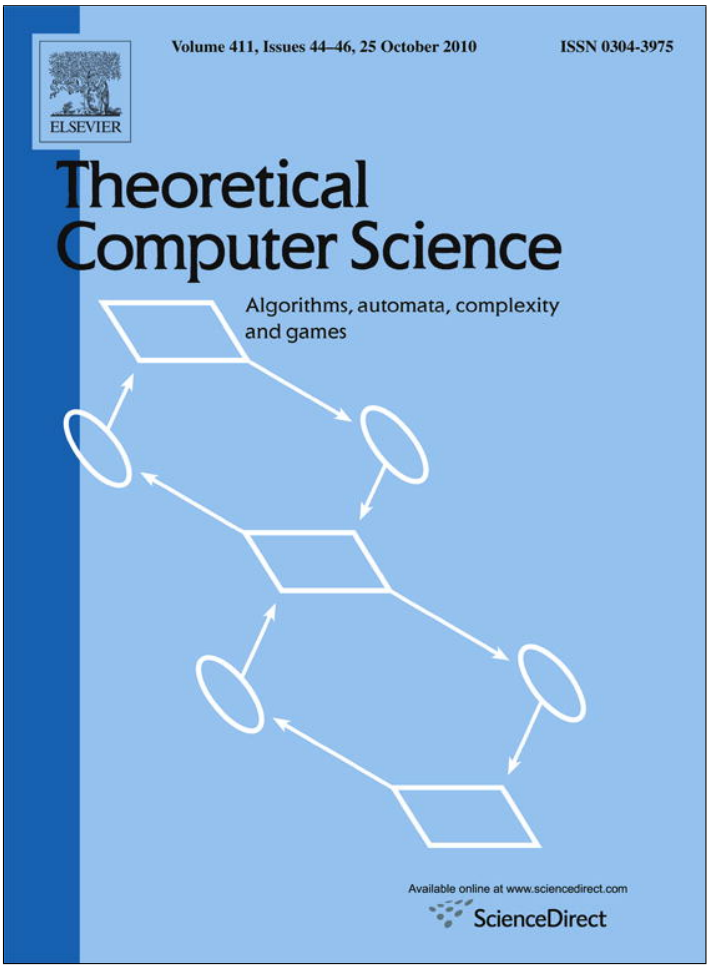

Theoretical Computer Science 411 (2010) 3894–3904

Contents lists available at ScienceDirect

Theoretical Computer Science

journal homepage: www.elsevier.com/locate/tcs

Computing isolated roots of sparse polynomial systems in affine space☆

María Isabel Herrero [a,1], Gabriela Jeronimo [a,*,1], Juan Sabia [a,b,1]

[a] Departamento de Matemática, Facultad de Ciencias Exactas y Naturales, Universidad de Buenos Aires, Ciudad Universitaria, Pab. I, (1428) Buenos Aires, Argentina

[b] Departamento de Ciencias Exactas, Ciclo Básico Común, Universidad de Buenos Aires, Ciudad Universitaria, Pab. III, (1428) Buenos Aires, Argentina

ARTICLE INFO

Article history:
Received 3 September 2009
Received in revised form 28 May 2010
Accepted 21 July 2010
Communicated by V.Y. Pan

Keywords:
Sparse polynomial systems
Algorithms
Complexity

ABSTRACT

We present a symbolic probabilistic algorithm to compute the isolated roots in $\mathbb{C}^n$ of sparse polynomial equation systems. As some already known numerical algorithms solving this task, our procedure is based on polyhedral deformations and homotopies, but it amounts to solving a smaller number of square systems of equations and in fewer variables. The output of the algorithm is a *geometric resolution* of a finite set of points including the isolated roots of the system. The complexity is polynomial in the size of the combinatorial structure of the system supports up to a pre-processing yielding the *mixed cells* in a subdivision of the family of these supports.

1. Introduction

The known algorithmic methods to solve *general* polynomial equation systems require a large number of calculations, which results in a long computing time. This is one of the reasons why several attempts to solve *particular* families of polynomial equation systems (for instance, polynomials with a specific fixed structure) have been made.

Bernstein [2], Kushnirenko [18] and Khovanskii [17] proved that the number of isolated solutions in $(\mathbb{C}^*)^n$ of a polynomial system with n equations is bounded by a combinatorial invariant (the *mixed volume*) associated with the sets of exponents of the monomials with nonzero coefficients in the polynomials involved (that is, their *support* sets). This result may be considered as the basis for the current study of *sparse* polynomial systems, namely polynomials with prescribed supports, and gave rise to the development of sparse elimination theory (see [9] for foundational results on this subject).

The most efficient algorithms to solve sparse polynomial systems in $(\mathbb{C}^*)^n$, both numerically and symbolically, use *polyhedral deformations* (see, for example, [29,13,25,16]). A deformation method to compute the isolated roots of a polynomial system consists in considering the given system as a particular instance of a parametric family of generic zero-dimensional systems; the isolated roots of the input system are then obtained from the zeroes of a sufficiently generic instance which is easy to solve. These techniques, originally applied for numerical solving of equations (see, for instance, [20,27] and the references therein), have also been used in symbolic procedures by means of the so-called Newton–Hensel lifting (see, for instance, [10,12,19,15]).

Polyhedral deformations preserve the monomial structure of the polynomial system under consideration, which implies that the number of "paths" to track along the deformation coincides with the expected number of solutions. For sparse systems, this results in a running time shorter than that of a general algorithm.

The first bounds for the number of isolated solutions in $\mathbb{C}^n$ of a sparse polynomial system were given in [24] and improved later in [22,26]. The most precise bounds known up until now are given in [14] in terms of *stable mixed volumes*, which are

☆ Partially supported by the following Argentinian research grants: UBACyT X847 (2006–2009) and PIP CONICET 5852/05.

* Corresponding author. Tel.: +54 11 45763335.
E-mail addresses: iherrero@dm.uba.ar (M.I. Herrero), jeronimo@dm.uba.ar (G. Jeronimo), jsabia@dm.uba.ar (J. Sabia).
1 CONICET, Argentina.

0304-3975/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.tcs.2010.07.015

also combinatorial invariants depending only on the supports of the polynomials. The effective proofs of the bounds in these papers were applied to obtain numerical algorithms to compute the isolated solutions based on the approach in [13] (see, for instance, [22,14]). A symbolic algorithm performing this task provided all the polynomials have nonzero constant term is given in [16].

The algorithm in [14] requires the use of recursive liftings, which may reflect negatively in the running time of the algorithm. An improved procedure which avoids recursive liftings was shown in [7] (see also [5]). These algorithms rely on solving a number of associated subsystems in $(\mathbb{C}^*)^n$ obtained from the liftings used.

In this paper, we present a new symbolic algorithm to compute the isolated solutions in $\mathbb{C}^n$ of a sparse system with n equations. As the procedure in [7], our algorithm avoids recursive liftings; moreover, it amounts to solving a smaller number of square systems of equations and in fewer variables. It can also be seen as a generalization to the algorithm in [16] in the sense that it does not require any hypothesis on the system supports. Our main result is the following (for a precise formulation, see Theorem 9):

Theorem. *Let $f_1, \ldots, f_n$ be polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$. There exists a probabilistic algorithm (see Algorithm* `AffineSolve`*) which computes a finite set of points containing the isolated common zeroes of $f_1, \ldots, f_n$ in $\mathbb{C}^n$ within a complexity which (up to a pre-processing) is polynomial in the size of the combinatorial structure of the system supports.*

As in [16], our algorithm takes as input the *sparse representation* of the polynomials $f_1, \ldots, f_n$ and the *mixed cells* in a *fine mixed subdivision* of their supports, which are assumed to be precomputed (see, for instance, [4,28,21,6] and [23] for different algorithms computing these cells). The output of the algorithm is a *geometric resolution*, that is, a univariate representation of a finite set of points parametrized by the values a linear form takes at them (see, for example, [11]).

The general idea of the algorithm is to recover the solutions of the input system from the solutions of a generic system with the same supports by means of a homotopic deformation. To deal with the deformed system, we adapt the polyhedral techniques introduced in [14] and refined in [7] in order to make a more careful analysis of the situation and determine the polynomial subsystems to be solved. Finally, we apply the symbolic deformation techniques for sparse elimination shown in [16].

The algorithm in [16] can be considered as a symbolic version of [13], which computes the isolated roots of a sparse polynomial system in $(\mathbb{C}^*)^n$. Provided the origin lies in all the polynomial supports, it computes the isolated roots of the system in $\mathbb{C}^n$ (see [22]). In this paper, our adaptation of the combinatorial construction in [14] allows us to extend the results in [16] to arbitrary supports, obtaining a procedure with a complexity depending polynomially on stable mixed volumes associated with the input system.

The theoretic results underlying the correctness of our algorithm could also be applied to design a new numerical procedure in the spirit of [14,7]. Although there are no explicit complexity estimates for the numerical algorithms in these papers, the fact that our approach deals with a smaller number of systems and with fewer variables than theirs would result in a better running time for the new algorithm.

The paper is organized as follows: In Section 2, some basic notation is introduced and the notions of geometric resolution, mixed subdivision and stable mixed volume are recalled. Section 3 is devoted to proving the theoretic geometric and combinatorial results that lead to the correctness of our algorithm, which is described in Section 4. Finally, in Section 5, we present some examples to show how our algorithm works and to compare it to previous procedures.

2. Preliminaries

2.1. Basic definitions and notation

Throughout this paper, K will be an algebraically closed field. If k is an arbitrary field, $\bar{k}$ will denote an algebraic closure of k.

We will describe zero-dimensional affine varieties by means of *geometric resolutions* (for a detailed historical account on the application of this representation in the algorithmic framework, see [11]). The precise definition we are going to use is the following:

Let k be a field of characteristic 0 and $V = \{\xi^{(1)}, \ldots, \xi^{(D)}\} \subset \bar{k}^n$ be a zero-dimensional variety defined by polynomials in $k[X_1, \ldots, X_n]$. Given a *separating* linear form $u = u_1X_1 + \cdots + u_nX_n \in k[X_1, \ldots, X_n]$ for V (that is, a linear form u such that $u(\xi^{(i)}) \neq u(\xi^{(j)})$ if $i \neq j$), the following polynomials completely characterize the variety V:

- the *minimal polynomial* $q := \prod_{1 \leq i \leq D}(Y - u(\xi^{(i)})) \in k[Y]$ of u over the variety V (where Y is a new variable),
- a polynomial $q_0 \in k[Y]$ with $\deg(q_0) < D$ and relatively prime to q,
- polynomials $v_1, \ldots, v_n \in k[Y]$ with $\deg(v_j) < D$ for every $1 \leq j \leq n$ satisfying $V = \left\{\left(\frac{v_1}{q_0}(\eta), \ldots, \frac{v_n}{q_0}(\eta)\right) \in \bar{k}^n \mid \eta \in \bar{k}, \ q(\eta) = 0\right\}$.

The family of univariate polynomials $q, q_0, v_1, \ldots, v_n \in k[Y]$ is called a *geometric resolution* of V (associated with the linear form u). As q_0 is invertible in $k[Y]/(q(Y))$, setting $\tilde{v}_k(Y) := q_0^{-1}(Y)v_k(Y) \mod (q(Y))$ for every $1 \leq k \leq n$, we are led to an equivalent definition of geometric resolution: a family of $n+1$ polynomials $q, \tilde{v}_1, \ldots, \tilde{v}_n$ in $k[Y]$ satisfying $V = \left\{\left(\tilde{v}_1(\eta), \ldots, \tilde{v}_n(\eta)\right) \in \bar{k}^n \mid \eta \in \bar{k}, \ q(\eta) = 0\right\}$.

The notion of geometric resolution can be extended to equidimensional curves. In this case, the polynomials $q, q_0, v_1, \ldots, v_n$ are in $k(T)[Y]$, where T is a free variable for all the irreducible components of the curve.

Although we work with polynomials, our algorithm will only deal with their coefficients, which are elements in $\mathbb{Q}$. The notion of *complexity* of an algorithm we consider is the number of operations and comparisons in $\mathbb{Q}$. We will encode multivariate polynomials in *sparse form*, that is, each polynomial will be given as the list of pairs (q, a_q) where q runs over the set of exponents of its monomials with nonzero coefficients and a_q is the corresponding coefficient. We will also use the standard *dense form* for univariate polynomials, which encodes a polynomial as the vector of its coefficients including zeroes.

In our complexity estimates, we will use the notation $M(d) := d\log^2(d)\log(\log(d))$ where log denotes logarithm to base 2. We will also use the usual O notation: Let $f, g : \mathbb{Z}_{\geq 0} \to \mathbb{R}$, $f(d) = O(g(d))$ if $|f(d)| \leq c|g(d)|$ for a positive constant c. We denote by Ω the exponent in the complexity estimate $O(d^\Omega)$ for the multiplication of two $(d \times d)$–matrices with coefficients in $\mathbb{Q}$. It is known that $\Omega < 2.376$ (see [8, Chapter 12]).

2.2. Sparse systems and subdivisions

Let $X_1, \ldots, X_n$ be indeterminates over K and write $X := (X_1, \ldots, X_n)$. Given a family $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ of finite subsets of $(\mathbb{Z}_{\geq 0})^n$, a *sparse polynomial system supported on* $\mathcal{A}$ is given by polynomials $f_j = \sum_{q \in \mathcal{A}_j} a_{j,q} X^q$, with $a_{j,q} \in K \setminus \{0\}$ for each $q \in \mathcal{A}_j$ and $1 \leq j \leq n$. We write $F = (f_1, \ldots, f_n)$ for this system. We denote by $\mathcal{M}(\mathcal{A})$ the mixed volume of the convex hulls of $\mathcal{A}_1, \ldots, \mathcal{A}_n$ in $\mathbb{R}^n$ (see, for example, [3, Chapter 7] for a definition).

Following [13], a *cell* of $\mathcal{A}$ is a tuple $C = (C_1, \ldots, C_n)$ with $C_j \neq \emptyset$ and $C_j \subset \mathcal{A}_j$ for $1 \leq j \leq n$. We define $\text{type}(C) := (\dim(conv(C_1)), \ldots, \dim(conv(C_n)))$ and $conv(C) := conv(C_1 + \cdots + C_n)$ where the sum is carried out pointwise. A *subdivision* of $\mathcal{A}$ is a collection of cells $\mathfrak{C} = \{C^1, \ldots, C^m\}$ of $\mathcal{A}$ satisfying the following conditions:

- $\dim(conv(C^\ell)) = n$ for $1 \leq \ell \leq m$,
- the intersection $conv(C^h) \cap conv(C^\ell) \subset \mathbb{R}^n$ is either the empty set or a face of both $conv(C^h)$ and $conv(C^\ell)$ for $1 \leq h < \ell \leq m$,
- $\bigcup_{\ell=1}^m conv(C^\ell) = conv(\mathcal{A})$.

Furthermore, we call the collection a *fine mixed subdivision* of $\mathcal{A}$ if

- for $1 \leq \ell \leq m$, $\dim(conv(C_j^\ell)) = \#C_j^\ell - 1$ and $\sum_{j=1}^n \dim(conv(C_j^\ell)) = n$.

The mixed volume $\mathcal{M}(\mathcal{A})$ can be computed as the sum of the n-dimensional volumes of the convex hulls of all the type $(1, \ldots, 1)$ cells (also called *mixed cells*) in a fine mixed subdivision (see [13, Theorem 2.4.]). For short, we write $1_n := (1, \ldots, 1) \in (\mathbb{Z}_{\geq 0})^n$.

A standard lifting process can be used to obtain subdivisions of $\mathcal{A}$ (see [13, Section 2]): For $1 \leq j \leq n$, let $\omega_j : \mathcal{A}_j \to \mathbb{R}$ be an arbitrary function. The tuple $\omega = (\omega_1, \ldots, \omega_n)$ is called a *lifting function* for $\mathcal{A}$. The graph of any subset C_j of $\mathcal{A}_j$ under ω_j will be denoted by $C_j(\omega_j) \subset \mathbb{R}^{n+1}$ and $(C_1(\omega_1), \ldots, C_n(\omega_n))$ will be denoted by $C(\omega)$. The set of cells C of $\mathcal{A}$ such that $conv(C(\omega))$ is an n-dimensional face of $conv(\mathcal{A}(\omega))$ whose inner normal vector has a positive last coordinate (that is, $conv(C(\omega))$ is a *lower facet* of $conv(\mathcal{A}(\omega))$) is a subdivision of $\mathcal{A}$ which will be denoted by $S_\omega(\mathcal{A})$. Moreover, for a generic lifting function, $S_\omega(\mathcal{A})$ is a fine mixed subdivision of $\mathcal{A}$. From this lifting, the mixed cells in the subdivision can be obtained algorithmically by means of linear programming based procedures. In [4], an algorithm following this approach is presented with worst-case complexity $(\max_i \#\mathcal{A}_i)^{O(n)}$ under certain mild assumptions. Successive improvements to this algorithm can be found in [21] and [6]. The dynamic enumeration procedure described in [23] appears to be the fastest known up until now. A different, dynamic approach, which does not use a random lifting function, is given in [28].

Let $F = (f_1, \ldots, f_n)$ be a sparse system supported on $\mathcal{A}$ given by polynomials $f_j = \sum_{q \in \mathcal{A}_j} a_{j,q} X^q$. For a given lifting function ω, we denote by $F^\omega := (f_1^{\omega_1}, \ldots, f_n^{\omega_n})$ the sparse system in $K[X_1, \ldots, X_n, y]$ supported on $\mathcal{A}(\omega)$ defined by $f_j^{\omega_j}(X, y) = \sum_{q \in \mathcal{A}_j} a_{j,q} X^q y^{\omega_j(q)}$ for $1 \leq j \leq n$.

The *stable mixed volume* of a given family of supports $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ (see [14]) is defined as follows: consider $\mathcal{A}^0 = (\mathcal{A}_1^0, \ldots, \mathcal{A}_n^0)$ the family of supports $\mathcal{A}_j^0 := \mathcal{A}_j \cup \{0\}$. Let k be a positive integer and $\omega^0 = (\omega_1^0, \ldots, \omega_n^0)$ a lifting for $\mathcal{A}^0$ defined by $\omega_j^0(q) = 0$ if $q \in \mathcal{A}_j$ and $\omega_j^0(0) = k$ if $0 \notin \mathcal{A}_j$. The stable mixed volume of $\mathcal{A}$, denoted by $\mathcal{SM}(\mathcal{A})$, is defined as the sum of the mixed volumes of all the cells in $S_{\omega^0}(\mathcal{A}^0)$ induced by facets having inner normal vectors with non-negative entries.

3. Theoretic results

3.1. Deformation of polynomial systems

Our algorithm to solve sparse polynomial systems relies on homotopic deformation techniques as many procedures appearing in the literature [29,13,7,16]. The solutions to these deformed systems can be seen alternatively as curves or points depending on the base field we consider. The following lemmas relate both points of view.

Lemma 1. *Let $P = (p_1, \ldots, p_n)$ in $K[T, X_1, \ldots, X_n]^n$. For every isolated zero $\xi_0 \in K^n$ of $P(\tau_0, X)$, there exists a one-dimensional irreducible component V of $\{(\tau, \xi) \in K^{n+1} \mid P(\tau, \xi) = 0\}$ such that $(\tau_0, \xi_0) \in V$ and the projection π_T to the first coordinate satisfies $\overline{\pi_T(V)} = K$ (that is, π_T is a dominant map from V to K).*

Proof. Taking into account that P consists of n polynomials in $n + 1$ variables, it follows that (τ_0, ξ_0) lies in an irreducible component V of dimension at least 1 of its solution set in K^{n+1}. Moreover, as (τ_0, ξ_0) is an isolated point in $V \cap \{T = \tau_0\}$, the dimension of V is exactly 1 and $\overline{\pi_T(V)} = K$. □

Lemma 2. *Let $P = (p_1, \ldots, p_n)$ in $K[T, X_1, \ldots, X_n]^n$ and let W be the union of all irreducible components V of $\{(\tau, \xi) \in K^{n+1} \mid P(\tau, \xi) = 0\}$ of dimension 1 such that π_T is a dominant map from V to K. For every $z \in K^n$ such that $(0, z) \in W$, there exists a Puiseux series $x_z \in \{x \in \overline{K(T)}^n \mid P(x) = 0\}$ such that $x_z(0) = z$.*

Proof. Let $\mathfrak{I}(W) \subset K[T, X]$ be the defining ideal of W. Consider the extended ideal $\mathfrak{I}(W)^e \subset K(T)[X]$ and let W^e be the zero-dimensional variety defined by this ideal in $\overline{K(T)}^n$. Let u be a linear form satisfying the conditions in [1, Lemma 12.32] (note that this implies that u separates the points in $W \cap \{T = 0\}$) and, following [1, Section 12.4], let $\widehat{\chi}_u(Y), \widehat{\varphi}_{u,1}(Y), \widehat{\varphi}_{u,X_i}(Y) \in K[T][Y]$, for $1 \leq i \leq n$, be polynomials giving geometric resolutions of both W^e and W.

Let $(0, z) \in W$, then $(0, u(z))$ lies in the curve $\{(\tau, y) \in K^2 \mid \widehat{\chi}_u(\tau, y) = 0\}$. By [30, Chapter IV, Theorem 2.3], there exists y_z in $\{y \in \overline{K(T)} \mid \widehat{\chi}_u(y) = 0\}$ such that $\lim_{T \to 0} y_z = u(z)$. For $1 \leq i \leq n$, let $(x_z)_i = \widehat{\varphi}_{u,X_i}(y_z)/\widehat{\varphi}_{u,1}(y_z)$. Then $x_z \in W^e$, and, by [1, Section 12.5], $z' := \lim_{T \to 0} x_z$ exists and $(0, z')$ is a point in W. As $u(x_z) = y_z$, then $u(z') = \lim_{T \to 0} u(x_z) = \lim_{T \to 0} y_z = u(z)$. By the separating assumptions on u, we conclude that $z = z'$. □

3.2. Generic sparse systems

In this section, we present some theoretic results on generic sparse systems and their supports which will imply the correctness of our algorithm.

Let $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ be a family of finite subsets of $(\mathbb{Z}_{\geq 0})^n$ and let $P = (p_1, \ldots, p_n)$ be a generic sparse system of polynomials in $K[X_1, \ldots, X_n]$ supported on $\mathcal{A}$ where $p_j = \sum_{q \in \mathcal{A}_j} c_{j,q} X^q$. Suppose that $0 \notin \bigcap_{j=1}^n \mathcal{A}_j$. By [14] and Lemma 2, the isolated common zeroes of P can be obtained as the limits when $t \to 0$ of the solutions of the deformed system $P^0 = (p_1^0, \ldots, p_n^0)$ where, for $j = 1, \ldots, n$,

$$p_j^0 := \begin{cases} p_j & \text{if } 0 \in \mathcal{A}_j \\ p_j + c_{j,0} t^k & \text{if } 0 \notin \mathcal{A}_j \end{cases}$$

with $c_{j,0} \in K$ generic if $0 \notin \mathcal{A}_j$ and $k \in \mathbb{N}$ (here, t is a new variable). More precisely, for every $I \subset \{1, \ldots, n\}$, the isolated common zeroes of the system P in

$$O_I := \{x \in K^n \mid x_i = 0 \iff i \in I\}$$

are obtained from the ones of P^0 which are of the type

$$x(t) = (\xi_1 t^{\gamma_1} + o(t^{\gamma_1}), \ldots, \xi_n t^{\gamma_n} + o(t^{\gamma_n})),$$

with

$$\gamma_i = 0 \text{ if } i \notin I \text{ and } \gamma_i > 0 \text{ if } i \in I,$$

where $o(t^{\gamma_i})$ denotes a Puiseux series where all the terms have exponents in t greater than γ_i. Moreover, the initial exponents $\gamma = (\gamma_1, \ldots, \gamma_n)$ are the first n coordinates of the inner normal vectors $(\gamma, 1) \in \mathbb{Q}^{n+1}$ of the facets of $conv(\mathcal{A}^0)$ where $\mathcal{A}^0 = (\mathcal{A}_1^0, \ldots, \mathcal{A}_n^0)$ is the family of supports of P^0. Furthermore, $\xi = (\xi_1, \ldots, \xi_n) \in (K^*)^n$ is a solution of the system $P_C^0 = ((p_1^0)_{C_1}, \ldots, (p_n^0)_{C_n})$ supported on the cell $C = (C_1, \ldots, C_n)$ of the subdivision $S_{\omega^0}(\mathcal{A}^0)$ with associated normal vector γ, where

$$(p_j^0)_{C_j} := \sum_{q \in C_j} c_{j,q} X^q.$$

Note that, in this case, $\lim_{t \to 0} x(t) = \tilde{\xi}$, where $\tilde{\xi}_i = \xi_i$ if $i \notin I$ and $\tilde{\xi}_i = 0$ if $i \in I$.

Remark 3. If P has isolated roots in O_I, there is a cell $C \in S_{\omega^0}(\mathcal{A}^0)$ with positive mixed volume such that its associated normal vector γ satisfies $\gamma_i = 0$ for $i \notin I$ and $\gamma_i > 0$ for $i \in I$.

For every $I \subset \{1, \ldots, n\}$, let P_I be the system formed by the polynomials obtained by evaluating $X_i = 0$ for every $i \in I$ in the polynomials P and considering only those which do not vanish identically under this evaluation.

Lemma 4. *Let $I \subset \{1, \ldots, n\}$ be such that the system P has isolated roots in O_I. Then the system P_I has exactly $n - \#I$ polynomials. In addition, for every cell C of $S_{\omega^0}(\mathcal{A}^0)$ whose associated normal vector γ satisfies $\gamma_i = 0$ if $i \notin I$ and $\gamma_i > 0$ if $i \in I$, the system P_C^0 consists of the polynomials in P_I and of $\#I$ polynomials which become constants when evaluating $X_i = 0$ for every $i \in I$.*

Proof. As P has isolated roots in O_I, P_I has isolated roots in O_I, and then the number of polynomials in P_I is at least $n - \#I$. In addition, as P_I is a generic system, by Bernstein's theorem, choosing exactly $n - \#I$ of these polynomials, they share finitely many roots in $(K^*)^{n-\#I} \cong O_I$. Then, if there is any polynomial left in P_I, it will not vanish at any of these roots.

Now, let $C \in S_{\omega^0}(\mathcal{A}^0)$ be a cell such that its associated normal vector $\gamma = (\gamma_1, \ldots, \gamma_n)$ satisfies $\gamma_i = 0$ for $i \notin I$ and $\gamma_i > 0$ for $i \in I$. For $j = 1, \ldots, n$, let $\alpha_j := \min\{\sum_{i=1}^n \gamma_i q_i + \omega_j^0(q) : q \in \mathcal{A}_j^0\} \geq 0$. Then $C = (C_1, \ldots, C_n)$, where $C_j = \mathcal{A}_j^0 \cap \{q \mid \sum_{i=1}^n \gamma_i q_i + \omega_j^0(q) = \alpha_j\}$.

Let $j_1, \ldots, j_{n-\#I}$ be the indices such that P_I is obtained from $p_{j_1}, \ldots, p_{j_{n-\#I}}$. Note that, for each $1 \leq k \leq n - \#I$, at least one of the monomials in p_{j_k} does not lie in $\langle X_i : i \in I\rangle$; then, for the exponent $q \in \mathcal{A}_{j_k}$ of this monomial we have that $\sum_{i=1}^n \gamma_i q_i + \omega_{j_k}^0(q) = 0$ and, therefore, $\alpha_{j_k} = 0$. Thus, the exponent vector of each monomial in $(p_{j_k})_I$ is in C_{j_k}. Moreover, for each q such that $X^q \in \langle X_i : i \in I\rangle$, we have that $q_{i_0} > 0$ for some $i_0 \in I$ and so, $\sum_{i=1}^n \gamma_i q_i \geq \gamma_{i_0} q_{i_0} > 0$ implying that $q \notin C_{j_k}$. Finally, if $0 \notin \mathcal{A}_{j_k}$, then $\omega_{j_k}^0(0) > 0$ and then, $0 \notin C_{j_k}$. We conclude that C_{j_k} consists exactly of the exponents of monomials in $(p_{j_k})_I$ (considered as n-variate polynomials).

For $j \notin \{j_1, \ldots, j_{n-\#I}\}$, each monomial of p_j lies in the ideal $\langle X_i : i \in I\rangle$. Then, $(p_j^0)_C$ is a sum of monomials in $\langle X_i : i \in I\rangle$ and (possibly) a constant term; therefore, it becomes constant when evaluating $X_i = 0$ for every $i \in I$. □

Let $S_\omega(\mathcal{A}^0)$ be the subdivision of $\mathcal{A}^0$ induced by a lifting function ω such that $\omega_j(q) \in \mathbb{R}_{\geq 0}$ for each $q \in \mathcal{A}_j$ and $\omega_j(0) = k \gg 0$ if $0 \notin \mathcal{A}_j$. Using [16, Lemma 2.1], it follows that for a generic ω, $S_\omega(\mathcal{A}^0)$ is a fine mixed subdivision. In [7, Proposition 1] it is proved that, taking $\omega_j(q) \in (0, 1)$ for every $q \in \mathcal{A}_j$, if $k > n(n+1)d^n$ where $d = \max_{1\leq j\leq n}\{q_1 + \cdots + q_n \mid q \in \mathcal{A}_j\}$, the subdivision $S_\omega(\mathcal{A}^0)$ refines $S_{\omega^0}(\mathcal{A}^0)$. Similarly, taking $\omega_j(q) \in (0, M)$, the same holds if $k > n(n+1)d^nM$. We use this result to consider a lifting function ω taking non-negative integer values.

Remark 5. Let C be a cell of $S_{\omega^0}(\mathcal{A}^0)$. Then P_C^0 has solutions in $(K^*)^n$ if and only if the cell C has positive mixed volume, which is equivalent to the fact that it contains a cell of $S_\omega(\mathcal{A}^0)$ of type 1_n.

For every $I \subset \{1, \ldots, n\}$, we denote by $J_I = \{j \in \{1, \ldots, n\} \mid \exists q \in \mathcal{A}_j : q_i = 0\ \forall i \in I\}$. Let $\pi_I : \mathbb{Z}^n \to \mathbb{Z}^{n-\#I}$ be the projection such that $\pi_I(q) = (q_i)_{i\notin I}$ and $\varphi_I : \mathbb{Z}^{n-\#I} \to \mathbb{Z}^n$ the map that inserts zeroes in the coordinates indexed by $i \in I$. We define $\mathcal{A}^I = (\mathcal{A}_j^I)_{j\in J_I}$ where $\mathcal{A}_j^I = \{\pi_I(q) \mid q \in \mathcal{A}_j,\ q_i = 0\ \forall i \in I\}$, and $\omega^I = (\omega_j^I)_{j\in J_I}$ where $\omega_j^I : \mathcal{A}_j^I \to \mathbb{Z}_{\geq 0}$ is defined as $\omega_j^I(\overline{q}) = \omega_j(\varphi_I(\overline{q}))$ (note that $\mathcal{A}^I$ is the family of supports of the polynomials P_I and ω^I is the lifting induced by ω over $\mathcal{A}^I$).

If $\nu \in \mathbb{R}^s$ and $C \subset \mathbb{R}^s$ is a compact set, we will write C_ν for the set of points in C which minimize the inner product $\langle \cdot, \nu\rangle$.

Lemma 6. *For every I such that P has isolated roots in O_I and any cell $C \in S_{\omega^0}(\mathcal{A}^0)$ with positive mixed volume and whose associated normal vector γ satisfies $\gamma_i = 0$ if $i \notin I$ and $\gamma_i > 0$ if $i \in I$, each cell of type $1_{n-\#I}$ of $S_{\omega^I}(\mathcal{A}^I)$ is of the form $\pi_I(D) := (\pi_I(D_j))_{j\in J_I}$ for a cell $D = (D_1, \ldots, D_n) \in S_\omega(C)$ of type 1_n.*

Proof. Without loss of generality, assume that $I = \{r+1, \ldots, n\}$ and $J_I = \{1, \ldots, r\}$. Then, by Lemma 4, for every cell C satisfying the assumptions, $C_j = \mathcal{A}_j^I \times \{0\}$ for every $1 \leq j \leq r$, and therefore, $C_j(\omega_j) \simeq \mathcal{A}_j^I(\omega_j^I) \times \{0\}$ for every $1 \leq j \leq r$.

Let $D \in S_\omega(C)$ a cell of type 1_n; that is, there exists $\mu \in \mathbb{Q}^n$ such that $C(\omega)_{(\mu,1)} = \left(\sum_{j=1}^n C_j(\omega_j)\right)_{(\mu,1)} = \sum_{j=1}^n C_j(\omega_j)_{(\mu,1)}$ and, if π denotes the projection to the first n coordinates, $D_j = \pi(C_j(\omega_j)_{(\mu,1)})\ \forall\, 1 \leq j \leq n$.

Consider now the vector $\mu_I := \pi_I(\mu)$. Then $\mathcal{A}^I(\omega^I)_{(\mu_I,1)} = \sum_{j=1}^r \mathcal{A}_j^I(\omega_j^I)_{(\mu_I,1)}$. On the other hand, $C_j(\omega_j) \simeq \mathcal{A}_j^I(\omega_j^I) \times \{0\}$ implies that $C_j(\omega_j)_{(\mu,1)} \simeq \mathcal{A}_j^I(\omega_j^I)_{(\mu_I,1)} \times \{0\}$ and, therefore, the cell of $\mathcal{A}^I$ associated with μ_I is $(\pi_I(D_1), \ldots, \pi_I(D_r))$. Since, for $1 \leq j \leq r$, $D_j \subset C_j$, we have that $D_j = \pi_I(D_j) \times \{0\}$. It follows that $(\pi_I(D_1), \ldots, \pi_I(D_r))$ is a cell of $S_{\omega^I}(\mathcal{A}^I)$ of type 1_r.

Conversely, let $D^I = (D_1^I, \ldots, D_r^I)$ be a type 1_r cell in the subdivision $S_{\omega^I}(\mathcal{A}^I)$ for I satisfying the assumptions of the lemma. If $(\mu_I, 1)$ is the inner normal vector to $\mathcal{A}^I(\omega^I)$ giving the facet associated with D^I, we have that μ_I is the vector of exponents of the initial terms of a solution $\xi(y)$ to the system $P_I^{\omega^I}(X, y)$.

Let C be a cell in $S_{\omega^0}(\mathcal{A}^0)$ with positive mixed volume and whose associated normal vector γ satisfies $\gamma_i = 0$ if $i \notin I$ and $\gamma_i > 0$ if $i \in I$. Consider the system P_C^0. By Lemma 4, this system consists of the polynomials P_I and $\#I$ polynomials which become constant when specializing $X_i = 0$ for $i \in I$. Then, the system $(P_C^0)^\omega(X, y)$ consists of the polynomials $P_I^{\omega^I}(X, y)$ plus $\#I$ polynomials. Now, each solution to $P_I^{\omega^I}(X, y) = 0$ leads to a solution to $(P_C^0)^\omega(X, y) = 0$ (by the genericity assumption on the system P and Bernstein's theorem) and so, there exists a solution $\widetilde{\xi}(y)$ such that its first r coordinates are formed by the vector $\xi(y)$. Note that the vector μ of exponents of the initial terms of the coordinates of $\widetilde{\xi}(y)$ satisfies that $(\mu, 1)$ is the inner normal vector to a facet of $C(\omega)$ producing a cell D of type 1_n in the subdivision $S_\omega(C)$.

Finally, our previous arguments imply that D^I is the projection of D. □

4. The algorithm

Let $F = (f_1, \ldots, f_n) \in \mathbb{Q}[X_1, \ldots, X_n]^n$ be a vector of polynomials with supports $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$. Our algorithm computes a finite set containing the isolated common zeroes of F. Let $G = (g_1, \ldots, g_n) \in \mathbb{Q}[X_1, \ldots, X_n]^n$ be generic polynomials

with the same supports $\mathcal{A}$. Consider the homotopic deformation

$$H(T, X) = (1 - T) \cdot F(X) + T \cdot G(X)$$

where T is a new variable.

By Lemma 1, for every isolated zero $z \in \mathbb{C}^n$ of F, there exists a one-dimensional irreducible component V of $\{(\tau, \xi) \in \mathbb{C}^{n+1} \mid H(\tau, \xi) = 0\}$ such that $(0, z) \in V$ and $\overline{\pi_T(V)} = \mathbb{C}$. These one-dimensional irreducible components correspond to isolated zeroes of H in $(\overline{\mathbb{C}(T)})^n$ considered as polynomials in the variables X with coefficients in $\mathbb{Q}[T]$ (see Lemma 2). Then, to find the isolated common zeroes of F, we deal with these isolated solutions. In order to find them, we adapt the polyhedral deformation techniques introduced in [13,14] and refined in [7], using symbolic methods as in [16].

Note that $H = (h_1, \ldots, h_n)$ are generic polynomials with supports $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$ and, therefore, all the results in Section 3.2 hold.

Our algorithm takes as part of the input the mixed cells in a fine mixed subdivision of $\mathcal{A}^0 = (\mathcal{A}_1^0, \ldots, \mathcal{A}_n^0)$, where $\mathcal{A}_j^0 = \mathcal{A}_j \cup \{0\}$ for every $1 \leq j \leq n$, induced by a lifting $\omega = (\omega_1, \ldots, \omega_n)$ such that $\omega_j(q) \in \mathbb{Z}_{\geq 0}$ for each $q \in \mathcal{A}_j$ and $\omega_j(0) = k$ if $0 \notin \mathcal{A}_j$, where $k \in \mathbb{Z}_{\geq 0}$ is fixed. A lifting constructed by randomly choosing $\omega_j(q) \in \mathbb{Z}_{\geq 0} \cap [0, M]$ for each $q \in \mathcal{A}_j$, and k in a fixed set of M integers greater than $n(n+1)d^nM$ induces a fine mixed subdivision with probability as close to 1 as wanted provided M is big enough (see Section 3.2). From this lifting, the mixed cells in the subdivision can be obtained algorithmically by means of linear programming based procedures, being the one in [23] the most efficient we know. We are going to consider this step as a pre-processing and, therefore, our complexity estimates will not include its cost.

In a first step, the algorithm finds a set $\mathcal{I}$ of subsets $I \subset \{1, \ldots, n\}$ such that the system H may have isolated solutions in $O_I = \{x \in \overline{\mathbb{C}(T)}^n \mid x_i = 0 \iff i \in I\}$ and then, it computes these solutions by solving the systems H_I in $(\overline{\mathbb{C}(T)}^*)^{n-\#I}$ and inserting zeroes in the coordinates indexed by $i \in I$. From these solutions, by taking the limits for $T \to 0$, the isolated zeroes of the input system F are obtained.

Finding the set $\mathcal{I}$. For every $D \in S_\omega(\mathcal{A}^0)$ of type 1_n, compute the normal vector $(\gamma, 1)$ to $conv(D(\omega^0))$. Discard the cells such that $\gamma_i < 0$ for some i. Using Remarks 3 and 5, we have that $\mathcal{I} = \{I \subset \{1, \ldots, n\} \mid \exists \gamma$ such that $\gamma_i > 0 \iff i \in I\}$.

In order to use it as input in the next step, we compute simultaneously $\mathcal{I}$ and, for every $I \in \mathcal{I}$, the set S_I of all the cells of type $1_{n-\#I}$ of $S_{\omega^I}(\mathcal{A}^I)$. Note that, by Lemma 6, for each $I \in \mathcal{I}$, it suffices to take a cell $C \in S_{\omega^0}(\mathcal{A}^0)$ whose normal vector satisfies $\{i \mid \gamma_i > 0\} = I$ and to consider $S_I = \{\pi_I(D) \mid D \in S_\omega(C)$ of type $1_{n-\#I}\}$.

To do this computation, for each cell $D \in S_\omega(\mathcal{A}^0)$ of type 1_n, consider (D, γ, χ_γ), where γ is the normal vector associated with D and χ_γ is defined as $(\chi_\gamma)_i = 0$ if $\gamma_i = 0$ and $(\chi_\gamma)_i = 1$ if $\gamma_i > 0$. Apply a standard sorting algorithm to order these vectors lexicographically in the coordinates χ_γ. For each different $\chi = \chi_\gamma$ in the list, the algorithm adds the set $I = \{i \mid \chi_i = 1\}$ to $\mathcal{I}$, takes the first element (D, γ, χ) and forms the set S_I using all other (D', γ, χ) with the same γ. The remaining triples with the same coordinate χ are discarded.

Remark 7. Due to Remark 5, each I in the set $\mathcal{I}$ constructed in this step corresponds to at least one of the cells $C \in S_{\omega^0}(\mathcal{A}^0)$ contributing to the stable mixed volume computation in [14].

Solving the system H_I for $I \in \mathcal{I}$. Given $I \in \mathcal{I}$, consider $J_I = \{j \in \{1, \ldots, n\} \mid \exists q \in \mathcal{A}_j : q_i = 0 \; \forall i \in I\}$. If $\#J_I \neq n - \#I$, discard I. Otherwise, consider F_I and G_I the systems formed by the polynomials obtained by evaluating $X_i = 0$ for every $i \in I$ in the polynomials F and G respectively and considering only the non-vanishing ones. Then, $H_I = (1 - T)F_I + TG_I$. To find the solutions of $H_I = 0$ in $(\overline{\mathbb{C}(T)}^*)^{n-\#I}$, we start by solving the generic system G_I (which has $n - \#I$ equations) in $(\mathbb{C}^*)^{n-\#I}$.

The solutions of G_I are obtained by using the set of cells S_I computed before, which are the cells of type $1_{n-\#I}$ in the fine mixed subdivision $S_{\omega^I}(\mathcal{A}^I)$, as input of the algorithm in [16, Section 5] (which will be referred to as `ToricSolve`). This algorithm produces a geometric resolution of the set of common zeroes of G_I in $(\mathbb{C}^*)^{n-\#I}$ (note that the algorithm in [16] computes the isolated common roots of a system in the torus without any assumptions on its support).

As the system G_I is generic, from a geometric resolution of the common zeroes of G_I in $(\mathbb{C}^*)^{n-\#I}$, a geometric resolution of the solutions of H_I in $(\overline{\mathbb{C}(T)}^*)^{n-\#I}$ can be computed as in [16, Section 6.1]. We call this subroutine `NewtonHenselLifting`.

Finally, by adding the polynomial zero for the coordinates indexed by $i \in I$ to the geometric resolution obtained, we get a geometric resolution of a finite set containing all the isolated zeroes of H in O_I.

Remark 8 (*See [16, Theorem 6.2]*)**.** With the previous assumptions and notations, the algorithm described above has complexity

$$O(((n - \#I)^3 N_I \log \mathcal{Q}_I + (n - \#I)^{\Omega+1}) M(\mathcal{D}_I)(M(\Upsilon_I)(M(\mathcal{D}_I) + M(E_I)) + M(E_I')))$$

where $N_I := \sum_{j \in J_I} \#(\mathcal{A}_j^I)$, $\mathcal{Q}_I := \max\{\|q\| \mid q \in \bigcup_{j \in J_I} \mathcal{A}_j^I\}$, $\mathcal{D}_I := \mathcal{M}(\mathcal{A}^I)$, $\Upsilon_I := \max \|\mu_I\|$ where the maximum is taken over all normal vectors to cells of type $1_{n-\#I}$ in $S_{\omega^I}(\mathcal{A}^I)$, $E_I := \mathcal{M}(\Delta_{n-\#I} \times \{0\}, (\mathcal{A}_j^I(\omega_j^I))_{j \in J_I})$, and $E_I' := \mathcal{M}(\{0\} \times \Delta_{n-\#I}, (\{0, 1\} \times \mathcal{A}_j^I)_{j \in J_I})$, where $\Delta_{n-\#I}$ is the set of vertices of the standard simplex of $\mathbb{R}^{n-\#I}$.

This algorithm works with any sufficiently generic linear form. As we want to join all the previous geometric resolutions in order to obtain a geometric resolution of all the isolated zeroes of H, we work with a unique linear form $u = \sum_{1 \leq i \leq n} u_i.X_i$. When dealing with a specific I, we consider $u_I = \sum_{i \notin I} u_i.X_i$. Note that, for every zero x of H_I, $u_I(x) = u(\varphi_I(x))$ and, therefore,

the computed geometric resolution represents the isolated zeroes of H in O_l using the linear form u. As a generic linear form meets all the requirements, we choose the coefficients of u at random from a sufficiently large set in $(\mathbb{Z}_{\geq 0})^n$.

Joining geometric resolutions. By repeating the procedure in the previous step for every $I \in \mathcal{I}$ using the same separating linear form, we obtain a family of geometric resolutions $\widetilde{R}_I$ representing all the isolated zeroes of H in $(\overline{\mathbb{C}(T)})^n$. From them, a single geometric resolution $R = \{M_u(T, Y), V_1(T, Y), \ldots, V_n(T, Y)\}$ representing all these points is obtained noticing that, if $\{q, q_0, w_1, \ldots, w_n\}$ and $\{\tilde{q}, \tilde{q}_0, \tilde{w}_1, \ldots, \tilde{w}_n\}$ are geometric resolutions of disjoint sets with q and $\tilde{q}$ relatively prime polynomials, then $\{q\tilde{q}, q_0\tilde{q} + \tilde{q}_0 q, w_1\tilde{q} + \tilde{w}_1 q, \ldots, w_n\tilde{q} + \tilde{w}_n q\}$ is a geometric resolution of their union.

Computing the isolated roots of F. The limit of the geometric resolution R when $T \to 0$ is obtained as in [16, Section 6.2]: compute $a(Y) = \gcd(M_u(0, Y), (\partial M_u/\partial Y)(0, Y))$ and the polynomials $m_u(Y) = M_u(0, Y)/a(Y)$, $b(Y) = ((\partial M_u/\partial Y)(0, Y)/a(Y))^{-1} \mod m_u(Y)$, and $v_i(Y) = b(Y)V_i(0, Y)/a(Y) \mod m_u(Y)$ $(1 \leq i \leq n)$. Then, $r = (m_u, v_1, \ldots, v_n)$ is a geometric resolution of a finite set containing all the isolated zeroes of the input system F in $\mathbb{C}^n$.

The complexity of the algorithm is stated in the following Theorem.

Theorem 9. *Let $F = (f_1, \ldots, f_n)$ in $\mathbb{Q}[X_1, \ldots, X_n]^n$ be a sparse polynomial system supported on $\mathcal{A} = (\mathcal{A}_1, \ldots, \mathcal{A}_n)$. Algorithm* `AffineSolve` *is a probabilistic procedure that, taking as input the sparse encoding of F and the mixed cells in a suitable fine mixed subdivision of $\mathcal{A}^0$, computes a geometric resolution of a finite set of points including the isolated common zeroes of F within complexity*

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

where

- Γ *is the number of type* 1_n *cells in* $S_\omega(\mathcal{A}^0)$
- $N := \sum_{1 \leq j \leq n} \#(\mathcal{A}_j)$
- $\mathcal{Q} := \max\{\|q\| \mid q \in \bigcup_{1 \leq j \leq n} \mathcal{A}_j\}$
- $\mathcal{D} := \mathcal{SM}(\mathcal{A})$
- $\Upsilon := \max \|\mu\|$ *where the maximum is taken over all normal vectors to cells of type* 1_n *in* $S_\omega(\mathcal{A})$
- $\mathcal{E} := \mathcal{SM}(\Delta_n \times \{0\}, \mathcal{A}_1(\omega_1), \ldots, \mathcal{A}_n(\omega_n))$ *(here, Δ_n is the set of vertices of the n-dimensional standard simplex)*
- $\mathcal{E}' := \mathcal{SM}(\{0\} \times \Delta_n, \{0, 1\} \times \mathcal{A}_1, \ldots, \{0, 1\} \times \mathcal{A}_n)$.

Proof. The correctness of the algorithm follows from the results in Section 3.2. Now, we are going to prove our complexity estimate.

Each of the Γ normal vectors in the first step can be obtained in $O(n^\Omega)$ operations using standard effective linear algebra techniques. We discard the ones with negative entries within the same order of complexity.

The determination of the set $\mathcal{I}$ and the sets of cells S_I for every $I \in \mathcal{I}$ can be carried out in $O(n \log(\mathcal{SM}(A))\mathcal{SM}(A))$ by applying a standard sorting algorithm (once the list is sorted, the rest of the step can be completed without changing the order of complexity).

For each $I \in \mathcal{I}$, the complexity of the computation of $\widetilde{R}_I$ is the one stated in Remark 8. Now we have to estimate the sum of all these complexities. Note that $N_I \leq N$, $\mathcal{Q}_I \leq \mathcal{Q}$ and $\Upsilon_I \leq \Upsilon$ for every $I \in \mathcal{I}$. By Remark 7, $\sum_{I \in \mathcal{I}} \mathcal{D}_I \leq \mathcal{D}$, and then $\sum_{I \in \mathcal{I}} M(\mathcal{D}_I) \leq M(\mathcal{D})$. In addition, considering for each $I \in \mathcal{I}$ an associated cell C from the stable mixed volume computation in [14] for the support sets $\mathcal{A}$, and looking for a corresponding cell in the computation of the stable mixed volume of $(\Delta_n \times \{0\}, \mathcal{A}_1(\omega_1), \ldots, \mathcal{A}_n(\omega_n))$, it follows that $\sum_{I \in \mathcal{I}} E_I \leq \mathcal{E}$. Similarly, $\sum_{I \in \mathcal{I}} E'_I \leq \mathcal{E}'$.

By using these upper bounds, we conclude that the overall complexity of the computation of the family of geometric resolutions $(\widetilde{R}_I)_{I \in \mathcal{I}}$ representing the common zeroes of H in O_I for $I \in \mathcal{I}$ is $O((n^3 N \log \mathcal{Q} + n^{\Omega+1}) M(\mathcal{D})(M(\Upsilon)(M(\mathcal{D}) + M(\mathcal{E})) + M(\mathcal{E}')))$. Each geometric resolution $\widetilde{R}_I$ involves polynomials of degree at most D_I in the variable Y with coefficients in $\mathbb{Q}[T]$ of degrees bounded by E'_I.

Following the splitting strategy given in [8, Algorithm 10.3], a single geometric resolution R representing the isolated zeroes of H can be obtained from the previously computed $(\widetilde{R}_I)_{I \in \mathcal{I}}$ within $O(nM(\mathcal{D})M(\mathcal{E}'))$ operations in $\mathbb{Q}$ taking into account that all the polynomials involved in the intermediate computations have degrees bounded by $\mathcal{D}$ in the main variable Y and their coefficients are polynomials in $\mathbb{Q}[T]$ with degrees bounded by $\mathcal{E}'$.

The complexity of the last step of the algorithm, performed as explained above, is $O(nM(\mathcal{D})\mathcal{E}')$. □

Algorithm `AffineSolve`

Input: Polynomials $f_1, \ldots, f_n$ in $\mathbb{Q}[X_1, \ldots, X_n]$ with supports $\mathcal{A}_1, \ldots, \mathcal{A}_n$ encoded in sparse form, and the mixed cells in a fine mixed subdivision $S_\omega(\mathcal{A}^0)$.

1. For every $D \in S_\omega(\mathcal{A}^0)$ of type 1_n:
   - Find the normal vector $(\gamma, 1)$ to $conv(D(\omega^0))$.
   - If $\gamma_i < 0$ for some i, discard D and γ.
2. Compute $\mathcal{I} = \{I \subset \{1, \ldots, n\} \mid \exists \gamma$ such that $\gamma_i > 0 \iff i \in I\}$ and, for each $I \in \mathcal{I}$, the set S_I of all the cells of type $1_{n-\#I}$ of $S_{\omega^I}(\mathcal{A}^I)$.

3. Choose coefficients in $\mathbb{Q}$ randomly to obtain polynomials $G = g_1, \ldots, g_n$ with supports $\mathcal{A}_1, \ldots, \mathcal{A}_n$, and a linear form $u \in \mathbb{Q}[X_1, \ldots, X_n]$.
4. For every $I \in \mathcal{I}$ such that $\#J_I = n - \#I$:
   - Find a geometric resolution r_I of the common zeroes of G_I in $(\mathbb{C}^*)^{n-\#I}$ by applying subroutine `ToricSolve` with the cells in S_I.
   - Find a geometric resolution R_I of the common zeroes of H_I in $(\overline{\mathbb{C}(T)}^*)^{n-\#I}$ by applying subroutine `NewtonHenselLifting` to r_I.
   - Insert zeroes in the coordinates indexed by $i \in I$ in R_I to obtain a geometric resolution $\widetilde{R}_I$ representing the isolated common zeroes of H in O_I.
5. From $(\widetilde{R}_I)_{I\in\mathcal{I}}$, compute a single geometric resolution R representing the isolated zeroes of H.
6. Compute the geometric resolution $r = \lim_{T\to 0} R$.

Output: The geometric resolution r of a finite set of points including the isolated zeroes of F.

5. Examples

In this section we present some examples illustrating how our algorithm works and some of its advantages with respect to previously known procedures.

We first show the different steps of our algorithm in a small well-known example taken from [13, Example 3]:

Example 1. Consider the bivariate polynomials

$$f_1(x, y) = ay + by^2 + cxy^3$$
$$f_2(x, y) = dx + ex^2 + fx^3y$$

with generic coefficients a, b, c, d, e, f. The family of supports of these polynomials is $\mathcal{A} = (\{(0, 1), (0, 2), (1, 3)\}, \{(1, 0), (2, 0), (3, 1)\})$. Fig. 1 shows the extended supports $\mathcal{A}^0$.

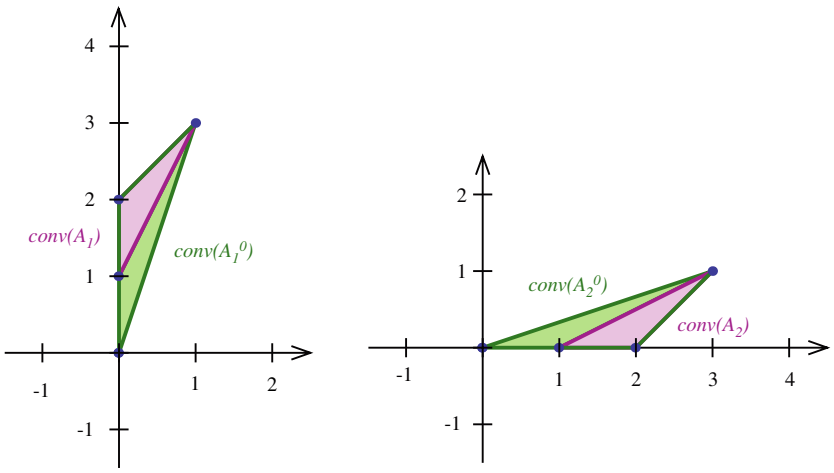

Fig. 1. Extended supports.

The input of our algorithm includes the polynomials f_1 and f_2 and the mixed cells in a fine mixed subdivision $S_\omega(\mathcal{A}^0)$ induced by a suitable generic lifting ω. Fig. 2 depicts (the convex hulls of the cells in) a fine mixed subdivision of $\mathcal{A}^0$, where the mixed cells are D_0, D_3, D_4, D_5, D_6 and D_7.

In the first step, our algorithm computes the normal vectors $(\gamma, 1)$ to $conv(D_i(\omega^0))$ for $i = 0, 3, 4, 5, 6, 7$ and discards those with some negative coordinate:

Cell	Normal vector	Non-negative entries?
D_0	$(0, 0, 1)$	Yes
D_3	$(k, -k, 1)$	No
D_4	$(-k, k, 1)$	No
D_5	$(k, 0, 1)$	Yes
D_6	$(0, k, 1)$	Yes
D_7	$(k, k, 1)$	Yes

Then, the set $\mathcal{I}$ defined in step 2 of the algorithm is $\mathcal{I} = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$; the associated systems and the mixed cells to solve them over $\mathbb{C}^*$ as in step 4 are:

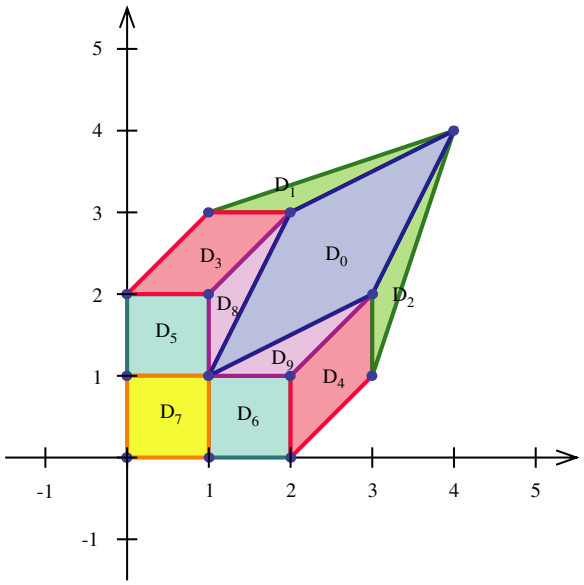

Fig. 2. Fine mixed subdivision.

I	Associated system	$\pi_I(D_i) \in S_I$
$\emptyset$	$\begin{cases} ay + by^2 + cxy^3 \\ dx + ex^2 + fx^3y \end{cases}$	$\pi_\emptyset(D_0) = (\{(0,1),(1,3)\},\{(1,0),(3,1)\})$
$\{1\}$	$ay + by^2$	$\pi_{\{1\}}(D_5) = \{1,2\}$
$\{2\}$	$dx + ex^2$	$\pi_{\{2\}}(D_6) = \{1,2\}$
$\{1,2\}$	$\emptyset$	$\pi_{\{1,2\}}(D_7) = \emptyset$

For instance, for the particular system

$$P = \begin{cases} y + 2y^2 - xy^3 = 0 \\ -x + 3x^2 - 2x^3y = 0 \end{cases}$$

after inserting 0 in the corresponding coordinates in the geometric resolutions of the associated systems computed in step 4, the algorithm produces:

I	Associated system P_I	Geometric resolution of roots
$\emptyset$	$\begin{cases} y + 2y^2 - xy^3 \\ -x + 3x^2 - 2x^3y \end{cases}$	$\left\{ \left(\frac{-3z^2+4z+4}{12z^2+22z+14}, \frac{-8z^2-32z-10}{12z^2+22z+14} \right) \Big/ \, 4z^3+11z^2+14z+2=0 \right\}$
$\{1\}$	$y + 2y^2$	$\left\{ (0,z) \,/\, z + \frac{1}{2} = 0 \right\}$
$\{2\}$	$-x + 3x^2$	$\left\{ (z,0) \,/\, z - \frac{1}{3} = 0 \right\}$
$\{1,2\}$	$\emptyset$	$\{(0,0)\}$

Finally, the algorithm obtains a single geometric resolution representing all the zeroes previously computed:

$$\left\{ \left(\frac{-10z^5 + 47z^4 + 70z^3 + 18z^2 - 2z}{144z^5+350z^4+364z^3+45z^2-24z-2}, \frac{-60z^5 - 229z^4 - 115z^3 + 30z^2 + 12z}{144z^5+350z^4+364z^3+45z^2-24z-2} \right) \Big/ \right.$$
$$\left. 24z^6 + 70z^5 + 91z^4 + 15z^3 - 12z^2 - 2z = 0 \right\}.$$

In the following example, we show a case in which our algorithm deals with systems in fewer variables than the procedures in [14,7].

Example 2. A generic system with the support sets of the Katsura4 System from PoSSo test suite (see [7]):

$$P = \begin{cases} a_{11}X_1^2 + a_{12}X_2^2 + a_{13}X_3^2 + a_{14}X_4^2 + a_{15}X_5^2 + a_{16}X_5 = 0 \\ a_{21}X_1X_2 + a_{22}X_2X_3 + a_{23}X_3X_4 + a_{24}X_4X_5 + a_{25}X_4 = 0 \\ a_{31}X_1X_3 + a_{32}X_2X_4 + a_{33}X_4^2 + a_{34}X_3X_5 + a_{35}X_3 = 0 \\ a_{41}X_1X_4 + a_{42}X_3X_4 + a_{43}X_2X_5 + a_{44}X_2 = 0 \\ a_{51}X_1 + a_{52}X_2 + a_{53}X_3 + a_{54}X_4 + a_{55}X_5 + a_{56} = 0. \end{cases}$$

According to [7, Example 6], $\mathcal{M}(\mathcal{A}) = 12$ and $\mathcal{SM}(\mathcal{A}) = 16$. Moreover, there are only three cells C^1, C^2 and C^3 in $S_{\omega^0}(\mathcal{A}^0)$ with positive mixed volume and non-negative normal vectors $(\gamma^1, 1) = (0, 0, 0, 0, 0, 1)$, $(\gamma^2, 1) = (0, k, 0, k, 0, 1)$ and $(\gamma^3, 1) = (0, k, k, k, 0, 1)$. Apart from solving the original system P in $(\mathbb{C}^*)^5$, if $I^2 = \{2, 4\}$ and $I^3 = \{2, 3, 4\}$, in order to obtain all the isolated roots of P in $\mathbb{C}^5$, our algorithm only computes the zeroes of

$$P_{I^2} = \begin{cases} a_{11}X_1^2 + a_{13}X_3^2 + a_{15}X_5^2 + a_{16}X_5 = 0 \\ a_{31}X_1X_3 + a_{34}X_3X_5 + a_{35}X_3 = 0 \\ a_{51}X_1 + a_{53}X_3 + a_{55}X_5 + a_{56} = 0 \end{cases}$$

and

$$P_{I^3} = \begin{cases} a_{11}X_1^2 + a_{15}X_5^2 + a_{16}X_5 = 0 \\ a_{51}X_1 + a_{55}X_5 + a_{56} = 0 \end{cases}$$

in $(\mathbb{C}^*)^3$ and $(\mathbb{C}^*)^2$ respectively, and inserts zeroes in the corresponding coordinates.

However, following the approach in [7], three systems in five variables (one for each cell) have to be solved to find all the isolated solutions of the original system P in $\mathbb{C}^5$.

Our last example shows an instance in which our algorithm deals with fewer systems (also in fewer variables) than the procedures in [14,7].

Example 3. Consider the following system of equations in three variables:

$$P = \begin{cases} a_{11}X_1^2 + a_{12}X_1^2X_2^2 + a_{13}X_1X_3 + a_{14}X_1X_2^2X_3 + a_{15}X_3^4 + a_{16}X_2^2X_3^4 = 0 \\ a_{21}X_1^4 + a_{22}X_1^4X_2^2 + a_{23}X_1^2X_3 + a_{24}X_1^2X_2^2X_3 + a_{25}X_3^4 + a_{26}X_2^2X_3^4 = 0 \\ a_{31}X_1 + a_{32}X_1X_2^2 + a_{33} + a_{34}X_2^2 + a_{35}X_3 + a_{36}X_2^2X_3 = 0. \end{cases}$$

There are two cells C^1 and C^2 of $S_{\omega^0}(\mathcal{A}^0)$ with positive mixed volume whose normal vectors are $\gamma^1 = (\frac{3k}{4}, 0, \frac{k}{4}, 1)$ and $\gamma^2 = (\frac{k}{3}, 0, \frac{k}{3}, 1)$. Both these normal vectors have nonzero coordinates for $I = \{1, 3\}$. In order to compute the isolated solutions with $X_1 = 0, X_2 \neq 0$ and $X_3 = 0$, our algorithm solves the associated system obtained by evaluating $X_1 = 0$ and $X_3 = 0$ in the original system and discarding the vanishing equations, which in this case is simply the equation

$$P_I = \{a_{33} + a_{34}X_2^2 = 0.$$

From this equation, the two isolated solutions of the system in O_I are obtained.

On the other hand, the algorithm in [7] (as the one in [14]) requires solving two associated systems, each one supported in one of those cells:

$$P_{C^1} = \begin{cases} a_{13}X_1X_3 + a_{14}X_1X_2^2X_3 + a_{15}X_3^4 + a_{16}X_2^2X_3^4 + c_1 = 0 \\ a_{25}X_3^4 + a_{26}X_2^2X_3^4 + c_2 = 0 \\ a_{33} + a_{34}X_2^2 = 0 \end{cases}$$

$$P_{C^2} = \begin{cases} a_{11}X_1^2 + a_{12}X_1^2X_2^2 + a_{13}X_1X_3 + a_{14}X_1X_2^2X_3 = 0 \\ a_{23}X_1^2X_3 + a_{24}X_1^2X_2^2X_3 + c_2 = 0 \\ a_{33} + a_{34}X_2^2 = 0 \end{cases}$$

where c_1 and c_2 are generic constants. These systems have $8 = \mathcal{M}(C^1)$ and $6 = \mathcal{M}(C^2)$ isolated roots in $(\mathbb{C}^*)^3$ respectively. The algorithm in [7] has to compute all these 14 solutions (and replace their first and third coordinates by 0) to obtain the only two isolated solutions of the system in O_I.

Acknowledgements

The authors wish to thank the referees for their helpful suggestions and comments.

References

[1] S. Basu, R. Pollack, M.-F. Roy, Algorithms in Real Algebraic Geometry, 2nd ed., in: Algorithms and Computation in Mathematics, vol. 10, Springer-Verlag, Berlin, 2006.
[2] D.N. Bernstein, The number of roots of a system of equations, Funct. Anal. Appl. 9 (1975) 183–185. Translated from Funkts. Anal. Prilozh. 9(3) (1975) 1–4.
[3] D. Cox, J. Little, D. O'Shea, Using algebraic geometry, in: Graduate Texts in Mathematics, vol. 185, Springer, New York, 1998.
[4] I.Z. Emiris, J.F. Canny, Efficient incremental algorithms for the sparse resultant and the mixed volume, J. Symbolic Comput. 20 (2) (1995) 117–149.
[5] I.Z. Emiris, J. Verschelde, How to count efficiently all affine roots of a polynomial system, Discrete Appl. Math. 93 (1) (1999) 21–32.
[6] T. Gao, T.Y. Li, Mixed volume computation for semi-mixed systems, Discrete Comput. Geom. 29 (2) (2003) 257–277.
[7] T. Gao, T.Y. Li, X. Wang, Finding all isolated zeroes of polynomial systems in $\mathbb{C}^n$ via stable mixed volumes. Polynomial elimination—algorithms and applications, J. Symbolic Comput. 28 (1–2) (1999) 187–211.
[8] J. von zur Gathen, J. Gerhard, Modern Computer Algebra, Cambridge University Press, Cambridge, 1999.
[9] I.M. Gelfand, M.M. Kapranov, A.V. Zelevinsky, Discriminants, resultants, and multidimensional determinants, in: Mathematics: Theory & Applications, Birkhäuser Boston, Inc., Boston, MA, 1994.
[10] M. Giusti, J. Heintz, J.E. Morais, J. Morgenstern, L.M. Pardo, Straight-line programs in geometric elimination theory, J. Pure Appl. Algebra 124 (1998) 101–146.
[11] M. Giusti, G. Lecerf, B. Salvy, A Gröbner free alternative for polynomial system solving, J. Complexity 17 (1) (2001) 154–211.
[12] J. Heintz, T. Krick, S. Puddu, J. Sabia, A. Waissbein, Deformation techniques for efficient polynomial equation solving, J. Complex. 16 (1) (2000) 70–109.
[13] B. Huber, B. Sturmfels, A polyhedral method for solving sparse polynomial systems, Math. Comput. 64 (212) (1995) 1541–1555.
[14] B. Huber, B. Sturmfels, Bernstein's theorem in affine space, Discrete Comput. Geom. 17 (1997) 137–141.
[15] G. Jeronimo, T. Krick, J. Sabia, M. Sombra, The computational complexity of the Chow form, Found, Comput. Math. 4 (1) (2004) 41–117.
[16] G. Jeronimo, G. Matera, P. Solernó, A. Waissbein, Deformation techniques for sparse systems, Found. Comput. Math. 9 (2009) 1–50.
[17] A.G. Khovanskii, Newton polyhedra and toroidal varieties, Funct. Anal. Appl. 11 (1978) 289–296.
[18] A.G. Kushnirenko, Newton polytopes and the Bezout theorem, Funct. Anal. Appl. 10 (1976) 233–235.
[19] G. Lecerf, Computing the equidimensional decomposition of an algebraic closed set by means of lifting fibers, J. Complex. 19 (4) (2003) 564–596.
[20] T.Y. Li, Numerical solution of multivariate polynomial systems by homotopy continuation methods, Acta Numer. 6 (1997) 399–436.
[21] T.Y. Li, X. Li, Finding mixed cells in the mixed volume computation, Found. Comput. Math. 1 (2) (2001) 161–181.
[22] T.Y. Li, X. Wang, The BKK root count in $\mathbb{C}^n$, Math. Comp. 65 (216) (1996) 1477–1484.
[23] T. Mizutani, A. Takeda, M. Kojima, Dynamic enumeration of all mixed cells, Discrete Comput. Geom. 37 (3) (2007) 351–367.
[24] J.M. Rojas, A convex geometrical approach to counting the roots of a polynomial system, Theoret. Comput. Sci. 133 (1994) 105–140.
[25] J.M. Rojas, Why polyhedra matter in non-linear equation solving, in: Topics in Algebraic Geometry and Geometric Modeling, in: Contemp. Math., vol. 334, Amer. Math. Soc., Providence, RI, 2003, pp. 293–320.
[26] J.M. Rojas, X. Wang, Counting affine roots of polynomial systems via pointed Newton polytopes, J. Complexity 12 (2) (1996) 116–133.
[27] A. Sommese, C. Wampler, The Numerical Solution of Systems of Polynomials Arising in Engineering and Science, World Scientific, Singapore, 2005.
[28] J. Verschelde, K. Gatermann, R. Cools, Mixed-volume computation by dynamic lifting applied to polynomial system solving, Discrete Comput. Geom. 16 (1) (1996) 69–112.
[29] J. Verschelde, P. Verlinden, R. Cools, Homotopies exploiting Newton polytopes for solving sparse polynomial systems, SIAM J. Numer. Anal. 31 (3) (1994) 915–930.
[30] R. Walker, Algebraic Curves, Springer, 1978.