Real root finding for rank defects in linear Hankel matrices

Didier Henrion[1,2,3] Simone Naldi[1,2] Mohab Safey El Din[4,5,6,7]

February 9, 2015

Abstract

Let $H_0, \ldots, H_n$ be $m \times m$ matrices with entries in $\mathbb{Q}$ and Hankel structure, i.e. constant skew diagonals. We consider the linear Hankel matrix $H(\mathbf{x}) = H_0 + x_1 H_1 + \cdots + x_n H_n$ and the problem of computing sample points in each connected component of the real algebraic set defined by the rank constraint $\mathsf{rank}(H(\mathbf{x})) \leq r$, for a given integer $r \leq m-1$. Computing sample points in real algebraic sets defined by rank defects in linear matrices is a general problem that finds applications in many areas such as control theory, computational geometry, optimization, etc. Moreover, Hankel matrices appear in many areas of engineering sciences. Also, since Hankel matrices are symmetric, any algorithmic development for this problem can be seen as a first step towards a dedicated exact algorithm for solving semi-definite programming problems, i.e. linear matrix inequalities. Under some genericity assumptions on the input (such as smoothness of an incidence variety), we design a probabilistic algorithm for tackling this problem. It is an adaptation of the so-called critical point method that takes advantage of the special structure of the problem. Its complexity reflects this: it is essentially quadratic in specific degree bounds on an incidence variety. We report on practical experiments and analyze how the algorithm takes advantage of this special structure. A first implementation outperforms existing implementations for computing sample points in general real algebraic sets: it tackles examples that are out of reach of the state-of-the-art.

[1]CNRS, LAAS, 7 avenue du colonel Roche, F-31400 Toulouse; France.
[2]Université de Toulouse; LAAS, F-31400 Toulouse, France.
[3]Faculty of Electrical Engineering, Czech Technical University in Prague, Czech Republic.
[4]Sorbonne Universités, UPMC Univ Paris 06, Equipe PolSys, LIP6, F-75005, Paris, France.
[5]INRIA Paris-Rocquencourt, PolSys Project, France.
[6]CNRS, UMR 7606, LIP6, France.
[7]Institut Universitaire de France.

1 Introduction

Problem statement and motivation Let $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ be respectively the fields of rational, real and complex numbers, and let m, n be positive integers. Given $m \times m$ matrices $H_0, H_1, \ldots, H_n$ with entries in $\mathbb{Q}$ and Hankel structure, i.e. constant skew diagonals, we consider the *linear Hankel matrix* $H(\mathbf{x}) = H_0 + x_1 H_1 + \ldots + x_n H_n$, denoted H for short, and the algebraic set

$$\mathcal{H}_r = \{\mathbf{x} \in \mathbb{C}^n : \operatorname{rank} H(\mathbf{x}) \leq r\}.$$

The goal of this paper is to provide an efficient algorithm for computing at least one sample point per connected component of the real algebraic set $\mathcal{H}_r \cap \mathbb{R}^n$.

Such an algorithm can be used to solve the matrix rank minimization problem for H. Matrix rank minimization mostly consists of minimizing the rank of a given matrix whose entries are subject to constraints defining a convex set. These problems arise in many engineering or statistical modeling applications and have recently received a lot of attention. Considering Hankel structures is relevant since it arises in many applications (e.g. for model reduction in linear dynamical systems described by Markov parameters, see [16, Section 1.3]).

Moreover, an algorithm for computing sample points in each connected component of $\mathcal{H}_r \cap \mathbb{R}^n$ can also be used to decide the emptiness of the feasibility set $S = \{\mathbf{x} \in \mathbb{R}^n : H(\mathbf{x}) \succeq 0\}$. Indeed, considering the minimum rank r attained in the boundary of S, it is easy to prove that one of the connected components of $\mathcal{H}_r \cap \mathbb{R}^n$ is actually contained in S. Note also that such feasibility sets, also called Hankel spectrahedra, have recently attracted some attention (see e.g. [3]).

The intrinsic algebraic nature of our problem makes relevant the design of exact algorithms to achieve reliability. On the one hand, we aim at exploiting algorithmically the special Hankel structure to gain efficiency. On the other hand, the design of a special algorithm for the case of linear Hankel matrices can bring the foundations of a general approach to e.g. the symmmetric case which is important for semi-definite programming, i.e. solving linear matrix inequalities.

Related works and state-of-the-art Our problem consists of computing sample points in real algebraic sets. The first algorithm for this problem is due to Tarski but its complexity was not elementary recursive [23]. Next, Collins designed the Cylindrical Algebraic Decomposition algorithm [5]. Its complexity is doubly exponential in the number of variables which is far from being optimal since the number of connected components of a real algebraic set defined by n-variate polynomial equations of degree $\leq d$ is upper bounded by $O(d)^n$. Next, Grigoriev and Vorobjov [12] introduced the first algorithm based on critical point computations computing sample point in real algebraic sets within $d^{O(n)}$ arithmetic operations. This work has next been improved and generalized (see [2] and references therein) from the complexity viewpoint. We may apply these algorithms to our problem by computing all $(r+1)$-minors of the Hankel matrix and compute sample points in the real algebraic set defined by the vanishing of these minors. This is done in time $(\binom{m}{r+1}\binom{n+r}{r})^{O(1)} + r^{O(n)}$ however since the constant in the exponent is rather high, these algorithms did not lead to efficient implementations in practice. Hence, another series of works, still using the critical point method but aiming at designing algorithms that combine asymptotically optimal complexity and practical efficiency has been developed (see e.g. [1, 19, 11] and references therein).

Under regularity assumptions, these yield probabilistic algorithms running in time which is essentially $O(d^{3n})$ in the smooth case and $O(d^{4n})$ in the singular case (see [18]). Practically, these algorithms are implemented in the library RAGLIB which uses Gröbner bases computations (see [8, 22] about the complexity of computing critical points with Gröbner bases).

Observe that determinantal varieties such as $\mathcal{H}_r$ are generically singular (see [4]). Also the aforementioned algorithms do not exploit the structure of the problem. In [14], we introduced an algorithm for computing real points at which a *generic* linear square matrix of size m has rank $\leq m-1$, by exploiting the structure of the problem. However, because of the requested genericity of the input linear matrix, we cannot use it for linear Hankel matrices. Also, it does not allow to get sample points for a given, smaller rank deficiency.

Methodology and main results Our main result is an algorithm that computes sample points in each connected component of $\mathcal{H}_r \cap \mathbb{R}^n$ under some genericity assumptions on the entries of the linear Hankel matrix H (these genericity assumptions are made explicit below). Our algorithm exploits the Hankel structure of the problem. Essentially, its complexity is quadratic in a multilinear Bézout bound on the number of complex solutions. Moreover, we find that, heuristically, this bound is less than $\binom{m}{r+1}\binom{n+r}{r}\binom{n+m}{r}$. Hence, for subfamilies of the real root finding problem on linear Hankel matrices where the maximum rank allowed r is fixed, the complexity is essentially in $(nm)^{O(r)}$.

The very basic idea is to study the algebraic set $\mathcal{H}_r \subset \mathbb{C}^n$ as the Zariski closure of the projection of an incidence variety, lying in $\mathbb{C}^{n+r+1}$. This variety encodes the fact that the kernel of H has dimension $\geq m-r$. This lifted variety turns out to be generically smooth and equidimensional and defined by quadratic polynomials with multilinear structure. When these regularity properties are satisfied, we prove that computing one point per connected component of the incidence variety is sufficient to solve the same problem for the variety $\mathcal{H}_r \cap \mathbb{R}^n$. We also prove that these properties are generically satisfied. We remark that this method is similar to the one used in [14], but in this case it takes strong advantage of the Hankel structure of the linear matrix, as detailed in Section 2. This also reflects on the complexity of the algorithm and on practical performances.

Let C be a connected component of $\mathcal{H}_r \cap \mathbb{R}^n$, and and Π_1, π_1 be the canonical projections $\Pi_1 : (x_1, \ldots, x_n, y_1, \ldots, y_{r+1}) \to x_1$ and $\pi_1 : (x_1, \ldots, x_n) \to x_1$. We prove that in generic coordinates, either *(i)* $\pi_1(C) = \mathbb{R}$ or *(ii)* there exists a critical point of the restriction of Π_1 to the considered incidence variety. Hence, after a generic linear change of variables, the algorithm consists of two main steps: *(i)* compute the critical points of the restriction of Π_1 to the incidence variety and *(ii)* instantiating the first variable x_1 to a generic value and perform a recursive call following a geometric pattern introduced in [19].

This latter step (i) is actually performed by building the Lagrange system associated to the optimization problem whose solutions are the critical points of the restriction of π_1 to the incidence variety. Hence, we use the algorithm in [15] to solve it. One also observes heuristically that these Lagrange systems are typically zero-dimensional.

However, we were not able to prove this finiteness property, but we prove that it holds when we restrict the optimization step to the set of points $\mathbf{x} \in \mathcal{H}_r$ such that $\operatorname{rank} H(\mathbf{x}) = p$, for any $0 \leq p \leq r$. However, this is sufficient to conclude that there are finitely many critical points of the restriction of π_1 to $\mathcal{H}_r \cap \mathbb{R}^n$, and that the algorithm returns the output correctly.

When the Lagrange system has dimension 0, the complexity of solving its equations is essentially quadratic in the number of its complex solutions. As previously announced, by the structure of these systems one can deduce multilinear Bézout bounds on the number of solutions that are polynomial in nm when r is fixed, and polynomial in n when m is fixed. This complexity result outperforms the state-of-the-art algorithms. We finally remark that the complexity gain is reflected also in the first implementation of the algorithm, which allows to solve instances of our problem that are out of reach of the general algorithms implemented in RAGlib.

Structure of the paper The paper is structured as follows. Section 2 contains preliminaries about Hankel matrices and the basic notation of the paper; we also prove that our regularity assumptions are generic. In Section 3 we describe the algorithm and prove its correctness. This is done by using preliminary results proved in Sections 5 and 6. Section 4 contains the complexity analysis and bounds for the number of complex solutions of the output of the algorithm. Finally, Section 7 presents the results of our experiments on generic linear Hankel matrices, and comparisons with the state-of-the-art algorithms for the real root finding problem.

2 Notation and preliminaries

Basic notations We denote by $\mathrm{GL}(n, \mathbb{Q})$ (resp. $\mathrm{GL}(n, \mathbb{C})$) the set of $n \times n$ non-singular matrices with rational (resp. complex) entries. For a matrix $M \in \mathbb{C}^{m \times m}$ and an integer $p \leq m$, one denotes with $\operatorname{minors}(p, M)$ the list of determinants of $p \times p$ sub-matrices of M. We denote by M' the transpose matrix of M.

Let $\mathbb{Q}[\mathbf{x}]$ be the ring of polynomials on n variables $\mathbf{x} = (x_1, \ldots, x_n)$ and let $\mathbf{f} = (f_1, \ldots, f_p) \in \mathbb{Q}[\mathbf{x}]^p$ be a polynomial system. The common zero locus of the entries of $\mathbf{f}$ is denoted by $\mathcal{Z}(\mathbf{f}) \subset \mathbb{C}^n$, and its dimension with $\dim \mathcal{Z}(\mathbf{f})$. The ideal generated by $\mathbf{f}$ is denoted by $\langle \mathbf{f} \rangle$, while if $\mathcal{V} \subset \mathbb{C}^n$ is any set, the ideal of polynomials vanishing on $\mathcal{V}$ is denoted by $I(\mathcal{V})$, while the set of regular (resp. singular) points of $\mathcal{V}$ is denoted by $\operatorname{reg} \mathcal{V}$ (resp. $\operatorname{sing} \mathcal{V}$). If $\mathbf{f} = (f_1, \ldots, f_p) \subset \mathbb{Q}[\mathbf{x}]$, we denote by $D\mathbf{f} = (\partial f_i / \partial x_j)$ the Jacobian matrix of $\mathbf{f}$. We denote by $\operatorname{reg}(\mathbf{f}) \subset \mathcal{Z}(\mathbf{f})$ the subset where $D\mathbf{f}$ has maximal rank.

A set $\mathcal{E} \subset \mathbb{C}^n$ is locally closed if $\mathcal{E} = \mathcal{Z} \cap \mathscr{O}$ where $\mathcal{Z}$ is a Zariski closed set and $\mathscr{O}$ is a Zariski open set.

Let $\mathcal{V} = \mathcal{Z}(\mathbf{f}) \subset \mathbb{C}^n$ be a smooth equidimensional algebraic set, of dimension d, and let $\mathbf{g} \colon \mathbb{C}^n \to \mathbb{C}^p$ be an algebraic map. The set of critical points of the restriction of $\mathbf{g}$ to $\mathcal{V}$ is the solution set of $\mathbf{f}$ and of the $(n-d+p)-$minors of the matrix $D(\mathbf{f}, \mathbf{g})$, and it is denoted by $\mathrm{crit}\,(\mathbf{g}, \mathcal{V})$. Finally, if $\mathcal{E} \subset \mathcal{V}$ is a locally closed subset of $\mathcal{V}$, we denote by $\mathrm{crit}\,(\mathbf{g}, \mathcal{E}) = \mathcal{E} \cap \mathrm{crit}\,(\mathbf{g}, \mathcal{V})$.

Finally, for $M \in \mathrm{GL}(n, \mathbb{C})$ and $f \in \mathbb{Q}[\mathbf{x}]$, we denote by $f^M(\mathbf{x}) = f(M\,\mathbf{x})$, and if $\mathbf{f} = (f_1, \ldots, f_p) \subset \mathbb{Q}[\mathbf{x}]$ and $\mathcal{V} = \mathcal{Z}(\mathbf{f})$, by $\mathcal{V}^M = \mathcal{Z}(\mathbf{f}^M)$ where $\mathbf{f}^M = (f_1^M, \ldots, f_p^M)$.

Hankel structure Let $\{h_1, \ldots, h_{2m-1}\} \subset \mathbb{Q}$. The matrix $H = (h_{i+j-1})_{1 \leq i,j \leq m} \in \mathbb{Q}^{m \times m}$ is called a Hankel matrix, and we use the notation $H = \mathsf{Hankel}(h_1, \ldots, h_{2m-1})$. The structure of a Hankel matrix induces structure on its kernel. By [13, Theorem 5.1], one has that if H is a Hankel matrix of rank at most r, then there exists a non-zero vector $\mathbf{y} = (y_1, \ldots, y_{r+1}) \in \mathbb{Q}^{r+1}$ such that the columns of the $m \times (m-r)$ matrix

$$Y(\mathbf{y}) = \begin{bmatrix} \mathbf{y} & 0 & \ldots & 0 \\ 0 & \mathbf{y} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \ldots & 0 & \mathbf{y} \end{bmatrix}$$

generate a $(m-r)-$dimensional subspace of the kernel of H. We observe that $H\,Y(\mathbf{y})$ is also a Hankel matrix.

The product $H\,Y(\mathbf{y})$ can be re-written as a matrix-vector product $\tilde{H}\,y$, with $\tilde{H}$ a given rectangular Hankel matrix. Indeed, let $H = \mathsf{Hankel}(h_1, \ldots, h_{2m-1})$. Then, as previously observed, $H\,Y(\mathbf{y})$ is a rectangular Hankel matrix, of size $m \times (m-r)$, whose entries coincide with the entries of

$$\tilde{H}\,\mathbf{y} = \begin{bmatrix} h_1 & \ldots & h_{r+1} \\ \vdots & & \vdots \\ h_{2m-r-1} & \ldots & h_{2m-1} \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_{r+1} \end{bmatrix}.$$

Let $H(\mathbf{x})$ be a linear Hankel matrix. From [6, Corollary 2.2] we deduce that, for $p \leq r$, then the ideals $\langle \mathrm{minors}\,(p+1, H(\mathbf{x})) \rangle$ and $\left\langle \mathrm{minors}\,(p+1, \tilde{H}(\mathbf{x})) \right\rangle$ coincides. One deduces that $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{C}^n$ satisfies $\mathrm{rank}\,H(\mathbf{x}) = p$ if and only if it satisfies $\mathrm{rank}\,\tilde{H}(\mathbf{x}) = p$.

Basic sets We first recall that the linear matrix $H(\mathbf{x}) = H_0 + x_1 H_1 + \ldots + x_n H_n$, where each H_i is a Hankel matrix, is also a Hankel matrix. It is identified by the $(2m-1)(n+1)$ entries of the matrices H_i. Hence we often consider H as an element of $\mathbb{C}^{(2m-1)(n+1)}$. For $M \in \mathrm{GL}(n, \mathbb{Q})$, we denote by $H^M(\mathbf{x})$ the linear matrix $H(M\mathbf{x})$.

We define in the following the main algebraic sets appearing during the execution of our algorithm, given $H \in \mathbb{C}^{(2m-1)(n+1)}$, $0 \leq p \leq r$, $M \in \mathrm{GL}(n, \mathbb{C})$ and $\mathbf{u} = (u_1, \ldots, u_{p+1}) \in \mathbb{Q}^{p+1}$.

Incidence varieties. We consider the polynomial system

$$\begin{array}{rccc} \mathbf{f}(H^M, \mathbf{u}, p): & \mathbb{C}^n \times \mathbb{C}^{p+1} & \longrightarrow & \mathbb{C}^{2m-p-1} \times \mathbb{C} \\ & (\mathbf{x}, \mathbf{y}) & \longmapsto & \left((\tilde{H}(M\,\mathbf{x})\,\mathbf{y})', \mathbf{u}'\mathbf{y} - 1 \right) \end{array}$$

where $\tilde{H}$ has been defined in the previous section. We denote by $\mathscr{J}(H^M, \mathbf{u}, p) = \mathcal{Z}(\mathbf{f}_p(H^M, \mathbf{u})) \subset \mathbb{C}^{n+p+1}$ and simply $\mathscr{J} = \mathscr{J}(H^M, \mathbf{u}, p)$ and $\mathbf{f} = \mathbf{f}(H^M, \mathbf{u}, p)$ when p, H, M and $\mathbf{u}$ are clear. We also denote by $\mathcal{K}(H^M, \mathbf{u}, p) = \mathscr{J}(H^M, \mathbf{u}, p) \cap \{(\mathbf{x}, \mathbf{y}) \in \mathbb{C}^{n+p+1} : \operatorname{rank} H(\mathbf{x}) = p\}$.

Fibers. Let $\alpha \in \mathbb{Q}$. We denote by $\mathbf{f}_\alpha(H^M, \mathbf{u}, p)$ (or simply $\mathbf{f}_\alpha$) the polynomial system obtained by adding $x_1 - \alpha$ to $\mathbf{f}(H^M, \mathbf{u}, p)$. The resulting algebraic set $\mathcal{Z}(\mathbf{f}_\alpha)$, denoted by $\mathscr{J}_\alpha$, equals $\mathscr{J} \cap \mathcal{Z}(x_1 - \alpha)$.

Lagrange systems. Let $\mathbf{v} \in \mathbb{Q}^{2m-p}$. Let $D_1\mathbf{f}$ denote the matrix of size $c \times (n+p)$ obtained by removing the first column of $D\,\mathbf{f}$ (the derivative w.r.t. x_1), and define $\ell = \ell(H^M, \mathbf{u}, \mathbf{v}, p)$ as the map

$$\begin{array}{rccc} \ell: & \mathbb{C}^{n+2m+1} & \to & \mathbb{C}^{n+2m+1} \\ & (\mathbf{x}, \mathbf{y}, \mathbf{z}) & \mapsto & (\tilde{H}(M\,\mathbf{x})\,\mathbf{y}, \mathbf{u}'\mathbf{y} - 1, \mathbf{z}' D_1\mathbf{f}, \mathbf{v}'\mathbf{z} - 1) \end{array}$$

where $\mathbf{z} = (z_1, \ldots, z_{2m-p})$ stand for Lagrange multipliers. We finally define $\mathcal{Z}(H^M, \mathbf{u}, \mathbf{v}, p) = \mathcal{Z}(\ell(H^M, \mathbf{u}, \mathbf{v}, p)) \subset \mathbb{C}^{n+2m+1}$.

Regularity property G We say that a polynomial system $\mathbf{f} \in \mathbb{Q}[x]^c$ satisfies Property G if the Jacobian matrix $D\,\mathbf{f}$ has maximal rank at any point of $\mathcal{Z}(\mathbf{f})$. We remark that this implies that:

1. the ideal $I(\mathbf{f})$ is radical;
2. the set $\mathcal{Z}(\mathbf{f})$ is either empty or smooth and equidimensional of co-dimension c.

We say that $\ell(H^M, \mathbf{u}, \mathbf{v}, p)$ satisfies G over $\mathcal{K}(H^M, \mathbf{u}, p)$ if the following holds: for $(\mathbf{x}, \mathbf{y}, \mathbf{z}) \in \mathcal{Z}(H^M, \mathbf{u}, \mathbf{v}, p)$ such that $(\mathbf{x}, \mathbf{y}) \in \mathcal{K}(H^M, \mathbf{u}, p)$, the matrix $D\,(\ell(H^M, \mathbf{u}, \mathbf{v}, p))$ has maximal rank at $(\mathbf{x}, \mathbf{y}, \mathbf{z})$.

Let $\mathbf{u} \in \mathbb{Q}^{p+1}$. We say that $H \in \mathbb{C}^{(2m-1)(n+1)}$ satisfies Property G if $\mathbf{f}(H, \mathbf{u}, p)$ satisfies Property G for all $0 \leq p \leq r$.

The first result essentially shows that G holds for $\mathbf{f}(H^M, \mathbf{u}, p)$ (resp. $\mathbf{f}_\alpha(H^M, \mathbf{u}, p)$) when the input parameter H (resp. α) is generic enough.

Proposition 1 *Let $M \in \mathrm{GL}(n, \mathbb{C})$.*

(a) There exists a non-empty Zariski-open set $\mathscr{H} \subset \mathbb{C}^{(2m-1)(n+1)}$ such that, if $H \in \mathscr{H} \cap \mathbb{Q}^{(2m-1)(n+1)}$, for all $0 \leq p \leq r$ and $\mathbf{u} \in \mathbb{Q}^{p+1} - \{\mathbf{0}\}$, $\mathbf{f}(H^M, \mathbf{u}, p)$ satisfies Property G;

(b) for $H \in \mathscr{H}$, and $0 \leq p \leq r$, if $\mathscr{J}(H^M, \mathbf{u}, p) \neq \emptyset$ then $\dim \mathcal{H}_p \leq n - 2m + 2p + 1$;

(c) For $0 \leq p \leq r$ and $\mathbf{u} \in \mathbb{Q}^{p+1}$, if $\mathbf{f}(H^M, \mathbf{u}, p)$ satisfies G, there exists a non-empty Zariski open set $\mathscr{A} \subset \mathbb{C}$ such that, if $\alpha \in \mathscr{A}$, the polynomial system $\mathbf{f}_\alpha$ satisfies G;

Proof : Without loss of generality, we can assume that $M = \mathrm{I}_n$. We let $0 \leq p \leq r$, $\mathbf{u} \in \mathbb{Q}^{p+1} - \{\mathbf{0}\}$ and recall that we identify the space of linear Hankel matrices with

$\mathbb{C}^{(2m-1)(n+1)}$. This space is endowed by the variables $\mathfrak{h}_{k,\ell}$ with $1 \leq k \leq 2m-1$ and $0 \leq \ell \leq n$; the generic linear Hankel matrix is then given by $\mathfrak{H} = \mathfrak{H}_0 + x_1\mathfrak{H}_1 + \cdots + x_n\mathfrak{H}_n$ with $\mathfrak{H}_i = \mathsf{Hankel}(\mathfrak{h}_{1,i}, \ldots, \mathfrak{h}_{2m-1,i})$.

We consider the map

$$q: \begin{array}{ccc} \mathbb{C}^{n+(p+1)+(2m-1)(n+1)} & \longrightarrow & \mathbb{C}^{2m-p} \\ (\mathbf{x}, \mathbf{y}, H) & \longmapsto & \mathbf{f}(H, \mathbf{u}, p) \end{array}$$

and, for a given $H \in \mathbb{C}^{(2m-1)(n+1)}$, its section-map $q_H : \mathbb{C}^{n+(p+1)} \to \mathbb{C}^{2m-p}$ sending $(\mathbf{x}, \mathbf{y})$ to $q(\mathbf{x}, \mathbf{y}, H)$. We also consider the map $\tilde{q}$ which associates to $(\mathbf{x}, \mathbf{y}, H)$ the entries of $\tilde{H}\mathbf{y}$ and its section map $\tilde{q}_H$; we will consider these latter maps over the open set $O = \{(\mathbf{x}, \mathbf{y}) \in \mathbb{C}^{n+p+1} \mid \mathbf{y} \neq \mathbf{0}\}$. We prove below that $\mathbf{0}$ is a regular value for both q_H and $\tilde{q}_H$.

Suppose first that $q^{-1}(\mathbf{0}) = \emptyset$ (resp. $\tilde{q}^{-1}(\mathbf{0})$). We deduce that for all $H \in \mathbb{C}^{(2m-1)(n+1)}$, $q_H^{-1}(\mathbf{0}) = \emptyset$ (resp $\tilde{q}_H^{-1}(\mathbf{0}) = \emptyset$) and $\mathbf{0}$ is a regular value for both maps q_H and $\tilde{q}_H$. Note also that taking $\mathscr{H} = \mathbb{C}^{(2m-1)(n+1)}$, we deduce that $\mathbf{f}(H, \mathbf{u}, p)$ satisfies G.

Now, suppose that $q^{-1}(\mathbf{0})$ is not empty and let $(\mathbf{x}, \mathbf{y}, H) \in q^{-1}(0)$. Consider the Jacobian matrix $D\,q$ of the map q with respect to the variables $\mathbf{x}, \mathbf{y}$ and the entries of H, evaluated at $(\mathbf{x}, \mathbf{y}, H)$. We consider the submatrix of $D\,q$ by selecting the column corresponding to:

- the partial derivatives with respect to $\mathfrak{h}_{1,0}, \ldots, \mathfrak{h}_{2m-1,0}$;
- the partial derivatives with respect to $y_1, \ldots, y_{p+1}$.

We obtain a $(2m-p) \times (2m+p)$ submatrix of $D\,q$; we prove below that it has full rank $2m-p$.

Indeed, remark that the $2m-p-1$ first lines correspond to the entries of $\tilde{H}\mathbf{y}$ and last line corresponds to the derivatives of $\mathbf{u}'\mathbf{y} - 1$. Hence, the structure of this submatrix is as below

$$\begin{bmatrix} y_1 & \ldots & y_{p+1} & 0 & \ldots & 0 & 0 & \cdots & 0 \\ 0 & y_1 & \ldots & y_{p+1} & \ldots & 0 & & & \\ \vdots & & \ddots & & \ddots & & \vdots & & \vdots \\ \vdots & & & y_1 & \ldots & y_{p+1} & 0 & & 0 \\ 0 & & \cdots & & \cdots & 0 & u_1 & \cdots & u_{p+1} \end{bmatrix}$$

Since this matrix is evaluated at the solution set of $\mathbf{u}'\mathbf{y} - 1 = 0$, we deduce straightforwardly that one entry of $\mathbf{u}$ and one entry of $\mathbf{y}$ are non-zero and that the above matrix is full rank and that $\mathbf{0}$ is a regular value of the map q.

We can do the same for $D\,\tilde{q}$ except the fact that we do not consider the partial derivatives with respect to $y_1, \ldots, y_{p+1}$. The $(2m-p-1) \times (2m-1)$ submatrix we obtain corresponds to the upper left block containing the entries of $\mathbf{y}$. Since $\tilde{q}$ is defined over the open set O in which $\mathbf{y} \neq \mathbf{0}$, we also deduce that this submatrix has full rank $2m-p-1$.

By Thom's Weak Transversality Theorem one deduces that there exists a non-empty Zariski open set $\mathscr{H}_p \subset \mathbb{C}^{(2m-1)(n+1)}$ such that if $H \in \mathscr{H}_p$, then $\mathbf{0}$ is a regular value of q_H (resp. $\tilde{q}_H$). We deduce that for $H \in \mathscr{H}_p$, the polynomial system $\mathbf{f}(H, \mathbf{u}, p)$ satisfies

G and using the Jacobian criterion [7, Theorem 16.19], $\mathcal{J}(H, \mathbf{u}, p)$ is either empty or smooth equidimensional of dimension $n - 2m + 2p + 1$. This proves assertion (a), with $\mathscr{H} = \bigcap_{0 \leq p \leq r} \mathscr{H}_p$.

Similarly, we deduce that $\tilde{q}_H^{-1}(\mathbf{0})$ is either empty or smooth and equidimensional of dimension $n - 2m + 2p + 2$. Let $\Pi_{\mathbf{x}}$ be the canonical projection $(\mathbf{x}, \mathbf{y}) \to \mathbf{x}$; note that for any $\mathbf{x} \in \mathcal{H}_r$, the dimension of $\Pi_{\mathbf{x}}^{-1}(x) \cap \tilde{q}_H^{-1}(\mathbf{0})$ is ≥ 1 (by homogeneity of the $\mathbf{y}$-variables). By the Theorem on the Dimension of Fibers [21, Sect.6.3,Theorem 7], we deduce that $n - 2m + 2p + 2 - \dim(\mathcal{H}_p) \geq 1$. We deduce that for $H \in \mathscr{H}$, $\dim(\mathcal{H}_p) \leq n - 2m + 2p + 1$ which proves assertion (b).

It remains to prove assertion (c). We assume that $\mathbf{f}(H, \mathbf{u}, p)$ satisfies G. Consider the restriction of the map $\Pi_1 \colon \mathbb{C}^{n+p+1} \to \mathbb{C}$, $\Pi_1(\mathbf{x}, \mathbf{y}) = x_1$, to $\mathcal{J}(H, \mathbf{u}, p)$, which is smooth and equidimensional by assertion (a).

By Sard's Lemma [20, Section 4.2], the set of critical values of the restriction of Π_1 to $\mathcal{J}(H, \mathbf{u}, p)$ is finite. Hence, its complement $\mathscr{A} \subset \mathbb{C}$ is a non-empty Zariski open set. We deduce that for $\alpha \in \mathscr{A}$, the Jacobian matrix of $\mathbf{f}_\alpha(H, \mathbf{u}, p)$ satisfies G. □

3 Algorithm and correctness

In this section we present the algorithm, which is called LowRankHankel, and prove its correctness.

3.1 Description

Data representation The algorithm takes as *input* a couple (H, r), where $H = (H_0, H_1, \ldots, H_n)$ encodes $m \times m$ Hankel matrices with entries in $\mathbb{Q}$, defining the linear matrix $H(\mathbf{x})$, and $0 \leq r \leq m - 1$.

The *output* is represented by a rational parametrization, that is a polynomial system

$$\mathbf{q} = (q_0(t), q_1(t), \ldots, q_n(t), q(t)) \subset \mathbb{Q}[t]$$

of univariate polynomials, with $gcd(q, q_0) = 1$. The set of solutions of

$$x_i - q_i(t)/q_0(t) = 0, \ i = 1 \ldots n \qquad q(t) = 0$$

is clearly finite and expected to contain at least one point per connected component of the algebraic set $\mathcal{H}_r \cap \mathbb{R}^n$.

Main subroutines and formal description We start by describing the main subroutines we use.

ZeroDimSolve. It takes as input a polynomial system defining an algebraic set $\mathcal{Z} \subset \mathbb{C}^{n+k}$ and a subset of variables $\mathbf{x} = (x_1, \ldots, x_n)$. If $\mathcal{Z}$ is finite, it returns a rational parametrization of the projection of $\mathcal{Z}$ on the $\mathbf{x}$-space else it returns an empty list.

ZeroDimSolveMaxRank. It takes as input a polynomial system $\mathbf{f} = (f_1, \ldots, f_c)$ such that $Z = \{\mathbf{x} \in \mathbb{C}^{n+k} \mid \mathsf{rank}(D\,\mathbf{f}(\mathbf{x})) = c\}$ is finite and a subset of variables $\mathbf{x} = (x_1, \ldots, x_n)$ that endows $\mathbb{C}^n$. It returns fail: the assumptions are not satisfied if assumptions are not satisfied, else it returns a rational parametrization of the projection of $\mathscr{Z}$ on the $\mathbf{x}$-space.

Lift. It takes as input a rational parametrization of a finite set $\mathscr{Z} \subset \mathbb{C}^N$ and a number $\alpha \in \mathbb{C}$, and it returns a rational parametrization of $\{(\alpha, \mathbf{x}) : \mathbf{x} \in \mathscr{Z}\}$.

Union. It takes as input two rational parametrizations encoding finite sets $\mathscr{Z}_1, \mathscr{Z}_2$ and it returns a rational parametrization of $\mathscr{Z}_1 \cup \mathscr{Z}_2$.

ChangeVariables. It takes as input a rational parametrization of a finite set $\mathscr{Z} \subset \mathbb{C}^N$ and a non-singular matrix $M \in \mathrm{GL}(N, \mathbb{C})$. It returns a rational parametrization of $\mathscr{Z}^M$.

The algorithm LowRankHankel is recursive, and it assumes that its input H satisfies Property G.

LowRankHankel(H, r):

1. If $n < 2m - 2r - 1$ then return [ ].
2. Choose randomly $M \in \mathrm{GL}(n, \mathbb{Q})$, $\alpha \in \mathbb{Q}$ and $\mathbf{u}_p \in \mathbb{Q}^{p+1}$, $\mathbf{v}_p \in \mathbb{Q}^{2m-p}$ for $0 \leq p \leq r$.
3. If $n = 2m - 2r - 1$ then return ZeroDimSolve$(\mathbf{f}(H, \mathbf{u}_r, r), \mathbf{x})$).
4. Let P = ZeroDimSolve$(\ell(\mathbf{f}(H, \mathbf{u}_r, r), \mathbf{v}))$
5. If P = [] then for p from 0 to r do
    (a) P′ = ZeroDimSolveMaxRank$(\ell(H^M, \mathbf{u}_p, \mathbf{v}_p), \mathbf{x})$;
    (b) P = Union(P, P′)
6. Q = Lift(LowRankHankel(Subs$(x_1 = \alpha, H^M), r), \alpha)$;
7. return(ChangeVariables(Union(Q, P), M^{-1})).

3.2 Correctness

The correctness proof is based on the two following results that are proved in Sections 5 and 6.

The first result states that when the input matrix H satisfies G and that, for a generic choice of M and $\mathbf{v}$, and for all $0 \leq p \leq r$, the set of solutions $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ to $\ell(H^M, \mathbf{u}, \mathbf{v}, p)$ at which rank $\tilde{H}(x) = p$ is finite and contains crit $(\pi_1, \mathcal{K}(H^M, \mathbf{u}, p))$.

Proposition 2 *Let $\mathscr{H}$ be the set defined in Proposition 1 and let $H \in \mathscr{H}$ and $\mathbf{u} \in \mathbb{Q}^{p+1} - \{\mathbf{0}\}$ for $0 \leq p \leq r$. There exist non-empty Zariski open sets $\mathscr{M}_1 \subset \mathrm{GL}(n, \mathbb{C})$ and $\mathscr{V} \subset \mathbb{C}^{2m-p}$ such that if $M \in \mathscr{M}_1 \cap \mathbb{Q}^{n \times n}$ and $\mathbf{v} \in \mathscr{V} \cap \mathbb{Q}^{2m-p}$, the following holds:*

(a) $\ell(H^M, \mathbf{u}, \mathbf{v}, p)$ satisfies G over $\mathcal{K}(H^M, u, p)$;

(b) *the projection of* $\operatorname{reg}(\ell(H^M, \mathbf{u}, \mathbf{v}, p))$ *on the* $(\mathbf{x}, \mathbf{y})$*-space contains* $\operatorname{crit}(\Pi_1, \mathcal{K}(H^M, \mathbf{u}, p))$

Proposition 3 *Let* $H \in \mathscr{H}$, $0 \leq p \leq r$ *and* $d_p = n - 2m + 2p + 1$ *and* $\mathcal{C}$ *be a connected component of* $\mathcal{H}_p \cap \mathbb{R}^n$. *Then there exist non-empty Zariski open sets* $\mathscr{M}_2 \subset \mathrm{GL}(n, \mathbb{C})$ *and* $\mathscr{U} \subset \mathbb{C}^{p+1}$ *such that for any* $M \in \mathscr{M}_2 \cap \mathbb{Q}^{n \times n}$, $\mathbf{u} \in \mathscr{U} \cap \mathbb{Q}^{p+1}$, *the following holds:*

(a) *for* $i = 1, \ldots, d_p$, $\pi_i(\mathcal{C}^M)$ *is closed;*

(b) *for any* $\alpha \in \mathbb{R}$ *in the boundary of* $\pi_1(\mathcal{C}^M)$, $\pi_1^{-1}(\alpha) \cap \mathcal{C}^M$ *is finite;*

(c) *for any* $\mathbf{x} \in \pi_1^{-1}(\alpha) \cap \mathcal{C}^M$ *and* p *such that* $\operatorname{rank} \tilde{H}_p(\mathbf{x}) = p$, *there exists* $(\mathbf{x}, \mathbf{y}) \in \mathbb{R}^n \times \mathbb{R}^{p+1}$ *such that* $(\mathbf{x}, \mathbf{y}) \in \mathcal{J}(H^M, \mathbf{u}, p)$.

Our algorithm is probabilistic and its correctness depends on the validity of the choices that are made at Step 2. We make this assumption that we formalize below.

We need to distinguish the choices of $M, \mathbf{u}$ and $\mathbf{v}$ that are made in the different calls of LowRankHankel; each of these parameter must lie in a non-empty Zariski open set defined in Propositions 1, 2 and 3.

We assume that the input matrix H satisfies G; we denote it by $H^{(0)}$, where the super script indicates that no recursive call has been made on this input; similarly $\alpha^{(0)}$ denotes the choice of α made at Step 2 on input $H^{(0)}$. Next, we denote by $H^{(i)}$ the input of LowRankHankel at the i-th recursive call and by $\mathscr{A}^{(i)} \subset \mathbb{C}$ the non-empty Zariski open set defined in Proposition 1 applied to $H^{(i)}$. Note that if $\alpha^{(i)} \in \mathscr{A}^{(i)}$, we can deduce that $H^{(i+1)}$ satisfies G.

Now, we denote by $\mathscr{M}_1^{(i)}, \mathscr{M}_2^{(i)}$ and $\mathscr{U}^{(p,i)}, \mathscr{V}^{(p,i)}$ the open sets defined in Propositions 1, 2 and 3 applied to $H^{(i)}$, for $0 \leq p \leq r$ and where i is the depth of the recursion.

Finally, we denote by $M^{(i)} \in \mathrm{GL}(n, \mathbb{Q})$, $\mathbf{u}_p^{(i)} \in \mathbb{Q}^{p+1}$ and $\mathbf{v}_p^{(i)}$, for $0 \leq p \leq r$, respectively the matrix and the vectors chosen at Step 2 of the i-th call of LowRankHankel.

Assumption A. We say that A is satisfied if $M^{(i)}$, $\alpha^{(i)}$, $\mathbf{u}_p^{(i)}$ and $\mathbf{v}_p^{(i)}$ satisfy:

- $M^{(i)} \in (\mathscr{M}_1^{(i)} \cap \mathscr{M}_2^{(i)}) \cap \mathbb{Q}^{i \times i}$;
- $\alpha^{(i)} \in \mathscr{A}^{(i)}$.
- $\mathbf{u}_p^{(i)} \in \mathscr{U}^{(p,i)} \cap \mathbb{Q}^{p+1} - \{\mathbf{0}\}$, for $0 \leq p \leq r$;
- $\mathbf{v}_p^{(i)} \in \mathscr{V}^{(p,i)} \cap \mathbb{Q}^{2m-p} - \{\mathbf{0}\}$ for $0 \leq p \leq r$;

Theorem 4 *Let* H *satisfy* G. *Then, if* A *is satisfied,* LowRankHankel *with input* (H, r), *returns a rational parametrization that encodes a finite algebraic set in* $\mathcal{H}_r$ *meeting each connected component of* $\mathcal{H}_r \cap \mathbb{R}^n$.

Proof : The proof is by decreasing induction on the depth of the recursion.

When $n < 2m - 2r - 1$, $\mathcal{H}_r$ is empty since the input H satisfies G (since A is satisfied). In this case, the output defines the empty set.

When $n = 2m-2r-1$, since A is satisfied, by Proposition **??**, either $\mathcal{H}_r = \emptyset$ or dim $\mathcal{H}_r = 0$. Suppose $\mathcal{H}_r = \emptyset$. Hence $\mathcal{J}_r = \emptyset$, since the projection of $\mathcal{J}_r$ on the $\mathbf{x}-$space is included in $\mathcal{H}_r$. Suppose now that $\dim \mathcal{H}_r = 0$: Proposition 3 guarantees that the output of the algorithm defines a finite set containing $\mathcal{H}_r$.

Now, we assume that $n > 2m-2r-1$; our induction assumption is that for any $i \geq 1$ $\mathsf{LowRankHankel}(H^{(i)}, r)$ returns a rational parametrization that encodes a finite set of points in the algebraic set defined by $\mathsf{rank}(H^{(i)}) \leq r$ and that meets every connected component of its real trace.

Let C be a connected component of $\mathcal{H}_r \cap \mathbb{R}^n$. To keep notations simple, we denote by $M \in \mathrm{GL}(n, \mathbb{Q})$, $\mathbf{u}_p$ and $\mathbf{v}_p$ the matrix and vectors chosen at Step 2 for $0 \leq p \leq r$. Since A holds one can apply Proposition 3. We deduce that the image $\pi_1(C^M)$ is closed. Then, either $\pi_1(C^M) = \mathbb{R}$ or it is a closed interval.

Suppose first that $\pi_1(\mathcal{C}^M) = \mathbb{R}$. Then for $\alpha \in \mathbb{Q}$ chosen at Step 2, $\pi_1^{-1}(\alpha) \cap \mathcal{C}^M \neq 0$. Remark that $\pi_1^{-1}(\alpha) \cap C^M$ is the union of some connected components of $\mathcal{H}_r^{(1)} \cap \mathbb{R}^{n-1} = \{\mathbf{x} = (x_2, \ldots, x_n) \in \mathbb{R}^{n-1} : \mathrm{rank}\, H^{(1)}(\mathbf{x}) \leq r\}$. Since A holds, assertion (c) of Proposition 1 implies that $H^{(1)}$ satisfies G. We deduce by the induction assumption that the parametrization returned by Step 6 where $\mathsf{LowRankHankel}$ is called recursively defines a finite set of points that is contained in $\mathcal{H}_r$ and that meets C.

Suppose now that $\pi_1(C^M) \neq \mathbb{R}$. By Proposition 3, $\pi_1(C^M)$ is closed. Since C^M is connected, $\pi_1(C^M)$ is a connected interval, and since $\pi_1(C^M) \neq \mathbb{R}$ there exists β in the boundary of $\pi_1(C^M)$ such that $\pi_1(C^M) \subset [\beta, +\infty)$ or $\pi_1(C^M) \subset (-\infty, \beta]$. Suppose without loss of generality that $\pi_1(C^M) \subset [\beta, +\infty)$, so that β is the minimum value attained by π_1 on C^M.

Let $\mathbf{x} = (\beta, x_2, \ldots, x_n) \in C^M$, and suppose that $\mathrm{rank}(\tilde{H}(\mathbf{x})) = p$. By Proposition 3 (assertion (c)), there exists $\mathbf{y} \in \mathbb{C}^{p+1}$ such that $(\mathbf{x}, \mathbf{y}) \in \mathcal{J}(H, \mathbf{u}, p)$. Note that since $\mathrm{rank}(\tilde{H}(\mathbf{x})) = p$, we also deduce that $(\mathbf{x}, \mathbf{y}) \in \mathcal{K}(H, \mathbf{u}, p)$.

We claim that there exists $\mathbf{z} \in \mathbb{C}^{2m-p}$ such that $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ lies on $\mathrm{reg}\,(\ell(H^M, \mathbf{u}, \mathbf{v}, p))$.

Since A holds, Proposition 2 implies that $\ell(H^M, \mathbf{u}, \mathbf{v}, p)$ satisfies G over $\mathcal{K}(H^M, \mathbf{u}, p)$. Also, note that the Jacobian criterion implies that $\mathrm{reg}\,(\ell(H^M, \mathbf{u}, \mathbf{v}, p))$ has dimension at most 0. We conclude that the point $\mathbf{x} \in C^M$ lies on the finite set encoded by the rational parametrization P obtained at Step 5 of $\mathsf{LowRankHankel}$ and we are done.

It remains to prove our claim, i.e. there exists $\mathbf{z} \in \mathbb{C}^{2m-p}$ such that $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ lies on $\mathrm{reg}\,(\ell(H^M, \mathbf{u}, \mathbf{v}, p))$.

Let C' be the connected component of $\mathcal{J}(H, \mathbf{u}, p)^M \cap \mathbb{R}^{n+m(m-r)}$ containing $(\mathbf{x}, \mathbf{y})$. We first prove that $\beta = \pi_1(\mathbf{x}, \mathbf{y})$ lies on the boundary of $\pi_1(C')$. Indeed, suppose that there exists $(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}) \in C'$ such that $\pi_1(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}) < \beta$. Since C' is connected, there exists a continuous semi-algebraic map $\tau\colon [0,1] \to C'$ with $\tau(0) = (\mathbf{x}, \mathbf{y})$ and $\tau(1) = (\tilde{\mathbf{x}}, \tilde{\mathbf{y}})$. Let $\varphi : (\mathbf{x}, \mathbf{y}) \to \mathbf{x}$ be the canonical projection on the $\mathbf{x}$-space.

Note that $\varphi \circ \tau$ is also continuous and semi-algebraic (it is the composition of continuous semi-algebraic maps), with $(\varphi \circ \tau)(0) = \mathbf{x}$, $(\varphi \circ \tau)(1) = \tilde{\mathbf{x}}$. Since $(\varphi \circ \tau)(\theta) \in \mathcal{H}_p$ for all $\theta \in [0,1]$, then $\tilde{\mathbf{x}} \in C$. Since $\pi_1(\tilde{\mathbf{x}}) = \pi_1(\tilde{\mathbf{x}}, \tilde{\mathbf{y}}) < \alpha$ we obtain a contradiction. So $\pi_1(\mathbf{x}, \mathbf{y})$ lies on the boundary of $\pi_1(C')$.

By the Implicit Function Theorem, and the fact that $\mathbf{f}(H, \mathbf{u}, p)$ satisfies Property G, one deduces that $(\mathbf{x}, \mathbf{y})$ is a critical point of the restriction of $\Pi_1 : (x_1, \ldots, x_n, y_1, \ldots, y_{r+1}) \to x_1$ to $\mathcal{J}(H, \mathbf{u}, p)$.

Since $\mathsf{rank}(H^M(\mathbf{x})) = p$ by construction, we deduce that $(\mathbf{x}, \mathbf{y})$ is a critical point of the restriction of Π_1 to $\mathcal{K}(H^M, \mathbf{u}, p)$ and that, by Proposition 2, there exists $\mathbf{z} \in \mathbb{C}^{2m-p}$ such that $(\mathbf{x}, \mathbf{y}, \mathbf{z})$ belongs to the set $\mathrm{reg}\,(\ell(H^M, \mathbf{u}, \mathbf{v}, p))$, as claimed. □

4 Degree bounds and complexity

We first remark that the complexity of subroutines Union, Lift and ChangeVariables (see [20, Chap. 10]) are negligible with respect to the complexity of ZeroDimSolveMaxRank. Hence, the complexity of LowRankHankel is at most n times the complexity of ZeroDimSolveMaxRank, which is computed below.

Let (H, r) be the input, and let $0 \leq p \leq r$. We estimate the complexity of ZeroDimSolveMaxRank with input $(H^M, \mathbf{u}_p, \mathbf{v}_p)$. It depends on the algorithm used to solve zero-dimensional polynomial systems. We choose the one of [15] that can be seen as a symbolic homotopy taking into account the sparsity structure of the system to solve. More precisely, let $\mathbf{p} \subset \mathbb{Q}[x_1, \ldots, x_n]$ and $s \in \mathbb{Q}[x_1, \ldots, x_n]$ such that the common complex solutions of polynomials in $\mathbf{p}$ at which s does not vanish is finite. The algorithm in [15] builds a system $\mathbf{q}$ that has the same monomial structure as $\mathbf{p}$ has and defines a finite algebraic set. Next, the homotopy system $\mathbf{t} = t\mathbf{p} + (1-t)\mathbf{q}$ where t is a new variable is built. The system $\mathbf{t}$ defines a 1-dimensional constructible set over the open set defined by $s \neq 0$ and for generic values of t. Abusing notation, we denote by $Z(\mathbf{t})$ the curve defined as the Zariski closure of this constructible set.

Starting from the solutions of $\mathbf{q}$ which are encoded with a rational parametrization, the algorithm builds a rational parametrization for the solutions of $\mathbf{p}$ which do not cancel s. Following [15], the algorithm runs in time $O\tilde{~}(Ln^{O(1)}\delta\delta')$ where L is the complexity of evaluating the input, δ is a bound on the number of isolated solutions of $\mathbf{p}$ and δ' is a bound on the degree of $Z(\mathbf{t})$ defined by $\mathbf{t}$.

Below, we estimate these degrees when the input is a Lagrange system as the ones we consider.

Degree bounds. We let $((\tilde{H}\,\mathbf{y})', \mathbf{u}_p{}'\mathbf{y} - 1)$, with $\mathbf{y} = (y_1, \ldots, y_{p+1})'$, defining $\mathcal{J}_p(H, \mathbf{u}_p)$. Since $\mathbf{y} \neq 0$, one can eliminate w.l.o.g. y_{p+1}, and the linear form $\mathbf{u}_p{}'\mathbf{y} - 1$, obtaining a system $\tilde{\mathbf{f}} \in \mathbb{Q}[\mathbf{x}, \mathbf{y}]^{2m-p-1}$. We recall that if $\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(c)}$ are c groups of variables, and $f \in \mathbb{Q}[\mathbf{x}^{(1)}, \ldots, \mathbf{x}^{(c)}]$, we say that the multidegree of f is $(d_1, \ldots, d_c)$ if its degree with respect to the group $\mathbf{x}^{(j)}$ is d_j, for $j = 1, \ldots, c$.

Let $\ell = (\tilde{\mathbf{f}}, \tilde{\mathbf{g}}, \tilde{\mathbf{h}})$ be the corresponding Lagrange system, where

$$(\tilde{\mathbf{g}}, \tilde{\mathbf{h}}) = (\tilde{g}_1, \ldots, \tilde{g}_{n-1}, \tilde{h}_1, \ldots, \tilde{h}_p) = \mathbf{z}' D_1 \tilde{\mathbf{f}}$$

with $\mathbf{z} = [1, z_2, \ldots, z_{2m-p-1}]$ a non-zero vector of Lagrange multipliers (we let $z_1 = 1$ w.l.o.g.). One obtains that ℓ is constituted by

- $2m - p - 1$ polynomials of multidegree bounded by $(1, 1, 0)$ with respect to $(\mathbf{x}, \mathbf{y}, \mathbf{z})$,

- $n-1$ polynomials of multidegree bounded by $(0,1,1)$ with respect to $(\mathbf{x},\mathbf{y},\mathbf{z})$,
- p polynomials of multidegree bounded by $(1,0,1)$ with respect to $(\mathbf{x},\mathbf{y},\mathbf{z})$,

that is by $n+2m-2$ polynomials in $n+2m-2$ variables.

Lemma 5 *With the above notations, the number of isolated solutions of $\mathcal{Z}(\ell)$ is at most*

$$\delta(m,n,p)=\sum_{\ell}\binom{2m-p-1}{n-\ell}\binom{n-1}{2m-2p-2+\ell}\binom{p}{\ell}$$

where $\ell\in\{\max\{0,n-2m+p+1\},\dots,\min\{p,n-2m+2p+1\}\}$.

Proof : By [20, Proposition 11.1], this degree is bounded by the multilinear Bézout bound $\delta(m,n,p)$ which is the sum of the coefficients of

$$(s_x+s_y)^{2m-p-1}(s_y+s_z)^{n-1}(s_x+s_z)^p\in\mathbb{Q}[s_x,s_y,s_z]$$

modulo $I=\left\langle s_x^{n+1},s_y^{p+1},s_z^{2m-p-1}\right\rangle$. The conclusion comes straightforwardly by technical computations. □

With input ℓ, the homotopy system $\mathbf{t}$ is constituted by $2m-p-1,n-1$ and p polynomials of multidegree respectively bounded by $(1,1,0,1),(0,1,1,1)$ and $(1,0,1,1)$ with respect to $(\mathbf{x},\mathbf{y},\mathbf{z},t)$. We prove the following.

Lemma 6 $\deg\mathcal{Z}(\mathbf{t})\in O(pn(2m-p)\delta(m,n,p))$.

Proof of Lemma 6: We use Multilinear Bézout bounds as in the proof of Lemma 5. The degree of $\mathcal{Z}(\mathbf{t})$ is bounded by the sum of the coefficients of

$$(s_x+s_y+s_t)^{2m-p-1}(s_y+s_z+s_t)^{n-1}(s_x+s_z+s_t)^p$$

modulo $I=\left\langle s_x^{n+1},s_y^{p+1},s_z^{2m-p-1},s_t^2\right\rangle\subset\mathbb{Q}[s_x,s_y,s_z,s_t]$. Since the variable s_t can appear up to power 1, the previous polynomial is congruent to $P_1+P_2+P_3+P_4$ modulo I, with

$$P_1=(s_x+s_y)^{2m-p-1}(s_y+s_z)^{n-1}(s_x+s_y)^p$$
$$P_2=(2m-p-1)s_t(s_x+s_y)^{2m-p-2}(s_y+s_z)^{n-1}\,(s_x+s_z)^p,$$
$$P_3=(n-1)s_t(s_y+s_z)^{n-2}(s_x+s_y)^{2m-p-1}(s_x+s_z)^p$$
$$P_4=p\,s_t(s_x+s_z)^{p-1}(s_x+s_y)^{2m-p-1}(s_y+s_z)^{n-1}.$$

We denote by $\Delta(P_i)$ the contribution of P_i to the previous sum.

Firstly, observe that $\Delta(P_1)=\delta(m,n,p)$ (compare with the proof of Lemma 5). Defining $\chi_1=\max\{0,n-2m+p+1\}$ and $\chi_2=\min\{p,n-2m+2p+1\}$, one has $\Delta(P_1)=\delta(m,n,p)=\sum_{\ell=\chi_1}^{\chi_2}\gamma(\ell)$ with $\gamma(\ell)=\binom{2m-p-1}{n-\ell}\binom{n-1}{2m-2p-2+\ell}\binom{p}{\ell}$.

Write now $P_2 = (2m-p-1)s_t\tilde{P}_2$, with $\tilde{P}_2 \in \mathbb{Q}[x,y,z]$. Let $\Delta(\tilde{P}_2)$ be the contribution of $\tilde{P}_2$, that is the sum of the coefficients of $\tilde{P}_2$ modulo $I' = \left\langle s_x^{n+1}, s_y^{p+1}, s_z^{2m-p-1}\right\rangle$, so that $\Delta(P_2) = (2m-p-1)\Delta(\tilde{P}_2)$. Then

$$\Delta(\tilde{P}_2) = \sum_{i,j,\ell} \binom{2m-p-2}{i}\binom{n-1}{j}\binom{p}{\ell}$$

where the sum runs in the set defined by the inequalities

$$i+\ell \leq n,\ \ 2m-p-2-i+j \leq p,\ \ n-1-j+p-\ell \leq 2m-p-2.$$

Now, since $\tilde{P}_2$ is homogeneous of degree $n+2m-3$, only three possible cases hold:

Case (A). $i+\ell = n$, $2m-p-2-i+j = p$ and $n-1-j+p-\ell = 2m-p-3$. Here the contribution is $\delta_a = \sum_{\ell=\alpha_1}^{\alpha_2} \varphi_a(\ell)$ with

$$\varphi_a(\ell) = \binom{2m-p-2}{n-\ell}\binom{n-1}{2m-2p-3+\ell}\binom{p}{\ell},$$

and $\alpha_1 = \max\{0, n-2m+p+2\}, \alpha_2 = \min\{p, n-2m+2p+2\}$. Suppose first that ℓ is an admissible index for $\Delta(P_1)$ and δ_a, that is $\max\{\chi_1,\alpha_1\} = \alpha_1 \leq \ell \leq \chi_2 = \min\{\chi_2,\alpha_2\}$. Then:

$$\begin{aligned}\varphi_a(\ell) \leq \binom{2m-p-1}{n-\ell}\binom{n-1}{2m-2p-3+\ell}\binom{p}{\ell} = \\ = \Psi(\ell)\gamma(\ell) \qquad \text{with } \Psi(\ell) = \frac{2m-2p-2+\ell}{n-(2m-2p-2+\ell)}.\end{aligned}$$

The rational function $\ell \longmapsto \Psi(\ell)$ is piece-wise monotone (its first derivative is positive), and its unique possible pole is $\ell = n-2m+2p+2$. Suppose that this value is a pole for $\Psi(\ell)$. This would imply $\alpha_2 = n-2m+2p+2$ and so $\chi_2 = n-2m+2p+1$; since ℓ is admissible for $\Delta(P_1)$, then one would conclude a contradiction. Hence the rational function $\Psi(\ell)$ has no poles, its maximum is atteined in χ_2 and its value is $\Psi(\chi_2) = n-1$. Hence $\varphi_a(\ell) \leq (n-1)\gamma(\ell)$. Now, we analyse any possible case:

(A1) $\chi_1 = 0, \alpha_1 = 0$. This implies $\chi_2 = n-2m+2p+1, \alpha_2 = n-2m+2p+2$. We deduce that

$$\begin{aligned}\delta_a = \sum_{\ell=0}^{\chi_2} \varphi_a(\ell) + \varphi_a(\alpha_2) \leq (n-1)\sum_{\ell=0}^{\chi_2}\gamma(\ell) + \\ + \varphi_a(\alpha_2) \leq (n-1)\Delta(P_1) + \varphi_a(\alpha_2).\end{aligned}$$

In this case we deduce the bound $\delta_a \leq n\Delta(P_1)$.

(A2) $\chi_1 = 0, \alpha_1 = n-2m+p+2$. This implies $\chi_2 = n-2m+2p+1, \alpha_2 = p$. In this case all indices are admissible, and hence we deduce the bound $\delta_a \leq (n-1)\Delta(P_1)$.

(A3) $\chi_1 = n-2m+p+1$. This implies $\alpha_1 = n-2m+p+2$, $\chi_2 = p, \alpha_2 = p$. Also in this case all indices are admissible, and $\delta_a \leq (n-1)\Delta(P_1)$.

Case (B). $i+\ell=n$, $2m-p-2-i+j=p-1$ and $n-1-j+p-\ell=2m-p-2$. Here the contribution is $\delta_b=\sum_\ell \varphi_b(\ell)$ where

$$\varphi_b(\ell)=\binom{2m-p-2}{n-\ell}\binom{n-1}{2m-2p-2+\ell}\binom{p}{\ell}.$$

One gets $\delta_b\le\Delta(P_1)$ since the sum above is defined in $\max\{0,n2m+p+2\}\le\ell\le\min\{p,n-2m+2p+1\}$, and the inequality $\varphi_b(\ell)\le\gamma(\ell)$ holds term-wise.

Case (C) $i+\ell=n-1$, $2m-p-2-i+j=p$ and $n-1-j+p-\ell=2m-p-2$. Here the contribution is $\delta_c=\sum_\ell \varphi_c(\ell)$ where

$$\varphi_c(\ell)=\binom{2m-p-2}{n-1-\ell}\binom{n-1}{2m-2p-2+\ell}\binom{p}{\ell}.$$

One gets $\delta_c\le\Delta(P_1)$ since the sum above is defined in $\max\{0,n2m+p+1\}\le\ell\le\min\{p,n-2m+2p+1\}$, and the inequality $\varphi_c(\ell)\le\gamma(\ell)$ holds term-wise. We conclude that $\delta_a\le n\Delta(P_1)$, $\delta_b\le\Delta(P_1)$ and $\delta_c\le\Delta(P_1)$. Hence $\Delta(P_2)=(2m-p-1)(\delta_a+\delta_b+\delta_c)\in O(n(2m-p)\Delta(P_1))$.

Analogously to $\Delta(P_2)$, one can conclude that $\Delta(P_3)\in O(n(n+2m-p)\Delta(P_1))$ and $\Delta(P_4)\in O(pn(n+2m-p)\Delta(P_1))$. □

Estimates.
We provide the whole complexity of ZeroDimSolveMaxRank.

Theorem 7 *Let $\delta=\delta(m,n,p)$ be given by Lemma 5. Then* ZeroDimSolveMaxRank *with input $\ell(H^M,\mathbf{u}_p,\mathbf{v}_p)$ computes a rational parametrization within*

$$O\tilde{~}(p(n+2m)^{O(1)}(2m-p)\delta^2),$$

arithmetic operations over $\mathbb{Q}$.

Proof : The polynomial entries of the system $\mathbf{t}$ (as defined in the previous section) are cubic polynomials in $n+2m-1$ variables, so the cost of their evaluation is in $O((n+2m)^3)$. Applying [15, Theorem 5.2] and bounds given in Lemma 5 and 6 yield the claimed complexity estimate. □

From Lemma 5, one deduces that for all $0\le p\le r$, the maximum number of complex solutions computed by ZeroDimSolveMaxRank is bounded above by $\delta(m,n,p)$. We deduce the following result.

Proposition 8 *Let H be a $m\times m$, $n-$variate linear Hankel matrix, and let $r\le m-1$. The maximum number of complex solutions computed by* LowRankHankel *with input (H,r) is*

$$\binom{2m-r-1}{r}+\sum_{k=2m-2r}^{n}\sum_{p=0}^{r}\delta(m,k,p).$$

where $\delta(m,k,p)$ is the bound defined in Lemma 5.

Proof : The maximum number of complex solutions computed by ZeroDimSolve is the degree of $\mathscr{J}(H, \mathbf{u}, r)$. Using, the multilinear Bézout bounds, this is bounded by the coefficient of the monomial $s_x^n s_y^r$ in the expression $(s_x + s_y)^{2m-r-1}$, that is exactly $\binom{2m-r-1}{r}$. The proof is now straightforward, since ZeroDimSolveMaxRank runs $r + 1$ times at each recursive step of LowRankHankel, and since the number of variables decreases from n to $2m - 2r$. $\square$

5 Proof of Proposition 2

We start with a local description of the algebraic sets defined by our Lagrange systems. This is obtained from a local description of the system defining $\mathscr{J}(H, \mathbf{u}, p)$. Without loss of generality, we can assume that $\mathbf{u} = (0, \ldots, 0, 1)$ in the whole section: such a situation can be retrieved from a linear change of the $\mathbf{y}$-variables that leaves invariant the $\mathbf{x}$-variables.

5.1 Local equations

Let $(\mathbf{x}, \mathbf{y}) \in \mathcal{K}(H, \mathbf{u}, p)$. Then, by definition, there exists a $p \times p$ minor of $\tilde{H}(\mathbf{x})$ that is non-zero. Without loss of generality, we assume that this minor is the determinant of the upper left $p \times p$ submatrix of $\tilde{H}$. Hence, consider the following block partition

$$\tilde{H}(\mathbf{x}) = \begin{bmatrix} N & Q \\ P & R \end{bmatrix} \tag{1}$$

with $N \in \mathbb{Q}[\mathbf{x}]^{p \times p}$, and $Q \in \mathbb{Q}[\mathbf{x}]^p$, $P \in \mathbb{Q}[\mathbf{x}]^{(2m-2p-1) \times p}$, and $R \in \mathbb{Q}[\mathbf{x}]^{2m-2p-1}$. We are going to exhibit suitable local descriptions of $\mathcal{K}(H, \mathbf{u}, p)$ over the Zariski open set $O_N \subset \mathbb{C}^{n+p+1}$ defined by $\det N \neq 0$; we denote by $\mathbb{Q}[\mathbf{x}, \mathbf{y}]_{\det N}$ the local ring of $\mathbb{Q}[\mathbf{x}, \mathbf{y}]$ localized by $\det N$.

Lemma 9 *Let N, Q, P, R be as above, and $\mathbf{u} \in \mathbb{Q}^{p+1} - \{\mathbf{0}\}$. Then there exist $\{q_i\}_{1 \leq i \leq p} \subset \mathbb{Q}[\mathbf{x}]_{\det N}$ and $\{\tilde{q}_i\}_{1 \leq i \leq 2m-2p-1} \subset \mathbb{Q}[\mathbf{x}]_{\det N}$ such that the constructible set $\mathcal{K}(H, \mathbf{u}, p) \cap O_N$ is defined by the equations*

$$\begin{aligned} y_i - q_i(\mathbf{x}) &= 0 \qquad 1 \leq i \leq p \\ \tilde{q}_i(\mathbf{x}) &= 0 \qquad 1 \leq i \leq 2m - 2p - 1 \\ y_{p+1} - 1 &= 0. \end{aligned}$$

Proof : Let $c = 2m - 2p - 1$. The proof follows by the equivalence

$$\begin{bmatrix} N & Q \\ P & R \end{bmatrix} \mathbf{y} = 0 \text{ iff } \begin{bmatrix} \mathrm{I}_p & 0 \\ -P & \mathrm{I}_c \end{bmatrix} \begin{bmatrix} N^{-1} & 0 \\ 0 & \mathrm{I}_c \end{bmatrix} \begin{bmatrix} N & Q \\ P & R \end{bmatrix} \mathbf{y} = 0$$

in the local ring $\mathbb{Q}[\mathbf{x}, \mathbf{y}]_{\det N}$, that is if and only if

$$\begin{bmatrix} \mathrm{I}_p & N^{-1}Q \\ 0 & R - PN^{-1}Q \end{bmatrix} \mathbf{y} = 0$$

Recall that we have assumed that $\mathbf{u} = (0, \ldots, 0, 1)$; then the equation $\mathbf{u}\mathbf{y} = 1$ is $y_{p+1} = 1$. Denoting by q_i and $\tilde{q}_i$ respectively the entries of vectors $-N^{-1}Q$ and $-(R - PN^{-1}Q)$ ends the proof. $\square$

The above local system is denoted by $\tilde{\mathbf{f}} \in \mathbb{Q}[\mathbf{x}, \mathbf{y}]_{\det N}^{2m-p}$. The Jacobian matrix of this polynomial system is

$$D\tilde{\mathbf{f}} = \begin{bmatrix} D_x\tilde{\mathbf{q}} & 0 \\ \star & \mathrm{I}_{p+1} \end{bmatrix}$$

with $\tilde{\mathbf{q}} = (\tilde{q}_1(\mathbf{x}), \ldots, \tilde{q}_{2m-2p-1}(\mathbf{x}))$. Its kernel defines the tangent space to $\mathcal{K}(H, \mathbf{u}, p) \cap O_N$. Let $\mathbf{w} = (\mathbf{w}_1, \ldots, \mathbf{w}_n) \in \mathbb{C}^n$ be a row vector; we denote by $\pi_{\mathbf{w}}$ the projection $\pi_{\mathbf{w}}(\mathbf{x}, \mathbf{y}) = \mathbf{w}_1 x_1 + \cdots + \mathbf{w}_n x_n$. Given a row vector $\mathbf{v} \in \mathbb{C}^{2m-p+1}$, we denote by $\mathsf{wlagrange}(\tilde{\mathbf{f}}, \mathbf{v})$ the following polynomial system

$$\tilde{\mathbf{f}}, \quad (\tilde{\mathbf{g}}, \tilde{\mathbf{h}}) = [z_1, \ldots, z_{2m-p}, z_{2m-p+1}] \begin{bmatrix} D\tilde{\mathbf{f}} \\ \mathbf{w} \quad 0 \end{bmatrix}, \quad \mathbf{v}'\mathbf{z} - 1. \tag{2}$$

For all $0 \leq p \leq r$, this polynomial system contains $n + 2m + 2$ polynomials and $n + 2m + 2$ variables. We denote by $\mathsf{L}_p(\tilde{\mathbf{f}}, \mathbf{v}, \mathbf{w})$ the set of its solutions whose projection on the $(\mathbf{x}, \mathbf{y})$-space lies in O_N.

Finally, we denote by $\mathsf{wlagrange}(\mathbf{f}, \mathbf{v})$ the polynomial system obtained when replacing $\tilde{\mathbf{f}}$ above with $\mathbf{f} = \mathbf{f}(H, \mathbf{u}, p)$. Similarly, its solution set is denoted by $\mathsf{L}_p(\mathbf{f}, \mathbf{v}, \mathbf{w})$.

5.2 Intermediate result

Lemma 10 *Let $\mathscr{H} \subset \mathbb{C}^{(2m-r)(n+1)}$ be the non-empty Zariski open set defined by Proposition 1, $H \in \mathscr{H}$ and $0 \leq p \leq r$. There exist non-empty Zariski open sets $\mathscr{V} \subset \mathbb{C}^{2m-p}$ and $\mathscr{W} \subset \mathbb{C}^n$ such that if $\mathbf{v} \in \mathscr{V}$ and $\mathbf{w} \in \mathscr{W}$, the following holds:*

(a) the set $\mathcal{L}_p(\mathbf{f}, \mathbf{v}, \mathbf{w}) = \mathcal{L}(\mathbf{f}, \mathbf{v}, \mathbf{w}) \cap \{(\mathbf{x}, \mathbf{y}, \mathbf{z}) \mid \operatorname{rank} \tilde{H}(\mathbf{x}) = p\}$ is finite and the Jacobian matrix of $\mathsf{wlagrange}(\mathbf{f}, \mathbf{v})$ *has maximal rank at any point of $\mathcal{L}_p(\mathbf{f}, \mathbf{v}, \mathbf{w})$;*

(b) the projection of $\mathcal{L}_p(\mathbf{f}, \mathbf{v}, \mathbf{w})$ in the $(\mathbf{x}, \mathbf{y})$-space contains the critical points of the restriction of $\pi_{\mathbf{w}}$ restricted to $\mathcal{K}(H, \mathbf{u}, p)$.

Proof : We start with Assertion (a).

The statement to prove holds over $\mathcal{K}(H, \mathbf{u}, p)$; hence it is enough to prove it on any open set at which one $p \times p$ minor of $\tilde{H}$ is non-zero. Hence, we assume that the determinant of the upper left $p \times p$ submatrix N of $\tilde{H}$ is non-zero; $O_N \subset \mathbb{C}^{n+p+1}$ is the open set defined by $\det N \neq 0$, and we reuse the notation introduced in this section. We prove that there exist non-empty Zariski open sets $\mathscr{V}'_N \subset \mathbb{C}^{2m-p}$ and $\mathscr{W}_N \subset \mathbb{C}^n$ such that for $\mathbf{v} \in \mathscr{V}'_N$ and $\mathbf{w} \in \mathscr{W}_N$, $\mathcal{L}_p(\tilde{\mathbf{f}}, \mathbf{v}, \mathbf{w})$ is finite and that the Jacobian matrix associated to $\mathsf{wlagrange}(\tilde{\mathbf{f}}, \mathbf{v})$ has maximal rank at any point of $\mathcal{L}_p(\tilde{\mathbf{f}}, \mathbf{v}, \mathbf{w})$. The Lemma follows straightforwardly by defining $\mathscr{V}'$ (resp. $\mathscr{W}$) as the intersection of $\mathscr{V}'_N$ (resp. $\mathscr{W}_N$) where N varies in the set of $p \times p$ minors of $\tilde{H}(\mathbf{x})$.

Equations $\tilde{\mathbf{h}}$ yield $z_j = 0$ for $j = 2m - 2p, \ldots, 2m - p$, and can be eliminated together with their $\mathbf{z}$ variables from the Lagrange system $\mathsf{wlagrange}(\tilde{\mathbf{f}}, \mathbf{v})$. It remains $\mathbf{z}$-variables

$z_1, \ldots, z_{2m-2p-1}, z_{2m-p+1}$; we denote by $\Omega \subset \mathbb{C}^{2m-2p}$ the Zariski open set where they don't vanish simultaneously.

Now, consider the map

$$\begin{array}{rccc} q: & O_N \times \Omega \times \mathbb{C}^n & \longrightarrow & \mathbb{C}^{n+2m-p} \\ & (\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) & \longmapsto & (\tilde{\mathbf{f}}, \tilde{\mathbf{g}}) \end{array}$$

and, for $\mathbf{w} \in \mathbb{C}^n$, its section map $q_{\mathbf{w}}(\mathbf{x}, \mathbf{y}, \mathbf{z}) = q(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w})$. We consider $\tilde{\mathbf{v}} \in \mathbb{C}^{2m-p}$ and we denote by $\tilde{\mathbf{z}}$ the remaining $\mathbf{z}-$variables, as above. Hence we define

$$\begin{array}{rccc} Q: & O_N \times \Omega \times \mathbb{C}^n \times \mathbb{C}^{2m-2p} & \longrightarrow & \mathbb{C}^{n+2m-p+1} \\ & (\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}, \tilde{\mathbf{v}}) & \longmapsto & (\tilde{\mathbf{f}}, \tilde{\mathbf{g}}, \tilde{\mathbf{v}}'\mathbf{z} - 1) \end{array}$$

and its section map $Q_{\mathbf{w},\tilde{\mathbf{v}}}(\mathbf{x}, \mathbf{y}, \mathbf{z}) = q(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}, \tilde{\mathbf{v}})$. We claim that $\mathbf{0} \in \mathbb{C}^{n+2m-p}$ (resp. $\mathbf{0} \in \mathbb{C}^{n+2m-p+1}$) is a regular value for q (resp. Q). Hence we deduce, by Thom's Weak Transversality Theorem, that there exist non-empty Zariski open sets $\mathscr{W}_N \subset \mathbb{C}^n$ and $\tilde{\mathscr{V}}_N \subset \mathbb{C}^{2m-2p}$ such that if $\mathbf{w} \in \mathscr{W}_N$ and $\tilde{\mathbf{v}} \in \tilde{\mathscr{V}}_N$, then $\mathbf{0}$ is a regular value for $q_{\mathbf{w}}$ and $Q_{\mathbf{w},\tilde{\mathbf{v}}}$.

We prove now this claim. Recall that since $H \in \mathscr{H}$, the Jacobian matrix $D_{\mathbf{x},\mathbf{y}}\tilde{\mathbf{f}}$ has maximal rank at any point $(\mathbf{x}, \mathbf{y}) \in \mathscr{Z}(\tilde{\mathbf{f}})$. Let $(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}) \in q^{-1}(\mathbf{0})$ (resp. $(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}, \tilde{\mathbf{v}}) \in Q^{-1}(\mathbf{0})$). Hence $(\mathbf{x}, \mathbf{y}) \in \mathscr{Z}(\tilde{\mathbf{f}})$. We isolate the square submatrix of $D\,q(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w})$ obtained by selecting all its rows and

- the columns corresponding to derivatives of $\mathbf{x}, \mathbf{y}$ yielding a non-singular submatrix of $D_{\mathbf{x},\mathbf{y}}\tilde{\mathbf{f}}(\mathbf{x}, \mathbf{y})$;
- the columns corresponding to the derivatives w.r.t. $\mathbf{w}_1, \ldots, \mathbf{w}_n$, hence this yields a block of zeros when applied to the lines corresponding to $\tilde{\mathbf{f}}$ and the block I_n when applied to $\tilde{\mathbf{g}}$.

For the map Q, we consider the same blocks as above. Moreover, since $(\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{w}, \tilde{\mathbf{v}}) \in Q^{-1}(\mathbf{0})$ verifies $\tilde{\mathbf{v}}'\mathbf{z} - 1 = 0$, there exists ℓ such that $z_\ell \neq 0$. Hence, we add the derivative of the polynomial $\tilde{\mathbf{v}}'\mathbf{z} - 1$ w.r.t. $\tilde{\mathbf{v}}_\ell$, which is $z_\ell \neq 0$. The claim is proved.

Note that $q_{\mathbf{w}}^{-1}(\mathbf{0})$ is defined by $n + 2m - p$ polynomials involving $n + 2m - p + 1$ variables. We deduce that for $\mathbf{w} \in \mathscr{W}_N$, $q_{\mathbf{w}}^{-1}(\mathbf{0})$ is either empty or it is equidimensional and has dimension 1. Using the homogeneity in the $\mathbf{z}$-variables and the Theorem on the Dimension of Fibers [21, Sect. 6.3, Theorem 7], we deduce that the projection on the $(\mathbf{x}, \mathbf{y})$-space of $q_{\mathbf{w}}^{-1}(\mathbf{0})$ has dimension ≤ 0. We also deduce that for $\mathbf{w} \in \mathscr{W}_N$ and $\tilde{\mathbf{v}} \in \tilde{\mathscr{V}}_N$, $Q_{\mathbf{w},\tilde{\mathbf{v}}}^{-1}(\mathbf{0})$ is either empty or finite.

Hence, the points of $Q_{\mathbf{v},\mathbf{w}}^{-1}(\mathbf{0})$ are in bijection with those in $\mathcal{L}(\tilde{\mathbf{f}}, \mathbf{v}, \mathbf{w})$ forgetting their 0-coordinates corresponding to $z_j = 0$. We define $\mathscr{V}_N' = \tilde{\mathscr{V}}_N \times \mathbb{C}^p \subset \mathbb{C}^{2m-2p}$. We deduce straightforwardly that for $\mathbf{v} \in \mathscr{V}_N'$ and $\mathbf{w} \in \mathscr{W}_N$, the Jacobian matrix of $\mathsf{wlagrange}(\tilde{\mathbf{f}}, \mathbf{v})$ has maximal rank at any point of $\mathcal{L}_p(\tilde{\mathbf{f}}, \mathbf{v}, \mathbf{w})$. By the Jacobian criterion, this also implies that the set $\mathcal{L}_p(\tilde{\mathbf{f}}, \mathbf{v}, \mathbf{w})$ is finite as requested.

We prove now Assertion (b).

Let $\mathscr{W} \subset \mathbb{C}^n$ and $\mathscr{V}' \subset \mathbb{C}^{2m-p}$ be the non-empty Zariski open sets defined in the proof of Assertion (a). For $\mathbf{w} \in \mathscr{W}$ and $\mathbf{v} \in \mathscr{V}'$, the projection of $\mathcal{L}_p(\tilde{\mathbf{f}}, \mathbf{v}, \mathbf{w})$ on the $(\mathbf{x}, \mathbf{y})-$space is finite. Since $H \in \mathscr{H}$, $\mathcal{K}(H, \mathbf{u}, p)$ is smooth and equidimensional.

Since we work on $\mathcal{K}(H, \mathbf{u}, p)$, one of the $p \times p$ minors of $\tilde{H}(\mathbf{x})$ is non-zero. Hence, suppose to work in $O_N \cap \mathcal{K}(H, \mathbf{u}, p)$ where $O_N \subset \mathbb{C}^{n+p+1}$ has been defined in the proof of Assertion (a). Remark that

$$\text{crit}\,(\pi_{\mathbf{w}}, \mathcal{K}(H, \mathbf{u}, p)) = \bigcup_N \text{crit}\,(\pi_{\mathbf{w}}, O_N \cap \mathcal{K}(H, \mathbf{u}, p))$$

where N runs over the set of $p \times p$ minors of $\tilde{H}(\mathbf{x})$. We prove below that there exists a non-empty Zariski open set $\mathscr{V} \subset \mathbb{C}^{2m-p}$ such that if $\mathbf{v} \in \mathscr{V}$, for all N and for $\mathbf{w} \in \mathscr{W}$, the set $\text{crit}\,(\pi_{\mathbf{w}}, O_N \cap \mathcal{K}(H, \mathbf{u}, p))$ is finite and contained in the projection of $\mathcal{L}_p(\mathbf{f}, \mathbf{v}, \mathbf{w})$. This straightforwardly implies that the same holds for $\text{crit}\,(\pi_{\mathbf{w}}, \mathcal{K}(H, \mathbf{u}, p))$.

Suppose w.l.o.g. that N is the upper left $p \times p$ minor of $\tilde{H}(\mathbf{x})$. We use the notation $\tilde{\mathbf{f}}, \tilde{\mathbf{g}}, \tilde{\mathbf{h}}$ as above. Hence, the set $\text{crit}\,(\pi_{\mathbf{w}}, O_N \cap \mathcal{K}(H, \mathbf{u}, p))$ is the image by the projection $\pi_{\mathbf{x},\mathbf{y}}$ over the $(\mathbf{x}, \mathbf{y})-$space, of the constructible set defined by $\tilde{\mathbf{f}}, \tilde{\mathbf{g}}, \tilde{\mathbf{h}}$ and $\mathbf{z} \neq 0$. We previously proved that, if $\mathbf{w} \in \mathscr{W}_N$, $q^{-1}(\mathbf{0})$ is either empty or equidimensional of dimension 1. Hence, the constructible set defined by $\tilde{\mathbf{f}}, \tilde{\mathbf{g}}, \tilde{\mathbf{h}}$ and $\mathbf{z} \neq 0$, which is isomorphic to $q^{-1}(\mathbf{0})$, is either empty or equidimensional of dimension 1.

Moreover, for any $(\mathbf{x}, \mathbf{y}) \in \text{crit}\,(\pi_{\mathbf{w}}, O_N \cap \mathcal{K}(H, \mathbf{u}, p))$, $\pi_{\mathbf{x},\mathbf{y}}^{-1}(\mathbf{x}, \mathbf{y})$ has dimension 1, by the homogeneity of polynomials w.r.t. variables $\mathbf{z}$. By the Theorem on the Dimension of Fibers [21, Sect. 6.3, Theorem 7], we deduce that $\text{crit}\,(\pi_{\mathbf{w}}, O_N \cap \mathcal{K}(H, \mathbf{u}, p))$ is finite.

For $(\mathbf{x}, \mathbf{y}) \in \text{crit}\,(\pi_{\mathbf{w}}, O_N \cap \mathcal{K}(H, \mathbf{u}, p))$, let $\mathscr{V}_{(\mathbf{x},\mathbf{y}),N} \subset \mathbb{C}^{2m-p}$ be the non-empty Zariski open set such that if $\mathbf{v} \in \mathscr{V}_{(\mathbf{x},\mathbf{y}),N}$ the hyperplane $\mathbf{v}'\mathbf{z} - 1 = 0$ intersects transversely $\pi_{\mathbf{x},\mathbf{y}}^{-1}(\mathbf{x}, \mathbf{y})$. Recall that $\mathscr{V}'_N \subset \mathbb{C}^{2m-p}$ has been defined in the proof of Assertion (a). Define

$$\mathscr{V}_N = \mathscr{V}'_N \cap \bigcap_{(\mathbf{x},\mathbf{y})} \mathscr{V}_{(\mathbf{x},\mathbf{y}),N}$$

and $\mathscr{V} = \bigcap_N \mathscr{V}_N$. This concludes the proof, since $\mathscr{V}$ is a finite intersection of non-empty Zariski open sets. □

5.3 Conclusion

We denote by $\mathscr{M}_1 \subset \text{GL}(n, \mathbb{C})$ the set of non-singular matrices M such that the first row $\mathbf{w}$ of M^{-1} lies in the set $\mathscr{W}$ given in Lemma 10: this set is non-empty and Zariski open since the entries of M^{-1} are rational functions of the entries of M. Let $\mathscr{V} \subset \mathbb{C}^{2m-p}$ be the non-empty Zariski open set given by Lemma 10 and let $\mathbf{v} \in \mathscr{V}$. Let $\mathbf{e}_1$ be the row vector $(1, 0, \ldots, 0) \in \mathbb{Q}^n$ and for all $M \in \text{GL}(n, \mathbb{C})$, let

$$\tilde{M} = \begin{bmatrix} M & 0 \\ 0 & \text{I}_m \end{bmatrix}.$$

Remark that for any $M \in \mathscr{M}_1$ the following identity holds:

$$\begin{bmatrix} D\,\mathbf{f}(H^M, \mathbf{u}, p) \\ \mathbf{e}_1 \quad 0 \cdots 0 \end{bmatrix} = \begin{bmatrix} D\,\mathbf{f}(H, \mathbf{u}, p) \\ \mathbf{w} \quad 0 \cdots 0 \end{bmatrix} \tilde{M}.$$

We conclude that the set of solutions of the system

$$\left(\mathbf{f}(H,\mathbf{u},p), \quad \mathbf{z}' \begin{bmatrix} D\,\mathbf{f}(H,\mathbf{u},p) \\ \mathbf{w} \quad 0 \cdots 0 \end{bmatrix}, \quad \mathbf{v}'\mathbf{z}-1\right) \tag{3}$$

is the image by the map $(\mathbf{x},\mathbf{y}) \mapsto \tilde{M}^{-1}(\mathbf{x},\mathbf{y})$ of the set S of solutions of the system

$$\left(\mathbf{f}(H,\mathbf{u},p), \quad \mathbf{z}' \begin{bmatrix} D\,\mathbf{f}(H,\mathbf{u},p) \\ \mathbf{e}_1 \quad 0 \cdots 0 \end{bmatrix}, \quad \mathbf{v}'\mathbf{z}-1\right). \tag{4}$$

Now, let φ be the projection that eliminates the last coordinate z_{2m-p+1}. Remark that $\varphi(S) = \mathsf{L}_p(\mathbf{f}^M, \mathbf{v}, \mathbf{e}_1)$.

Now, applying Lemma 10 ends the proof.

□

6 Proof of Proposition 3

The proof of Proposition 3 relies on results of [14, Section 5] and of [19]. We use the same notation as in [14, Section 5], and we recall them below.

Notations For $\mathcal{Z} \subset \mathbb{C}^n$ of dimension d, we denote by $\Omega_i(\mathcal{Z})$ its $i-$equidimensional component, $i = 0, \ldots, d$. We denote by $\mathscr{S}(\mathcal{Z})$ the union of:

- $\Omega_0(\mathcal{Z}) \cup \cdots \cup \Omega_{d-1}(\mathcal{Z})$
- the set $\mathrm{sing}\,(\Omega_d(\mathcal{Z}))$ of singular points of $\Omega_d(\mathcal{Z})$.

Let π_i be the map $(x_1, \ldots, x_n) \to (x_1, \ldots, x_i)$. We denote by $\mathscr{C}(\pi_i, \mathcal{Z})$ the Zariski closure of the union of the following sets:

- $\Omega_0(\mathcal{Z}) \cup \cdots \cup \Omega_{i-1}(\mathcal{Z})$;
- the union for $r \geq i$ of the sets $\mathrm{crit}\,(\pi_i, \mathrm{reg}\,(\Omega_r(\mathcal{Z})))$.

For $M \in \mathrm{GL}(n, \mathbb{C})$ and $\mathcal{Z}$ as above, we define the collection of algebraic sets $\{\mathcal{O}_i(\mathcal{Z}^M)\}_{0 \leq i \leq d}$ as follows:

- $\mathcal{O}_d(\mathcal{Z}^M) = \mathcal{Z}^M$;
- $\mathcal{O}_i(\mathcal{Z}^M) = \mathscr{S}(\mathcal{O}_{i+1}(\mathcal{Z}^M)) \cup \mathscr{C}(\pi_{i+1}, \mathcal{O}_{i+1}(\mathcal{Z}^M)) \cup$
$\cup\, \mathscr{C}(\pi_{i+1}, \mathcal{Z}^M)$ for $i = 0, \ldots, d-1$.

We finally recall the two following properties:

Property $\mathsf{P}(\mathcal{Z})$. Let $\mathcal{Z} \subset \mathbb{C}^n$ be an algebraic set of dimension d. We say that $M \in \mathrm{GL}(n, \mathbb{C})$ satisfies $\mathsf{P}(\mathcal{Z})$ when for all $i = 0, 1, \ldots, d$:

1. $\mathcal{O}_i(\mathcal{Z}^M)$ has dimension $\leq i$ and
2. $\mathcal{O}_i(\mathcal{Z}^M)$ is in Noether position with respect to $x_1, \ldots, x_i$.

Property Q. We say that an algebraic set $\mathcal{Z}$ of dimension d satisfies $\mathsf{Q}_i(\mathcal{Z})$ (for a given $1 \leq i \leq d$) if for any connected component C of $\mathcal{Z} \cap \mathbb{R}^n$ the boundary of $\pi_i(C)$ is contained in $\pi_i(\mathcal{O}_{i-1}(\mathcal{Z}) \cap C)$. We say that $\mathcal{Z}$ satisfies Q if it satisfies $\mathsf{Q}_1, \ldots, \mathsf{Q}_d$.

Let $\mathcal{Z} \subset \mathbb{C}^n$ be an algebraic set of dimension d. By [14, Proposition 15], there exists a non-empty Zariski open set $\mathscr{M} \subset \mathrm{GL}(n, \mathbb{C})$ such that for $M \in \mathscr{M} \cap \mathrm{GL}(n, \mathbb{Q})$ Property $\mathsf{P}(\mathcal{Z})$ holds. Moreover, if $M \in \mathrm{GL}(n, \mathbb{Q})$ satisfies $\mathsf{P}(\mathcal{Z})$, then $\mathsf{Q}_i(\mathcal{Z}^M)$ holds for $i = 1, \ldots, d$ [14, Proposition 16]. We use these results in the following proof of Proposition 3.

Proof : We start with assertion (a). Let $\mathscr{M}_2 \subset \mathrm{GL}(n, \mathbb{C})$ be the non-empty Zariski open set of [14, Proposition 17] for $\mathcal{Z} = \mathcal{H}_p$: for $M \in \mathscr{M}_2$, M satisfies $\mathsf{P}(\mathcal{H}_p)$. Remark that the connected components of $\mathcal{H}_p \cap \mathbb{R}^n$ and are in bijection with those of $\mathcal{H}_p^M \cap \mathbb{R}^n$ (given by $C \leftrightarrow C^M$). Let $C^M \subset \mathcal{H}_p^M \cap \mathbb{R}^n$ be a connected component of $\mathcal{H}_p^M \cap \mathbb{R}^n$. Let π_1 be the projection on the first variable $\pi_1 \colon \mathbb{R}^n \to \mathbb{R}$, and consider its restriction to $\mathcal{H}_r^M \cap \mathbb{R}^n$. Since $M \in \mathscr{M}_2$, by [14, Proposition 16] the boundary of $\pi_1(C^M)$ is included in $\pi_1(\mathcal{O}_0(\mathcal{H}_p^M) \cap C^M)$ and in particular in $\pi_1(C^M)$. Hence $\pi_1(C^M)$ is closed.

We prove now assertion (b). Let $M \in \mathscr{M}_2$, C a connected component of $\mathcal{H}_p \cap \mathbb{R}^n$ and $\alpha \in \mathbb{R}$ be in the boundary of $\pi_1(C^M)$. By [14, Lemma 19] $\pi_1^{-1}(\alpha) \cap C^M$ is finite.

We claim that, up to genericity assumptions on $\mathbf{u} \in \mathbb{Q}^{p+1}$, for $\mathbf{x} \in \pi_1^{-1}(\alpha) \cap C^M$, the linear system $\mathbf{y} \mapsto \mathbf{f}(H^M, \mathbf{u}, p)$ has at least one solution. We deduce that there exists a non-empty Zariski open set $\mathscr{U}_{C,\mathbf{x}} \subset \mathbb{C}^{p+1}$ such that if $\mathbf{u} \in \mathscr{U}_{C,\mathbf{x}} \cap \mathbb{Q}^{p+1}$, there exists $\mathbf{y} \in \mathbb{Q}^{p+1}$ such that $(\mathbf{x}, \mathbf{y}) \in \mathcal{J}(H^M, \mathbf{u}, p)$. One concludes by taking

$$\mathscr{U} = \bigcap_{C \subset \mathcal{H}_p \cap \mathbb{R}^n} \bigcap_{\mathbf{x} \in \pi_1^{-1}(\alpha) \cap C^M} \mathscr{U}_{C,\mathbf{x}},$$

which is non-empty and Zariski open since:

- the collection $\{C \subset \mathcal{H}_p \cap \mathbb{R}^n \text{ connected component}\}$ is finite;
- the set $\pi_1^{-1}(\alpha) \cap C^M$ is finite.

It remains to prove the claim we made. For $\mathbf{x} \in \pi_1^{-1}(\alpha) \cap C^M$, the matrix $\tilde{H}(\mathbf{x})$ is rank defective, and let $p' \leq p$ be its rank. The linear system

$$\begin{bmatrix} \tilde{H}(\mathbf{x}) \\ \mathbf{u} \end{bmatrix} \cdot \mathbf{y} = \begin{bmatrix} \mathbf{0} \\ 1 \end{bmatrix}$$

has a solution if and only if

$$\operatorname{rank} \begin{bmatrix} \tilde{H}(\mathbf{x}) \\ \mathbf{u} \end{bmatrix} = \operatorname{rank} \begin{bmatrix} \tilde{H}(\mathbf{x}) & \mathbf{0} \\ \mathbf{u} & 1 \end{bmatrix},$$

and the rank of the second matrix is $p' + 1$. Denoting by $\mathscr{U}_{C,\mathbf{x}} \subset \mathbb{C}^{p+1}$ the complement in $\mathbb{C}^{p+1}$ of the $p'-$dimensional linear space spanned by the rows of $\tilde{H}(\mathbf{x})$, proves the claim and concludes the proof. □

7 Experiments

The algorithm LowRankHankel has been implemented under MAPLE. We use the FGB [9] library implemented by J.-C. Faugère for solving solving zero-dimensional polynomial systems using Gröbner bases. In particular, we used the new implementation of [10] for computing rational parametrizations. Our implementation checks the genericity assumptions on the input.

We test the algorithm with input $m \times m$ linear Hankel matrices $H(\mathbf{x}) = H_0 + x_1 H_1 + \ldots + x_n H_n$, where the entries of $H_0, \ldots, H_n$ are random rational numbers, and an integer $0 \leq r \leq m-1$. None of the implementations of Cylindrical Algebraic Decomposition solved our examples involving more that 3 variables. Also, on all our examples, we found that the Lagrange systems define finite algebraic sets.

We compare the practical behavior of LowRankHankel with the performance of the library RAGLIB, implemented by the third author (see [17]). Its function PointsPerComponents, with input the list of $(r+1)-$minors of $H(\mathbf{x})$, returns one point per connected component of the real counterpart of the algebraic set $\mathcal{H}_r$, that is it solves the problem presented in this paper. It also uses critical point methods. The symbol ∞ means that no result has been obtained after 24 hours. The symbol matbig means that the standard limitation in FGB to the size of matrices for Gröbner bases computations has been reached.

We report on timings (given in seconds) of the two implementations in the next table. The column New corresponds to timings of LowRankHankel. Both computations have been done on an Intel(R) Xeon(R) CPU $E7540$ @2.00GHz 256 Gb of RAM. We remark that RAGLIB is competetitive for problems of small size (e.g. $m = 3$) but when the size increases LowRankHankel performs much better, especially when the determinantal variety has not co-dimension 1. It can tackle problems that are out reach of RAGLIB. Note that for fixed r, the algorithm seems to have a behaviour that is polynomial in nm (this is particularly visible when m is fixed, e.g. to 5).

Finally, we report in column TotalDeg the degree of the rational parametrization obtained as output of the algorithm, that is the number of its complex solutions. We observe that this value is definitely constant when m, r are fixed and n grows, as for the maximum degree (column MaxDeg) appearing during the recursive calls.

The same holds for the multilinear bound given in Section 4 for the total number of complex solutions.

(m, r, n)	RAGlib	New	TotalDeg	MaxDeg
$(3, 2, 2)$	0.3	5	9	6
$(3, 2, 3)$	0.6	10	21	12
$(3, 2, 4)$	2	13	33	12
$(3, 2, 5)$	7	20	39	12
$(3, 2, 6)$	13	21	39	12
$(3, 2, 7)$	20	21	39	12
$(3, 2, 8)$	53	21	39	12
$(4, 2, 3)$	2	2.5	10	10
$(4, 2, 4)$	43	6.5	40	30
$(4, 2, 5)$	56575	18	88	48
$(4, 2, 6)$	∞	35	128	48
$(4, 2, 7)$	∞	46	143	48
$(4, 2, 8)$	∞	74	143	48
$(4, 3, 2)$	0.3	8	16	12
$(4, 3, 3)$	3	11	36	52
$(4, 3, 4)$	54	31	120	68
$(4, 3, 5)$	341	112	204	84
$(4, 3, 6)$	480	215	264	84
$(4, 3, 7)$	528	324	264	84
$(4, 3, 8)$	2638	375	264	84
$(5, 2, 5)$	25	4	21	21
$(5, 2, 6)$	31176	21	91	70
$(5, 2, 7)$	∞	135	199	108
$(5, 2, 8)$	∞	642	283	108
$(5, 2, 9)$	∞	950	311	108
$(5, 2, 10)$	∞	1106	311	108
$(5, 3, 3)$	2	2	20	20
$(5, 3, 4)$	202	18	110	90
$(5, 3, 5)$	∞	583	338	228
$(5, 3, 6)$	∞	6544	698	360
$(5, 3, 7)$	∞	28081	1058	360
$(5, 3, 8)$	∞	∞	-	-

Table 1: Timings and degrees

(m, r, n)	RAGlib	New	TotalDeg	MaxDeg
$(5,4,2)$	1	5	25	20
$(5,4,3)$	48	30	105	80
$(5,4,4)$	8713	885	325	220
$(5,4,5)$	∞	15537	755	430
$(5,4,6)$	∞	77962	1335	580
$(6,2,7)$	∞	6	36	36
$(6,2,8)$	∞	matbig	-	-
$(6,3,5)$	∞	10	56	56
$(6,3,6)$	∞	809	336	280
$(6,3,7)$	∞	49684	1032	696
$(6,3,8)$	∞	matbig	-	-
$(6,4,3)$	3	5	35	35
$(6,4,4)$	∞	269	245	210
$(6,4,5)$	∞	30660	973	728
$(6,4,6)$	∞	∞	-	-
$(6,5,2)$	1	9	36	30
$(6,5,3)$	915	356	186	150
$(6,5,4)$	∞	20310	726	540
$(6,5,5)$	∞	∞	-	-

Table 2: Timings and degrees (continued)

References

[1] B. Bank, M. Giusti, J. Heintz, M. Safey El Din, and É. Schost. On the geometry of polar varieties. *Applicable Algebra in Engineering, Communication and Computing*, 21(1):33–83, 2010.

[2] S. Basu, R. Pollack, and M.-F. Roy. *Algorithms in real algebraic geometry*, volume 10 of *Algorithms and Computation in Mathematics*. Springer-Verlag, second edition, 2006.

[3] G. Blekherman and R. Sinn. Extreme rays of the Hankel spectrahedra for ternary forms. `arXiv:1406.1873v2`, October 2014.

[4] W. Bruns and U. Vetter. *Determinantal rings*, volume 1327. Springer-Verlag Berlin-Heidelberg, 1988.

[5] G. Collins. Quantifier elimination for real closed fields by cylindrical algebraic decompostion. In *Automata Theory and Formal Languages*, pages 134–183. Springer, 1975.

[6] A. Conca. Straightening law and powers of determinantal ideals of Hankel matrices. *Advances in Mathematics*, 138(2):263–292, 1998.

[7] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, 1995.

[8] J-C. Faugère, M. Safey El Din, and P-J. Spaenlehauer. Critical points and Gröbner bases: the unmixed case. In *Proceedings of ISSAC*, pages 162–169. ACM, 2012.

[9] Jean-Charles Faugère. FGb: a library for computing gröbner bases. In *Mathematical Software–ICMS 2010*, pages 84–87. Springer, 2010.

[10] Jean-Charles Faugère and Chenqi Mou. Fast algorithm for change of ordering of zero-dimensional Gröbner bases with sparse multiplication matrices. In *Proceedings of ISSAC*, pages 115–122. ACM, 2011.

[11] A. Greuet and M. Safey El Din. Probabilistic algorithm for polynomial optimization over a real algebraic set. *SIAM Journal on Optimization*, 24(3):1313–1343, 2014.

[12] D. Grigoriev and N. Vorobjov. Solving systems of polynomial inequalities in subexponential time. *Journal of Symbolic Computation*, 5:37–64, 1988.

[13] G. Heinig and K. Rost. *Algebraic methods for Toeplitz-like matrices and operators*. Springer-Verlag, Berlin, 1984.

[14] D. Henrion, S. Naldi, and M. Safey El Din. Real root finding for determinants of linear matrices. `arXiv:1412.5873`, December 2014.

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

[16] I. Markovsky. *Low rank approximation: algorithms, implementation, applications*. Communications and Control Engineering. Springer, 2012.

[17] M. Safey El Din. RAGLib (Real Algebraic Geometry Library), Maple Package. `www-polsys.lip6.fr/~safey`

[18] M. Safey El Din. Finding sampling points on real hypersurfaces is easier in singular situations. In *MEGA (Effective Methods in Algebraic Geometry) Electronic Proceedings*, 2005.

[19] M. Safey El Din and É. Schost. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In *Proceedings of ISSAC*, pages 224–231. ACM, 2003.

[20] M. Safey El Din and É. Schost. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. `arXiv:1307.7836`, 2013.

[21] I. Shafarevich. *Basic Algebraic Geometry 1*. Springer Verlag, 1977.

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

[23] A. Tarski. *A decision method for elementary algebra and geometry*. University of California Press, 1951.