algorithm `GeomResProj` is applied to q_{X_5}, w_3, w_5 and a primitive element μ for $K(\overline{\pi(V^*(\mathbf{f}))})$. In this case, we take $\mu = X_3$ and obtain

- $q_{X_3}(Y) = Y^5 + \frac{C_{11}}{C_{12}X_1X_2}Y^4 + \frac{2C_{12}C_{23}X_1X_2^4-C_{13}C_{21}X_1^2}{C_{12}C_{22}X_2^2}Y^3 + \frac{2C_{23}C_{22}C_{11}X_2^4+C_{21}^2C_{14}X_1}{C_{12}C_{22}^2X_2^3}Y^2 + \frac{C_{12}C_{23}^2X_1^2X_2^4-C_{13}C_{21}C_{23}X_1^3}{C_{12}C_{22}^2}Y + \frac{C_{23}^2C_{11}X_1X_2^3}{C_{22}^2C_{12}}$
- $v_3(Y) = Y$

4.4 Computation for Generic Rational Coefficients

We are now going to show that, for a system with generic rational coefficients, the same steps as the ones in Algorithm K-`Projection` can be performed using these rational coefficients to obtain a geometric resolution of the Zariski closure of the projection of the associated variety.

Let $\{X_1, \dots, X_t, X_{t+r+1}, \dots, X_n\}$ be a transcendence basis of $K(V^*(\mathbf{f}))$ such that $\{X_1, \dots, X_t\}$ is a maximal algebraically independent subset of $\{X_1, \dots, X_\ell\}$.

As shown in [11, Appendix A], there exists a non-empty Zariski open set $\mathcal{U}_1 \subset \mathbb{A}^N$ such that if $c = (c_1, \dots, c_r) \in \mathcal{U}_1 \cap \mathbb{Q}^N$, then:

- the ideal $I_c := (f_1(c, X), \dots, f_r(c, X)) : (X_1 \cdots X_n)^\infty$ is radical equidimensional of dimension $n - r$,

- $\{X_1, \dots, X_t, X_{t+r+1}, \dots, X_n\}$ is algebraically independent modulo each of the associated primes of I_c,
- for every $1 \le k \le \ell - t$, $\{X_1, \dots, X_t, X_{t+k}\}$ is algebraically dependent modulo I_c.

Assume $c \in \mathcal{U}_1 \cap \mathbb{Q}^N$ and consider the variety $V^*(\mathbf{f}(c)) \subset \mathbb{A}^n$. Let W be an irreducible component of $V^*(\mathbf{f}(c))$. We have $\dim(W) = n - r$ and $\{X_1, \dots, X_t, X_{t+r+1}, \dots, X_n\}$ is a transcendence basis of $\mathbb{Q}(W)$. Then, the projection of W over the last $n - t - r$ coordinates is a dominant map. Therefore, there is a Zariski open subset $\mathcal{O}_W \subset \mathbb{A}^{n-t-r}$ such that, for every $b \in \mathcal{O}_W \cap \mathbb{Q}^{n-t-r}$:

- $W_b := W \cap \{x_{t+r+1} = b_{t+r+1}, \dots, x_n = b_n\}$ is an equidimensional variety of dimension t,
- $\{X_1, \dots, X_t\}$ is algebraically independent modulo $I(W_b)$.

Then, for every $b \in \mathcal{O}_W \cap \mathbb{Q}^{n-t-r}$, the identity $\overline{\pi(W)} = \overline{\pi(W_b)}$ holds.

As the dimension of the set $\partial(\mathbf{f}(c)) := V^*(\mathbf{f}(c)) - \{x \in (\mathbb{C}^*)^n : \mathbf{f}(c, x) = 0\}$ is less than $n - r$, for every $\{i_1, \dots, i_t\} \subset \{1, \dots, t + r\}$, there exists a non-zero polynomial $p_{i_1,\dots,i_t}(X_{i_1}, \dots, X_{i_t}, X_{t+r+1}, \dots, X_n)$ vanishing identically on this set. Then, there is a non-empty Zariski open set $\mathcal{O}_1 \subset \mathbb{A}^{n-t-r}$ such that for every $b \in \mathcal{O}_1$, the dimension of $\partial(\mathbf{f}(c)) \cap \{x_{t+r+1} = b_{t+r+1}, \dots, x_n = b_n\}$ is less than t.

Then, for every $b \in \mathcal{O}_1 \cap \bigcap_W \mathcal{O}_W \cap (\mathbb{Q}^*)^{n-t-r}$, we have

$$V^*\big(\mathbf{f}(c)\big) \cap \{x_{t+r+1} = b_{t+r+1}, \dots, x_n = b_n\} = \overline{\Big\{\hat{x} \in \big(\mathbb{C}^*\big)^{t+r} : \mathbf{f}(c, \hat{x}, b) = 0\Big\} \times \{b\}}$$

and $\pi(V^*(\mathbf{f}(c))) = \bigcup_W \pi(W) = \bigcup_W \pi(W_b) = \pi(V^*(\mathbf{f}(c)) \cap \{x_{t+r+1} = b_{t+r+1}, \dots, x_n = b_n\})$; therefore,

$$\overline{\pi\big(V^*\big(\mathbf{f}(c)\big)\big)} = \overline{\pi\Big(\Big\{\hat{x} \in \big(\mathbb{C}^*\big)^{t+r} : \mathbf{f}(c, \hat{x}, b) = 0\Big\} \times \{b\}\Big)}.$$

For $j = 1, \dots, r$, let $\mathcal{S}_j \subset (\mathbb{Z}_{\ge 0})^{t+r}$ be the projection of $\mathcal{A}_j$ to the first $t + r$ coordinates. Then $f_j = \sum_{\hat{a} \in \mathcal{S}_j} (\sum_{(\hat{a},\tilde{a}) \in \mathcal{A}_j} c_{j,(\hat{a},\tilde{a})} \tilde{X}^{\tilde{a}}) \hat{X}^{\hat{a}}$. Algorithm `ParametricToricGeomRes` works for generic sparse polynomial systems $\mathbf{g}$ supported on $\mathcal{S} = (\mathcal{S}_1, \dots, \mathcal{S}_r)$, that is, there is a polynomial $p_{\mathcal{S}}$ in the coefficients of the system such that it computes a geometric resolution of $V^*(\mathbf{g}(\hat{c}))$ for every vector of coefficients $\hat{c}$ with $p_{\mathcal{S}}(\hat{c}) \ne 0$. Let $\mathcal{U}_2 \subset \mathbb{A}^N$ be a non-empty Zariski open set such that, for every $c := (c_1, \dots, c_r)$, the polynomial $p_{\mathcal{S}}((\sum_{(\hat{a},\tilde{a}) \in \mathcal{A}_j} c_{j,(\hat{a},\tilde{a})} \tilde{X}^{\tilde{a}})_{1 \le j \le r, \hat{a} \in \mathcal{S}_j})$ does not vanish identically.

For $c \in \mathcal{U}_2 \cap \mathbb{Q}^N$, there exists a non-empty Zariski open set $\mathcal{O}_2 \subset \mathbb{A}^{n-t-r}$ such that for every $b \in \mathcal{O}_2 \cap \mathbb{Q}^{n-t-r}$, the algorithm `ParametricToricGeomRes` can be applied to the system $\mathbf{f}(c, \hat{x}, b)$.

We conclude that, for coefficient vectors $c \in \mathcal{U}_1 \cap \mathcal{U}_2 \cap (\mathbb{Q}^*)^N$, a probabilistic algorithm $\mathbb{Q}$-`Projection` which follows the same steps as Algorithm K-`Projection` can be applied in order to compute a geometric resolution of $\overline{\pi(V^*(\mathbf{f}(c)))}$. Taking into account the complexity estimates in Theorem 10, this proves Theorem 1.

Finally, we show an example where, following the steps of the algorithm $\mathbb{Q}$-`Projection`, we obtain a geometric resolution of $\overline{\pi(V^*(\mathbf{f}))}$ for a sparse system $\mathbf{f}$ with rational coefficients.

Example Let $\mathbf{f}$ be the following sparse system with the same support family $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ as in the example of Sect. 4.3:

$$\mathbf{f} = \begin{cases} f_1 = 3 + 2X_1X_2X_3 - X_1^2X_4^4X_5^2 + 5X_4^8X_5^4, \\ f_2 = 2X_1X_3X_4X_5^2 - 3X_2X_3^2X_4^5X_5^4 + 7X_1X_2^3X_4^5X_5^4 \end{cases}$$

and let $\pi : \mathbb{C}^5 \to \mathbb{C}^3$ be the projection $\pi(x_1, x_2, x_3, x_4, x_5) = (x_1, x_2, x_3)$.

We use the same choices $b = 1$, $\lambda = X_5$ and $\mu = X_3$ as in Sect. 4.3 and look at steps 4 and 6 of the algorithm.

In Step 4, the algorithm `ParametricToricGeomRes` computes the geometric resolution of $V^*(\mathbf{f}_1)$ with free variables X_1, X_2 associated to the linear form λ:

- $\widehat{q}_{X_5}(Y) = Y^{10} - \frac{2X_1^2}{5}Y^8 + \frac{X_1^4+30}{25}Y^6 + \frac{2X_1^2}{75}Y^4 - \frac{4X_1^4-27+28X_1^3X_2^4}{75}Y^2 + \frac{4X_1^2}{25}$,
- $\widehat{w}_3(Y) = \frac{-5}{2X_1X_2}Y^4 + \frac{X_1}{2X_2}Y^2 - \frac{3}{2X_1X_2}$,
- $\widehat{w}_5(Y) = Y$.

In Step 6, if Algorithm `GeomResProj` is applied to the geometric resolution obtained in Step 4 and the linear form μ, the geometric resolution $(\widehat{q}_{X_3}, \widehat{v}_3)$ is obtained, where

- $\widehat{q}_{X_3}(Y) = Y^5 + \frac{3}{2X_1X_2}Y^4 - \frac{14X_1X_2^4+X_1^2}{3X_2^2}Y^3 + \frac{-63X_2^4+10X_1}{9X_2^3}Y^2 + \frac{49X_1^2X_2^4+7X_1^3}{9}Y + \frac{49X_1X_2^3}{6}$,
- $\widehat{v}_3(Y) = Y$.

This is, in fact, the geometric resolution of $\overline{\pi(V^*(\mathbf{f}))}$ with free variables X_1, X_2 associated to the linear form $\mu = X_3$, as can be checked, for instance, by applying a Groebner basis elimination-based procedure.

Acknowledgements The authors thank the referees for their helpful comments and suggestions. This work was partially supported by the Argentinian research grants CONICET PIP 0099/11, UBACYT 20020090100069 (2010–2013) and UBACYT 20020120100133 (2013–2016).

References

1. Adrovic, D., Verschelde, J.: Computing Puiseux series for algebraic surfaces. In: Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation (ISSAC 2012), Grenoble, France, July 22–25, 2012, pp. 20–27 (2012)
2. Adrovic, D., Verschelde, J.: Polyhedral methods for space curves exploiting symmetry applied to the cyclic n-roots problem. In: Gerdt, V.P., Koepf, W., Mayr, E.W., Vorozhtsov, E.V. (eds.) Computer Algebra in Scientific Computing, 15th International Workshop, CASC 2013, Berlin, Germany. Lecture Notes in Computer Science, vol. 8136, pp. 10–29 (2013)
3. Berkowitz, S.J.: On computing the determinant in small parallel time using a small number of processors. Inf. Process. Lett. **18**(3), 147–150 (1984)
4. Bernstein, D.N.: The number of roots of a system of equations. Funct. Anal. Appl. **9**, 183–185 (1975)
5. Bini, D., Pan, V.Y.: Polynomial and Matrix Computations. Vol. 1. Fundamental Algorithms. Progress in Theoretical Computer Science. Birkhäuser Boston, Boston (1994)
6. Bürgisser, P., Clausen, M., Shokrollahi, M.A.: Algebraic Complexity Theory. Grundlehren Math. Wiss., vol. 315. Springer, Berlin (1997)
7. Caniglia, L.: How to compute the Chow form of an unmixed polynomial ideal in single exponential time. Appl. Algebra Eng. Commun. Comput. **1**(1), 25–41 (1990)

8. Canny, J., Emiris, I.Z.: A subdivision-based algorithm for the sparse resultant. J. ACM **47**(3), 417–451 (2000)
9. Chistov, A.L., Grigor'ev, D.Yu.: Complexity of quantifier elimination in the theory of algebraically closed fields. In: Mathematical Foundations of Computer Science, 1984, Prague, 1984. Lecture Notes in Computer Science, vol. 176, pp. 17–31. Springer, Berlin (1984)
10. Cox, D., Little, J., O'Shea, D.: Using Algebraic Geometry. Grad. Texts Math., vol. 185. Springer, New York (1998)
11. D'Alfonso, L., Jeronimo, G., Ollivier, F., Sedoglavic, A., Solernó, P.: A geometric index reduction method for implicit systems of differential algebraic equations. J. Symb. Comput. **46**(10), 1114–1138 (2011)
12. D'Andrea, C.: Macaulay style formulas for sparse resultants. Trans. Am. Math. Soc. **354**(7), 2595–2629 (2002)
13. D'Andrea, C., Dickenstein, A.: Explicit formulas for the multivariate resultant. J. Pure Appl. Algebra **164**(1–2), 59–86 (2001). Effective methods in algebraic geometry (Bath, 2000)
14. Dyer, M., Gritzmann, P., Hufnagel, A.: On the complexity of computing mixed volumes. SIAM J. Comput. **27**(2), 356–400 (1998)
15. Edmonds, J.: Submodular functions, matroids, and certain polyhedra. In: Combinatorial Structures and Their Applications, Proc. Calgary Internat. Conf., Calgary, Alta., 1969, pp. 69–87. Gordon & Breach, New York (1970)
16. Emiris, I.Z., Canny, J.F.: Efficient incremental algorithms for the sparse resultant and the mixed volume. J. Symb. Comput. **20**(2), 117–149 (1995)
17. Emiris, I.Z., Verschelde, J.: How to count efficiently all affine roots of a polynomial system. Discrete Appl. Math. **93**(1), 21–32 (1999). 13th European Workshop on Computational Geometry CG'97 (Würzburg, 1997)
18. Fitchas, N., Galligo, A., Morgenstern, J.: Precise sequential and parallel complexity bounds for quantifier elimination over algebraically closed fields. J. Pure Appl. Algebra **67**(1), 1–14 (1990)
19. Gao, T., Li, T.Y.: Mixed volume computation for semi-mixed systems. Discrete Comput. Geom. **29**(2), 257–277 (2003)
20. Gao, T., Li, T.Y., Wang, X.: Finding all isolated zeroes of polynomial systems in $\mathbb{C}^n$ via stable mixed volumes. Polynomial elimination—algorithms and applications. J. Symb. Comput. **28**(1–2), 187–211 (1999)
21. Giusti, M., Heintz, J.: Algorithmes—disons rapides—pour la décomposition d'une variété algébrique en composantes irréductibles et équidimensionelles. In: Proc. Effective Methods in Algebraic Geometry, Castiglioncello, 1990. Progr. Math., vol. 94, pp. 169–194. Birkhäuser Boston, Boston (1991)
22. Giusti, M., Lecerf, G., Salvy, B.: A Gröbner free alternative for polynomial system solving. J. Complex. **17**(1), 154–211 (2001)
23. Heintz, J.: Definability and fast quantifier elimination in algebraically closed fields. Theor. Comput. Sci. **24**(3), 239–277 (1983)
24. Herrero, M.I., Jeronimo, G., Sabia, J.: Computing isolated roots of sparse polynomial systems in affine space. Theor. Comput. Sci. **411**(44–46), 3894–3904 (2010)
25. Herrero, M.I., Jeronimo, G., Sabia, J.: Affine solution sets of sparse polynomial systems. J. Symb. Comput. **51**, 34–54 (2013)
26. Huber, B., Sturmfels, B.: A polyhedral method for solving sparse polynomial systems. Math. Comput. **64**(212), 1541–1555 (1995)
27. Huber, B., Sturmfels, B.: Bernstein's theorem in affine space. Discrete Comput. Geom. **17**(2), 137–141 (1997)
28. Jeronimo, G., Sabia, J.: Computing multihomogeneous resultants using straight-line programs. J. Symb. Comput. **42**(1–2), 218–235 (2007)
29. Jeronimo, G., Krick, T., Sabia, J., Sombra, M.: The computational complexity of the Chow form. Found. Comput. Math. **4**(1), 41–117 (2004)
30. Jeronimo, G., Matera, G., Solernó, P., Waissbein, A.: Deformation techniques for sparse systems. Found. Comput. Math. **9**(1), 1–50 (2009)
31. Khovanskii, A.G.: Newton polyhedra and toroidal varieties. Funct. Anal. Appl. **11**, 289–296 (1978)
32. Kushnirenko, A.G.: Newton polytopes and the Bézout theorem. Funct. Anal. Appl. **10**, 233–235 (1976)
33. Li, T.Y., Li, X.: Finding mixed cells in the mixed volume computation. Found. Comput. Math. **1**(2), 161–181 (2001)
34. Li, T.Y., Wang, X.: The BKK root count in $\mathbb{C}^n$. Math. Comput. **65**(216), 1477–1484 (1996)

35. Mizutani, T., Takeda, A., Kojima, M.: Dynamic enumeration of all mixed cells. Discrete Comput. Geom. **37**(3), 351–367 (2007)
36. Puddu, S., Sabia, J.: An effective algorithm for quantifier elimination over algebraically closed fields using straight line programs. J. Pure Appl. Algebra **129**(2), 173–200 (1998)
37. Rojas, J.M.: A convex geometrical approach to counting the roots of a polynomial system. Theor. Comput. Sci. **133**(1), 105–140 (1994)
38. Rojas, J.M.: Why polyhedra matter in non-linear equation solving. In: Topics in Algebraic Geometry and Geometric Modeling. Contemp. Math., vol. 334, pp. 293–320. Am. Math. Soc., Providence (2003)
39. Rojas, J.M., Wang, X.: Counting affine roots of polynomial systems via pointed Newton polytopes. J. Complex. **12**(2), 116–133 (1996)
40. Schost, É.: Computing parametric geometric resolutions. Appl. Algebra Eng. Commun. Comput. **13**(5), 349–393 (2003)
41. Schwartz, J.: Fast probabilistic algorithms for verification of polynomial identities. J. ACM **27**, 701–717 (1980)
42. Steffens, R., Theobald, T.: Mixed volume techniques for embeddings of Laman graphs. J. Comput. Geom. **43**(2), 84–93 (2010)
43. Sturmfels, B.: On the Newton polytope of the resultant. J. Algebr. Comb. **3**(2), 207–236 (1994)
44. Tarski, A.: A Decision Method for Elementary Algebra and Geometry, 2nd edn. University of California Press, Berkeley/Los Angeles (1951)
45. Verschelde, J.: Polyhedral methods in numerical algebraic geometry. In: Interactions of Classical and Numerical Algebraic Geometry. Contemp. Math., vol. 496, pp. 243–263. Am. Math. Soc., Providence (2009)
46. Verschelde, J., Verlinden, P., Cools, R.: Homotopies exploiting Newton polytopes for solving sparse polynomial systems. SIAM J. Numer. Anal. **31**(3), 915–930 (1994)
47. Verschelde, J., Gatermann, K., Cools, R.: Mixed-volume computation by dynamic lifting applied to polynomial system solving. Discrete Comput. Geom. **16**(1), 69–112 (1996)
48. von zur Gathen, J., Gerhard, J.: Modern Computer Algebra. Cambridge University Press, Cambridge (1999)
49. Zippel, R.: Effective Polynomial Computation. Kluwer Int. Ser. Eng. Comput. Sci., vol. 241. Kluwer, Dordrecht (1993)