

Homotopy techniques for solving sparse column support determinantal polynomial systems

George Labahn, Mohab Safey El Din, Éric Schost, Thi Xuan Vu

▶ **To cite this version:**

George Labahn, Mohab Safey El Din, Éric Schost, Thi Xuan Vu. Homotopy techniques for solving sparse column support determinantal polynomial systems. Journal of Complexity, 2021, 66, pp.101557. 10.1016/j.jco.2021.101557 . hal-02927630

HAL Id: hal-02927630

https://hal.sorbonne-universite.fr/hal-02927630

Submitted on 1 Sep 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Homotopy techniques for solving sparse column support determinantal polynomial systems

George Labahn [*], Mohab Safey El Din [†], Éric Schost[*], Thi Xuan Vu[†*]

Abstract

Let $\mathbf{K}$ be a field of characteristic zero with $\overline{\mathbf{K}}$ its algebraic closure. Given a sequence of polynomials $\boldsymbol{g} = (g_1, \ldots, g_s) \in \mathbf{K}[x_1, \ldots, x_n]^s$ and a polynomial matrix $\boldsymbol{F} = [f_{i,j}] \in \mathbf{K}[x_1, \ldots, x_n]^{p \times q}$, with $p \leq q$, we are interested in determining the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{g})$, the algebraic set of points in $\overline{\mathbf{K}}$ at which all polynomials in $\boldsymbol{g}$ and all p-minors of $\boldsymbol{F}$ vanish, under the assumption $n = q - p + s + 1$. Such polynomial systems arise in a variety of applications including for example polynomial optimization and computational geometry.

We design a randomized sparse homotopy algorithm for computing the isolated points in $V_p(\boldsymbol{F}, \boldsymbol{g})$ which takes advantage of the determinantal structure of the system defining $V_p(\boldsymbol{F}, \boldsymbol{g})$. Its complexity is polynomial in the maximum number of isolated solutions to such systems sharing the same sparsity pattern and in some combinatorial quantities attached to the structure of such systems. It is the first algorithm which takes advantage both on the determinantal structure and sparsity of input polynomials.

We also derive complexity bounds for the particular but important case where $\boldsymbol{g}$ and the columns of $\boldsymbol{F}$ satisfy weighted degree constraints. Such systems arise naturally in the computation of critical points of maps restricted to algebraic sets when both are invariant by the action of the symmetric group.

1 Introduction

Let $\boldsymbol{g} = (g_1, \ldots, g_s)$ be a sequence of polynomials in $\mathbf{K}[x_1, \ldots, x_n]^s$, and let $\boldsymbol{F} = [f_{i,j}]$ be a polynomial matrix in $\mathbf{K}[x_1, \ldots, x_n]^{p \times q}$, where $\mathbf{K}$ is a field of characteristic zero with algebraic closure $\overline{\mathbf{K}}$. Assuming $p \leq q$, we are interested in describing the set

$$V_p(\boldsymbol{F}, \boldsymbol{g}) = \{\boldsymbol{x} \in \overline{\mathbf{K}}^n \mid \operatorname{rank}(\boldsymbol{F}(\boldsymbol{x})) < p \text{ and } g_1(\boldsymbol{x}) = \cdots = g_s(\boldsymbol{x}) = 0\}. \quad (1)$$

[*]David R. Cheriton School of Computer Science, University of Waterloo, Waterloo ON, Canada N2L 3G1, emails:{glabahn, eschost, txvu}@uwaterloo.ca

[†]Sorbonne Université, CNRS, Laboratoire d'Informatique de Paris 6 (LIP6, UMR7606), Équipe POLSYS, 4 place Jussieu, F-75252, Paris Cedex 05, France, email:Mohab.Safey@lip6.fr

If for any positive integer r we let $M_r(\boldsymbol{F})$ be the set of all r-minors of $\boldsymbol{F}$ then our set of points is given by

$$V(\langle M_p(\boldsymbol{F})\rangle + \langle g_1, \ldots, g_s\rangle).$$

As an example, when $\boldsymbol{F}$ denotes the Jacobian of $(g_1, \ldots, g_s, \phi)$ with respect to the variables $x_1, \ldots, x_n$, for some $\phi \in \mathbf{K}[x_1, \ldots, x_n]$, then $V_{s+1}(\boldsymbol{F}, \boldsymbol{g})$ is the set of critical points of ϕ over the algebraic set $V(\boldsymbol{g})$, assuming $\boldsymbol{g}$ is a reduced regular sequence and $V(\boldsymbol{g})$ is smooth. The problem of computing such points appear in many areas such as polynomial optimization and real algebraic geometry. Note that in this example we have $n = q - p + s + 1$ (since $\boldsymbol{F}$ has dimensions $p = s + 1$ and $q = n$); we will assume that this holds throughout this paper.

We wish to describe the *isolated* zeros of our algebraic set $V_p(\boldsymbol{F}, \boldsymbol{g})$ when all entries of $\boldsymbol{F}$ and $\boldsymbol{g}$ are *sparse polynomials*. We also want to take advantage of the special determinantal structure of our algebraic set to obtain complexity results which are polynomial in the *generic* number of solutions in $\overline{\mathbf{K}}^n$ of such systems (this is the number of solutions obtained when the coefficients of terms appearing in the entries of $\boldsymbol{F}, \boldsymbol{g}$ are algebraically independent indeterminates) and some combinatorial data attached to the monomial structure of the entries.

In order to achieve this, we make use of the technique of *symbolic homotopy continuation* and show how it can be used to obtain a solver with such a good complexity. Homotopy continuation has become a foundational tool for numerical algorithms while the use of symbolic homotopy continuation algorithms is more recent. Such algorithms first appeared in [7, 19] without any structure on the system. Later symbolic homotopies were used in square sparse systems [25, 20, 21, 22] and multi-homogeneous systems [30, 18, 17].

Homotopy continuation involves defining a deformation between our system defining $V_p(\boldsymbol{F}, \boldsymbol{g})$ and a second system defining $V_p(\boldsymbol{M}, \boldsymbol{r})$ which is similar but whose solutions are easy to describe. Formally, we let t be a new variable and construct a matrix

$$\boldsymbol{V} = (1 - t) \cdot \boldsymbol{M} + t \cdot \boldsymbol{F} \in \mathbf{K}[t, x_1, \ldots, x_n]^{p \times q} \tag{2}$$

which connects a *start matrix* $\boldsymbol{M} \in \mathbf{K}[x_1, \ldots, x_n]^{p \times q}$ to our target matrix $\boldsymbol{F}$, together with polynomials $\boldsymbol{u} = (u_1, \ldots, u_s)$ of the form

$$\boldsymbol{u} = (1 - t) \cdot \boldsymbol{r} + t \cdot \boldsymbol{g} \in \mathbf{K}[t, x_1, \ldots, x_n]^s, \tag{3}$$

that connects a starting polynomial system $\boldsymbol{r}$ to our target system $\boldsymbol{g}$. Such a homotopy allows us to define a *homotopy curve*, steering the solutions of the start system to the isolated solutions to our input system (we do not assume that our input system has finitely many solutions).

We will use a data-structure known as *zero-dimensional parametrization* to represent finite algebraic sets. If V is such a set, defined by polynomials over $\mathbf{K}$, a zero-dimensional parametrization $\mathscr{R} = ((\mathfrak{w}, v_1, \ldots, v_n), \Lambda)$ of V consists of

(i) a square-free polynomial $\mathfrak{w}$ in $\mathbf{K}[y]$, where y is a new indeterminate,

(ii) polynomials $(v_1, \ldots, v_n)$ in $\mathbf{K}[y]$ with each $\deg(v_i) < \deg(\mathfrak{w})$ and satisfying

$$V = \{(v_1(\tau), \ldots, v_n(\tau)) \in \overline{\mathbf{K}}^n \mid \mathfrak{w}(\tau) = 0\},$$

(iii) a linear form $\Lambda = \lambda_1 x_1 + \cdots + \lambda_n x_n$ with coefficients in $\mathbf{K}$, such that $\lambda_1 v_1 + \cdots + \lambda_n v_n = y$ (so the roots of $\mathfrak{w}$ are the values taken by Λ on V).

When this holds, we write $V = Z(\mathscr{R})$. This representation was introduced in early work of Kronecker and Macaulay [26, 27] and has been widely used as a data structure in computer algebra, see for instance [13, 1, 14, 15, 28, 16].

Then, given a zero-dimensional parametrization $\mathscr{R}_0$ of $V_p(\boldsymbol{M}, \boldsymbol{r})$, we will apply the algorithm in [17] to the system $(M_p(\boldsymbol{V}), \boldsymbol{u})$ to lift $\mathscr{R}_0$ to a zero-dimensional parametrization $\mathscr{R}_1$ of the isolated zeros of $V_p(\boldsymbol{F}, \boldsymbol{g})$. At a high level the strategy for using homotopy methods to determine isolated zeros is relatively simple to describe, but also difficult to realize. The start system should have at least the same number of solutions as the target system and should be 'easy' to solve. Also, we want a *sparse* homotopy algorithm, that is, we also wish to have a complexity which depends on the support of the polynomials appearing in our target system.

The main contribution in this paper is to provide the needed ingredients for a sparse homotopy algorithm for our determinantal systems which makes use of the *column support* of $\boldsymbol{F}$. We determine a family of possible start systems, and we show that a generic member of this family allows us to carry out the procedure successfully; we also show how to compute the solutions of this start system. Our runtime is polynomial in the degree of the start system and the degree of the homotopy curve, both depending on certain mixed volumes related to the polynomials $\boldsymbol{g}$ and the columns of $\boldsymbol{F}$, see Theorem 5.1. As far as we are aware, this is the first homotopy algorithm which simultaneously exploits both determinantal structure and sparsity.

The tools used to create our sparse column support homotopy also allow us to build a column homotopy algorithm for determinantal systems for weighted degree polynomials. These are important when all our input polynomials (including those in the input matrix) are invariant under the action of the group of permutations on n letters. In that case, one can perform an algebraic change of coordinates to express all entries with respect to elementary symmetric functions which are naturally weighted (the k-th elementary symmetric function then has weighted degree k). We show that one obtains a speed-up which is polynomial in the product of the weights, see Theorem 5.3.

This is not the first time that determinantal structures have been exploited to speed-up polynomial system solvers. Previous work includes, for example, [17], which is also based on homotopy techniques: we borrow some results and techniques from that reference, but our discussion of the "sparse" aspects is new. Note also that one can encode rank deficiencies in a polynomial matrix using extra variables (sometimes called Lagrange multipliers in the context of polynomial optimization) to encode that the kernel of the considered matrix is non-trivial. This would lead to Lagrange systems with a sparse structure, which could be solved using homotopy techniques from [25, 20, 21, 22]. However, this technique does not

work when isolated solutions to our determinantal system lead to rank deficiencies higher than one: such isolated points of our determinantal system do not correspond to isolated points of the Lagrange system. Still, we will see that such systems play an important role to prove intermediate results needed to achieve our results.

The use of geometric resolution algorithms is investigated in the series of works [2, 3, 4, 31] (and references therein). In this latter setting, relating the complexity parameters (which are mainly geometric degrees of some algebraic sets defined by the input) with the sparsity of these inputs is still a non-trivial problem. Determinantal systems in the context of Gröbner bases are also considered in [11, 12, 32]. Again, this series of works do not take into account the sparsity of the entries.

The structure of the paper is as follows. Section 2 gives some of the preliminary background on sparse polynomials; it is followed by Section 3 which introduces the template of a homotopy algorithm and states properties that will guarantee it succeeds; at this stage, we do not specify how to choose the start system. In Section 4, we introduce a family of start systems and prove that a generic member of this family satisfies the properties needed for our symbolic homotopy algorithm. The cost of our algorithm is analyzed in Section 5, first in the general case of sparse polynomials, then in the important case of weighted domains. An example illustrating the steps of our homotopy algorithm is given in Section 6. The paper ends with a conclusion and topics for future research.

2 Preliminaries

Sparse polynomials. Consider a set $\boldsymbol{x} = (x_1, \ldots, x_n)$ of indeterminates. Polynomials in $\boldsymbol{x}$ are represented in the form of finite sums $f = \sum_{\boldsymbol{\alpha}=(\alpha_1,\ldots,\alpha_n)\in\mathcal{A}} c_{\boldsymbol{\alpha}} x_1^{\alpha_1}\cdots x_n^{\alpha_n}$, with $\mathcal{A}$ being a finite subset of $\mathbb{N}^n$, the set $\{\boldsymbol{\alpha}\in\mathbb{N}^n : c_{\boldsymbol{\alpha}} \neq 0\} \subset \mathcal{A}$ being the *support* $\mathrm{supp}(f)$ of f. The *Newton polytope* of f, denoted by $\mathrm{conv}(f)$, is the convex hull of the support of f in $\mathbb{R}^n$.

We will often work in the following setup. Consider ℓ finite sets $\mathcal{A}_1, \ldots, \mathcal{A}_\ell$ in $\mathbb{N}^n$, with k_i denoting the cardinality of $\mathcal{A}_i$ for all i. For each i, we let $\mathcal{M}_i = (m_{i,1}, \ldots, m_{i,k_i})$ be the corresponding set of monomials in $x_1, \ldots, x_n$. This allows us to define the "generic polynomials" $\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell$ supported on $\mathcal{A}_1, \ldots, \mathcal{A}_\ell$ by

$$\mathfrak{f}_i = \sum_{j=1}^{k_i} \mathfrak{c}_{i,j} m_{i,j} \in \mathbf{K}[\mathfrak{C}][x_1, \ldots, x_n],$$

where $\mathfrak{C} = (\mathfrak{c}_{i,j})_{1\leq i\leq \ell, 1\leq j\leq k_i}$ are new indeterminates. The total number of indeterminates $\mathfrak{C}$ is $N = \sum_{i=1}^{\ell} k_i$.

Identifying $\overline{\mathbf{K}}^N$ with $\overline{\mathbf{K}}^{k_1} \times \cdots \times \overline{\mathbf{K}}^{k_\ell}$, we can view any element $\rho \in \overline{\mathbf{K}}^N$ as a vector of coefficients, first for $\mathfrak{f}_1$, then for $\mathfrak{f}_2$, etc. Then, for such a ρ, we will denote by Θ_ρ the mapping

$$\begin{array}{rcl} \mathbf{K}[\mathfrak{C}][x_1, \ldots, x_n] & \to & \overline{\mathbf{K}}[x_1, \ldots, x_n] \\ \displaystyle\sum_{\boldsymbol{\alpha}\in\mathbb{N}^n} \mathfrak{c}_{i,j} x_1^{\alpha_1}\cdots x_n^{\alpha_n} & \mapsto & \displaystyle\sum_{\boldsymbol{\alpha}\in\mathbb{N}^n} \rho_{i,j} x_1^{\alpha_1}\cdots x_n^{\alpha_n}. \end{array}$$

The notation carries over to vectors or matrices of polynomials. In this paragraph, we discuss some properties of the zeros of systems $\Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)$.

For the first proposition, ℓ is arbitrary, but we impose a restriction on the sets $\mathcal{A}_i$.

Proposition 2.1. *Suppose that for $i = 1, \ldots, \ell$, $\mathcal{A}_i$ contains the origin $\mathbf{0} \in \mathbb{N}^n$. Then there exists a non-empty Zariski open set $\mathscr{O} \subset \overline{\mathbf{K}}^N$ such that for $\rho \in \mathscr{O}$, we have the following:*

(i) if $\ell \leq n$, $\Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)$ generates a radical ideal, whose zero-set in $\overline{\mathbf{K}}^n$ is either empty or smooth and $(n-\ell)$-equidimensional;

(ii) if $\ell > n$, the zero-set of $\Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)$ in $\overline{\mathbf{K}}^n$ is empty.

Proof. Without loss of generality, assume that $m_{i,k_i} = 1$ holds since we assume that $\mathcal{A}_i$ contains the origin $\mathbf{0} \in \mathbb{N}^n$ for all $1 \leq i \leq \ell$. Consider the mapping

$$\Phi : (\boldsymbol{x}, \rho) \in \overline{\mathbf{K}}^n \times \overline{\mathbf{K}}^N \mapsto \Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)(\boldsymbol{x}).$$

We first claim that $\mathbf{0}$ is a regular value of Φ, that is, the Jacobian matrix of this sequence of polynomials has full rank at all points $(\boldsymbol{x}, \rho)$ of its zero-set. Indeed, since $m_{i,k_i} = 1$, the columns corresponding to partial derivatives with respect to $\mathfrak{C}$ contain an $\ell \times \ell$ identity matrix.

As a result, by Thom's weak transversality theorem (see the algebraic version in e.g. [29]), there exists a non-empty Zariski open set $\mathscr{O} \subset \overline{\mathbf{K}}^N$ such that for ρ in $\mathscr{O}$, $\mathbf{0}$ is a regular value of the induced mapping

$$\Phi_\rho : \boldsymbol{x} \in \overline{\mathbf{K}}^n \mapsto \Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)(\boldsymbol{x}).$$

In other words, the Jacobian matrix of $\Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)$ has rank ℓ at any zero $\boldsymbol{x} \in \overline{\mathbf{K}}^n$ of $\Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell)$. For $\ell \leq n$, by the Jacobian criterion [9, Theorem 16.19], the ideal $\langle \Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_\ell) \rangle$ is therefore radical, and its zero-set is either empty or smooth and $(n-\ell)$-equidimensional. For $\ell > n$, this means that this set is empty (since the matrix above has n columns, it cannot have rank ℓ). □

For the next properties, we take $\ell = n$. In what follows, $\mathcal{C}_1, \ldots, \mathcal{C}_n$ are the convex hulls of $\mathcal{A}_1, \ldots, \mathcal{A}_n$, respectively, with the Euclidean volume of $\mathcal{C}_i$ in $\mathbb{R}^n$ being denoted by $\mathrm{vol}_{\mathbb{R}^n}(\mathcal{C}_i)$. Consider the function

$$\varphi \, : \, (\lambda_1, \ldots, \lambda_n) \mapsto \mathrm{vol}_{\mathbb{R}^n}(\lambda_1 \mathcal{C}_1 + \cdots + \lambda_n \mathcal{C}_n),$$

where

$$\lambda_1 \mathcal{C}_1 + \cdots + \lambda_n \mathcal{C}_n = \{\boldsymbol{x} \in \mathbb{R}^n \, : \, \boldsymbol{x} = \sum_{i=1}^{n} \lambda_i \, x_i \, \text{with} \, x_i \in \mathcal{C}_i\}$$

is the Minkowski sum of polytopes. The function φ is a homogeneous polynomial function of degree n in λ_i (see e.g. [8, Proposition 4.9]). The *mixed volume* $\mathsf{MV}(\mathcal{C}_1, \ldots, \mathcal{C}_n)$ is then defined as the coefficient of the monomial $\lambda_1 \cdots \lambda_n$ in φ. Then, the Bernstein-Khovanskii-Kushnirenko (BKK) theorem [6] gives a bound on the number of isolated zeros of $\Theta_\rho(\mathfrak{f}_1, \ldots, \mathfrak{f}_n)$ in the torus in terms of this quantity (note that here, we do not assume that the supports $\mathcal{A}_i$ contain the origin).

Proposition 2.2. *For any ρ in $\overline{\mathbf{K}}^N$, the number of isolated zeros of $\Theta_\rho(\mathfrak{f}_1,\dots,\mathfrak{f}_n)$ in $(\overline{\mathbf{K}}-\{0\})^n$ is at most $\mathsf{MV}(\mathcal{C}_1,\dots,\mathcal{C}_n)$. Furthermore, there exists a non-empty Zariski-open set $\mathscr{O}_{\mathrm{BKK}}\subset\overline{\mathbf{K}}^N$ such that the bound is tight for ρ in $\mathscr{O}_{\mathrm{BKK}}$.*

A first application of Proposition 2.1 is the following refinement of this statement (which of course requires the assumptions of Proposition 2.1 to hold). Again, we take $\ell = n$.

Proposition 2.3. *Suppose that for $i=1,\dots,n$, $\mathcal{A}_i$ contains the origin $\mathbf{0}\in\mathbb{N}^n$. Then, there exists a non-empty Zariski-open set $\mathscr{O}'_{\mathrm{BKK}}\subset\overline{\mathbf{K}}^N$ such that for ρ in $\mathscr{O}'_{\mathrm{BKK}}$, $\Theta_\rho(\mathfrak{f}_1,\dots,\mathfrak{f}_n)$ has $\mathsf{MV}(\mathcal{C}_1,\dots,\mathcal{C}_n)$ solutions in $\overline{\mathbf{K}}^n$.*

Proof. Consider a subset $\boldsymbol{i}=\{i_1,\dots,i_m\}$ of $\{1,\dots,n\}$, with $1\le m\le n$, and let $(\mathfrak{f}_{\boldsymbol{i},1},\dots,\mathfrak{f}_{\boldsymbol{i},n})$ be the polynomials $(\mathfrak{f}_1,\dots,\mathfrak{f}_n)$ where the coordinates $x_{i_1},\dots,x_{i_m}$ have been set to zero; they depend on a certain number $N_{\boldsymbol{i}}\le N$ of indeterminate coefficients $\rho_{\boldsymbol{i}}$.

This is thus a system of n equations in $n-m<n$ unknowns, and the support of each of these equations still contains the origin. Proposition 2.1 then implies that there exists a non-empty Zariski-open $\omega_{\boldsymbol{i}}\subset\overline{\mathbf{K}}^{N_{\boldsymbol{i}}}$ such that for $\rho_{\boldsymbol{i}}$ in $\omega_{\boldsymbol{i}}$, $\Theta_{\rho_{\boldsymbol{i}}}(\mathfrak{f}_{\boldsymbol{i},1},\dots,\mathfrak{f}_{\boldsymbol{i},n})$ has no solution in $\overline{\mathbf{K}}^{n-m}$. Let then $\Omega_{\boldsymbol{i}}$ be the preimage of $\omega_{\boldsymbol{i}}$ in $\overline{\mathbf{K}}^N$ (under the canonical projection), and define Ω as the intersection of all $\Omega_{\boldsymbol{i}}$, for $\boldsymbol{i}=\{i_1,\dots,i_m\}$ a subset of $\{1,\dots,n\}$. For ρ in Ω, all coordinates of all solutions of $\Theta_\rho(\mathfrak{f}_1,\dots,\mathfrak{f}_n)$ are non-zero. To conclude, we define $\mathscr{O}'_{\mathrm{BKK}}$ as the intersection of $\mathscr{O}_{\mathrm{BKK}}$ (from Proposition 2.2) and Ω. □

Initial forms. Let $\boldsymbol{e}=(e_1,\dots,e_n)$ be non-zero in $\mathbb{Q}^n$ and consider a polynomial

$$p=\sum_{\boldsymbol{\alpha}=(\alpha_1,\dots,\alpha_n)\in S} c_{\boldsymbol{\alpha}}\,x_1^{\alpha_1}\cdots x_n^{\alpha_n}$$

with support $S=\mathrm{supp}(p)$. The field of definition may be our field $\mathbf{K}$, or, as will also happen below, a rational function field. Define

$$m(\boldsymbol{e},p)=\min(\langle\boldsymbol{e},\boldsymbol{\alpha}\rangle\,|\,\boldsymbol{\alpha}\in S)\quad\text{and}\quad S_{\boldsymbol{e},p}=\{\boldsymbol{\alpha}\in S\,|\,\langle\boldsymbol{e},\boldsymbol{\alpha}\rangle=m(\boldsymbol{e},p)\},$$

where $\langle\ ,\ \rangle$ is the usual dot-product in $\mathbb{R}^n$. Thus, $S_{\boldsymbol{e},p}$ is the intersection of S with its "support hyperplane" in the direction $\boldsymbol{e}$. The *initial form* of p with respect to $\boldsymbol{e}$ is defined as

$$\mathrm{init}_{\boldsymbol{e}}(p)=\sum_{\boldsymbol{\alpha}=(\alpha_1,\dots,\alpha_n)\in S_{\boldsymbol{e},p}} c_{\boldsymbol{\alpha}}\,x_1^{\alpha_1}\cdots x_n^{\alpha_n}.$$

In other words, $\mathrm{init}_{\boldsymbol{e}}(p)$ is the sum over all terms $c_{\boldsymbol{\alpha}}\,x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ for which the dot-product $\langle\boldsymbol{e},\boldsymbol{\alpha}\rangle$ is minimized. For a vector $\boldsymbol{p}=(p_1,\dots,p_n)$ of polynomials, we let

$$\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{p})=(\mathrm{init}_{\boldsymbol{e}}(p_1),\dots,\mathrm{init}_{\boldsymbol{e}}(p_n)).$$

Even though there is an infinite number of possible directions $\boldsymbol{e}$, the number of polynomial systems $\{\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{p})\,|\,\boldsymbol{e}\text{ non-zero in }\mathbb{Q}^n\}$ obtained in this manner is finite, since the support of each p_i has finitely many support hyperplanes.

3 Determinantal homotopy

In this section, we review a few useful properties of homotopy continuation methods for determinantal ideals. As input, we are given $\boldsymbol{g} = (g_1, \ldots, g_s)$ and $\boldsymbol{F}$ in $\mathbf{K}[x_1, \ldots, x_n]^{p\times q}$, and we assume $n = q - p + s + 1$. Let t be a new variable and construct a matrix

$$\mathbf{V} = (1-t)\cdot \boldsymbol{M} + t \cdot \boldsymbol{F} \in \mathbf{K}[t, x_1, \ldots, x_n]^{p\times q}$$

which connects a *start matrix* $\boldsymbol{M} \in \mathbf{K}[x_1, \ldots, x_n]^{p\times q}$ to our target matrix $\boldsymbol{F}$, together with polynomials $\boldsymbol{u} = (u_1, \ldots, u_s)$ of the form

$$\boldsymbol{u} = (1-t)\cdot \boldsymbol{r} + t \cdot \boldsymbol{g} \in \mathbf{K}[t, x_1, \ldots, x_n]^{s},$$

which connect a starting polynomial system $\boldsymbol{r}$ to our target system $\boldsymbol{g}$. Then, $\mathbf{V}$ and $\boldsymbol{u}$ define a deformation which allows us to connect the solutions of the start system $V_p(\boldsymbol{M}, \boldsymbol{r})$ to the isolated solutions of our system $V_p(\boldsymbol{F}, \boldsymbol{g})$.

Algorithms for symbolic homotopy continuation require several ingredients. We need a start system that can be solved efficiently and has the "right" number of solutions, a description of the solutions of this start system, and a bound ϱ that determines the number of steps we perform.

Proposition 3.1 below makes these requirements more precise; it is a minor modification of [17, Propositions 13 and 24]. To state it, it will be convenient to describe our homotopy process using only vectors of polynomials. To this end, we fix an ordering $\succ$ on the p-minors of $p \times q$ matrices and set $m = s + \binom{q}{p}$. Consider the system of equations

$$\boldsymbol{B} = (u_1, \ldots, u_s, b_{s+1}, \ldots, b_m) \in \mathbf{K}[t, x_1, \ldots, x_n]^{m},$$

where $u_1, \ldots, u_s$ are as defined above, and where the polynomials $(b_{s+1}, \ldots, b_m)$ are the p-minors of $\mathbf{V}$, following the ordering $\succ$. For $\tau \in \overline{\mathbf{K}}$, we write $\boldsymbol{B}_{t=\tau}$ for the polynomials in $\overline{\mathbf{K}}[x_1, \ldots, x_n]$ obtained by the evaluation $t \mapsto \tau$ in $\boldsymbol{B}$. In particular, $\boldsymbol{B}_{t=0}$ is the set of equations in our start system, and $\boldsymbol{B}_{t=1}$ are the equations we want to solve.

Consider the ideal J generated by $\boldsymbol{B}$ in $\mathbf{K}(t)[x_1, \ldots, x_n]$. The roots of J have coordinates in an algebraic closure of $\mathbf{K}(t)$, so we can view them in $\overline{\mathbf{K}}\langle\langle t\rangle\rangle^n$, where $\overline{\mathbf{K}}\langle\langle t\rangle\rangle$ is the field of Puiseux series with coefficients in $\overline{\mathbf{K}}$. Thus, these solutions are meant to describe the local behaviour of the solutions of $\boldsymbol{B}$ at $t = 0$. A vector $\boldsymbol{\alpha}$ in $\overline{\mathbf{K}}\langle\langle t\rangle\rangle^n$ admits a *valuation* $\nu(\boldsymbol{\alpha})$, defined as the minimum of the valuations (with respect to t) of its coordinates, and we say that $\boldsymbol{\alpha}$ is *bounded* when $\nu(\boldsymbol{\alpha}) \geq 0$. This will be one of the conditions we impose on the solutions of J.

The algorithm is in essence a form of Newton iteration with respect to t. One input needed for the algorithm is an upper bound ϱ on the precision in t at which we need to do the computations. A sufficient upper bound for ϱ is the degree of the *homotopy curve*, which is the union of all dimension-1 irreducible components of $V(\boldsymbol{B}) \subset \overline{\mathbf{K}}^{n+1}$ whose projections on the t-space are Zariski dense. In effect, this is the number of isolated solutions of the system in $\mathbf{K}[t, x_1, \ldots, x_n]$ obtained by taking all equations in $\boldsymbol{B}$, together with a linear form in $t, x_1, \ldots, x_n$ with random coefficients.

Finally, as in [17], the following proposition assumes that we are given a *straight-line program* Γ that computes the polynomials $\boldsymbol{B}$, that is, is a sequence of operations $+, -, \times$ that takes as input $t, x_1, \ldots, x_n$ and evaluates $\boldsymbol{B}$. Its *length* is simply the number of operations it performs.

Proposition 3.1. *Suppose that the following conditions hold:*

(*i*) *the ideal generated by* $\boldsymbol{B}_{t=0}$ *is radical and of dimension zero in* $\mathbf{K}[x_1, \ldots, x_n]$*, with* χ *solutions;*

(*ii*) *all points in* $V(\boldsymbol{B}) \subset \overline{\mathbf{K}}\langle\langle t \rangle\rangle^n$ *are bounded.*

Then, the ideal J *generated by* $\boldsymbol{B}$ *in* $\mathbf{K}(t)[x_1, \ldots, x_n]$ *is radical and of dimension zero, with* χ *solutions, and the system* $\boldsymbol{B}_{t=1}$ *admits at most* χ *isolated solutions (counted with multiplicities).*

Furthermore, given a zero-dimensional parametrization of the solutions of $\boldsymbol{B}_{t=0}$*, a straight-line program* Γ *of length* β *that computes* $\boldsymbol{B}$*, and the upper bound* ϱ *as above, there exists a randomized algorithm* Homotopy *which computes a zero-dimensional parametrization of the isolated solutions of* $\boldsymbol{B}_{t=1}$ *using*

$$\tilde{O}(\chi(\varrho + \chi^5)n^4\beta) \tag{4}$$

operations in $\mathbf{K}$*.*

4 Main algorithm

Given $\boldsymbol{g} = (g_1, \ldots, g_s)$ and $\boldsymbol{F} = [f_{i,j}]_{1 \le i \le p,\ 1 \le j \le q}$ as in Section 3, our goal in this section is to specify the homotopy algorithm. We design a suitable start system for the symbolic homotopy algorithm, and we establish that this system satisfies the assumptions of Proposition 3.1. The cost analysis is done in the next section.

In order to build the polynomials $\boldsymbol{r} = (r_1, \ldots, r_s)$ of (3), we take polynomials with the same supports at $\boldsymbol{g} = (g_1, \ldots, g_s)$ and generic coefficients, taking care to add the constant 1 to their monomial supports if it is missing. The main new ingredient is the determination of the start matrix $\boldsymbol{M}$ of (2). In this paper, we focus on what we call the *column support homotopy* where the construction of $\boldsymbol{M}$ is derived from the unions of the supports of the entries of $\boldsymbol{F}$ per columns. This extends a similar construction given in [17] for dense polynomials, but which was instead based on the total degrees of the columns of $\boldsymbol{F}$.

4.1 Column support homotopy

For $1 \le i \le s$, let $\mathcal{A}_i \subset \mathbb{N}^n$ denote the support of g_i, to which we add the origin $\mathbf{0} \in \mathbb{N}^n$. For $1 \le j \le q$, let $\mathcal{B}_j \subset \mathbb{N}^n$ be the *union* of the supports of the polynomials in the j-th column of $\boldsymbol{F}$, to which we add $\mathbf{0}$ as well.

For given i and j we denote by κ_i the cardinality of $\mathcal{A}_i$ and by μ_j the cardinality of $\mathcal{B}_j$, and let $(n_{i,1}, \ldots, n_{i,\kappa_i})$ and $(m_{j,1}, \ldots, m_{j,\mu_j})$ denote the monomials in $x_1, \ldots, x_n$ supported

by $\mathcal{A}_i$ and $\mathcal{B}_j$, respectively. We can then define the "generic" polynomials supported on $\mathcal{A}_1, \ldots, \mathcal{A}_s$ and $\mathcal{B}_1, \ldots, \mathcal{B}_q$:

$$\mathfrak{r}_i = \sum_{k=1}^{\kappa_i} \mathfrak{d}_{i,k} n_{i,k} \quad (1 \le i \le s) \qquad \text{and} \quad \mathfrak{m}_j = \sum_{k=1}^{\mu_j} \mathfrak{e}_{j,k} m_{j,k} \quad (1 \le j \le q),$$

where all $\mathfrak{d}_{i,k}$ and $\mathfrak{e}_{j,k}$ are new indeterminates. Let $\mathfrak{c}_{i,j}$, for $1 \le i \le p$ and $1 \le j \le q$, be pq additional new indeterminates so that $\mathfrak{A} = \{(\mathfrak{d}_{i,k})_{1\le i\le s, 1\le k\le \kappa_i}, (\mathfrak{e}_{j,k})_{1\le j\le q, 1\le k\le \mu_j}, (\mathfrak{c}_{i,j})_{1\le i\le p, 1\le j\le q}\}$, the set of all these new indeterminates, has size

$$N = \sum_{i=1}^{s} \kappa_i + \sum_{i=1}^{q} \mu_i + pq.$$

We then define the matrix

$$\mathfrak{M} = \begin{pmatrix} \mathfrak{c}_{1,1}\,\mathfrak{m}_1 & \mathfrak{c}_{1,2}\,\mathfrak{m}_2 & \ldots & \mathfrak{c}_{1,q}\,\mathfrak{m}_q \\ \vdots & \vdots & & \vdots \\ \mathfrak{c}_{p,1}\,\mathfrak{m}_1 & \mathfrak{c}_{p,2}\,\mathfrak{m}_2 & \ldots & \mathfrak{c}_{p,q}\,\mathfrak{m}_q \end{pmatrix} \in \mathbf{K}[\mathfrak{A}][x_1, \ldots, x_n]^{p\times q}.$$

As before, for ρ in $\overline{\mathbf{K}}^N$, for any polynomial f having coefficients in $\overline{\mathbf{K}}[\mathfrak{A}]$, $\Theta_\rho(f)$ is the polynomial with coefficients in $\overline{\mathbf{K}}$ obtained through evaluation of the indeterminates $\mathfrak{A}$ at ρ; the notation carries over to polynomial matrices.

We will use $\mathfrak{M}$ and $\mathfrak{r} = (\mathfrak{r}_1, \ldots, \mathfrak{r}_s)$ to construct our start system, by assigning random values to all indeterminates in $\mathfrak{A}$. Thus, we let t be a new indeterminate and we denote by $\mathfrak{B}$ the polynomials in $\mathbf{K}[\mathfrak{A}][t, x_1, \ldots, x_n]$ obtained by considering the equations $(1-t)\cdot\mathfrak{r} + t\cdot\boldsymbol{g}$ and the p-minors of $(1-t)\cdot\mathfrak{M} + t\cdot\boldsymbol{F}$. Our goal in this section is to establish the following result.

Proposition 4.1. *There exists a non-empty Zariski open subset Ω of $\overline{\mathbf{K}}^N$ such that for ρ in Ω, $\boldsymbol{B} := \Theta_\rho(\mathfrak{B})$ satisfies the assumptions of Proposition 3.1.*

In other words, we will prove that, for such a choice of ρ, the ideal generated by $\boldsymbol{B}_{t=0}$ in $\overline{\mathbf{K}}[x_1, \ldots, x_n]$ is radical and zero-dimensional (this is done in the next subsection) and that the solutions of $\boldsymbol{B}$ in $\overline{\mathbf{K}}\langle\langle t\rangle\rangle^n$ are bounded. This boundedness properties is proved in Subsection 4.4 using properties of Lagrange type systems which are established in Subsection 4.3.

Note also the following consequence of Proposition 3.1: the number of isolated solutions of the system we want to solve (counting multiplicities) is bounded above by the number of solutions of a generic start system $\Theta_\rho(\mathfrak{B})_{t=0}$.

4.2 Properties of the start system

In this subsection, we prove that for a generic choice of ρ in $\overline{\mathbf{K}}^N$, if we write $\boldsymbol{B} := \Theta_\rho(\mathfrak{B})$ then the ideal generated by $\boldsymbol{B}_{t=0}$ in $\overline{\mathbf{K}}[x_1, \ldots, x_n]$ is radical and zero-dimensional.

Proposition 4.2. *There exists a non-empty Zariski open set $\Omega_1 \subset \overline{\mathbf{K}}^N$ such that for ρ in Ω_1, writing $\boldsymbol{B} := \Theta_\rho(\mathfrak{B})$, the ideal generated by $\boldsymbol{B}_{t=0}$ in $\overline{\mathbf{K}}[x_1, \ldots, x_n]$ is radical of dimension zero.*

Proof. Note first that the equations $\boldsymbol{B}_{t=0}$ that we are considering are the p-minors of $\Theta_\rho(\mathfrak{M})$, together with $\Theta_\rho(\mathfrak{r}_1, \ldots, \mathfrak{r}_s)$. Now, any p-minor of $\mathfrak{M}$ has the form $\mathfrak{C}_{i_1,\ldots,i_p}\mathfrak{m}_{i_1}\cdots\mathfrak{m}_{i_p}$, for some choice of columns $i_1, \ldots, i_p$, where $\mathfrak{C}_{i_1,\ldots,i_p}$ is the determinant

$$\mathfrak{C}_{i_1,\ldots,i_p} = \begin{vmatrix} \mathfrak{c}_{1,i_1} & \mathfrak{c}_{1,i_2} & \cdots & \mathfrak{c}_{1,i_p} \\ \vdots & \vdots & & \vdots \\ \mathfrak{c}_{p,i_1} & \mathfrak{c}_{p,i_2} & \cdots & \mathfrak{c}_{p,i_p} \end{vmatrix} \in \mathbf{K}[\mathfrak{A}].$$

Our first constraint on ρ is thus that $\Theta_\rho(\mathfrak{C}_{i_1,\ldots,i_p}) \in \overline{\mathbf{K}}$ is non-zero for all $\{i_1, \ldots, i_p\}$. In this case, a point $\boldsymbol{\alpha}$ in $\overline{\mathbf{K}}^n$ cancels all the p-minors of $\Theta_\rho(\mathfrak{M})$ if and only if it cancels all products $\Theta_\rho(\mathfrak{m}_{i_1})\cdots\Theta_\rho(\mathfrak{m}_{i_p})$. This is the case if and only if there exists $\boldsymbol{i} = \{i_1, \ldots, i_{q-p+1}\} \subset \{1, \ldots, q\}$ such that $\Theta_\rho(\mathfrak{m}_{i_1}), \ldots, \Theta_\rho(\mathfrak{m}_{i_{q-p+1}})$ all vanish at $\boldsymbol{\alpha}$.

Since we assume $n = q - p + s + 1$, we can rewrite $q - p + 1$ as $n - s$. Then, for a subset $\boldsymbol{i} = \{i_1, \ldots, i_{n-s}\} \subset \{1, \ldots, q\}$, consider the polynomials $\mathfrak{M}_{\boldsymbol{i}} = (\mathfrak{m}_{i_1}, \ldots, \mathfrak{m}_{i_{n-s}})$. By Proposition 2.1(i), there exists a non-empty Zariski open set $\mathscr{O}_{\boldsymbol{i}} \subset \overline{\mathbf{K}}^N$ such that for ρ in $\mathscr{O}_{\boldsymbol{i}}$, the ideal generated by $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \mathfrak{r})$ is radical and admits finitely many solutions. For subsets $\boldsymbol{i}'$ and $\boldsymbol{i}$ of $\{1, \ldots, q\}$ of cardinalities $n - s$ such that $\boldsymbol{i} \neq \boldsymbol{i}'$, the system defined by $\mathfrak{M}_{\boldsymbol{i}\cup\boldsymbol{i}'}$ and $\mathfrak{r}$ contains at least $n + 1$ polynomials in $\mathbf{K}[\mathfrak{A}][x_1, \ldots, x_n]$. By using Proposition 2.1(ii), there exists a non-empty Zariski open set $\mathscr{O}_{\boldsymbol{i}\cup\boldsymbol{i}'} \subset \overline{\mathbf{K}}^N$ such that for ρ in $\mathscr{O}_{\boldsymbol{i}\cup\boldsymbol{i}'}$, the system $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}\cup\boldsymbol{i}'}, \mathfrak{r})$ has no solutions in $\overline{\mathbf{K}}^n$.

Taking the intersection of these $\mathscr{O}_{\boldsymbol{i}}$ and $\mathscr{O}_{\boldsymbol{i}\cup\boldsymbol{i}'}$ (which are finite in number), together with the condition that the determinants $\Theta_\rho(\mathfrak{C}_{i_1,\ldots,i_p})$ do not vanish, defines a non-empty Zariski open $\Omega_1 \subset \overline{\mathbf{K}}^N$. Thus, for ρ in Ω_1, the sets $V(\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \mathfrak{r}))$, for any subset $\boldsymbol{i}$ of $\{1, \ldots, q\}$ of cardinality $n - s$, are finite and pairwise disjoint, and their union is $V(\boldsymbol{B}_{t=0})$. In particular, the latter set is finite.

Take ρ in Ω_1 and $\boldsymbol{\alpha}$ in $V(\boldsymbol{B}_{t=0})$. We now prove that the ideal generated by $\boldsymbol{B}_{t=0}$, that is, by the p-minors of $\Theta_\rho(\mathfrak{M})$ and $\Theta_\rho(\mathfrak{r}_1, \ldots, \mathfrak{r}_s)$, has multiplicity one at $\boldsymbol{\alpha}$. This will imply that $\boldsymbol{B}_{t=0}$ generates a radical ideal. For this, we will use the fact that $\boldsymbol{\alpha}$ is the root of the system $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \mathfrak{r})$, for a unique subset $\boldsymbol{i} = (i_1, \ldots, i_{n-s})$ of $\{1, \ldots, q\}$ of cardinality $n - s$, and that $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \mathfrak{r})$ has multiplicity one at $\boldsymbol{\alpha}$.

Let then $\boldsymbol{j} = (j_1, \ldots, j_{p-1})$ denote the $q-(n-s) = p-1$ columns of $\mathfrak{M}$ not indexed by $\boldsymbol{i}$. For i in $\boldsymbol{i}$, the equation $\Theta_\rho(\mathfrak{C}_{j_1,\ldots,j_{p-1},i}\mathfrak{m}_{j_1}\cdots\mathfrak{m}_{j_{p-1}}\mathfrak{m}_i)$ appears among the generators of $\boldsymbol{B}_{t=0}$. In the local ring at $\boldsymbol{\alpha}$, we can divide by the non-zero quantity $\Theta_\rho(\mathfrak{C}_{j_1,\ldots,j_{p-1},i}\mathfrak{m}_{j_1}\cdots\mathfrak{m}_{j_{p-1}})(\boldsymbol{\alpha})$. This implies that locally at $\boldsymbol{\alpha}$, $\boldsymbol{B}_{t=0}$ is generated by the polynomials $\Theta_\rho(\mathfrak{m}_{i_1}), \ldots, \Theta_\rho(\mathfrak{m}_{i_{n-s}})$ and $\Theta_\rho(\mathfrak{r})$. The conclusion follows. □

4.3 The associated Lagrange system

To establish the boundedness property, since $\mathfrak{B}$ is overdetermined, it will be convenient to introduce new variables $\boldsymbol{\ell} = (\ell_1, \ldots, \ell_p)$ and to work with the *Lagrange system*, which consits

of $s+q+1$ equations defined by

$$(1-t)\mathfrak{r}+t\boldsymbol{g} \;=\; [\ell_1 \;\cdots\; \ell_p]((1-t)\mathfrak{M}+t\boldsymbol{F}) \;=\; \mathfrak{t}_1\ell_1+\cdots+\mathfrak{t}_p\ell_p-1=0, \tag{5}$$

where $\mathfrak{t}=(\mathfrak{t}_1,\dots,\mathfrak{t}_p)$ are new indeterminate coefficients. Recall that $n=q-p+s+1$, so $s+q+1=n+p$; we will write these equations as $\mathfrak{H}=(\mathfrak{H}_1,\dots,\mathfrak{H}_{n+p})$.

There are now $N+p$ parameters in these equations, with elements of the parameter space $\overline{\mathbf{K}}^{N+p}$ written as $\sigma=(\rho,\tau)$, with ρ in $\overline{\mathbf{K}}^N$ and τ in $\overline{\mathbf{K}}^p$. For σ in $\overline{\mathbf{K}}^{N+p}$ and f a polynomial with coefficients in $\mathbf{K}[\mathfrak{A},\mathfrak{t}]$, we write as usual $\Theta_\sigma(f)$ for the polynomial whose coefficients are obtained from those of f, with $\mathfrak{A}$ evaluated at ρ and $\mathfrak{t}$ evaluated at τ. As before, the notation carries over to vectors or matrices of polynomials.

For $1\le i\le n+p$, $\mathfrak{H}_i$ can be decomposed as $\mathfrak{H}_i=\eta_i+t\mathfrak{h}_i$ with both η_i and $\mathfrak{h}_i$ in $\mathbf{K}[\mathfrak{A},\mathfrak{t}][\boldsymbol{x},\boldsymbol{\ell}]$. In particular, note that the polynomials $\boldsymbol{\eta}=(\eta_1,\dots,\eta_{n+p})$ form the Lagrange system

$$\mathfrak{r}_1=\cdots=\mathfrak{r}_s \;=\; [\ell_1 \;\cdots\; \ell_p]\mathfrak{M} \;=\; \mathfrak{t}_1\ell_1+\cdots+\mathfrak{t}_p\ell_p+1=0$$

in $\mathbf{K}[\mathfrak{A},\mathfrak{t}][\boldsymbol{x},\boldsymbol{\ell}]$, so for $i=1,\dots,q$, the polynomial η_{s+i} is $(\mathfrak{c}_{1,i}\ell_1+\cdots+\mathfrak{c}_{p,i}\ell_p)\mathfrak{m}_i$.

In what follows, we discuss properties of the polynomials $\Theta_\sigma(\boldsymbol{\eta})$ and their initial forms $\mathrm{init}_{\boldsymbol{e}}(\Theta_\sigma(\boldsymbol{\eta}))$, for $\boldsymbol{e}$ in $\mathbb{Q}^{n+p}$. Our first claim is the following; the proof is straightforward.

Lemma 4.3. *For σ in $(\overline{\mathbf{K}}-\{0\})^{N+p}$ and $\boldsymbol{e}$ in $\mathbb{Q}^{n+p}$, $\mathrm{init}_{\boldsymbol{e}}(\Theta_\sigma(\boldsymbol{\eta}))=\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta}))$.*

The second proposition uses the specific shape of the equations $\mathfrak{H}$ to derive information about their roots.

Proposition 4.4. *Let $\boldsymbol{\phi}=(t^{e_1}c_1+\dots,\dots,t^{e_{n+p}}c_{n+p}+\dots)$ be in $\overline{\mathbf{K}}\langle\langle t\rangle\rangle^{n+p}$ with, for all $i=1,\dots,n+p$, e_i in $\mathbb{Q}$ and c_i in $\overline{\mathbf{K}}-\{0\}$.*

Then for σ in $(\overline{\mathbf{K}}-\{0\})^{N+p}$, we have the following: if $\boldsymbol{\phi}$ cancels $\Theta_\sigma(\mathfrak{H})$, then $\boldsymbol{c}=(c_1,\dots,c_{n+p})$ cancels $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta}))$, with $\boldsymbol{e}=(e_1,\dots,e_{n+p})$.

Proof. For $i=1,\dots,s$, we have $\mathfrak{H}_i=\mathfrak{r}_i+t(g_i-\mathfrak{r}_i)$, so $\eta_i=\mathfrak{r}_i$ and $\mathfrak{h}_i=g_i-\mathfrak{r}_i$. Thus by construction, the monomial support of $\mathfrak{h}_i$ (with respect to $x_1,\dots,x_n,\ell_1,\dots,\ell_p$) is the same as that of $\mathfrak{r}_i$. This means that for any term $kx_1^{u_1}\cdots\ell_p^{u_{n+p}}$ in $\mathfrak{h}_i$, with k in $\mathbf{K}[\mathfrak{A}]$, there exists a term $k'x_1^{u_1}\cdots\ell_p^{u_{n+p}}$ in η_i, where k' is one of the indeterminates $\mathfrak{d}_{i,j}$.

Take σ as in the statement of the proposition, and write $a=\Theta_\sigma(\mathfrak{H}_i)$, $b=\Theta_\sigma(\eta_i)$ and $c=\Theta_\sigma(\mathfrak{h}_i)$, so that $b(\boldsymbol{\phi})+tc(\boldsymbol{\phi})=a(\boldsymbol{\phi})=0$. Using our assumption on σ, we deduce that for any term of the form $kt\phi_1^{u_1}\cdots\phi_{n+p}^{u_{n+p}}$ appearing in $tc(\boldsymbol{\phi})$, there is a term $k'\phi_1^{u_1}\cdots\phi_{n+p}^{u_{n+p}}$ appearing in $b(\boldsymbol{\phi})$, with non-zero coefficient k'. In particular, all terms of smallest valuation in $a(\boldsymbol{\phi})$ appear in $b(\boldsymbol{\phi})$, and must add up to zero. Taking their first coefficient, this implies that $\boldsymbol{c}$ cancels $\mathrm{init}_{\boldsymbol{e}}(b)$.

The proof for the polynomials $\mathfrak{H}_{s+1},\dots,\mathfrak{H}_{s+q}$, $\eta_{s+1},\dots,\eta_{s+q}$ and $\mathfrak{h}_{s+1},\dots,\mathfrak{h}_{s+q}$ is similar, taking into account that $\eta_{s+i}=(\mathfrak{c}_{1,i}\ell_1+\cdots+\mathfrak{c}_{p,i}\ell_p)\mathfrak{m}_i$. Indeed, again, for $i=1\dots,q$, the monomial support of $\mathfrak{h}_{s+i}$ is the same as that of η_{s+i}; if we define a,b,c as above, our assumption that no entry of σ vanishes implies as before that all terms of smallest valuation in $a(\boldsymbol{\phi})$ appear in $b(\boldsymbol{\phi})$, and add up to zero. Finally, for $\mathfrak{H}_{s+q+1}=\mathfrak{H}_{n+p}$, we have that $\mathfrak{h}_{n+p}=0$, and the claim follows as above. ∎

Our last property requires a longer proof. For generic choices of σ, it constrains the possible roots of the system $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta}))$ introduced in the previous proposition.

Proposition 4.5. *There exists a non-empty Zariski open set $\Omega_2 \subset \overline{\mathbf{K}}^{N+p}$ such that for $\sigma \in \Omega_2$, the following holds for any $\boldsymbol{e}$ in $\mathbb{Q}^{n+p}$: for $j = 1, \ldots, n+p$, the system obtained by setting the j-th variable to 1 in $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta}))$ has no solution in $(\overline{\mathbf{K}} - \{0\})^{n+p-1}$.*

Proof. Even though there is an infinite number of vectors $\boldsymbol{e}$ to take into account, there is only a finite number of possible systems $\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta})$. Thus, in what follows, we assume $\boldsymbol{e}$ is fixed and prove the existence of a suitable Zariski open set, knowing that we will eventually take the intersection of the open sets corresponding to the finite number of systems $\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta})$. Similarly, without loss of generality, we assume $j = 1$, so that we are setting x_1 to 1.

Thus, we call $\bar{\boldsymbol{\eta}} = (\bar{\eta}_1, \ldots, \bar{\eta}_{n+p})$ the polynomials in $\mathbf{K}[\mathfrak{A}, \mathfrak{t}][x_2, \ldots, x_n, \ell_1, \ldots, \ell_p]$ obtained by setting x_1 to 1 in $\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta})$. We will prove that for a generic σ in $\overline{\mathbf{K}}^{N+p}$, the system $\Theta_\sigma(\bar{\boldsymbol{\eta}}) \subset \overline{\mathbf{K}}[x_2, \ldots, x_n, \ell_1, \ldots, \ell_p]$ has no solution in $(\overline{\mathbf{K}} - \{0\})^{n+p-1}$ (this system is indeed the one mentioned in the statement of the proposition, since Θ_σ and variable evaluation commute).

For $i = 1, \ldots, n+p$, denote by $\mathfrak{S}_i$ the subset of $(\mathfrak{A}, \mathfrak{t})$ consisting of those indeterminates that appear in the coefficients of η_i (so it also contains those that appear in the coefficients of $\bar{\eta}_i$). With this convention, the sets $\mathfrak{S}_i$ are pairwise disjoint, and $(\mathfrak{S}_1, \ldots, \mathfrak{S}_{n+p})$ is the set of all indeterminate coefficients $(\mathfrak{A}, \mathfrak{t})$ that appear in $\boldsymbol{\eta}$. For all i, we let t_i be the cardinality of $\mathfrak{S}_i$, and we will write the elements of $\overline{\mathbf{K}}^{t_i}$ as ρ_i, so that a vector $\sigma \in \overline{\mathbf{K}}^{N+p}$ can be decomposed as $\sigma = (\rho_1, \ldots, \rho_{n+p})$. Given $(\rho_1, \ldots, \rho_i)$ in $\overline{\mathbf{K}}^{t_1+\cdots+t_i}$, $\Theta_{(\rho_1,\ldots,\rho_i)}$ denotes as usual the mapping that evaluates the $t_1 + \cdots + t_i$ indeterminates $\mathfrak{S}_1, \ldots, \mathfrak{S}_i$ at $(\rho_1, \ldots, \rho_i)$.

The key property we will use below is the following: *for any $\boldsymbol{\alpha}$ in $(\overline{\mathbf{K}} - \{0\})^{n+p-1}$, the polynomial $\gamma \in \overline{\mathbf{K}}[\mathfrak{S}_i]$ obtained by evaluating $x_2, \ldots, x_n, \ell_1, \ldots, \ell_p$ at the coordinates of $\boldsymbol{\alpha}$ in $\bar{\eta}_i$ is non-zero.* For $i = 1, \ldots, s$ and $i = n+p$, this is because the coefficients of $\bar{\eta}_i$ are sums of elements of $\mathfrak{S}_i$, no element in $\mathfrak{S}_i$ appears in two such coefficients, and all coordinates of $\boldsymbol{\alpha}$ are non-zero. For $i = s+1, \ldots, n+p-1$, since η_i is $(\mathfrak{c}_{1,i-s}\ell_1 + \cdots + \mathfrak{c}_{p,i-s}\ell_p)\mathfrak{m}_{i-s}$, its initial form $\mathrm{init}_{\boldsymbol{e}}(\eta_i)$ is the product $\mathrm{init}_{\boldsymbol{e}}(\mathfrak{c}_{1,i-s}\ell_1 + \cdots + \mathfrak{c}_{p,i-s}\ell_p)\mathrm{init}_{\boldsymbol{e}}(\mathfrak{m}_{i-s})$. After setting x_1 to 1, we deduce that $\bar{\eta}_i$ factors as $\bar{\eta}_i = f_i g_i$, where the coefficients of both f_i and g_i are sums of elements of $\mathfrak{S}_i$, and again, no element in $\mathfrak{S}_i$ appears in two such coefficients. Thus, the evaluations of f_i and g_i at $\boldsymbol{\alpha}$ are non-zero, and the same holds for $\bar{\eta}_i$.

To describe algebraic sets in the torus $(\overline{\mathbf{K}} - \{0\})^{n+p-1}$, we work in $\overline{\mathbf{K}}^{n+p}$, using a new indeterminate Z and taking into account the relation $x_2 \cdots x_n \ell_1 \cdots \ell_p Z = 1$. Then, for $i = 0, \ldots, n+p$, we will prove the following: *for a generic choice of $(\rho_1, \ldots, \rho_i)$ in $\overline{\mathbf{K}}^{t_1+\cdots+t_i}$ (in the Zariski sense), the zero-set of $\Theta_{(\rho_1,\ldots,\rho_i)}(\bar{\eta}_1, \ldots, \bar{\eta}_i)$ and $x_2 \cdots x_n \ell_1 \cdots \ell_p Z - 1$ has dimension at most $n+p-1-i$ in $\overline{\mathbf{K}}^{n+p}$.* Taking $i = n+p$ proves our claim.

The proof is by induction on i. For $i = 0$, there is nothing to prove, so let us assume that our claim holds for $i-1$ (for some index $i \geq 1$), and prove that it holds at index i. We proceed by contradiction, assuming our claim does not hold. In this case, the vectors $(\rho_1, \ldots, \rho_i)$ for which the zeros of $\Theta_{(\rho_1,\ldots,\rho_i)}(\bar{\eta}_1, \ldots, \bar{\eta}_i)$ and $x_2 \cdots x_n \ell_1 \cdots \ell_p Z - 1$ have dimension at most $n+p-1-i$ in $\overline{\mathbf{K}}^{n+p}$ are contained in a hypersurface of the parameter space $\overline{\mathbf{K}}^{t_1+\cdots+t_i}$. Thus

they satisfy a relation $P(\rho_1, \ldots, \rho_i) = 0$, for some non-zero polynomial P in $\overline{\mathbf{K}}[\mathfrak{S}_1, \ldots, \mathfrak{S}_i]$. Then, take $(\rho_1, \ldots, \rho_{i-1})$ in $\overline{\mathbf{K}}^{t_1+\cdots+t_{i-1}}$ such that

- $P(\rho_1, \ldots, \rho_{i-1}, \mathfrak{S}_i) \in \overline{\mathbf{K}}[\mathfrak{S}_i]$ is not identically zero;
- the zero-set V of $\Theta_{(\rho_1,\ldots,\rho_{i-1})}(\bar{\eta}_1, \ldots, \bar{\eta}_{i-1})$ and $x_2 \cdots x_n \ell_1 \cdots \ell_p Z - 1$ has dimension at most $n + p - i$ in $\overline{\mathbf{K}}^{n+p}$ (this is possible by the induction assumption). By Krull's theorem, all its irreducible components have dimension exactly $n + p - i$.

The first condition implies that for a generic ρ_i in $\overline{\mathbf{K}}^{t_i}$, the zero-set of $\Theta_{(\rho_1,\ldots,\rho_i)}(\bar{\eta}_1, \ldots, \bar{\eta}_i)$ and $x_2 \cdots x_n \ell_1 \cdots \ell_p Z - 1$ has dimension at least $n + p - i$. Equivalently, this means that intersection of V and $\Theta_{(\rho_1,\ldots,\rho_i)}(\bar{\eta}_i)$ has dimension $n + p - i$. Let us see how to derive a contradiction.

Let $V_1, \ldots, V_d$ be the irreducible components of V. Pick $\boldsymbol{\alpha}_1$ in V_1, $\ldots$, $\boldsymbol{\alpha}_d$ in V_d, and let $\gamma_1, \ldots, \gamma_d$ be the polynomials in $\overline{\mathbf{K}}[\mathfrak{S}_i]$ obtained by evaluating $x_2, \ldots, x_n, \ell_1, \ldots, \ell_p$ at the coordinates of $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_d$, respectively, in $\bar{\eta}_i$. As we pointed out above, all γ_i's are non-zero, and thus so is $\Gamma := \gamma_1 \cdots \gamma_d \in \overline{\mathbf{K}}[\mathfrak{S}_i]$. In particular, for a generic choice of ρ_i in $\overline{\mathbf{K}}^{t_i}$, $\Theta_{(\rho_1,\ldots,\rho_i)}(\bar{\eta}_i)$ vanishes at none of $\boldsymbol{\alpha}_1, \ldots, \boldsymbol{\alpha}_d$, and so it intersects each V_i (and thus V) in dimension $n + p - i - 1$. This contradicts the previous paragraph. □

4.4 Boundedness property

Using the results in the previous subsection, we finally establish the second property needed for our homotopy algorithm: we prove that for a generic ρ in $\overline{\mathbf{K}}^N$, the solutions of $\boldsymbol{B} = \Theta_\rho(\mathfrak{B})$ in $\overline{\mathbf{K}}\langle\langle t \rangle\rangle^n$ are bounded.

Proposition 4.6. *There exists a non-empty Zariski open set $\Omega_3 \subset \overline{\mathbf{K}}^N$ such that for $\rho \in \Omega_3$, writing $\boldsymbol{B} := \Theta_\rho(\mathfrak{B})$, all points in $V(\boldsymbol{B}) \subset \overline{\mathbf{K}}\langle\langle t \rangle\rangle^n$ are bounded.*

Proof. By Proposition 4.5, there exists a non-empty Zariski open set $\Omega_2 \subset \overline{\mathbf{K}}^{N+p}$ such that for any $\sigma = (\rho, \tau)$ in Ω_2, the following holds: for any $\boldsymbol{e}$ in $\mathbb{Q}^{n+p}$ and any j in $\{1, \ldots, n+p\}$, the system obtained by setting the j-th variable to 1 in $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta}))$ has no solution in $(\overline{\mathbf{K}} - \{0\})^{n+p-1}$.

We then let $\Omega_2' \subset \overline{\mathbf{K}}^N$ be the image of Ω_2 through the projection $\pi : \sigma = (\rho, \tau) \mapsto \rho$; this is a non-empty Zariski open. Finally, we let Ω_3 be the intersection of Ω_2' with $(\overline{\mathbf{K}} - \{0\})^N \subset \overline{\mathbf{K}}^N$. We take ρ in Ω_3 and we prove that all solutions of $\Theta_\rho(\mathfrak{B})$ in $\overline{\mathbf{K}}\langle\langle t \rangle\rangle^n$ are bounded.

Take such a solution, and write it $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n) \in \overline{\mathbf{K}}\langle\langle t \rangle\rangle^n$. By construction, there exists a non-zero $(\lambda_1, \ldots, \lambda_p) \in \overline{\mathbf{K}}\langle\langle t \rangle\rangle^p$ such that $[\lambda_1 \ \cdots \ \lambda_p]$ is in the left nullspace of $\mathfrak{M}(\boldsymbol{\alpha})$. Let $v \in \mathbb{Q}$ be the valuation of this vector, and let $(\lambda_1', \ldots, \lambda_p') \in \overline{\mathbf{K}}^p$ be the vector of coefficients of t^v in $(\lambda_1, \ldots, \lambda_p)$, so that $(\lambda_1', \ldots, \lambda_p')$ is not identically zero. Let us then take $\tau = (\tau_1, \ldots, \tau_p)$ such that $\sigma := (\rho, \tau)$ is in Ω_2 and in addition $\tau_1 \neq 0, \ldots, \tau_p \neq 0$ and $\tau_1\lambda_1' + \cdots + \tau_p\lambda_p' \neq 0$ (this is possible, since all these conditions are Zariski-open). In particular, $\tau_1\lambda_1 + \cdots + \tau_p\lambda_p \neq 0$. We can then define $\bar{\boldsymbol{\lambda}} = (\bar{\lambda}_1, \ldots, \bar{\lambda}_p)$ by $\bar{\lambda}_i = \lambda_i/(\tau_1\lambda_1 + \cdots + \tau_p\lambda_p)$ for all i. Let us write $\boldsymbol{\phi} = (\boldsymbol{\alpha}, \bar{\boldsymbol{\lambda}})$; our goal is then to prove that $\boldsymbol{\phi}$ is bounded, since it will imply that $\boldsymbol{\alpha}$ is bounded.

By construction, the vector $[\bar{\lambda}_1 \ \cdots \ \bar{\lambda}_p]$ is still in the left nullspace of $\mathfrak{M}(\boldsymbol{\alpha})$ and satisfies $\tau_1\bar{\lambda}_1 + \cdots + \tau_p\bar{\lambda}_p - 1 = 0$. Hence, the vector $\boldsymbol{\phi}$ is in $V(\Theta_\sigma(\mathfrak{H}))$. Let us then write $\boldsymbol{\phi} = (t^{e_1}c_1 + \ldots, \ldots, t^{e_{n+p}}c_{n+p} + \ldots)$ with, for all $i = 1, \ldots, n+p$, e_i in $\mathbb{Q}$ and c_i in $\overline{\mathbf{K}} - \{0\}$. Because none of the coordinates of σ vanishes, we can apply Proposition 4.4, and deduce that $\boldsymbol{c} = (c_1, \ldots, c_{n+p})$ cancels $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta}))$, with $\boldsymbol{e} = (e_1, \ldots, e_{n+p})$.

Suppose then by way contradiction that some e_i is negative; without loss of generality, we can assume that $e_1 < 0$. The polynomials $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta}))$ are weighted-homogeneous, for the weight vector $\boldsymbol{e}$. In particular, the point

$$\tilde{\boldsymbol{c}} = \left(1, \frac{c_2}{\epsilon^{e_2}}, \ldots, \frac{c_{n+p}}{\epsilon^{e_{n+p}}}\right)$$

is also a solution of these equations, where ϵ denotes any element in $\overline{\mathbf{K}}$ such that $\epsilon^{e_1} = c_1$. Note that none of the coordinates of the vector $\tilde{\boldsymbol{c}}$ vanishes. However, by construction, σ is in Ω_2, so Proposition 4.5 asserts that the system obtained by setting the first variable x_1 to 1 in $\Theta_\sigma(\mathrm{init}_{\boldsymbol{e}}(\boldsymbol{\eta}))$ has no solution in $(\overline{\mathbf{K}} - \{0\})^{n+p-1}$. This is the contradiction we wanted, so we have $e_i \geq 0$ for all i, as claimed. □

At this stage, to prove Proposition 4.1, it suffices to let Ω be the intersection of Ω_1 (from Proposition 4.2) and Ω_3 (from the proposition above).

5 Cost analysis

Let the polynomials in $\boldsymbol{g} = (g_1, \ldots, g_s)$ and $\boldsymbol{F} = [f_{i,j}]_{1\leq i\leq p,\ 1\leq j\leq q}$ be as before. To find the isolated points in $V_p(\boldsymbol{F}, \boldsymbol{g})$, we take $\boldsymbol{B} = \Theta_\rho(\mathfrak{B})$ as in the previous section, for a randomly chosen $\rho \in \mathbf{K}^N$ and apply the Homotopy algorithm of Proposition 3.1.

Proposition 4.1 established the basic properties needed for the correctness of our homotopy algorithm. To finish the analysis, and establish a cost bound, we now give upper bounds on the parameters that appear in the runtime reported in Proposition 3.1, such as the size of the input, the number of solutions to our start system and on the degree of the homotopy curve; we also have to give the cost of solving the start system.

We first consider the case of arbitrary sparse polynomials, for which we state our results in terms of certain mixed volumes; later we discuss the particular case of weighted-degree polynomials. Some quantities will be defined similarly in both cases. As before, for $i = 1, \ldots, s$, $\mathcal{A}_i \subset \mathbb{N}^n$ denotes the support of g_i, to which we add the origin $\mathbf{0} \in \mathbb{N}^n$, and for $j = 1, \ldots, q$, $\mathcal{B}_j \subset \mathbb{N}^n$ is the union of the supports of the polynomials in the j-th column of $\boldsymbol{F}$, to which we add $\mathbf{0}$ as well. For indices i, j as above, we let a_i, respectively b_j, be the cardinality of $\mathcal{A}_i$, respectively $\mathcal{B}_j$. As input, in either case, we are given $\boldsymbol{g}$ and $\boldsymbol{F}$ through the list of their non-zero terms; this involves $O(\gamma)$ elements in $\mathbf{K}$, with

$$\gamma := a_1 + \cdots + a_s + p(b_1 + \cdots + b_q). \tag{6}$$

Finally, we let d be the maximum degree of all the polynomials in $\boldsymbol{g}$ and $\boldsymbol{F}$.

5.1 General sparse polynomials

Representing the input. The algorithm in Proposition 3.1 takes as input a straight-line program representation of the polynomials $\boldsymbol{B} = \Theta_\rho(\mathfrak{B})$. To obtain such a straight-line program is straightforward. We first compute the values of all monomials supported on $\mathcal{A}_1, \ldots, \mathcal{A}_s, \mathcal{B}_1, \ldots, \mathcal{B}_q$; we then combine them to obtain the polynomials $(1-t)\cdot\Theta_\rho(\mathfrak{r}) + t\cdot\boldsymbol{g}$ and the matrix $(1-t)\cdot\Theta_\rho(\mathfrak{M}) + t\cdot\boldsymbol{F}$, and take all p-minors in this matrix.

Computing the value of a single monomial supported on $\mathcal{A}_i$, respectively $\mathcal{B}_j$, can be done through repeated squaring, using $O(n\log(d))$ operations in $\mathbf{K}$. Hence, we can obtain the values of all monomials supported on $\mathcal{A}_1, \ldots, \mathcal{A}_s, \mathcal{B}_1, \ldots, \mathcal{B}_q$ by using a straight-line program of length $O(n\gamma\log(d))$. Combining these monomials to obtain $(1-t)\cdot\Theta_\rho(\mathfrak{r}) + t\cdot\boldsymbol{g}$ and $(1-t)\cdot\Theta_\rho(\mathfrak{M}) + t\cdot\boldsymbol{F}$ takes another $O(\gamma)$ operations. Finally, it takes $O(p^4\binom{q}{p})$ operations to compute all p-minors of the latter matrix using a division-free determinant algorithm. Altogether, we obtain a straight-line program of length

$$\beta \in O\left(n\gamma\log(d) + p^4\binom{q}{p}\right) \tag{7}$$

to compute all entries of $\boldsymbol{B}$.

Number of solutions of the start system. For ρ in the open set $\Omega \subset \overline{\mathbf{K}}^N$ defined in Proposition 4.1, we saw that the solutions of the start system $\boldsymbol{B}_{t=0}$ are the disjoint union of the solutions of the systems $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \boldsymbol{r})$, where for a subset $\boldsymbol{i} = \{i_1, \ldots, i_{n-s}\}$ of $\{1, \ldots, q\}$ we write $\mathfrak{M}_{\boldsymbol{i}} = (\mathfrak{m}_{i_1}, \ldots, \mathfrak{m}_{i_{n-s}})$.

For $i = 1, \ldots, s$ and $j = 1, \ldots, q$, we let $\mathcal{C}_i$ and $\mathcal{D}_j$ be the convex hulls of respectively $\mathcal{A}_i$ and $\mathcal{B}_j$. Proposition 2.3 then implies that, for $\boldsymbol{i}$ as above, the number of solutions of $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \mathfrak{r})$ in $\overline{\mathbf{K}}^n$ is the mixed volume

$$\chi_{\boldsymbol{i}} := \mathsf{MV}(\mathcal{C}_1, \ldots, \mathcal{C}_s, \mathcal{D}_{i_1}, \ldots, \mathcal{D}_{i_{n-s}})$$

for any ρ in a certain non-empty Zariski open set $\mathscr{O}_{\mathrm{BKK}\boldsymbol{i}} \subset \overline{\mathbf{K}}^N$. Define

$$\chi := \sum_{\boldsymbol{i}=\{i_1,\ldots,i_{n-s}\}\subset\{1,\ldots,q\}} \chi_{\boldsymbol{i}} = \sum_{\boldsymbol{i}=\{i_1,\ldots,i_{n-s}\}\subset\{1,\ldots,q\}} \mathsf{MV}(\mathcal{C}_1, \ldots, \mathcal{C}_s, \mathcal{D}_{i_1}, \ldots, \mathcal{D}_{i_{n-s}}), \tag{8}$$

and let Ω' be the intersection of Ω with the finitely many $\mathscr{O}_{\mathrm{BKK}\boldsymbol{i}}$. Then, for ρ in Ω', the start system $\boldsymbol{B}_{t=0}$ has precisely χ solutions. As we pointed out after Proposition 4.1, this implies that the system $\boldsymbol{B}_{t=1}$ which we want to solve admits at most χ isolated solutions, counted with multiplicities.

Solving the start system. To solve the systems $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \mathfrak{r})$, we rely on the sparse symbolic homotopy algorithm of [25, Section 5]. This algorithm finds the solutions of a sparse system of n equations in n unknowns, with arbitrary support and generic coefficients (in the Zariski sense); this means that in addition to the constraint $\rho \in \Omega$, our choice of ρ will also have to satisfy the constraints stated in that reference.

The runtime of this algorithm depends on some combinatorial quantities (we refer to the original reference for a more extensive discussion): we need a so-called *lifting function* $\boldsymbol{\omega_i}$, and the associated *fine mixed subdivision* $M_{\boldsymbol{i}}$, for the support $\mathcal{A}_1, \ldots, \mathcal{A}_s, \mathcal{B}_{i_1}, \ldots, \mathcal{B}_{i_{n-s}}$ of $\mathfrak{r}$ and $\mathfrak{M}_{\boldsymbol{i}}$ [23]. We then let $w_{\boldsymbol{i}}$ be the maximum value taken by $\boldsymbol{\omega_i}$ on the support, and $\mu_{\boldsymbol{i}}$ be the maximum norm of the (primitive, integer) normal vectors to the cells of $M_{\boldsymbol{i}}$. Then, the algorithm in [25, Theorem 6.2] compute as zero-dimensional parametrization $\mathscr{R}_{\boldsymbol{i}}$ such that $Z(\mathscr{R}_{\boldsymbol{i}}) = V(\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \mathfrak{r}))$ using $O^{\sim}(n^5 \gamma \log(d) \chi_{\boldsymbol{i}}^2 \mu_{\boldsymbol{i}} w_{\boldsymbol{i}})$ operations in $\mathbf{K}$.

Taking the union of all these parametrizations, using for example, [29, Lemma J.3], does not introduce any added cost. Thus we obtain a randomized algorithm to compute a zero-dimensional parametrization of $V_p(\Theta_\rho(\mathfrak{M}, \mathfrak{r}))$ using

$$O^{\sim}(n^5 \gamma \log(d) \chi^2 \mu w) \tag{9}$$

operations in $\mathbf{K}$, where we write $\mu := \max_{\boldsymbol{i}}(\mu_{\boldsymbol{i}})$ and $w := \max_{\boldsymbol{i}}(w_{\boldsymbol{i}})$.

Degree of the homotopy curve. The complexity of the Homotopy algorithm depends on χ, which measures the number of solutions which are tracked during the homotopy, and on the precision t^{ϱ} at which we need to do the computations. As mentioned in Section 3, an upper bound for ϱ is the number of isolated points defined by the equations in $\boldsymbol{B} = \Theta_\rho(\mathfrak{B})$ together with a generically chosen hyperplane.

Let $h = \zeta_0 + \zeta_1 x_1 + \cdots + \zeta_n x_n + \zeta_{n+1} t$ be a linear form defining such a hyperplane (here, we take $\zeta_i \in \mathbf{K}$). Using it allows us to rewrite t as

$$\wp(x_1, \ldots, x_n) = -(\zeta_0 + \zeta_1 x_1 + \cdots + \zeta_n x_n)/\zeta_{n+1}.$$

The isolated points in $V(\boldsymbol{B}) \cap V(h)$ are in one-to-one correspondence with the isolated solutions of the system $\boldsymbol{B'} = (b'_1, \ldots, b'_s, b'_{s+1}, \ldots, b'_m)$, where $b'_i = (1 - \wp) r_i + \wp g_i$, for $i = 1, \ldots, s$, and $(b'_{s+1}, \ldots, b'_m)$ are the p-minors of the matrix $\mathbf{V'} = [v'_{i,j}] = (1 - \wp)\boldsymbol{M} + \wp \boldsymbol{F} \in \mathbf{K}[x_1, \ldots, x_n]^{p \times q}$. Hence it is sufficient to bound the number of isolated solutions of $V(\boldsymbol{B'})$.

For $i = 1, \ldots, p$ and $j = 1, \ldots, q$, let $\mathcal{B}'_{i,j}$ be the support of $v'_{i,j}$. We then define $\mathcal{B}'_j = \cup_{1 \le i \le p} \mathcal{B}'_{i,j}$, to which we add the origin if needed, and let $\mathcal{D}'_j$ be its Newton polytope. Similarly, for $i = 1, \ldots, s$ we let $\mathcal{C}'_i$ denote the Newton polytope of the support of b'_i. Then, the discussion on the number of solutions of the target system still applies, and shows that the system $\boldsymbol{B'}$ admits at most

$$\varrho = \sum_{\{i_1, \ldots, i_{n-s}\} \subset \{1, \ldots, q\}} \mathsf{MV}(\mathcal{C}'_1, \ldots, \mathcal{C}'_s, \mathcal{D}'_{i_1}, \ldots, \mathcal{D}'_{i_{n-s}}) \tag{10}$$

solutions.

Completing the cost analysis. The previous discussion allows us to use the Homotopy algorithm from Proposition 3.1. In addition to the polynomials $\boldsymbol{g}$ and matrix $\boldsymbol{F}$, we also need the combinatorial information $\boldsymbol{\omega_i}, M_{\boldsymbol{i}}$ described previously. The sum of the costs of solving the start system, and of the Homotopy algorithm is as follow.

Theorem 5.1. *The set $V_p(\boldsymbol{F}, \boldsymbol{g})$ admits at most χ isolated solutions, counted with multiplicities. There exists a randomized algorithm which takes $\boldsymbol{g}$, $\boldsymbol{F}$, all lifting functions $\boldsymbol{\omega}_i$ and subdivisions $\boldsymbol{M_i}$ as input and computes a zero-dimensional parametrization of these isolated solutions using*

$$O^{\sim}\left(n^5\left(\gamma\log(d)\chi^2\mu w + \chi(\varrho+\chi^5)\binom{q}{p}\right)\right)$$

operations in $\mathbf{K}$, where γ, χ, ϱ are as in respectively (6), (8) and (10), and μ and w as in (9).

5.2 Weighted-degree polynomials

Weighted polynomial domains are multivariate polynomial rings $\mathbf{K}[x_1, \ldots, x_n]$ where each variable x_i has an integer weight $w_i \geq 1$ (denoted by $\mathrm{wdeg}(x_i) = w_i$). The weighted degree of a monomial $x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ is then $\sum_{i=1}^n w_i\alpha_i$, and the weighted degree $\mathrm{wdeg}(f)$ of a polynomial f is the maximum of the weighted degrees of its terms with non-zero coefficients.

Weighted domains arise naturally in determining isolated critical points of a symmetric function ϕ defined over a variety $V(f_1, \ldots, f_s)$ defined by symmetric functions f_i. In [10], with J.-C. Faugère, we show that the orbits of these critical points can be described by domains of the form $\mathbf{K}[e_{1,1}, \ldots, e_{1,\ell_1}, e_{2,1}, \ldots, e_{2,\ell_2}, \ldots, e_{r,1}, \ldots, e_{r,\ell_r}]$ with $e_{i,k}$ the k-th elementary symmetric function on ℓ_i letters. Measured in terms of these letters, each $e_{i,k}$ has naturally weighted degree k.

Polynomials in weighted domains have a natural sparse structure when compared to polynomials in classical domains. For example, a polynomial $p \in \mathbf{K}[x_1, x_2, x_3]$ having total degree bounded by 10 has 286 possible terms in a classical domain. However in a weighted domain with weights $\boldsymbol{w} = (5, 3, 2)$ there are only 19 possible terms. Such a reduction also exists when considering bounds for solutions of polynomial systems when comparing classical to weighted domains. For instance, Bézout's theorem bounds the number of isolated solutions to polynomial systems of equations by the product of their degrees. With polynomial systems lying in a weighted polynomial domain $\mathbf{K}[x_1, \ldots, x_n]$ having weights $\boldsymbol{w} = (w_1, \ldots, w_n) \in \mathbb{Z}^n_{>0}$, the weighted Bézout theorem (see e.g. [24]) states that the number of isolated points of $V(f_1, \ldots, f_n) \subset \overline{\mathbf{K}}^n$ is bounded by

$$\delta = \frac{d_1\cdots d_n}{w_1\cdots w_n} \quad \text{with} \quad d_i = \mathrm{wdeg}(f_i). \tag{11}$$

In this section we show how our sparse homotopy algorithm also allows us to describe the isolated points of $V_p(\boldsymbol{F}, \boldsymbol{g})$ where $\boldsymbol{F} = [f_{i,j}] \in \mathbf{K}[x_1, \ldots, x_n]^{p\times q}$ and $\boldsymbol{g} = (g_1, \ldots, g_s) \in \mathbf{K}[x_1, \ldots, x_n]^s$ with $n = q - p + s + 1$, assuming bounds on the weighted degrees of all polynomials $f_{i,j}$ and g_j. Without loss of generality, we will assume that $w_1 \leq \cdots \leq w_n$, and we will let $(\gamma_1, \ldots, \gamma_s)$ be the weighted degrees of $(g_1, \ldots, g_s)$ and $(\delta_1, \ldots, \delta_q)$ be the weighted column degrees of $\boldsymbol{F}$.

In particular, the monomial supports $\mathcal{A}_1, \ldots, \mathcal{A}_s$ of $g_1, \ldots, g_s$ are contained in the sets $\mathcal{A}'_1, \ldots, \mathcal{A}'_s$, where $\mathcal{A}'_i$ is the set of all $(e_1, \ldots, e_n) \in \mathbb{N}^n$ such that $w_1e_1 + \cdots + w_ne_n \leq \gamma_i$. Similarly, for $1 \leq j \leq q$, $\mathcal{B}_j \subset \mathbb{N}^n$ is contained in the set $\mathcal{B}'_j$ of all $(e_1, \ldots, e_n) \in \mathbb{N}^n$ for which

$w_1e_1+\cdots+w_ne_n \le \delta_j$. The sets $\mathcal{A}'_i$, respectively $\mathcal{B}'_j$, are the supports of generic polynomials of weighted degrees at most γ_i, respectively δ_j. We denote their cardinalities by $a'_1,\ldots,a'_s$ and $b'_1,\ldots,b'_q$.

Representing the input. We follow the same approach as in the last subsection to obtain a straight-line program for $\boldsymbol{B} = \Theta_\rho(\mathfrak{B})$, simply by computing all monomials of respective weighted degrees at most $(\gamma_1,\ldots,\gamma_s)$ and $(\delta_1,\ldots,\delta_q)$, combining them to form the polynomials $(1-t)\cdot\Theta_\rho(\mathfrak{r})+t\cdot\boldsymbol{g}$ and the matrix $(1-t)\cdot\Theta_\rho(\mathfrak{M})+t\cdot\boldsymbol{F}$ and taking the p-minors of the latter. We benefit from a minor improvement here, as for a fixed γ_i or δ_j we can compute all these monomials in an incremental manner, starting from the monomial 1, foregoing the use of repeated squaring: this saves a factor $n\log(d)$. Altogether, this results in a straight-line program of size

$$\Gamma \in O\left((a'_1+\cdots+a'_s+p(b'_1+\cdots+b'_q))+p^4\binom{q}{p}\right)$$

to compute all entries of $\boldsymbol{B}$.

Recall that a term such as a'_i denotes the number of monomials of weighted degree at most γ_i in n variables, with $\gamma_i \le d$ for all i (and similarly for b'_j, for the weighted degree bound δ_j). A crude bound is thus $a'_i, b'_j \le \binom{n+d}{n}$, resulting in the estimate

$$\Gamma \in O\left(n^2\binom{n+d}{n}+n^4\binom{q}{p}\right). \tag{12}$$

This is not the sharpest possible bound. Bounding a'_i by the volume of the non-negative simplex defined by

$$w_1(e_1-1)+\cdots+w_n(e_n-1) \le \gamma_i$$

results in the upper bound $a'_i \le (\gamma_i+w_1+\cdots+w_n)^n/(n!w_1\cdots w_n)$. Using [5] and [33, Theorem 1.1] gives more refined results for a'_i and b'_j and hence also for Γ.

Number of solutions of the start system. As in the case of sparse polynomials, we take ρ in the open set $\Omega \subset \overline{\mathbf{K}}^N$ of Proposition 4.1 and set $\boldsymbol{B} = \Theta_\rho(\mathfrak{B})$. In this case, the solutions of the start system $\boldsymbol{B}_{t=0}$ are the disjoint union of the solutions of systems $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}},\boldsymbol{r})$, with $\mathfrak{M}_{\boldsymbol{i}} = (\mathfrak{m}_{i_1},\ldots,\mathfrak{m}_{i_{n-s}})$ for $\boldsymbol{i} = \{i_1,\ldots,i_{n-s}\} \subset \{1,\ldots,q\}$.

By the weighted Bézout theorem, the system $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}},\boldsymbol{r})$ has

$$c_{\boldsymbol{i}} = \frac{\gamma_1\cdots\gamma_s\delta_{i_1}\cdots\delta_{i_{n-s}}}{w_1\cdots w_n}$$

solutions in $\overline{\mathbf{K}}^n$. Taking the sum over all subsets $\boldsymbol{i}$ of $\{1,\ldots,q\}$ of cardinality $n-s$, we deduce that the number of solutions of $\boldsymbol{B}_{t=0}$ is at most

$$c = \sum_{\boldsymbol{i}} c_{\boldsymbol{i}} = \frac{\gamma_1\cdots\gamma_s\,\eta_{n-s}(\delta_1,\ldots,\delta_q)}{w_1\cdots w_n}, \tag{13}$$

where $\eta_{n-s}(\delta_1,\ldots,\delta_q)$ is the elementary symmetric polynomial of degree $n-s$ in $\delta_1,\ldots,\delta_q$. The discussion following Proposition 4.1 implies that the system $\boldsymbol{B}_{t=1}$ which we want to solve admits at most c isolated solutions.

Solving the start system. To find these solutions, as in the previous subsection, we solve all systems $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \boldsymbol{r})$ independently. We are not aware of a dedicated algorithm for weighted-degree polynomial systems whose complexity would be suitable; instead, we rely on the geometric resolution algorithm as presented in [16]. In what follows, our first requirement is that ρ be in the open set $\Omega \subset \overline{\mathbf{K}}^N$ of Proposition 4.1, but we will add finitely many Zariski-open conditions on ρ.

For a subset $\boldsymbol{i} = \{i_1, \ldots, i_{n-s}\} \subset \{1, \ldots, q\}$, let $(d_{\boldsymbol{i},1}, \ldots, d_{\boldsymbol{i},n})$ denote the sequence $(\gamma_1, \ldots, \gamma_s, \delta_{i_1}, \ldots, \delta_{i_{n-s}})$ sorted in non-decreasing order; we write

$$\kappa_{\boldsymbol{i}} = \max_{1 \le k \le n} (d_{\boldsymbol{i},1} \cdots d_{\boldsymbol{i},k} w_{k+1} \cdots w_n) \quad \text{and} \quad \kappa = \sum_{\boldsymbol{i}=\{i_1,\ldots,i_{n-s}\} \subset \{1,\ldots,q\}} \kappa_{\boldsymbol{i}}. \tag{14}$$

Recall as well that we set $d = \max(\gamma_1, \ldots, \gamma_s, \delta_1, \ldots, \delta_q)$.

Lemma 5.2. *For $\boldsymbol{i} = \{i_1, \ldots, i_{n-s}\} \subset \{1, \ldots, q\}$, and a generic $\rho \in \overline{\mathbf{K}}^N$, one can solve $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \boldsymbol{r})$ by a randomized algorithm that uses*

$$O^{\tilde{}}\left(n^4 \Gamma d^2 \left(\frac{\kappa_i}{w_1 \cdots w_n}\right)^2\right)$$

operations in $\mathbf{K}$.

Proof. The polynomials $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \boldsymbol{r})$ have weighted degrees at most $(\gamma_1, \ldots, \gamma_s, \delta_{i_1}, \ldots, \delta_{i_{n-s}})$. We first reorder these equations in non-decreasing order of weigthed degree; we write the reordered sequence of polynomials as $(h_1, \ldots, h_n)$, their respective weighted degrees being at most $(d_{\boldsymbol{i},1}, \ldots, d_{\boldsymbol{i},n})$.

By Proposition 4.2, since the supports of $\mathfrak{M}_{\boldsymbol{i}}$ and $\boldsymbol{r}$ contain the origin, for a generic choice of ρ, the equations $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \boldsymbol{r})$ define a reduced regular sequence (possibly terminating early and thus defining the empty set). We can thus apply the geometric resolution algorithm as in [16, Theorem 1].

The algorithm in [16] takes its input represented as a straight-line program. To obtain one, we take our straight-line program of length Γ that computes $\boldsymbol{B}$ and set $t = 0$; the resulting straight-line program computes all $\Theta_\rho(\boldsymbol{r})$ and $\Theta_\rho(\mathfrak{m}_1, \ldots, \mathfrak{m}_q)$, and in particular $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}})$. We deduce that we can compute a zero-dimensional parametrization of the solutions of $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \boldsymbol{r})$ using $O^{\tilde{}}(n^4 \Gamma d^2 \boldsymbol{\Sigma}_{\boldsymbol{i}}^2)$ operations in $\mathbf{K}$. Here, $\boldsymbol{\Sigma}_{\boldsymbol{i}}$ is the maximum of the degrees of the "intermediate varieties" $V_1, \ldots, V_n$, where V_i is defined by the first i equations in $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \boldsymbol{r})$. Hence, to conclude, it suffices to prove that $\boldsymbol{\Sigma}_{\boldsymbol{i}} \le \kappa_{\boldsymbol{i}}/(w_1 \cdots w_n)$.

Fix an index ℓ in $\{1, \ldots, n\}$. We identify degree-1 polynomials $P = p_0 + p_1 x_1 + \cdots + p_n x_n$ in $\overline{\mathbf{K}}[x_1, \ldots, x_n]$ with points in $\overline{\mathbf{K}}^{n+1}$. Then, there exists a non-empty Zariski open set $\mathscr{P} \subset \overline{\mathbf{K}}^{(n+1)(n-\ell)}$ such that for $(p_{i,j})_{0 \le j \le n, 1 \le i \le n-\ell} \in \mathscr{P}$, defining P_i as

$$P_i = p_{i,0} + p_{i,1} x_1 + \cdots + p_{i,n} x_n$$

implies that $V_\ell \cap V(P_1) \cdots \cap V(P_{n-\ell})$ has cardinality $\deg(V_\ell)$. Up to taking the $p_{i,j}$'s in the intersection of $\mathscr{P}$ with another non-empty Zariski open set, one can perform Gaussian

elimination to rewrite $P_1, \ldots, P_{n-\ell}$ as

$$x_{\ell+1} - \wp_{\ell+1}(x_1, \ldots, x_\ell), \ldots, x_n - \wp_n(x_1, \ldots, x_\ell).$$

For $k = 1, \ldots, \ell$, let $g_k(x_1, \ldots, x_\ell) = h_k(x_1, \ldots, x_\ell, \wp_{\ell+1}(x_1, \ldots, x_\ell), \ldots, \wp_n(x_1, \ldots, x_\ell))$ in $\mathbf{K}[x_1, \ldots, x_\ell]$. Because the sequence of weights is non-decreasing, these have respective weighted degrees at most $d_{\boldsymbol{i},1}, \ldots, d_{\boldsymbol{i},\ell}$ and, by construction, $V(g_1, \ldots, g_\ell)$ is finite and $\deg(V_\ell) = \deg(V(g_1, \ldots, g_\ell))$. Using the weighted Bézout's theorem implies

$$\deg(V(g_1, \ldots, g_\ell)) \leq \frac{d_{\boldsymbol{i},1} \cdots d_{\boldsymbol{i},\ell}}{w_1 \cdots w_\ell} = \frac{d_{\boldsymbol{i},1} \cdots d_{\boldsymbol{i},\ell} w_{\ell+1} \cdots w_n}{w_1 \cdots w_n} = \frac{\kappa_{\boldsymbol{i}}}{w_1 \cdots w_n}. \qquad \square$$

Taking all possible $\boldsymbol{i}$ into account, we see that for a generic ρ we can compute zero-dimensional parametrizations for all $\Theta_\rho(\mathfrak{M}_{\boldsymbol{i}}, \boldsymbol{r})$ using

$$O^{\sim}\left(n^4 \Gamma d^2 \left(\frac{\kappa}{w_1 \cdots w_n}\right)^2\right)$$

operations in $\mathbf{K}$. As in the previous subsection, taking the union of all these parametrizations does not introduce any added cost.

Degree of the homotopy curve. Finally, we need an upper bound on the precision t^e to which we do the computations. As before, a suitable upper bound is the number of isolated intersection points in $\overline{\mathbf{K}}^{n+1}$ between $V(\boldsymbol{B})$ and a generic hyperplane.

Let $\zeta = \zeta_0 + \zeta_1 x_1 + \cdots + \zeta_n x_n + \zeta_{n+1} t$ be a linear form defining such a hyperplane (here, we take $\zeta_i \in \mathbf{K}$). We are interested in counting the isolated solutions of all equations $\boldsymbol{g}' = (\zeta, (1-t) \cdot \Theta_\rho(\mathfrak{r}) + t \cdot \boldsymbol{g})$, and all p-minors of $\boldsymbol{F}' = (1-t) \cdot \Theta_\rho(\mathfrak{M}) + t \cdot \boldsymbol{F}$, that is, of $V_p(\boldsymbol{F}', \boldsymbol{g}')$.

Assign weight $w_t = 1$ to t, so the weighted degree of ζ is w_n. Then, the system above is of the kind considered in this section, but with $n+1$ variables instead of n, and $s+1$ equations $\boldsymbol{g}'$ instead of s. The weighted degrees of the equations $\boldsymbol{g}'$ are $(w_n, \gamma_1 + 1, \ldots, \gamma_s + 1)$ and the weighted column degrees of $\boldsymbol{F}'$ are $(\delta_1 + 1, \ldots, \delta_q + 1)$. As we pointed out when counting the solutions of the start system, this implies that our equations admit at most e isolated solutions, with

$$e = \frac{(\gamma_1 + 1) \cdots (\gamma_s + 1)\, \eta_{n-s}(\delta_1 + 1, \ldots, \delta_q + 1)}{w_1 \cdots w_{n-1}}, \tag{15}$$

where η_{n-s} is the elementary symmetric polynomial of degree $n - s$.

Completing the weighted homotopy algorithm. The previous paragraphs allow us to use the Homotopy algorithm from Proposition 3.1; we obtain the following result.

Theorem 5.3. *The set $V_p(\boldsymbol{F}, \boldsymbol{g})$ admits at most c isolated solutions, counted with multiplicities. There exists a randomized algorithm which takes $\boldsymbol{g}$ and $\boldsymbol{F}$ as input and computes a zero-dimensional parametrization of these isolated solutions using*

$$O^{\sim}\Big(\big(c(e + c^5) + d^2 \big(\frac{\kappa}{w_1 \cdots w_n}\big)^2\big) n^4 \Gamma\Big)$$

operations in $\mathbf{K}$*, where* Γ, c, κ, e *are as in respectively* (12), (13), (14) *and* (15).

6 Example

In this section we provide an example illustrating the steps of our homotopy algorithm. Let

$$\boldsymbol{g} = (99x_1^3 + 92x_1^2 - 228x_1x_2 + 67x_1 - 140x_2 + 98x_3 + 25) \in \mathbb{Q}[x_1, x_2, x_3]$$

and $\boldsymbol{F} \in \mathbb{Q}[x_1, x_2, x_3]^{2\times 3}$ be

$$\begin{pmatrix} 9x_1^2 + 65471x_1 + 59x_2 + 42308x_3 + 65504 & 86x_1^2 + 65460x_1 + 65414x_2 + 12381x_3 + 44 & 65477x_1 + 59898x_3 + 76 \\ 65501x_1^2 + 51x_1 + 65466x_2 + 57496x_3 + 35 & 16x_1^2 + 99x_1 + 65503x_2 + 17950x_3 + 31 & 65454x_1 + 41178x_3 + 65453 \end{pmatrix}.$$

The support of g is $\mathcal{A} = \{(3,0,0), (2,0,0), (1,1,0), (1,0,0), (0,1,0), (0,0,1), (0,0,0)\} \subset \mathbb{Z}^3$ with unions of the column supports of $\boldsymbol{F}$ being

$$\begin{aligned} \mathcal{B}_1 &= \{(2,0,0), (1,0,0), (0,1,0), (0,0,1), (0,0,0)\}, \\ \mathcal{B}_2 &= \{(2,0,0), (1,0,0), (0,1,0), (0,0,1), (0,0,0)\}, \\ \mathcal{B}_3 &= \{(1,0,0), (0,0,1), (0,0,0)\}. \end{aligned}$$

Start system. The start system for $(\boldsymbol{F}, g)$ is built as follows. Let $r = 88x_1^3 - 82x_1^2 - 70x_1x_2 + 41x_1 + 91x_2 + 29x_3 + 70 \in \mathbb{Q}[x_1, x_2, x_3]$ a polynomial supported by $\mathcal{A}$ and define $m_1 = -78x_1^2 - 4x_1 + 5x_2 - 91x_3 - 44$, $m_2 = 63x_1^2 + 10x_1 - 61x_2 - 26x_3 - 20$, and $m_3 = 88x_1 + 95x_3 + 9$, polynomials in $\mathbb{Q}[x_1, x_2, x_3]$ supported by $(\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3)$. The starting polynomial system $\boldsymbol{r} = (r)$ and the start matrix are given as

$$\boldsymbol{M} = \begin{pmatrix} -62m_1 & 26m_2 & 10m_3 \\ -83m_1 & -3m_2 & -44m_3 \end{pmatrix} \in \mathbb{Q}[x_1, x_2, x_3]^{2\times 3}.$$

We remark that the coefficients in the start vector and start matrix for this example were chosen randomly, in this case with the help of the rand() command in Maple.

A parametrization of the start system. The set of 2-minors of $\boldsymbol{M}$ is given by $(2344m_1m_2, 3558m_1m_3, -1114m_2m_3)$ and hence $V_2(\boldsymbol{M}, r) = V_1 \cup V_2 \cup V_3$, where

$$V_1 = V(m_1, m_2, r),\ V_2 = V(m_1, m_3, r),\ \text{and}\ V_3 = V(m_2, m_3, r).$$

Parametrizations of V_1, V_2, and V_3 are given by

$$\begin{aligned}
\mathscr{R}_{0,1} = \ & \big((10671923044484y^3 + 164650405712264y^2 + 541980679674061y \ + 393540496795784, \\
& \frac{23707677043321206}{205138445880446701}y^2 + \frac{197994419338092137}{205138445880446701}y + \frac{3859258707817950}{205138445880446701}, \\
& \frac{2817387683743776}{205138445880446701}y^2 \ - \frac{334804957251324375}{205138445880446701}y - \frac{199554818581221524}{205138445880446701}, y), x_3\big), \\
\mathscr{R}_{0,2} = \ & \big((1076005625y^3 + 2749690925y^2 + 2278375403y + 797867887, \\
& -\frac{95}{88}y - \frac{9}{88}, \frac{70395}{3872}y^2 + \frac{201161}{9680}y + \frac{171943}{19360}, y), x_3\big), \\
\mathscr{R}_{0,3} = \ & \big((410682625y^3 + 773879025y^2 + 2045246267y - 666910765, \\
& -\frac{95}{88}y - \frac{9}{88}, \frac{568575}{472384}y^2 - \frac{88607}{236192}y - \frac{157697}{472384}, y), x_3\big).
\end{aligned}$$

Taking the union of $(\mathscr{R}_{0,i})_{1\leq i\leq 3}$ gives a parametrization $\mathscr{R}_0$ of $V_p(\boldsymbol{M}, r)$ with

$$\begin{aligned}
\mathscr{R}_0 = \ & ((q_0, v_{0,1}, v_{0,2}, v_{0,3}), \Lambda_0) \\
= \ & \big((47158887989045932382580090625 00y^9 + \cdots, \\
& \frac{1047634696676655387879016713234375 0}{205138445880446701}y^8 + \cdots, \\
& \frac{2265193491697540283699777221137124035318470625}{24226029904697233601296}y^8 + \cdots, \\
& 15866264491953179878625y^7 + \cdots), x_3\big).
\end{aligned}$$

Degree bounds. The mixed volumes associated to our square sub-systems are $\mathsf{MV}_1 = \mathsf{MV}(\mathrm{conv}(\mathcal{A}), \mathrm{conv}(\mathcal{B}_1), \mathrm{conv}(\mathcal{B}_2)) = 3$, $\mathsf{MV}_2 = \mathsf{MV}(\mathrm{conv}(\mathcal{A}), \mathrm{conv}(\mathcal{B}_1), \mathrm{conv}(\mathcal{B}_3)) = 3$, and finally $\mathsf{MV}_3 = \mathsf{MV}(\mathrm{conv}(\mathcal{A}), \mathrm{conv}(\mathcal{B}_2), \mathrm{conv}(\mathcal{B}_3)) = 3$. So $\chi = \mathsf{MV}_1 + \mathsf{MV}_2 + \mathsf{MV}_3 = 9$ which is a bound on the number of isolated solutions of $V_2(\boldsymbol{F}, g)$. Note that this number coincides with the actual number of isolated solutions of $V_2(\boldsymbol{M}, r)$ as the degree of q_0 equals 9.

A parametrization $\mathscr{R}_1$ of $V_2(\boldsymbol{F}, g)$. We apply the Homotopy algorithm to the system $(M_2((1-t)\boldsymbol{F} + t\boldsymbol{M}), (1-t)r + tg)$ and $\mathscr{R}_0$ to obtain $\mathscr{R}_1$. As the coefficients of the result over $\mathbb{Q}$ are quite large we illustrate this calculation over $\mathbb{F}_{65521}$, the finite field of 65521 elements. In this case we obtain

$$\begin{aligned}
\mathscr{R}_0 = \ & \big((y^9 + 42377y^8 + 63439y^7 + 23268y^6 + 1541y^5 + 21916y^4 \\
& + 24479y^3 + 1064y^2 + 47617y + 765, 18447y^8 + 58286y^7 + 48619y^6 \\
& + 49312y^5 + \ 42721y^4 + 44021y^3 + 47621y^2 + 39038y + 13072, \\
& 9852y^8 + 30892y^7 + \ 29236y^6 + 63043y^5 + 623y^4 + 8249y^3 \\
& + 22956y^2 + 23577y + 41427, \ 3y^7 + 19233y^6 + 56323y^5 + 58151y^4 \\
& + 8939y^3 + 30577y^2 + 13156y), x_3\big)
\end{aligned}$$

and

$$\begin{aligned}\mathscr{R}_1 = \quad & \big((y^9 + 27502y^8 + 1022y^7 + 42474y^6 + 21370y^5 + 47501y^4 \\ & + 37694y^3 + \ 13474y^2 + 49870y + 26489, 19690y^8 + 28497y^7 \\ & + 23045y^6 + 29265y^5 + \ 32212y^4 + 8948y^3 + 16460y^2 \\ & + 19357y + 9600, 26426y^8 + 24119y^7 + \ 48429y^6 + 34031y^5 \\ & + 32994y^4 + 13559y^3 + 34993y^2 + 59636y + 64778, y), x_3\big).\end{aligned}$$

We note that using the non-sparse homotopy algorithm from [17] produces a degree bound of 24, a considerable over estimate of the number of isolated zeros.

7 Topics for future research

We have presented a new homotopy algorithm for determining isolated solutions of algebraic sets $V_p(\boldsymbol{F}, \boldsymbol{g})$ for $\boldsymbol{F}$ a $p \times q$ matrix and $\boldsymbol{g}$ a vector having entries from a multivariate polynomial domain. Our algorithm determines the bounds central to homotopy algorithms based on the column support of the matrix $\boldsymbol{F}$. Our column supported homotopy algorithm can be applied to the case where our entries come from a weighted polynomial domain. Such weighted domains arise when we determine the isolated critical points of a symmetric function ϕ defined over a variety $V(\boldsymbol{f})$ generated by symmetric functions in $\boldsymbol{f}$. The resulting complexity is improved by a factor depending on the size of the symmetric group.

Still regarding critical point computations, but for non symmetic input $\boldsymbol{F}, \boldsymbol{g}$, the natural bounds for a sparse homotopy would come from considering the row support rather than the column support of $\boldsymbol{F}$. An interesting approach would be the follow the algorithm given in [17] for dense polynomials. However, proving that in the sparse case, the corresponding start systems satisfy the genericity properties we need is not straightforward; this is the subject of future work.

Acknowledgements. G. Labahn is supported by the Natural Sciences and Engineering Research Council of Canada (NSERC), grant number RGPIN-2020-04276. É. Schost is supported by an NSERC Discovery Grant. T.X. Vu is supported by a labex CalsimLab fellowship/scholarship. The labex CalsimLab, reference ANR-11-LABX-0037-01, is funded by the program "Investissements d'avenir" of the Agence Nationale de la Recherche, reference ANR-11-IDEX-0004-02. M. Safey El Din and T.X. Vu are supported by the ANR grants ANR-18-CE33-0011 Sesame, ANR-19-CE40-0018 De Rerum Natura and ANR-19-CE48-0015 ECARP, the PGMO grant CAMiSAdo and the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement N. 813211 (POEMA).

References

[1] M.-E. Alonso, E. Becker, M.-F. Roy, and T. Wörmann. Zeros, multiplicities, and idempotents for zero-dimensional systems. In *Algorithms in Algebraic Geometry and Applications*, pages 1–15. Springer, 1996.

[2] B. Bank, M. Giusti, J. Heintz, G. Lecerf, G. Matera, and P. Solernó. Degeneracy loci and polynomial equation solving. *Foundations of Computational Mathematics*, 15(1):159–184, 2015.

[3] B. Bank, M. Giusti, J. Heintz, and Luis M. Pardo. Generalized polar varieties and an efficient real elimination. *Kybernetika*, 40(5):519–550, 2004.

[4] B. Bank, M. Giusti, J. Heintz, and Luis M. Pardo. Generalized polar varieties: Geometry and algorithms. *Journal of Complexity*, 21(4):377–412, 2005.

[5] Aharon Gavriel Beged-Dov. Lower and upper bounds for the number of lattice points in a simplex. *SIAM Journal on Applied Mathematics*, 22(1):106–108, 1972.

[6] D. N. Bernstein. The number of roots of a system of equations. *Funkcional. Anal. i Priložen.*, 9(3):1–4, 1975.

[7] A. Bompadre, G. Matera, R. Wachenchauzer, and A. Waissbein. Polynomial equation solving by lifting procedures for ramified fibers. *Theoretical Computer Science*, 315(2-3):335–369, May 2004.

[8] D.A. Cox, J. Little, and D. O'Shea. *Using Algebraic Geometry*, volume 185. Springer Science & Business Media, 2006.

[9] D. Eisenbud. *Commutative Algebra: with a View Toward Algebraic Geometry*. Graduate Texts in Mathematics. Springer, New York, Berlin, Heildelberg, 1995.

[10] J-C. Faugère, G. Labahn, M. Safey El Din, É. Schost, and T.X. Vu. Computing critical points for invariant algebraic systems. 2020.

[11] J-C. Faugère, M. Safey El Din, and P-J. Spaenlehauer. Computing loci of rank defects of linear matrices using Gröbner bases and applications to cryptology. In *Proceedings of the 2010 International Symposium on Symbolic and Algebraic Computation*, pages 257–264, 2010.

[12] J-C. Faugère, M. Safey El Din, and P-J. Spaenlehauer. Critical points and Gröbner bases: the unmixed case. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, pages 162–169, 2012.

[13] P. Gianni and T. Mora. Algebraic solution of systems of polynomial equations using Groebner bases. In *AAECC*, volume 356 of *LNCS*, pages 247–257. Springer, 1989.

[14] M. Giusti, J. Heintz, J.-E. Morais, J. Morgenstern, and L.-M. Pardo. Straight-line programs in geometric elimination theory. *J. of Pure and Applied Algebra*, 124:101–146, 1998.

[15] M. Giusti, J. Heintz, J.-E. Morais, and L.-M. Pardo. When polynomial equation systems can be solved fast? In *AAECC-11*, volume 948 of *LNCS*, pages 205–231. Springer, 1995.

[16] M. Giusti, G. Lecerf, and B. Salvy. A Gröbner-free alternative for polynomial system solving. *Journal of Complexity*, 17(1):154–211, 2001.

[17] J.D. Hauenstein, M. Safey El Din, É. Schost, and T.X. Vu. Solving determinantal systems using homotopy techniques. 2019.

[18] J. Heintz, G. Jeronimo, J. Sabia, and P. Solerno. Intersection theory and deformation algorithms: the multi-homogeneous case, 2002.

[19] J. Heintz, T. Krick, S. Puddu, J. Sabia, and A. Waissbein. Deformation techniques for efficient polynomial equation solving. *Journal of Complexity*, 16(1):70 – 109, 2000.

[20] M. I. Herrero, G. Jeronimo, and J. Sabia. Computing isolated roots of sparse polynomial systems in affine space. *Theoretical Computer Science*, 411(44):3894 – 3904, 2010.

[21] M. I. Herrero, G. Jeronimo, and J. Sabia. Affine solution sets of sparse polynomial systems. *Journal of Symbolic Computation*, 51:34 – 54, 2013.

[22] M. I. Herrero, G. Jeronimo, and J. Sabia. Elimination for generic sparse polynomial systems. *Discrete and Computational Geometry*, 51(3):578–599, 2014.

[23] B. Huber and B. Sturmfels. A polyhedral method for solving sparse polynomial systems. *Mathematics of Computation.*, 64(212):1541–1555, October 1995.

[24] D. James. A global weighted version of Bézout's theorem. *The Arnoldfest (Toronto, ON, 1997)*, 24:115–129, 1999.

[25] G. Jeronimo, G. Matera, P. Solernó, and A. Waissbein. Deformation techniques for sparse systems. *Foundations of Computational Mathematics.*, 9(1):1–50, 2009.

[26] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *Journal für die Reine und Angewandte Mathematik*, 92:1–122, 1882.

[27] F. S. Macaulay. *The Algebraic Theory of Modular Systems.* Cambridge University Press, 1916.

[28] F. Rouillier. Solving zero-dimensional systems through the Rational Univariate Representation. *Applicable Algebra in Engineering, Communication and Computing*, 9(5):433–461, 1999.

[29] M. Safey El Din and É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *Journal of ACM*, 63(6):1–48, 2017.

[30] M. Safey El Din and É. Schost. Bit complexity for multi-homogeneous polynomial system solving - application to polynomial minimization. *Journal of Symbolic Computation*, 87:176–206, 2018.

[31] M. Safey El Din and P-J. Spaenlehauer. Critical point computations on smooth varieties: degree and complexity bounds. In *Proceedings of the ACM on International Symposium on Symbolic and Algebraic Computation*, pages 183–190, 2016.

[32] P-J. Spaenlehauer. On the complexity of computing critical points with Gröbner bases. *SIAM Journal on Optimization*, 24(3):1382–1401, 2014.

[33] S.S.-T. Yau and L. Zhang. An upper estimate on integral points in real simplices with an application in singularity theory. *Mathematical Research Letters*, 6:911–921, 2006.