



Contents lists available at ScienceDirect

Journal of Symbolic Computation

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

Solving parametric linear matrix inequalities

Simone Naldi^a, Mohab Safey El Din^b, Adrien Taylor^c,
Weijia Wang^b^a Université de Limoges, CNRS, XLIM, Limoges, France^b Sorbonne Université, CNRS, LIP6, Paris, France^c Inria, École normale supérieure, PSL Research University, Paris, France

ARTICLE INFO

Article history:

Received 30 January 2026

Received in revised form 21 June 2026

Accepted 24 June 2026

Available online 29 June 2026

Keywords:

Linear matrix inequality

Quantifier elimination

Optimization

ABSTRACT

We consider linear matrices $A = A_0 + x_1 A_1 + \dots + x_n A_n$, where the A_i 's are $m \times m$ symmetric matrices with entries in a ring $\mathcal{R}$. When $\mathcal{R} = \mathbb{R}$, the feasibility problem consists in deciding whether the linear matrix inequality (LMI) $A \succeq 0$ is feasible, i.e., the x_i 's can be instantiated to obtain a positive semi-definite matrix. When $\mathcal{R} = \mathbb{Q}[y_1, \dots, y_t]$, the problem asks for a formula on the parameters $y_1, \dots, y_t$, which describes the values of the parameters for which the specialized LMI is feasible. This problem can be solved using general quantifier elimination algorithms, with a complexity that is exponential in n . In this work, we leverage the LMI structure of the problem to design an algorithm that computes a formula Φ describing a dense subset of the feasible region of parameters. The complexity of this algorithm is exponential in n, m and t but becomes polynomial in n when m and t are fixed. We apply the algorithm to a parametric sum-of-squares problem and to the convergence analyses of certain first-order optimization methods. Both problems are known to be equivalent to the feasibility of certain parametric LMIs and lead instances which are out of reach of the previous state of the art. We demonstrate that our implementations of our algorithm can tackle these problems in practice, already for small values of n, m and t .

© 2026 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

E-mail address: weijia.wang@sorbonne-universite.fr (W. Wang).<https://doi.org/10.1016/j.jsc.2026.102605>0747-7171/© 2026 The Authors. Published by Elsevier Ltd. This is an open access article under the CC BY license (<http://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Problem statement For a set $\mathcal{E}$ and $m \in \mathbb{N}$, we denote by $\mathbb{S}_m(\mathcal{E})$ the set of $m \times m$ symmetric matrices with entries in $\mathcal{E}$. For n and t in $\mathbb{N}$, we consider sequences of variables $\mathbf{x} = (x_1, \dots, x_n)$ and parameters $\mathbf{y} = (y_1, \dots, y_t)$ and the ring $\tilde{R} = \mathbb{Q}[\mathbf{y}][\mathbf{x}]$. The set of polynomials in $\tilde{R}$ of degree at most 1 in $\mathbf{x}$ is denoted by $\tilde{R}_{\leq 1}$.

A matrix $A = A_0 + x_1 A_1 + \dots + x_n A_n$ in $\mathbb{S}_m(\tilde{R}_{\leq 1})$ is said to be a *parametric linear matrix*. For any $y \in \mathbb{R}^t$, we denote by A_y the matrix obtained by specializing the parameters $\mathbf{y}$ to y . The linear matrix inequality $A_y \geq 0$ defines the spectrahedron $\text{spec}(A_y) \subset \mathbb{R}^n$, i.e., the set of points x in $\mathbb{R}^n$ such that $A_y(x)$ is positive semi-definite. It is well-known that $\text{spec}(A_y)$ is a convex semi-algebraic set, defined by $g_i(y, \cdot) \geq 0$, where $g_i \in \tilde{R}$ is the coefficient of λ^i in $\det(A + \lambda I_m)$ (see, e.g., Henrion et al., 2016a, Sec. 5.2).

Problem 1 (*Generic feasibility problem*). Given a parametric linear matrix $A \in \mathbb{S}_m(\tilde{R}_{\leq 1})$, compute a semi-algebraic formula Φ in $\mathbb{Q}[\mathbf{y}]$, such that Φ defines a dense subset of the set of feasible parameters $\mathcal{P} := \{y \in \mathbb{R}^t \mid \exists x \in \mathbb{R}^n : A(y, x) \geq 0\}$.

The problem is a natural generalization of the decisional feasibility problem for LMIs. Indeed, once the semi-algebraic formula Φ is computed, one can decide whether a generically chosen parameter y is in $\mathcal{P}$ by checking whether $\Phi(y)$ is true.

Example 1. Let $\mathbf{y} = a, b, c$ and $\mathbf{x} = x$. For the parametric linear matrix

$$A = \begin{bmatrix} ax + b & x + c \\ x + c & 1 \end{bmatrix},$$

the algorithm presented in this paper establishes that $\mathcal{P} = \{(a, b, c) \in \mathbb{R}^3 \mid a^2 + 4b - 4ac \geq 0\}$, so that the formula $\Phi(a, b, c) := a^2 + 4b - 4ac > 0$ defines a dense subset of $\mathcal{P}$.

Prior works From an algorithmic viewpoint, methods for solving LMIs split into two main families: numerical methods and symbolic methods. Numerical semi-definite programming (SDP) solvers are highly effective in practice and, under fixed-precision and standard arithmetic models, exhibit polynomial complexity behavior in the input size (see, e.g., Boyd and Vandenberghe, 2004). However, they return approximate solutions and are not designed to output exact semi-algebraic descriptions in the parametric setting.

Symbolic methods, in contrast, target exact formulas and solutions. Eliminating the existential quantifier in the definition of $\mathcal{P}$, or equivalently, in the formula

$$\exists x \in \mathbb{R}^n : g_0(y, x) \geq 0 \wedge \dots \wedge g_m(y, x) \geq 0,$$

falls within the scope of quantifier elimination (QE) for the first-order theory of the reals, a problem known to be decidable since Tarski's work Tarski (1951). However, Tarski's original algorithm has a complexity that is not elementary recursive. A major practical milestone was achieved by Collins' cylindrical algebraic decomposition (CAD) algorithm (Collins, 1975), which achieves doubly exponential complexity in the total number of unknowns. Despite this improvement, the worst-case complexity remains prohibitively high, limiting the practical applicability of such general-purpose QE methods to medium-size parametric LMIs.

It should be noted that, here, we have a quantifier elimination problem with a single block of variables to eliminate. The idea to exploit such a block structure to improve the complexity of quantifier elimination originates from Grigor'ev (1988) and culminates in the work (Basu et al., 1996) (see Basu et al., 2016, Sec. 14.6 for more bibliographic notes). This yields algorithms which are doubly exponential in the number of alternates of quantifiers and exponential in the total number of unknowns. Still, putting into practice such algorithms is an open problem. A weakened variant for one-block quantifier elimination is proposed in Le and Safey El Din (2021) (see also Hong and Safey El Din, 2012 and Hong

Table 1
Method families for solving LMIs.

Family	Representative methods	Typical guarantees	Relevance for Problem 1
Numerical SDP solvers	Interior point method (Boyd and Vandenberghe, 2004)	Approximate feasibility certificates; polynomial-time behavior under fixed precision	Fast on large instances, but no exact semi-algebraic formula output
General-purpose QE methods	CAD (Collins, 1975)	Exact formulas, doubly exponential worst-case complexity in $n + t$	Applicable in principle, often intractable on medium-size instances
General-purpose QE methods	Critical point method (Basu et al., 1996)	Exact formulas, worst-case complexity in n and t	Applicable in principle, often intractable on medium-size instances
Symbolic LMI solvers	Dedicated critical point method (Henrion et al., 2016a, 2021; Le and Safey El Din, 2021)	Exact certificates using determinantal structure	Targeted for LMIs, with better complexity than general QE methods

and Safey El Din, 2009) but is restricted to systems of polynomial equations which enjoy regularity properties and do not involve inequalities.

To overcome these limitations, we aim to exploit the specific structure of LMIs. Our study goes back to Henrion et al. (2016a) which yields an *exact* algorithm for solving linear matrix inequalities, combining its principles with those of Le and Safey El Din (2021). Table 1 summarizes the landscape.

Contributions Our contributions are organized in two parts.

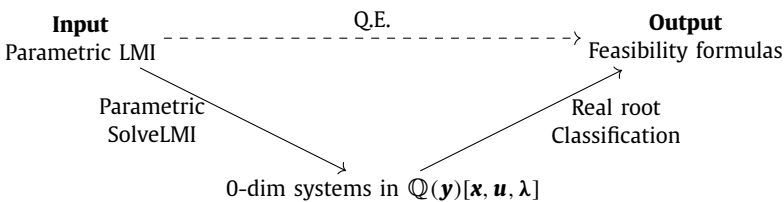
Part I (generic inputs). We first solve Problem 1 under genericity assumptions on the input parametric linear matrix A .

Our genericity assumptions concern the coefficients of the entries of A and define non-empty Zariski open subsets of the coefficient space. Hence, a generic small perturbation of coefficients (i.e. the coefficients do not cancel some prescribed polynomial) places the input in the generic regime. These genericity assumptions are made precise in Proposition 7.

The algorithm can be seen as a generalization of the results in Henrion et al. (2016a) to the parametric setting. It first computes a finite set of polynomial systems $(f_i)_i$ in $\mathbb{R}[\mathbf{u}, \lambda]$, where $\mathbf{u}$ and λ are auxiliary variables, inspired by the subroutines in Henrion et al. (2016a), used to solve *exactly* linear matrix inequalities. The specifics of this finite set of polynomial systems will be clarified in Sections 2.3 and 3.2. As A is chosen generically, the polynomial systems $(f_i)_i$ satisfy the following *specialization property*, which we prove (see Proposition 7).

For generic values of the parameters $y \in \mathbb{R}^t$, each $f_i(y, \cdot) = 0$ has a finite number of complex solutions, and the non-emptiness of $\text{spec}(A_y)$ is determined by the existence of at least one solution to a certain $f_i(y, \cdot) = 0 \wedge g(y, \cdot) \geq 0$ where $g = (g_0, \dots, g_m)$ are defined above.

To extract the formula Φ characterizing this condition, the algorithm applies to each relation $f_i = 0 \wedge g \geq 0$ the real root counting method described in Gaillard and Safey El Din (2024), based on Hermite's quadratic form Hermite (1856).



The algorithm works on Example 1 as follows. By definition, we have

$$\begin{aligned} g_0 &= -x^2 + ax - 2cx + b - c^2, \\ g_1 &= 1 + b + ax, \end{aligned}$$

which are the coefficients of degree 0 and 1 in the characteristic polynomial of A , respectively. The procedure in Henrion et al. (2016a) yields the following system $\mathbf{f} = (f_1, f_2, f_3, f_4, f_5, f_6)$. For a detailed computation of $\mathbf{f}$, see Example 2.

$$\begin{aligned} f_1 &= ax + b + cu_{2,1} + xu_{2,1}, \\ f_2 &= c + x + u_{2,1}, \\ f_3 &= u_{1,1} - 1, \\ f_4 &= a\lambda_1 + u_{2,1}\lambda_1 + \lambda_2 - 1, \\ f_5 &= \lambda_3, \\ f_6 &= c\lambda_1 + x\lambda_1 + \lambda_2. \end{aligned} \tag{1}$$

Then, the real root classification method in Gaillard and Safey El Din (2024) on $\mathbf{f} = 0 \wedge \mathbf{g} \geq 0$ concludes that $\Phi(a, b, c)$ holds if and only if the following matrix is positive definite:

$$H = \begin{bmatrix} 2 & a - 2c \\ a - 2c & a^2 - 4ac + 2b + 2c^2 \end{bmatrix}.$$

As the minors of H are 2 and $\det(H) = a^2 + 4b - 4ac$, Sylvester's criterion then yields $\Phi(a, b, c) := a^2 + 4b - 4ac > 0$.

Note that for an input $\mathbf{f}_i$, the algorithm in Gaillard and Safey El Din (2024) is based on Gröbner bases computations, and, consequently, extra genericity assumptions on the input are required to control the complexity.

By contrast, in this generic part, the ideal generated by the input $\mathbf{f}_i$ turns out to be “generically radical” (i.e. it is radical in $\mathbb{Q}(\mathbf{y})[\mathbf{x}, \mathbf{u}, \lambda]$), but does not satisfy the genericity assumptions used in Gaillard and Safey El Din (2024), because of the special structure of the $\mathbf{f}_i$'s.

Still, we show how to control the complexity in this case, replacing Gröbner bases computations with the computation of parametric geometric resolutions (Schost, 2003) of the input $\mathbf{f}_i$.

Singular instances may remain outside our genericity assumptions; this motivates the second part below.

Part II (degenerate inputs). We remove genericity assumptions by infinitesimal deformation: we perturb A into a “nearby” generic instance (through a symbolic deformation), solve the perturbed problem, and recover boundary information by letting the perturbation parameter tend to zero. This infinitesimal-deformation paradigm is standard in effective real algebraic geometry (see, e.g., Grigor'ev and Vorobjov, 1988; Heintz et al., 1990; Basu et al., 1996).

Theorem 1. *There exists an algorithm which, given a parametric linear matrix $A \in \mathbb{S}_m(\tilde{R}_{\leq 1})$ of any fixed maximum total degree d as input, outputs a semi-algebraic formula Φ in $\mathbb{Q}[\mathbf{y}]$ that solves Problem 1 for the input A , in*

$$2^{O(mt)} n^{O(1)} (md)^{O(t)} (\delta^* \Delta^*)^{O(t)} \tag{2}$$

arithmetic operations in $\mathbb{Q}$, where

$$\delta^* \in n^{O(m^2)} \quad \text{and} \quad \Delta^* \in e^{O(m^2 \log m)} n^{O(1)} d^{O(m^2+t)} t^{O(1)}.$$

Observe that for fixed m and t , the above complexity is polynomial in d and n , which is useful for the applications we have in mind (see below).

To obtain this result, we rely on techniques, based on the critical point method for quantifier elimination, introduced in Le and Safey El Din (2021). These are restricted to the case of systems of polynomial constraints involving equations only. We use reductions to such a situation introduced in Henrion et al. (2016a), but extending them to the parametric setting. As already sketched above, we are then bound to real root classification problems, which we solve by combining Hermite's quadratic forms as in Gaillard and Safey El Din (2024). However, the techniques used in Gaillard and Safey El Din (2024) to control the complexity do not apply to our situation anymore because of the specific structure of the $\mathbf{f}_i$'s. Instead, we show how to leverage this specific structure to obtain degree bounds on algebraic sets defined by the $\mathbf{f}_i$'s (the quantities δ^* and Δ^* are maxima of these bounds), so that one can control adequately the cost of the calls to the parametric geometric resolution algorithm (Schost, 2003) in replacement of Gröbner bases in the real root classification algorithm.

Next, we show how to remove the genericity assumptions on the input parametric linear matrix A . Our approach relies on a deformation technique, introduced in Henrion et al. (2021) for the non-parametric setting: we perturb A into a generic parametric linear matrix, solve the perturbed instance, and then recover boundary information by letting the perturbation tend to zero. While (Henrion et al., 2021) focuses on the related task of minimizing a linear functional over a spectrahedron, we show that the same ideas can be adapted to decide the emptiness of the spectrahedron, in both the non-parametric and parametric cases. As a result, we obtain an algorithm that solves Problem 1 for arbitrary input parametric linear matrix A , with the same asymptotic arithmetic complexity as in Theorem 1.

We focus on parameter-dependent LMIs of moderate matrix size and number of parameters, for which symbolic computation is realistic and practically useful. A key practical point is that the reduction phase ends with zero-dimensional systems. For practical experiments, we rely on optimized low level implementations for solving zero-dimensional systems of polynomial equations through Gröbner bases computations such as Berthomieu et al. (2021), since we are not aware on similar implementations for parametric geometric resolutions. Note that, in this setting, Gröbner basis routines are often effective, with costs polynomial in some Bézout-type bound. For the complexity proof, we still rely on geometric resolutions because they provide tighter specialization control in our structured families.

Finally, we report on implementation details and practical experiments of our algorithm, demonstrating that our approach allows us to solve instances of problems which were out of reach to previous algorithms (even for moderate values of n, m and t). Tests include topical examples of parametric LMIs which are used to encode convergence properties of first-order optimization algorithms (Drori and Teboulle, 2014; Taylor et al., 2017a,b). This yields a new application area in computer algebra. As a matter of fact, these parametric LMIs appear to have a moderate size m and number of parameters t which justify our approach. These experiments show that our algorithm is able to tackle such problems which are out of reach of the state-of-the-art implementations of real quantifier elimination in Maple (Chen and Moreno Maza, 2016) and Wolfram (Strzeboński, 2006): in particular, the instances GRD14, GRD23 and DRS43 are representative examples where our approach succeeds while generic QE is intractable. For more details and comparisons, we refer the reader to Section 9.

Relation to the ISSAC 2025 paper (Naldi et al., 2025) This paper is an extended version of our earlier work (Naldi et al., 2025), published in the proceedings of ISSAC 2025. Theorem 1 is a strict generalization of the ISSAC result: it keeps the same asymptotic complexity while extending correctness from the generic case to degenerate inputs. This extension is important for automated convergence analysis of optimization schemes, where singular parameter configurations can naturally appear. We also report practical results from a new implementation in Julia and describe, in full detail, the techniques that enabled us to solve examples that were previously out of reach in Naldi et al. (2025). (See Table 2.)

Plan of the paper Section 2 presents the basic notions of determinantal and incidence varieties which are used to define the $\mathbf{f}_i$'s. Section 3 presents the algorithm in Henrion et al. (2016a, Sec. 3.3) for solving generic LMIs. Section 4 describes our algorithm for solving generic parametric LMIs, whose correctness is proven in Section 5, and whose complexity is analyzed in Section 6. Section 7 presents

Table 2

Positioning with respect to the ISSAC 2025 version.

Feature	ISSAC 2025 (Naldi et al., 2025)	This paper
Assumptions on inputs	Generic only	Arbitrary
Degeneracy handling	Not covered	Deformation-based
Relevance for convergence analysis of LMLs	Limited to regular instances	Covers singular instances
Implementation	Maple	Julia
Experiments	Limited	Expanded, with more instances resolved

our approach to handle non-generic inputs. Section 8 discusses implementation details of our algorithm. Section 9 reports on practical experiments.

2. Preliminaries

Throughout the paper, we denote by $\tilde{R} = \mathbb{Q}[\mathbf{y}][\mathbf{x}]$, and $R = \mathbb{Q}[\mathbf{x}]$, as a special case of $\tilde{R}$ with $t = 0$.

2.1. Basic notions

Critical points Let $\mathcal{V} \subset \mathbb{C}^n$ be a smooth and equidimensional algebraic set, and $\phi : \mathbb{C}^n \rightarrow \mathbb{C}^i$ be a regular map, with $i \in \llbracket 1, n \rrbracket$ (where $\llbracket 1, n \rrbracket := \{1, \dots, n\}$). We denote by $\text{crit}(\phi, \mathcal{V})$ the set of critical points of the restriction of ϕ to $\mathcal{V}$, i.e., the points where the Jacobian matrix $\text{jac}(\mathbf{f}, \phi)$ of $(\mathbf{f}, \phi)$ has rank $\leq n - \dim(\mathcal{V})$, where $\mathbf{f} \subset R$ is a polynomial system generating the ideal $I(\mathcal{V})$ associated with $\mathcal{V}$ (see, e.g., Safey El Din and Schost (2003, Sec. 3.1)).

Properness Let E be a topological space, $\mathcal{V} \subset E^n$, and $\phi : \mathcal{V} \mapsto \mathbb{C}^i$ be a map, with $i \in \llbracket 1, n \rrbracket$. We say that ϕ is proper if for all $y \in \phi(\mathcal{V})$, there exists a Euclidean closed neighborhood $\mathcal{O}_y$ of y such that $\phi^{-1}(\overline{\mathcal{O}})$ is Euclidean closed and bounded, where $\overline{\mathcal{O}}$ denotes the closure of $\mathcal{O}$.

Change of variables Let F be a field of characteristic 0, and $M \in \text{GL}_n(\mathbb{Q})$ be an invertible matrix. For any polynomial $p \in F[\mathbf{x}]$, we denote by p^M the polynomial satisfying $p^M(\mathbf{x}) = p(M\mathbf{x})$. Analogously, for any set $\mathcal{E} \subset F^n$, we denote by $\mathcal{E}^M := \{M^{-1}\mathbf{x} \mid \mathbf{x} \in \mathcal{E}\}$.

Projections Let $\mathcal{V}$ be an algebraic set of $\mathbb{C}^{t+n}$ defined by a polynomial system in $\tilde{R}$. We write $\pi_{\mathbf{x}}(\mathcal{V}) \subset \mathbb{C}^n$ for the image of $\mathcal{V}$ under the projection onto the $\mathbf{x}$ -coordinates, and similarly $\pi_{\mathbf{y}}(\mathcal{V}) \subset \mathbb{C}^t$ for the projection onto the $\mathbf{y}$ -coordinates. More generally, for each $i \in \llbracket 1, n \rrbracket$, we denote by $\pi_{x_i}(\mathcal{V}) \subset \mathbb{C}$ the projection of $\mathcal{V}$ onto the coordinate x_i , and by $\pi_i(\mathcal{V}) \subset \mathbb{C}^i$ the projection of $\mathcal{V}$ onto the first i $\mathbf{x}$ -coordinates $x_{[1,i]} := x_1, \dots, x_i$.

2.2. Regularity and auxiliary results

Let $\mathcal{V}$ be a locally closed set of $\mathbb{C}^n$. We say that $\mathcal{V}$ satisfies **P** (resp. **P**(d)) if the Zariski closure of $\mathcal{V}$ is either empty or smooth and equidimensional (resp. of dimension d).

We say that a polynomial system $\mathbf{f} \subset \tilde{R}$ satisfies assumption **A** (resp. **A**(d)) if $\mathbf{f}$ generates a radical ideal, whose associated algebraic set $V(\mathbf{f})$ satisfies **P** (resp. **P**(d)).

The following lemma then serves as an equidimensional version of the Theorem on the Dimension of Fibres (Shafarevich and Reid, 1994, Th. 1.25).

Lemma 2. *Let $\mathbf{f} \subset \mathbb{Q}[\mathbf{y}, \mathbf{x}]$ be a finite set of polynomials satisfying **A**(d), with $d \geq t$. Denote by $d' = d - t$. Then, there exists a non-empty Zariski open set $\mathcal{Y} \subset \mathbb{C}^t$ such that for all $y \in \mathcal{Y}$, the specialization $\mathbf{f}(y, \cdot)$ satisfies **A**(d').*

Proof. If $V(\mathbf{f})$ is empty, it generates the ideal $\langle 1 \rangle$, as does $\mathbf{f}(y, \cdot)$ for all $y \in \mathbb{C}^t$, and the lemma holds. We assume now $V(\mathbf{f}) \neq \emptyset$.

If $\pi_y(V(\mathbf{f}))$ is contained in a proper Zariski closed subset of $\mathbb{C}^t$, we take $\mathcal{Y}$ to be the complement of this subset. Then, for all $y \in \mathcal{Y}$, $V(\mathbf{f}(y, \cdot))$ is empty, so the lemma also holds trivially.

Hence, assume that $\pi_y(V(\mathbf{f}))$ is Zariski dense in $\mathbb{C}^t$. By the Theorem on the Dimension of Fibres (Shafarevich and Reid, 1994, Th. 1.25), there exists a non-empty Zariski open set $\mathcal{Y}'$ of $\mathbb{C}^t$ such that for all $y \in \mathcal{Y}'$, $\pi_y^{-1}(y) \cap V(\mathbf{f})$ is an algebraic set of dimension d' .

Since $\mathbf{f}$ satisfies A(d), $\text{crit}(\pi_y, V(\mathbf{f}))$ is defined by the vanishing of $\mathbf{f}$ and the $(n - d')$ -minors of $\text{jac}(\mathbf{f}, \pi_y)$ (Safey El Din and Schost, 2017, Lem. A.2). By Sard's theorem (Safey El Din and Schost, 2017, Prop. B.2), $\pi_y(\text{crit}(\pi_y, V(\mathbf{f})))$ is contained in a proper Zariski closed subset $Z \subset \mathbb{C}^t$. Let $\mathcal{Y} = (\mathbb{C}^t \setminus Z) \cap \mathcal{Y}'$. Then, for all $y \in \mathcal{Y}$, $x \in \pi_x(\pi_y^{-1}(y) \cap V(\mathbf{f}))$, $\text{jac}(\mathbf{f})(y, x)$ has rank $n - d'$. By the Jacobian criterion (Eisenbud, 2013, Th. 16.19), $\mathbf{f}(y, \cdot)$ satisfies A(d'). $\square$

2.3. Determinantal and incidence varieties

Let $A \in \mathbb{S}_m(\tilde{R}_{\leq 1})$ be a parametric linear matrix, and $r \in \llbracket 0, m - 1 \rrbracket$. The determinantal variety $\mathcal{D}_r \subset \mathbb{C}^{t+n}$ of A of rank r is defined as

$$\mathcal{D}_r := \{(y, x) \in \mathbb{C}^{t+n} \mid \text{rank}(A(y, x)) \leq r\}.$$

A desingularization of $\mathcal{D}_r$ in the sense of Room-Kempf (Bank et al., 2010) is given as follows: let $U = (u_{i,j})_{i \in \llbracket 1, m \rrbracket, j \in \llbracket 1, m-r \rrbracket}$ be a matrix of variables. For all $\iota \subset \llbracket 1, m \rrbracket$ with $|\iota| = m - r$, define the incidence variety $\mathcal{V}_{r,\iota} \subset \mathbb{C}^{t+n+m(m-r)}$ of A as

$$\mathcal{V}_{r,\iota} := \{(y, x, u) \in \mathbb{C}^{t+n+m(m-r)} \mid A(y, x) \cdot U = 0, U_\iota = \text{Id}_{m-r}\},$$

where U_ι is formed by the rows of U indexed by ι .

Following (Henrion et al., 2016a, Lem. 3.2), we construct a defining system $\mathbf{f}_{r,\iota} \subset \tilde{R}[\mathbf{u}]$ for $\mathcal{V}_{r,\iota}$ as follows: let $G = (g_{i,j})_{i \in \llbracket 1, m \rrbracket, j \in \llbracket 1, m-r \rrbracket}$ the matrix obtained by substituting the entries of $U_\iota = \text{Id}_{m-r}$ into $A \cdot U$, so that G is independent of $u_{i,j}$'s for $i \in \iota$. Then, $\mathbf{f}_{r,\iota}$ is defined by the polynomials in $(g_{i,j})_{i \geq j}$ and $U_\iota - \text{Id}_{m-r}$.

Example 2. For the parametric linear matrix A in Example 1, we have $r = 1$, $U = (u_{1,1}, u_{2,1})^T$, and $\iota = \{1\}$, so that

$$G = A \cdot U = \begin{bmatrix} axu_{1,1} + bu_{1,1} + cu_{2,1} + xu_{2,1} \\ cu_{1,1} + xu_{1,1} + u_{2,1} \end{bmatrix}.$$

Imposing $U_\iota = \text{Id}_{m-r}$ yields $u_{1,1} = 1$. After substituting this into G , we obtain $\mathbf{f}_{r,\iota} = (ax + b + cu_{2,1} + xu_{2,1}, c + x + u_{2,1}, u_{1,1} - 1)$, which corresponds to the first three polynomials appearing in Equation (1).

For the last three polynomials, we refer the reader to the continuation of this example in Section 3.2.

Properties of determinantal and incidence varieties The dimension of $\mathcal{D}_r$ and its fibers $\mathcal{D}_r(y, \cdot)$ are classical results.

Theorem 3 (Anjos and Lasserre, 2011, Prop. 3.2). *For all $d \in \mathbb{N}$, there exists a non-empty Zariski open set $\mathcal{A}_d \subset \mathbb{S}_m(\mathbb{C}[\mathbf{y}]_{\leq d}[\mathbf{x}]_{\leq 1})$ such that for all $A \in \mathcal{A}_d \cap \mathbb{S}_m(\mathbb{Q}[\mathbf{y}]_{\leq d}[\mathbf{x}]_{\leq 1})$ and $r \in \llbracket 0, m - 1 \rrbracket$,*

1. $\mathcal{D}_r$ is empty or of dimension $t + n - \binom{m-r+1}{2}$;
2. In the case where $t \geq 1$, there exists a non-empty Zariski open set $\mathcal{Y}_A \subset \mathbb{C}^t$ such that for all $y \in \mathcal{Y}_A \cap \mathbb{R}^t$, $\mathcal{D}_r(y, \cdot)$ is either empty or of dimension $n - \binom{m-r+1}{2}$.

The dimension of $\mathcal{V}_{r,\iota}$ and its fibers $\mathcal{V}_{r,\iota}(y, \cdot)$, as well as their regularity, are given by the following lemma, which is a generalization of Henrion et al. (2016a, Prop. 3.4). Its proof is given in Section 5.

Lemma 4. For all $d \in \mathbb{N}$, there exists a non-empty Zariski open set $\mathcal{A}_d \subset \mathbb{S}_m(\mathbb{C}[\mathbf{y}]_{\leq d}[\mathbf{x}]_{\leq 1})$ such that for all $A \in \mathcal{A}_d \cap \mathbb{S}_m(\mathbb{Q}[\mathbf{y}]_{\leq d}[\mathbf{x}]_{\leq 1})$, $r \in \llbracket 0, m-1 \rrbracket$, $\iota \in \llbracket 1, m \rrbracket$ with $|\iota| = m-r$,

1. $\mathbf{f}_{r,\iota}$ satisfies $P(t+n - \binom{m-r+1}{2})$;
2. when $t \geq 1$, there exists a non-empty Zariski open set $\mathcal{Y}_A \subset \mathbb{C}^t$ such that for all $y \in \mathcal{Y}_A \cap \mathbb{R}^t$, $\mathbf{f}_{r,\iota}(y, \cdot)$ satisfies $P(n - \binom{m-r+1}{2})$.

3. Algorithms for LMIs

3.1. Principles

Let $A \in \mathbb{S}_m(R_{\leq 1})$ (recall that $R = \mathbb{Q}[\mathbf{x}]$). Algorithm from Henrion et al. (2016a, Sec. 3.3) allows to decide whether the LMI $A \geq 0$ is feasible. For the ease of the reader, we recall in the following Henrion et al. (2016a, Th. 1.2), which leverages the relation between the boundary structure of $\mathcal{S} := \text{spec}(A)$ and the rank stratification of A :

Let $A \in \mathbb{S}_m(R_{\leq 1})$ be a linear matrix, $r_{\min} = \min_{x \in \mathcal{S}} \text{rank}(A(x))$, and suppose that the boundary of $\mathcal{S}$ is non-empty, i.e., $\partial \mathcal{S} \neq \emptyset$. Let $\mathcal{C}$ be a connected component of $\mathcal{D}_{r_{\min}} \cap \mathbb{R}^n$ such that $\mathcal{C} \cap \mathcal{S} \neq \emptyset$. Then $\mathcal{C} \subset \mathcal{S}$.

Consequently, solving the LMI $A \geq 0$ boils down to:

1. Pick $x \in \mathbb{Q}^n$, and decide if $x \in \mathcal{S} \setminus \partial \mathcal{S}$. If yes, return `true`;
2. Otherwise, $\mathcal{S} \neq \mathbb{R}^n$, so that $\mathcal{S} \neq \emptyset$ if and only if $\partial \mathcal{S} \neq \emptyset$. We compute at least one point per connected component of $\mathcal{D}_r \cap \mathbb{R}^n$, for all $r \in \llbracket 0, m-1 \rrbracket$, and then decide if the points intersect $\mathcal{S}$. If yes, return `true`, otherwise return `false`.

3.2. Critical point methods

For all $i \in \llbracket 1, n \rrbracket$, recall that $\pi_i : \mathbb{C}^n \rightarrow \mathbb{C}^i$ denotes the coordinate projection $x \mapsto x_{[1,i]} := (x_1, \dots, x_i)$. By a slight abuse of notation, we also set $\pi_0 : x \mapsto \bullet$. We start by recalling (Safey El Din and Schost, 2003, Th. 2). Let $\mathbf{f} \subset R$ and $\mathcal{V} = V(\mathbf{f})$.

Assume that $\mathbf{f}$ satisfies A(d). There exists a non-empty Zariski open set $\mathcal{M} \subset \text{GL}_n(\mathbb{C})$ such that for all $M \in \mathcal{M} \cap \text{GL}_n(\mathbb{Q})$,

1. The restriction of π_{i-1} to $\text{crit}(\pi_i, \mathcal{V}^M)$ is proper;
2. For all $i \in \llbracket 1, d+1 \rrbracket$, $\text{crit}(\pi_i, \mathcal{V}^M)$ satisfies $P(i-1)$;
3. For all $\tau = (\tau_1, \dots, \tau_d) \in \mathbb{R}^d$, the set

$$\bigcup_{i=1}^{d+1} (\text{crit}(\pi_i, \mathcal{V}^M) \cap \pi_{i-1}^{-1}(\tau_{[1,i-1]}))$$

is finite and meets all the connected components of $\mathcal{V}^M \cap \mathbb{R}^n$.

We use (Elliott et al., 2023, Sec. 5.2) to derive Lagrange polynomial systems defining the sets of critical points $\text{crit}(\pi_i, V(\mathbf{f}^M))$.

Lemma 5 (Elliott et al., 2023, Sec. 5.2). Assume that $\mathbf{f}$ satisfies A(d). There exists a non-empty Zariski open set $\mathcal{M} \subset \text{GL}_n(\mathbb{C})$ such that for all $M \in \mathcal{M} \cap \text{GL}_n(\mathbb{Q})$, it holds that

4. There exists a non-empty Zariski open set $\mathcal{T}_M \subset \mathbb{C}^n$ such that for all $\tau \in \mathcal{T}_M \cap \mathbb{Q}^n$, $i \in \llbracket 1, d+1 \rrbracket$,

$$\text{crit}(\pi_i, V(\mathbf{f}^M)) \cap \pi_{i-1}^{-1}(\tau_{[1,i-1]}) = \pi_{\mathbf{x}}(\text{Lag}(\mathbf{f}^M(\tau_{[1,i-1]}, \cdot))),$$

where $\text{Lag}(\mathbf{f}) = \mathbf{f} \cup (\lambda^T \text{jac}(\mathbf{f}) - (1, 0, \dots, 0))$ is the Lagrange system associated with $\mathbf{f}$, with λ a vector of variables.

We denote by POLARVARIETIES an algorithm which takes as input polynomials $\mathbf{f} = (f_1, \dots, f_s)$ and returns the Lagrange systems defined in Lemma 5. Under the assumptions of Safey El Din and Schost (2003, Th. 2), their solutions meet all connected components of $V(\mathbf{f}) \cap \mathbb{R}^n$.

Example 2 (continued). After obtaining $\mathbf{f}_{r,l} = (ax + b + cu_{2,1} + xu_{2,1}, c + x + u_{2,1}, u_{1,1} - 1)$ with variables $(x, u_{1,1}, u_{2,1})$, we have $\lambda = (\lambda_1, \lambda_2, \lambda_3)$, and

$$\text{jac}(\mathbf{f}_{r,l}) = \begin{bmatrix} a + u_{2,1} & 0 & x + c \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}.$$

Hence, $\lambda^T \text{jac}(\mathbf{f}_{r,l}) - (1, 0, \dots, 0) = (a\lambda_1 + u_{2,1}\lambda_1 + \lambda_2 - 1, \lambda_3, c\lambda_1 + x\lambda_1 + \lambda_2)$, which corresponds to the last three polynomials appearing in Equation (1).

3.3. Bridging the regularity gap

Let $A \in \mathbb{S}_m(R_{\leq 1})$ be a linear matrix. As $\mathcal{D}_r$ is not smooth in general, we cannot apply POLARVARIETIES directly to its defining system, but only to its desingularizations $\mathcal{V}_{r,l}$, where $l \subset \llbracket 1, m \rrbracket$ with $|l| = m - r$.

To compute at least one point per connected component of $\mathcal{D}_r \cap \mathbb{R}^n$ outside $\mathcal{D}_{r-1}$, Henrion et al. (2016a, Prop. 3.5, 3.6) show that it suffices to compute critical points on the incidence varieties $\mathcal{V}_{r,l}$, or the points given by the Lagrange systems of $\mathbf{f}_{r,l}$. We restate the result as follows:

Proposition 6 (Henrion et al., 2016a, Prop. 3.5 and 3.6). Assume that $\mathcal{V}_{r,l}$ satisfies $P(n - \binom{m-r+1}{2})$. Then, there exists a non-empty Zariski open set $\mathcal{M} \subset \text{GL}_n(\mathbb{C})$ such that for all $M \in \mathcal{M} \cap \text{GL}_n(\mathbb{Q})$, for any connected component $C \subset \mathcal{D}_r \cap \mathbb{R}^n$, the following holds:

1. For all $i \in \llbracket 1, d \rrbracket$, $\pi_i(C^M)$ is Euclidean closed; furthermore, for all $\tau \in \mathbb{R}$ lying on the boundary of $\pi_1(C^M)$, $\pi_1^{-1}(\tau) \cap C^M$ is finite.
2. Let τ in the boundary of $\pi_1(C^M)$. Then, for all $x \in \pi_1^{-1}(\tau) \cap C^M$ such that $x \in \mathcal{D}_r^M \setminus \mathcal{D}_{r-1}^M$, there exists $u \in \mathbb{R}^{m(m-r)}$, $l \subset \llbracket 1, m \rrbracket$ with $|l| = m - r$, such that $(x, u) \in \text{crit}(\pi_1, \mathcal{V}_{r,l}^M)$.
3. The saturation of the ideal generated by $\text{Lag}(\mathbf{f}_{r,l}^M)$ by an ideal associated with $\mathcal{D}_{r-1}^M$ is radical, and the locally closed set $\mathcal{E}_{r,l}^M := V(\text{Lag}(\mathbf{f}_{r,l}^M)) \cap \pi_{\mathbf{x}}^{-1}(\mathcal{D}_r^M \setminus \mathcal{D}_{r-1}^M)$ satisfies $P(\binom{m-r}{2})$.
4. $\pi_{\mathbf{x}}(\mathcal{E}_{r,l}^M)$ is either empty or finite.
5. Let $(x, u) \in \text{crit}(\pi_1, \mathcal{V}_{r,l}^M)$ such that $x \in \mathcal{D}_r^M \setminus \mathcal{D}_{r-1}^M$. Then, there exists $\lambda \in \mathbb{R}^{m(m-r) + \binom{m-r+1}{2}}$ such that $(x, u, \lambda) \in \mathcal{E}_{r,l}^M$.

We denote by REALDET an algorithm which takes as input $A \in \mathbb{S}_m(R_{\leq 1})$, generates for all $r \in \llbracket 0, m-1 \rrbracket$ and $l \subset \llbracket 1, m \rrbracket$ with $|l| = m - r$ the systems $\mathbf{f}_{r,l}$ describing the aforementioned incidence varieties and returns $(\mathbf{f}_{r,l,i})_{i \in \llbracket 1, d+1 \rrbracket}$, the output of POLARVARIETIES, when called on these systems with their associated rank r , with extra polynomials for the saturation of rank defects. The algorithm therefore consists purely of ring operations over R .

The routine PSDMATRIXCOND simply takes as input A and returns the coefficients of $\det(A + \lambda I_m)$ in R (where λ is a new variable).

Finally, the algorithm SOLVELMI takes as input $A \in \mathbb{S}_m(R_{\leq 1})$ and calls REALDET and PSDMATRIXCOND, to decide the existence of solutions to the systems returned by REALDET outside the appropriate determinantal varieties $\mathcal{D}_{r-1}$ and which make non-negative the polynomials output from PSDMATRIXCOND.

4. Algorithms for parametric LMIs

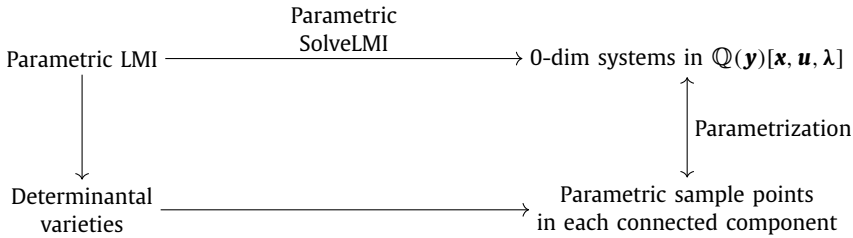
4.1. Principles

We consider now a parametric linear matrix $A \in \mathbb{S}_m(\tilde{R}_{\leq 1})$ (recall that $\tilde{R} = \mathbb{Q}[\mathbf{y}][\mathbf{x}]$). We have remarked that all operations performed by REALDET are ring operations over the coefficients of the entries of A . Hence, it can be used with entries in $\tilde{R}$. Hence, it returns a set of polynomial systems F in $\tilde{R}[\mathbf{u}, \lambda]$, which, specialized at any parameter $y \in \mathbb{Q}^t$, gives us the same result if we pass the linear matrix $A(y, \cdot) \in \mathbb{S}_m(R_{\leq 1})$ to the algorithm. Furthermore, we have the expected properties for a generic choice of y , as stated in the following proposition.

Proposition 7. *For all $d \in \mathbb{N}$, there exists a non-empty Zariski open set $\mathcal{A}_d \subset \mathbb{S}_m(\mathbb{C}[\mathbf{y}]_{\leq d}[\mathbf{x}]_{\leq 1})$ such that for all $A \in \mathcal{A}_d \cap \mathbb{S}_m(\mathbb{Q}[\mathbf{y}]_{\leq d}[\mathbf{x}]_{\leq 1})$, there exists a non-empty Zariski open set $\mathcal{M}_A \subset \text{GL}_n(\mathbb{C})$ such that for all $M \in \mathcal{M}_A \cap \text{GL}_n(\mathbb{Q})$, there exists a non-empty Zariski open set $\mathcal{T}_{A,M} \subset \mathbb{C}^n$ such that for all $\tau \in \mathcal{T}_{A,M} \cap \mathbb{Q}^n$, there exists a non-empty Zariski open set $\mathcal{Y}_{A,M,\tau} \subset \mathbb{C}^t$ such that for all $y \in \mathcal{Y}_{A,M,\tau} \cap \mathbb{R}^t$, $r \in \llbracket 0, m-1 \rrbracket$, $\iota \in \llbracket 1, m \rrbracket$ with $|\iota| = m - r$, $\bigcup_{r,\iota,i} \pi_{\mathbf{x}}(V(\mathbf{f}_{r,\iota,i}^M(y, \cdot)))$ is finite and contains at least one point per connected component of each $\mathcal{D}_r^M(y, \cdot)$.*

Proposition 7 introduces what we call the *generic assumptions*: a parametric linear matrix $A \in \mathbb{S}_m(\mathbb{Q}[\mathbf{y}]_{\leq d}[\mathbf{x}]_{\leq 1})$ is said to be generic if it lies in the non-empty Zariski open set $\mathcal{A}_d$ described in Proposition 7.

The proof of the proposition is technical and is given in Section 5. For the moment, let us focus on the consequence of the proposition. Intuitively, the polynomial systems $\mathbf{f} \in F$ are zero-dimensional in $\mathbb{Q}(\mathbf{y})[\mathbf{x}, \mathbf{u}, \lambda]$ for a generic choice of A . Moreover, for generic values of $y \in \mathbb{R}^t$, the union of the $\mathbf{x}$ -projections of $V(\mathbf{f}(y, \cdot))$ give points in each connected component of the determinantal varieties $\mathcal{D}_r(y, \cdot)$. F can therefore be seen as a parametric representation of sample points in each connected component of the determinantal varieties of A .



For such values of y , recall that deciding whether $\text{spec}(A(y, \cdot))$ is empty reduces to checking whether one of the sample points $x \in \mathbb{R}^n$ satisfies $A(y, x) \geq 0$, or equivalently, $\mathbf{g}(y, x) \geq 0$. Hence, to solve Problem 1, it is enough to compute, for each $\mathbf{f} \in F$, a semi-algebraic formula on $y \in \mathbb{R}^t$ that is true exactly when the conjunction $\mathbf{f}(y, \cdot) = 0$ and $\mathbf{g}(y, \cdot) \geq 0$ admits at least one real solution. Taking the disjunction of these formulas then yields the desired feasibility formula. Assume that we have the following subroutine:

- **CLASSIFICATION.**

Input: $\mathbf{f} = (f_1, \dots, f_p) \in \tilde{R}[\mathbf{u}, \lambda]$ such that $\langle \mathbf{f} \rangle_{\mathbb{Q}(\mathbf{y})}$ is zero-dimensional, $\mathbf{g} = (g_1, \dots, g_s) \in \tilde{R}$.

Output: a list of tuples of the form (Φ_i, y_i, r_i) , with Φ_i a semi-algebraic formula in $\mathbb{Q}[\mathbf{y}]$ defining $\mathcal{T}_i \subset \mathbb{R}^t$, $y_i \in \mathcal{T}_i$, $r_i \in \mathbb{N}$, such that

- For all $y \in \mathcal{T}_i$, $\mathbf{f}(y, \cdot) = 0 \wedge \mathbf{g}(y, \cdot) \geq 0$ has r_i real solutions,
- The union of $\mathcal{T}_i$ is dense in $\mathbb{R}^t$.

Algorithm 1 PARAMETRICSOLVEMLI.**Input:** $A \in S_m(\tilde{R}_{\leq 1})$ **Output:** A semi-algebraic formula Φ in $\mathbb{Q}[\mathbf{y}]$ defining a dense subset of the set $\{y \in \mathbb{R}^t \mid \exists x \in \mathbb{R}^n : A(y, x) \succeq 0\}$.

```

1: choose  $M \in GL_n(\mathbb{Q})$ 
2: choose  $\tau \in \mathbb{Q}^n$ 
3:  $\mathbf{F}^M \leftarrow \text{REALDET}(A, M, \tau)$ 
4:  $\mathbf{g}^M \leftarrow \text{CHANGEVARS}(\text{PSDMATRIXCOND}(A), M)$ 
5:  $\Phi \leftarrow \text{PSDMATRIXCOND}(A(\cdot, 0)) > 0$ 
6: for all  $\mathbf{f}_{r,\iota,i}^M \in \mathbf{F}^M$  do
7:    $\Phi_{r,\iota,i} \leftarrow \text{CLASSIFICATION}(\mathbf{f}_{r,\iota,i}^M, \mathbf{g}^M)$ 
8:    $\Phi \leftarrow \Phi \vee \bigvee_{j:r_j > 0} \Phi_{r,\iota,i,j}$ 
9: end for
10: return  $\Phi$ 

```

Then, it suffices to take the disjunction of Φ_i for which $r_i > 0$ to obtain the desired semi-algebraic formulas. We deduce Algorithm 1 for solving the generic feasibility problem for parametric LMIs.

Proof of Theorem 1 (generic inputs, algorithmic correctness)

Proposition 8. Let $A \in S_m(\tilde{R}_{\leq 1})$ be a parametric linear matrix. Assume that A is generic in the sense of Proposition 7, and all parameters chosen in Algorithm 1 satisfy the generic assumptions of Proposition 7. Then, Algorithm 1 is correct.

Proof. Let Φ be the output of Algorithm 1. For all $y \in \mathbb{R}^t$, $\Phi(y)$ holds implies that either $A_y(0) \succeq 0$, or there exists r, ι, i and $x \in \pi_{\mathbf{x}}(V(\mathbf{f}_{r,\iota,i}^M(y, \cdot)))$ such that $\mathbf{g}^M(y, x) \succeq 0$. In both cases, we have found a point $x \in \text{spec}(A_y)^M$, so that $\text{spec}(A_y) \neq \emptyset$. Hence, Φ defines a subset of $\{y \in \mathbb{R}^t \mid \text{spec}(A_y) \neq \emptyset\}$. Now, let $\mathcal{Y} \subset \mathbb{C}^t$ be the Zariski open set given by Proposition 7, and let $y \in \mathcal{Y} \cap \mathbb{R}^t$. Suppose that $\text{spec}(A_y) \neq \emptyset$. If $\text{spec}(A_y) = \mathbb{R}^n$, then $A_y(0) \succeq 0$, and therefore $\Phi(y)$ holds. Otherwise, $\partial \text{spec}(A_y) \neq \emptyset$. Proposition 7 then gives us r, ι, i such that $\pi_{\mathbf{x}}(V(\mathbf{f}_{r,\iota,i}^M(y, \cdot)))$ is finite and meets $\partial \text{spec}(A_y)^M$; this implies $\Phi_{r,\iota,i}(y)$ holds, and therefore $\Phi(y)$ holds. Hence, Φ defines a dense subset of $\{y \in \mathbb{R}^t \mid \text{spec}(A_y) \neq \emptyset\}$, which concludes the proof. $\square$

Finally, we explain how to implement the CLASSIFICATION subroutine. We first take (Gaillard and Safey El Din, 2024, Alg. 2), which deals with the condition $\mathbf{f}(y, \cdot) = 0 \wedge \mathbf{g}(y, \cdot) > 0$. Then, in Line 26 of Gaillard and Safey El Din (2024, Alg. 2), we change the definition of r_y , from the entry corresponding to $(1, \dots, 1) \in \{0, 1, -1\}^s$, to the sum of entries corresponding to $\{0, 1\}^s$. Then, r_y is the number of real solutions such that $\text{sign}(\mathbf{g}(y, \cdot)) \in \{0, 1\}^s$.

4.2. Hermite's quadratic form

Let $\mathbb{K}$ be a base field of characteristic 0, and $\mathbf{f} \subset \mathbb{K}[\mathbf{x}]$ be a polynomial system generating a zero-dimensional ideal $\langle \mathbf{f} \rangle_{\mathbb{K}}$. By Basu et al. (2016, Th. 4.86), the vector space $\mathcal{A}_{\mathbb{K}} := \mathbb{K}[\mathbf{x}] / \langle \mathbf{f} \rangle_{\mathbb{K}}$ has finite dimension, denoted δ . For all $g \in \mathcal{A}_{\mathbb{K}}$, the Hermite's bilinear map is defined by

$$\begin{aligned} \text{herm}(\mathbf{f}, g) : \mathcal{A}_{\mathbb{K}} \times \mathcal{A}_{\mathbb{K}} &\rightarrow \mathbb{K} \\ (p, q) &\mapsto \text{Tr}(L_{gpq}), \end{aligned}$$

where L_{gpq} is the multiplication map $h \mapsto gpqh$ on $\mathcal{A}_{\mathbb{K}}$, and Tr denotes the trace. The associated quadratic form $\text{Herm}(\mathbf{f}, g) : p \mapsto \text{herm}(\mathbf{f}, g)(p, p)$ is then called Hermite's quadratic form.

Hermite's theorem Basu et al. (2016, Th. 4.102) When $\mathbb{K} \subset \mathbb{R}$, for all $g \in \mathbb{K}[\mathbf{x}]$, denote by $\text{TaQ}(g, \mathbf{f})$ the Tarski-query of g for $\mathbf{f}$, defined as

$$\text{TaQ}(g, \mathbf{f}) := |\{x \in V(\mathbf{f}) \mid g(x) > 0\}| - |\{x \in V(\mathbf{f}) \mid g(x) < 0\}|.$$

The following identities hold:

- $\text{rank}(\text{Herm}(\mathbf{f}, g)) = |\{x \in V(\mathbf{f}) \mid g(x) \neq 0\}|$.
- $\text{Sign}(\text{Herm}(\mathbf{f}, g)) = \text{TaQ}(g, \mathbf{f})$,

where $\text{Sign}(\Phi)$ denotes the signature of the quadratic form Φ .

Hermite matrices Let $\mathcal{B} = (b_1, \dots, b_\delta)$ be a basis of $\mathcal{A}_{\mathbb{K}}$. For all $g \in \mathcal{A}_{\mathbb{K}}$, the Hermite matrix associated with g with respect to $\mathcal{B}$ is then defined as the matrix $\mathcal{H}_{\mathbf{g}} = (h_{i,j})_{i,j \in \llbracket 1, \delta \rrbracket} \in \mathbb{S}_\delta(\mathbb{K})$, where $h_{i,j} = \text{herm}(\mathbf{f}, g)(b_i, b_j) = \text{Tr}(L_{gb_i b_j})$.

To compute $h_{i,j}$, let $M_{gb_i b_j} = (m_{k,\ell})_{k,\ell \in \llbracket 1, \delta \rrbracket}$ be the multiplication matrix of $L_{gb_i b_j}$ with respect to $\mathcal{B}$. By definition, $m_{k,\ell}$ is the coefficient of b_ℓ in the representative of $gb_i b_j b_k$ in $\mathcal{A}_{\mathbb{K}}$, which can be obtained by a normal form computation if $\mathbf{f}$ is given by a Gröbner basis. We can then proceed by $h_{i,j} = \text{Tr}(M_{gb_i b_j}) = \sum_{k \in \llbracket 1, \delta \rrbracket} m_{k,k}$.

Specialization property of parametric Hermite matrices Let $\mathbb{K} = \mathbb{Q}(\mathbf{y})$, $\mathbf{f} \subset \mathbb{K}[\mathbf{x}]$ generating a zero-dimensional ideal $\langle \mathbf{f} \rangle_{\mathbb{K}}$, and $g \in \mathbb{K}[\mathbf{x}]$. Let $\succ_{\mathbf{x}}$ and $\succ_{\mathbf{y}}$ be monomial orders for $\mathbf{x}$ and $\mathbf{y}$, respectively, and $\succ$ be an elimination order which eliminates $\mathbf{x}$, built with $\succ_{\mathbf{x}}$ and $\succ_{\mathbf{y}}$. Let $\mathcal{G}$ be the reduced Gröbner basis of $\langle \mathbf{f} \rangle$ with respect to $\succ$, and $\mathcal{B}$ be the monomial basis formed by the monomials of $\mathbb{K}[\mathbf{x}]$ irreducible by $\mathcal{G}$.

The following generalizes (Gaillard and Safey El Din, 2024, Prop. 3.1), by dropping the assumption that $\succ_{\mathbf{x}}$ and $\succ_{\mathbf{y}}$ are graded reverse lexicographic orders.

Theorem 9. Let $\mathcal{W}_\infty := \bigcup_{\gamma \in \mathcal{G}} V(\text{lc}_{\mathbf{x}}(\gamma))$, where $\text{lc}_{\mathbf{x}}(\gamma)$ is the leading coefficient of the polynomial $\gamma \in \mathbb{K}[\mathbf{x}]$ with respect to $\succ_{\mathbf{x}}$. Then, for all $y \in \mathbb{C}^t \setminus \mathcal{W}_\infty$,

1. The specialization $\mathcal{G}(y, \cdot)$ is a Gröbner basis of $\langle \mathbf{f}(y, \cdot) \rangle$ with respect to $\succ_{\mathbf{x}}$.
2. Consequently, $\text{Herm}(\mathbf{f}, g)(y, \cdot) = \text{Herm}(\mathbf{f}(y, \cdot), g(y, \cdot))$.

Proof. For $y \in \mathbb{C}^t \setminus \mathcal{W}_\infty$, $\text{lc}_{\mathbf{x}}(g)$ does not vanish at y for every $g \in \mathcal{G}$. By Kalkbrener (1997, Th. 3.1), $\mathcal{G}(y, \cdot)$ is then a Gröbner basis of $\langle \mathbf{f}(y, \cdot) \rangle$ with respect to $\succ_{\mathbf{x}}$. We then conclude by the same proof as in Le and Safey El Din (2022, Prop. 10): for $y \in \mathbb{C}^t \setminus \mathcal{W}_\infty$, none of the denominators appearing in the normal form reductions by $\mathcal{G}$ vanish at y , so that $\text{Herm}(\mathbf{f}, g)$ specializes correctly to $\text{Herm}(\mathbf{f}(y, \cdot), g(y, \cdot))$ at y . $\square$

4.3. Real root counting

Let $\mathbb{K} = \mathbb{R}$, $\mathbf{f} \subset \mathbb{R}[\mathbf{x}]$ be a polynomial system, and $g \in \mathbb{R}[\mathbf{x}]$. Denote by $c(\sigma, \mathbf{f}) := |\{x \in V(\mathbf{f}) \mid \text{sign}(g(x)) = \sigma\}|$, we have

$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & -1 \\ 0 & 1 & 1 \end{bmatrix} \begin{bmatrix} c(0, \mathbf{f}) \\ c(1, \mathbf{f}) \\ c(-1, \mathbf{f}) \end{bmatrix} = \begin{bmatrix} \text{TaQ}(g^0, \mathbf{f}) \\ \text{TaQ}(g^1, \mathbf{f}) \\ \text{TaQ}(g^2, \mathbf{f}) \end{bmatrix}.$$

The identity can be generalized to a tensor identity, in the case where $\mathbf{g} = (g_1, \dots, g_s) \subset \mathbb{R}[\mathbf{x}]$. Denote by $\text{SIGN}(\mathbf{g}, \mathbf{f}) \subset \{0, 1, -1\}^s$ the set of realizable signs of $\mathbf{g}$ on $V(\mathbf{f})$.

Theorem 10 (Basu et al., 2016, Prop. 10.70). Let $A = (\alpha_1, \dots, \alpha_{|A|}) \subset \{0, 1, 2\}^s$, $\Sigma = (\sigma_1, \dots, \sigma_{|\Sigma|}) \subset \{0, 1, -1\}^s$, each in the lexicographic order. Suppose that $\Sigma \supset \text{SIGN}(\mathbf{g}, \mathbf{f})$. Then,

$$\text{Mat}(A, \Sigma) \cdot c(\Sigma, \mathbf{f}) = \text{TaQ}(\mathbf{g}^A, \mathbf{f}),$$

where

- $\text{Mat}(A, \Sigma) = (\sigma_j^{\alpha_i})_{i \in \llbracket 1, |A| \rrbracket, j \in \llbracket 1, |\Sigma| \rrbracket}$,
- $c(\Sigma, \mathbf{f}) = (c(\sigma_j, \mathbf{f}))_{j \in \llbracket 1, |\Sigma| \rrbracket}$,
- $\text{TaQ}(\mathbf{g}^A, \mathbf{f}) = (\text{TaQ}(\mathbf{g}^{\alpha_i}, \mathbf{f}))_{i \in \llbracket 1, |A| \rrbracket}$.

A trivial choice of Σ is $\Sigma = \{0, 1, -1\}^S$, which gives $\mathbf{c}$ simply by inverting the square matrix $\text{Mat}(A, \Sigma)$. By summing the coefficients corresponding to $\sigma \in \{0, 1\}^S$, we obtain $a_1, \dots, a_{|A|} \in \mathbb{Q}$ such that

$$|\{x \in V(\mathbf{f}) \mid \mathbf{g}(x) \geq 0\}| = \sum_{i=1}^{|A|} a_i \text{Sign}(\text{Herm}(\mathbf{g}^{\alpha_i}, \mathbf{f})). \quad (3)$$

It suffices to extract a semi-algebraic formula corresponding to the positivity of the linear combination of signatures. For this, we have several options:

- (O1) We can directly return the positivity assertion (3), which is itself a semi-algebraic formula.
- (O2) Let $S \subset \mathbb{R}^t$ be the semi-algebraic set defined by the non-vanishing of the non-zero principal minor of maximal size of all Hermite matrices. Then, on each connected component of S , the signatures of the Hermite matrices are constant. Thus, we can then return the *realizable* combinations of signatures after computing one point per connected component of S and examining the signatures on these points.
- (O3) Moreover, the signature of a Hermite matrix is generically determined by the sign variation of its leading principal minors (see, e.g., Gaillard and Safey El Din, 2024, Lem. 4.8). If we add the condition of their non-vanishing in the definition of S , we can refine the formula into a combination of signs of the leading principal minors of the Hermite matrices.

When $\mathbb{K} = \mathbb{R}(\mathbf{y})$, by Theorem 9, Equation (3) holds for generic specializations of $\mathbf{y} \in \mathbb{R}^t$, if we further intersect S with $\mathbb{R}^t \setminus \mathcal{W}_\infty$. This leads us to the use of Gaillard and Safey El Din (2024, Alg. 2) which performs real root classification for parametric zero-dimensional systems using Hermite matrices, combined with the following subroutine:

- **SAMPLEPOINTS.**

Input: a semi-algebraic formula Φ in $\mathbb{Q}[\mathbf{y}]$.

Output: a finite set of points in $\mathbb{R}^t$ containing at least one point per connected component of the semi-algebraic set defined by Φ . We refer to Le and Safey El Din (2022) for an algorithm having such a specification (see also references therein).

5. Proof of genericity

This section is dedicated to the proof of Proposition 7, which gives us the last piece of the puzzle to prove the correctness of Algorithm 1. The main difficulty is to show that the choices of $M \in \text{GL}_n(\mathbb{Q})$ and $\tau \in \mathbb{Q}^n$ in Proposition 7 do not depend on the choice of parameters $\mathbf{y} \in \mathbb{R}^t$. The proof requires a careful analysis of all the propositions and lemmas presented in the previous sections.

5.1. Expected dimension of incidence varieties

Proof of Lemma 4(1). For all $d \in \mathbb{N}$, denote by n_d the dimension of $\mathbb{Q}[\mathbf{y}]_{\leq d}$. Observe that, as a vector space, $\mathbb{S}_m(\mathbb{Q}[\mathbf{y}]_{\leq d}[\mathbf{x}]_{\leq 1})$ is isomorphic to $\mathbb{S}_m^{(n+1)n_d}(\mathbb{Q})$, so that we can rewrite A as

$$A(\mathbf{y}, \mathbf{x}) = \sum_{\substack{k \in \mathbb{N}^t, |k| \leq d \\ \ell \in \mathbb{N}^n, |\ell| \leq 1}} A_{k, \ell} \mathbf{y}^k \mathbf{x}^\ell,$$

where $A_{k, \ell} = (a_{k, \ell, i, j})_{i, j \in \llbracket 1, m \rrbracket} \in \mathbb{S}_m(\mathbb{Q})$. Denote then, by abuse of notation, $A \in \mathbb{S}_m^{(n+1)n_d}(\mathbb{Q})$ the parametric linear matrix.

Suppose w.l.o.g. that r is fixed, $\iota = \llbracket 1, m-r \rrbracket$. Consider the map

$$\begin{aligned} \varphi : \mathbb{C}^{t+n+m(m-r)} \times \mathbb{S}_m^{(n+1)n_d}(\mathbb{C}) &\rightarrow \mathbb{C}^{m(m-r)+\binom{m-r+1}{2}}, \\ (y, x, u, A) &\mapsto \mathbf{f}_{r,\iota}, \end{aligned}$$

and, for $A \in \mathbb{S}_m^{(n+1)n_d}(\mathbb{Q})$, its induced map

$$\begin{aligned} \varphi_A : \mathbb{C}^{t+n+m(m-r)} &\rightarrow \mathbb{C}^{m(m-r)+\binom{m-r+1}{2}}, \\ (y, x, u) &\mapsto \varphi(y, x, u, A) = \mathbf{f}_{r,\iota}, \end{aligned}$$

so that $\varphi_A^{-1}(0) = V(\mathbf{f}_{r,\iota}) = \mathcal{V}_{r,\iota}$. If $\varphi^{-1}(0) = \emptyset$, for all $A \in \mathbb{S}_m^{(n+1)n_d}(\mathbb{Q})$, $\varphi_A^{-1}(0)$ is empty and we are done. Otherwise, assume that $\varphi^{-1}(0) \neq \emptyset$. Note that for all $(y, x, u, A) \in \varphi^{-1}(0)$, $\text{jac}(\varphi)(y, x, u, A)$ has full rank, given by

- the derivatives w.r.t. $(a_{0,0,i,j})_{i \in \llbracket 1, m-r \rrbracket \vee j \in \llbracket 1, m-r \rrbracket}$ of the entries of G , and,
- the derivatives w.r.t. $(u_{i,j})_{i \in \iota, j \in \llbracket 1, m-r \rrbracket}$ of the entries of $U_\iota - \text{Id}_{m-r}$.

Hence, 0 is a regular value of φ . By Thom's weak transversality theorem (Safey El Din and Schost, 2017, Prop. B.3), there exists a non-empty Zariski open set $\mathcal{A}_d \subset \mathbb{S}_m^{(n+1)n_d}(\mathbb{C})$ such that for all $A \in \mathcal{A}_d \cap \mathbb{S}_m^{(n+1)n_d}(\mathbb{Q})$, 0 is a regular value of φ_A . By the Jacobian criterion (Eisenbud, 2013, Th. 16.19), $\mathbf{f}_{r,\iota}$ satisfies $P(t+n-\binom{m-r+1}{2})$. $\square$

Proof of Lemma 4 (2). As $\mathbf{f}_{r,\iota}$ satisfies $P(t+n-\binom{m-r+1}{2})$, by Lemma 2, there exists a non-empty Zariski open set $\mathcal{Y} \subset \mathbb{C}^t$ such that for all $y \in \mathcal{Y} \cap \mathbb{R}^t$, $\mathbf{f}_{r,\iota}(y, \cdot)$ satisfies $P(n-\binom{m-r+1}{2})$. $\square$

We then generalize Lemma 4 (2), so that the choice of $\tau \in \mathbb{Q}^n$ in REALDET becomes independent of the choice of $y \in \mathbb{R}^t$ in the following proposition.

Proposition 11. *Under the assumptions of Lemma 4, the following additional result holds:*

3. In the case where $t \geq 1$, there exists a non-empty Zariski open set $\mathcal{T} \subset \mathbb{C}^n$ such that for all $\tau \in \mathcal{T} \cap \mathbb{Q}^n$, there exists a non-empty Zariski open set $\mathcal{Y}_\tau \subset \mathbb{C}^t$ such that for all $y \in \mathcal{Y}_\tau \cap \mathbb{R}^t$, for all $i \in \llbracket 1, n+1 \rrbracket$, $\mathbf{f}_{r,\iota}(y, \tau_{\llbracket 1, i-1 \rrbracket}, \cdot)$ satisfies $P(n-\binom{m-r+1}{2}-i)$.

Proof. As $\mathbf{f}_{r,\iota}$ satisfies $P(t+n-\binom{m-r+1}{2})$, by Lemma 2, for all $i \in \llbracket 1, n+1 \rrbracket$, there exists a non-empty Zariski open set $\mathcal{T}_i \subset \mathbb{C}^n$ such that for all $\tau \in \mathcal{T}_i \cap \mathbb{Q}^n$, there exists a non-empty Zariski open set $\mathcal{Y}_{i,\tau} \subset \mathbb{C}^t$ such that for all $y \in \mathcal{Y}_{i,\tau} \cap \mathbb{R}^t$, $\mathbf{f}_{r,\iota}(y, \tau_{\llbracket 1, i-1 \rrbracket}, \cdot)$ satisfies $P(n-\binom{m-r+1}{2}-i)$. We then take $\mathcal{T} = \cap_{i=1}^{n+1} \mathcal{T}_i$ and $\mathcal{Y}_\tau = \cap_{i=1}^{n+1} \mathcal{Y}_{i,\tau}$. $\square$

5.2. Dancing with genericity

We now give parametric generalizations of Proposition 6. These will imply that one can run over a fraction field the algorithms of Henrion et al. (2016a) to reduce to real root classification problems the one of solving a parametric LMI.

Lemma 12. *Assume that for all $r \in \llbracket 0, m-1 \rrbracket$, $\iota \in \llbracket 1, m \rrbracket$ with $|\iota| = m-r$, $\mathcal{V}_{r,\iota}$ satisfies $P(t+n-\binom{m-r+1}{2})$. Then, there exists a non-empty Zariski open set $\mathcal{M} \subset \text{GL}_n(\mathbb{C})$ such that for all $M \in \mathcal{M} \cap \text{GL}_n(\mathbb{Q})$, there exists a non-empty Zariski open set $\mathcal{Y}_M \subset \mathbb{C}^t$ such that for all $y \in \mathcal{Y}_M \cap \mathbb{R}^t$, for any connected component $\mathcal{C} \subset \mathcal{D}_r(y, \cdot) \cap \mathbb{R}^n$, the results of Proposition 6 hold.*

Proof. The proof of Proposition 6 follows from Henrion et al. (2016b, Prop. 17, 18). As the proof of Henrion et al. (2016b, Prop. 17) is purely algebraic and thus valid over the base field $\mathbb{C}(\mathbf{y})$, we can then invert the order of choosing $\mathbf{y}$ and M as in Le and Safey El Din (2021, Prop. 6). $\square$

Lemma 13. Assume that for all $r \in \llbracket 0, m-1 \rrbracket$, $\iota \in \llbracket 1, m \rrbracket$ with $|\iota| = m-r$, $\mathcal{V}_{r,\iota}$ satisfies $P(t+n - \binom{m-r+1}{2})$. Then, there exists a non-empty Zariski open set $\mathcal{M} \subset \mathrm{GL}_n(\mathbb{C})$ such that for all $M \in \mathcal{M} \cap \mathrm{GL}_n(\mathbb{Q})$, there exists a non-empty Zariski open set $\mathcal{Y}_M \subset \mathbb{C}^t$ such that for all $\mathbf{y} \in \mathcal{Y}_M \cap \mathbb{R}^t$, $\iota \in \llbracket 1, m \rrbracket$ with $|\iota| = m-r$, the results of Proposition 6 hold.

Proof. The proof of Proposition 6 follows from Henrion et al. (2016a, Lem. 4.2 (i)). Applying the same proof shows that for generic choice of M , the system (f, g, h) in Henrion et al. (2016a, Eq. 4.3) satisfies Q in $\mathcal{O} = \{(x, y, z) : \mathrm{rank} A(x) = r\}$, i.e., the rank of $D(f, g, h)$ is the codimension of $V((f, g, h))$ in $V((f, g, h)) \cap \mathcal{O}$. The choice of $\mathbf{y}$ is then generic and follows from the Th. on the Dimension of Fibres (Shafarevich and Reid, 1994, Th. 1.25). $\square$

Proof of Proposition 7. For all $d \in \mathbb{N}$, let $\mathcal{A}_d$ be the intersection of the Zariski open sets defined in Theorem 3 and Lemma 4. Then, for all $A \in \mathcal{A}_d \cap \mathbb{S}_m(\mathbb{Q}[\mathbf{y}]_{\leq d}[\mathbf{x}]_{\leq 1})$, the assumptions of the above lemmas are satisfied. It is then straightforward to show that for generic choices of $M \in \mathrm{GL}_n(\mathbb{Q})$ and $\tau \in \mathbb{Q}^n$, there exists a non-empty Zariski open set $\mathcal{Y}_{A,M,\tau} \subset \mathbb{C}^t$ such that for all $\mathbf{y} \in \mathcal{Y}_{A,M,\tau} \cap \mathbb{R}^t$, the results of Proposition 6 hold for $A(\mathbf{y}, \cdot) \in \mathbb{S}_m(R_{\leq 1})$, and that for all $r \in \llbracket 0, m-1 \rrbracket$, $\iota \in \llbracket 1, m \rrbracket$ with $|\iota| = m-r$, $i \in \llbracket 1, n+1 \rrbracket$, $\mathcal{D}_r(\mathbf{y}, \cdot)$, $\mathcal{V}_{r,\iota}(\mathbf{y}, \cdot)$, and $\mathbf{f}_{r,\iota,i}(\mathbf{y}, \cdot)$ satisfy all the results in Henrion et al. (2016a). The correctness of Proposition 7 then follows from the correctness of Henrion et al. (2016a, Th. 3.7). $\square$

6. Complexity analysis

We give now a complexity analysis of Gaillard and Safey El Din (2024, Alg. 2) (and hence, by construction, of CLASSIFICATION), without the extra genericity condition assumed in Gaillard and Safey El Din (2024), i.e., the homogeneous components of $\mathbf{f}$ of highest degree form a regular sequence. Denote $\mathcal{M}_{a,b} = \binom{a+b}{a}$.

6.1. Parametric geometric resolutions

Let $\mathbf{f} = (f_1, \dots, f_p) \in \tilde{R}[\mathbf{u}, \boldsymbol{\lambda}]$ generating a zero-dimensional ideal $\langle \mathbf{f} \rangle_{\mathbb{Q}(\mathbf{y})}$, and $\mathbf{g} = (g_1, \dots, g_s) \in \tilde{R}$. In the case where $\mathbf{f}$ generates a radical ideal, we can use parametric geometric resolutions.

Definition 14. Let $P \in \mathbb{Q}(\mathbf{y})[\mathbf{x}]$ be a polynomial. We denote by $\mathrm{denom}(P) \in \mathbb{Q}[\mathbf{y}]$ the least common multiple of the denominators of the coefficients of P , and by $\mathrm{num}(P) = P \mathrm{denom}(P) \in \tilde{R}$.

Proposition 15 (Parametric geometric resolution, Schost, 2003, Th. 1). Denote by $\Delta := \deg(V(\mathbf{f}))$ the affine degree (see, e.g., Heintz, 1983) of the algebraic set $V(\mathbf{f})$, and $\delta := \deg_{\pi}(\mathbf{f})$ the generic cardinality of the fibers of the canonical projection $\pi : (\mathbf{y}, \mathbf{x}) \mapsto \mathbf{y}$ to $V(\mathbf{f})$. Then,

1. There exists a monic irreducible polynomial $q \in \mathbb{Q}(\mathbf{y})[T]$ and polynomials $v_1, \dots, v_n \in \mathbb{Q}(\mathbf{y})[T]$, with

$$\begin{aligned} \deg_T(q) &= \delta, & \deg_T(v_i) &\leq \delta - 1, \\ \deg(\mathrm{denom}(q)) &\leq \Delta, & \deg(\mathrm{denom}(v_i)) &\leq \Delta, \\ \deg_{\mathbf{y}}(\mathrm{num}(q)) &\leq 2\Delta, & \deg_{\mathbf{y}}(\mathrm{num}(v_i)) &\leq 2\Delta, \end{aligned}$$

such that the parametrization

$$q(\mathbf{y}, T) = 0, \quad x_i = \frac{v_i(\mathbf{y}, T)}{q'(\mathbf{y}, T)} \quad \forall i \in \llbracket 1, n \rrbracket$$

gives the solutions of the system $\mathbf{f}(y, x) = 0$ when both systems are specialized at all parameters $y = (y_1, \dots, y_t) \in \mathbb{Q}^t$ such that $q, v_1, \dots, v_n$ are well-defined and q' is not identically zero.

2. There exist polynomials $\tilde{v}_1, \dots, \tilde{v}_s \in \mathbb{Q}(\mathbf{y})[T]$, with

$$\begin{aligned} \deg_T(\tilde{v}_i) &\leq \delta - 1, & \deg(\text{denom}(\tilde{v}_i)) &\leq \Delta \deg(g_i), \\ \deg_{\mathbf{y}}(\text{num}(\tilde{v}_i)) &\leq 2\Delta \deg(g_i), \end{aligned}$$

such that, when denoting by

$$\tilde{g}_i := \frac{\tilde{v}_i(y, T)}{q'(y, T)} \quad \forall i \in \llbracket 1, s \rrbracket,$$

the sign of $\mathbf{g}(y, x)$ is the same as the sign of $\tilde{\mathbf{g}}_i$ for all solutions of the parametrization.

Proof. 1. Let $\mathbb{Q}(\mathbf{y}) \rightarrow \mathbb{Q}(\mathbf{y})[\mathbf{x}]/(\mathbf{f})_{\mathbb{Q}(\mathbf{y})}$ be a field extension, and u be a primitive element of the extension with coefficients in $\mathbb{Q}$, so that $q, v_1, \dots, v_n$, as well as the degree bounds, are given by the parametric geometric resolution of $\mathbf{f}(y, x) = 0$ for u (Schost, 2003, Th. 1).
2. Consider the system $\mathbf{f}(y, x) = 0$, $g_i(y, x) - \tilde{g}_i = 0$, where $\tilde{g}_i$ is a new variable. As the value of $\tilde{g}_i$ is uniquely determined by other variables, u is a primitive element of the extension $\mathbb{Q}(\mathbf{y}) \rightarrow \mathbb{Q}(\mathbf{y})[\mathbf{x}, \tilde{\mathbf{g}}]/(\mathbf{f}, g_i - \tilde{g}_i)_{\mathbb{Q}(\mathbf{y})}$, and $\deg_{\pi}(\mathbf{f}, g_i - \tilde{g}_i) = \deg_{\pi}(\mathbf{f})$. The parametrization of $\tilde{\mathbf{g}}_i$ is then given by the parametric geometric resolution of the system for u . Finally, Bézout's theorem gives $\deg(V(\mathbf{f}, g_i - \tilde{g}_i)) \leq \Delta \deg(g_i)$. The degree bounds follow. $\square$

We recall that the Lagrange systems with saturation of rank defects generically satisfy the assumptions above. Hence, we compute the parametric geometric resolution, and pass $\mathbf{f} = q$ and $\mathbf{g} = (\tilde{g}_1, \dots, \tilde{g}_t)$ to CLASSIFICATION instead. We then have $\mathcal{B} = \{1, T, \dots, T^{\delta-1}\}$, as the unique monomial basis of $\mathbb{Q}(\mathbf{y})[T]/\langle q \rangle_{\mathbb{Q}(\mathbf{y})}$. For $\alpha \in \{0, 1, 2\}^s$, the Hermite matrix $\mathcal{H}_{\mathbf{g}^\alpha}$ w.r.t. $\mathcal{B}$ is, using the notations of Basu et al. (2016),

$$(\mathcal{H}_{\mathbf{g}^\alpha})_{i,j} = \text{Tr}(M_{T^{i+j}\mathbf{g}^\alpha}) = \sum_{k=1}^{\delta} \text{cof}(T^k, \text{Rem}_T(T^{i+j+k}\mathbf{g}^\alpha, q)). \quad (4)$$

Complexity analysis Let $\deg(\mathbf{f}) := \max_i \deg(f_i)$ and $\deg(\mathbf{g}) := \max_i \deg(g_i)$. By Schost (2003, Th. 2), there exists a probabilistic algorithm which computes the polynomials in Proposition 15 (1) using

$$\tilde{O}\left((n\Gamma_{\mathbf{f}} + n^4 + t^2n)\delta\mathcal{M}_{t,4\Delta}\right)$$

arithmetic operations in $\mathbb{Q}$, where $\Gamma_{\mathbf{f}}$ is the length of a straight-line program evaluating $\mathbf{f}$, and the notation $g = \tilde{O}(f)$ refers to $g = O(f \log^{\kappa}(f))$ for some $\kappa > 0$. For Proposition 15 (2), by simply reapplying the algorithm for each $i \in \llbracket 1, s \rrbracket$, we arrive at

$$\tilde{O}\left(\sum_{i=1}^s (n(\Gamma_{\mathbf{f}} + \Gamma_{g_i}) + n^4 + t^2n)\delta\mathcal{M}_{t,4\Delta \deg(\mathbf{g})}\right). \quad (5)$$

Bounds on p, s . Let $\mathbf{f} = \mathbf{f}_{r,t,i} \in \tilde{R}[\mathbf{u}, \lambda]$ be one of the polynomial systems given by Line 3 of Algorithm 1, and $\mathbf{g} \subset \tilde{R}$ be given by PSDMATRIXCOND. By definition, each Lagrange system of $\mathbf{f}_{r,t}$ has at most $O(n + m^2)$ polynomials, on which we add $\binom{m}{r}$ polynomials for the saturation of rank defects. We then denote by $p^* \in O(n + 2^m)$ a global bound on p , and similarly, $s^* \in O(m)$.

Bounds on $\Gamma_{\mathbf{f}}, \Gamma_{g_i}$. Let $\mathbf{f} = \mathbf{f}_{r,t,i} \in \tilde{R}[\mathbf{u}, \lambda]$ be one of the polynomial systems given by Line 3 of Algorithm 1, and $\mathbf{g} \subset \tilde{R}$ be given by PSDMATRIXCOND. To evaluate each polynomial in $\mathbf{f}_{r,t,i}$ or $\mathbf{g}$, we

can first evaluate the linear matrix in $O(m^2 n \mathcal{M}_{d,t})$ arithmetic operations in $\mathbb{Q}$, and then compute the evaluation of $\mathbf{f}$ and $\mathbf{g}$ purely in $\mathbb{Q}$. Hence, we have $\Gamma_{\mathbf{f}}^* \in \tilde{O}(2^m n^2 \mathcal{M}_{d,t})$ and $\Gamma_{\mathbf{g}}^* \in O(m^{O(1)} n \mathcal{M}_{d,t})$.

Bound on $\deg(\mathbf{g})$. Let $\mathbf{g} \subset \tilde{R}$ be the polynomial system given by PSDMATRIXCOND. Then, we have $\deg(\mathbf{g}) \leq \deg(\det(\lambda I_m + A)) = m(d+1)$, where $d := \deg_{\mathbf{y}}(A)$ is the maximum degree of the entries of A in $\mathbf{y}$. We then have $\deg(\mathbf{g})^* \in O(md)$.

Bounds on $\deg(\mathbf{f}), \delta$. Let $\mathbf{f} = \mathbf{f}_{r,t,i} \subset \tilde{R}[\mathbf{u}, \lambda]$ be one of the polynomial systems given by Line 3 of Algorithm 1. By Henrion et al. (2016a, Prop. 5.1), for all $y \in \mathbb{R}^t$ such that $\mathbf{f}_{r,t,i}(\mathbf{y}, \cdot)$ is well-defined, the specialized Lagrange system is of maximum degree 2, hence of total degree $d+2$, and that $\delta \leq \delta^* := \mathcal{M}_{n, m(m+1)/2}^3$ when $n \leq m(m+1)/2$, and 0 otherwise. Furthermore, the saturation of rank defects consists of polynomials of total degree $r(d+1)$, so that $\deg(\mathbf{f}) = \max(d+2, r(d+1))$, i.e., $\deg(\mathbf{f})^* \in O(md)$.

Bound on Δ . Let $\mathcal{U} = (u_{ij})_{i,j \in \llbracket 1, m \rrbracket}$ be the general symmetric matrix with entries variables u_{ij} (with $u_{ji} = u_{ij}$), and $m^* := m(m+1)/2$. One has $\text{sing}(\mathcal{D}_r) = \mathcal{D}_{r-1}$ and $\mathcal{D}_r \subset \mathbb{C}^{m^*}$ is equidimensional of codimension $c := \binom{m-r+1}{2}$ (Bruns and Vetter (2006)). Thus, $\mathcal{D}_r \setminus \mathcal{D}_{r-1}$ is a constructible set of local pure codimension c and locally defined by c equations $\boldsymbol{\mu} = (\mu_1, \dots, \mu_c)$ of degree $\leq r+1$ in the entries of $\mathcal{U}$.

Consider the groups of variables $\mathbf{u} = (u_{ij}, 1 \leq i \leq j \leq m)$, $\mathbf{y} = (y_1, \dots, y_t)$ and $\mathbf{x} = (x_1, \dots, x_n)$. Let $\mathbf{v} = [u_{ij} - a_{ij}(\mathbf{y}, \mathbf{x}), 1 \leq i \leq j \leq m]$ be the list of polynomials defining the entries of the parametric LMI, of degree 1 with respect to $\mathbf{u}$ and $\mathbf{x}$, and of degree d with respect to $\mathbf{y}$.

Define the system $\mathbf{f} = [\boldsymbol{\mu}, \mathbf{v}]$ consisting of $c + m^*$ polynomials in $n + t + m^*$ variables. The Jacobian matrix of $\mathbf{f}$ with respect to the three variable groups above is:

$$\text{jac}(\mathbf{f}) = \begin{bmatrix} \text{jac}_{\mathbf{u}}(\boldsymbol{\mu}) & 0 & 0 \\ \text{Id}_{m^*} & \text{jac}_{\mathbf{y}}(\mathbf{v}) & \text{jac}_{\mathbf{x}}(\mathbf{v}) \end{bmatrix}.$$

Remark that $\text{jac}_{\mathbf{x}}(\mathbf{v})$ is constant in $\mathbf{x}$. Next we introduce Lagrange multipliers $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_{c+m^*})$ and consider the augmented system $[\mathbf{f}, \boldsymbol{\lambda}^T \text{jac}(\mathbf{f})]$. With respect to $(\mathbf{u}, \mathbf{y}, \mathbf{x}, \boldsymbol{\lambda})$, one has:

$$\boldsymbol{\mu} \rightarrow c \text{ polynomials of } \text{mdeg} \leq (r+1, 0, 0, 0)$$

$$\mathbf{v} \rightarrow m^* \text{ polynomials of } \text{mdeg} \leq (1, d, 1, 0)$$

$$\boldsymbol{\lambda}^T \text{jac}_{\mathbf{u}}(\mathbf{f}) \rightarrow m^* \text{ polynomials of } \text{mdeg} \leq (r, 0, 0, 1)$$

$$\boldsymbol{\lambda}^T \text{jac}_{\mathbf{y}}(\mathbf{f}) \rightarrow t \text{ polynomials of } \text{mdeg} \leq (0, d-1, 1, 1)$$

$$\boldsymbol{\lambda}^T \text{jac}_{\mathbf{x}}(\mathbf{f}) \rightarrow n \text{ polynomials of } \text{mdeg} \leq (0, d, 0, 1)$$

The value of Δ , by Safey El Din and Schost (2017, Prop. I.1), is bounded from above by a multilinear Bézout bound given by the sum of coefficients of

$$\begin{aligned} & ((r+1)\theta_u)^c (\theta_u + d\theta_y + \theta_x)^{m^*} (r\theta_u + \theta_\lambda)^{m^*} \\ & ((d-1)\theta_y + \theta_x + \theta_\lambda)^t (d\theta_y + \theta_\lambda)^n \end{aligned}$$

modulo $\langle \theta_u^{m^*+1}, \theta_y^{t+1}, \theta_x^{n+1}, \theta_\lambda^{c+m^*+1} \rangle$. Since the polynomial is homogeneous of degree $t + n + 2m^* + c$, this is also $(r+1)^c$ times the coefficient of $\theta_u^{m^*-c} \theta_y^t \theta_x^n \theta_\lambda^{c+m^*}$ of the polynomial

$$\begin{aligned} P &:= (\theta_u + d\theta_y + \theta_x)^{m^*} (r\theta_u + \theta_\lambda)^{m^*} \\ & ((d-1)\theta_y + \theta_x + \theta_\lambda)^t (d\theta_y + \theta_\lambda)^n. \end{aligned}$$

The multilinear bound, denoted by $\text{MBB}(\Delta)$, is thus

$$(r+1)^c \text{cof}(\theta_u^{m^*-c} \theta_y^t \theta_x^n \theta_\lambda^{c+m^*}, P) \\ = (r+1)^c \sum_{\Theta} d^{\alpha_y} r^{\beta_u} (d-1)^{\gamma_y} d^{\delta_y} \binom{m^*}{\alpha_u, \alpha_y, \alpha_x} \binom{m^*}{\beta_u} \binom{t}{\gamma_y, \gamma_x, \gamma_\lambda} \binom{n}{\delta_y},$$

where Θ is the set of $(\alpha_u, \alpha_y, \alpha_x, \beta_u, \gamma_y, \gamma_x, \gamma_\lambda, \delta_y)$ satisfying

$$\begin{aligned} \alpha_u + \alpha_y + \alpha_x &= m^* & \gamma_y + \gamma_x + \gamma_\lambda &= t \\ \alpha_u + \beta_u &= m^* - c & \alpha_y + \gamma_y + \delta_y &= t \\ \alpha_x + \gamma_x &= n & m^* - \beta_u + \gamma_\lambda + n - \delta_y &= c + m^*. \end{aligned} \quad (6)$$

Lemma 16. For $n > m^* + t$, we have $\text{MBB}(\Delta) = 0$. In particular, if m and t are fixed, the bound is 0 for large n .

Proof. The contribution of θ_x in P is only given by factors $(\theta_u + d\theta_y + \theta_x)^{m^*}$ and $((d-1)\theta_y + \theta_x + \theta_\lambda)^t$, thus any monomial of P has degree $\leq m^* + t$ in θ_x , so that $\Theta = \emptyset$ if $n > m^* + t$. If m and t are fixed, so does $m^* + t$, hence for large n the bound is 0. $\square$

We remark that this is also true for the bound on δ in Henrion et al. (2016a, Prop. 5.1). Let us now bound the size of Θ .

Lemma 17. $|\Theta| \leq \min\{(t+1)^3, (t+1)(n+1)^2\}$.

Proof. Equation (6) can be reduced to $L = [\alpha_u = \gamma_y + \delta_y + \gamma_x + m^* - t - n, \alpha_y = -\gamma_y - \delta_y + t, \alpha_x = -\gamma_x + n, \gamma_\lambda = -\gamma_y - \gamma_x + t, \beta_u = -\gamma_y - \delta_y - \gamma_x + t + n - c]$, with free $\gamma_y, \gamma_x, \delta_y$: these latter verify the bounds $0 \leq \gamma_y \leq t$, $0 \leq \gamma_x \leq \min\{t, n\}$, and $0 \leq \delta_y \leq \min\{t, n\}$. Thus $|\Theta| \leq (t+1)(\min\{t, n\} + 1)^2$ as claimed. $\square$

Lemma 18. Let Δ^* be defined as

$$(6r+6)^{m^*} d^{2t+m^*} \left(e \frac{m^* + c + t}{m^* + c} \right)^{m^*+c} 3^t \min\{(t+1)^3, (t+1)(n+1)^2\}.$$

Then, $\text{MBB}(\Delta)$ is bounded from above by Δ^* .

Proof. Recall that $\delta_y \leq t$ in Θ . Let $D = m^* + c - (n - \delta_y)$, which is nonnegative (from the last equation in (6), using $\beta_u \leq m^*$). One has $n + D = m^* + c + \delta_y \leq m^* + c + t$ and hence

$$\binom{n}{\delta_y} = \binom{n}{n - \delta_y} = \binom{n}{m^* + c - D} \leq \binom{n+D}{m^* + c} \leq \binom{m^* + c + t}{m^* + c},$$

and the last binomial is bounded by $\left(e \frac{m^* + c + t}{m^* + c} \right)^{m^*+c}$. Thus from $(\alpha_u, \alpha_y, \alpha_x) \leq 3^{m^*}$ and $(\beta_u) \leq 2^{m^*}$, $\text{MBB}(\Delta)$ is at most

$$\begin{aligned} (r+1)^c d^{m^*} r^{m^*-c} (d-1)^t d^t \sum_{\Theta} \binom{m^*}{\alpha_u, \alpha_y, \alpha_x} \binom{m^*}{\beta_u} \binom{t}{\gamma_y, \gamma_x, \gamma_\lambda} \binom{n}{\delta_y} \\ \leq (r+1)^c d^{m^*} r^{m^*-c} (d-1)^t d^t \left(e \frac{m^* + c + t}{m^* + c} \right)^{m^*+c} 3^{m^*} 2^{m^*} 3^t |\Theta|, \end{aligned}$$

and we conclude by Lemma 17. $\square$

6.2. Degree bounds on Hermite matrices

We recall that a Hermite matrix $\mathcal{H}_{\mathbf{g}^\alpha}$ has its entries given by Equation (4). To compute the remainders in the equation, as each $\tilde{g}_i$ has denominator q' , we need to find the inverse of q' modulo q , or the inverse of $\text{num}(q')$ modulo $\text{num}(q)$. Let $c = \text{Res}(\text{num}(q), \text{num}(q')) \in \mathbb{Q}[\mathbf{y}]$, and denote by $a, b \in \mathbb{Q}[\mathbf{y}][T]$ the polynomials of degree at most $\deg_T(q)$ such that $a \text{num}(q) + b \text{num}(q') = c$. Once b is known, $c^{-1}b$ is the inverse of $\text{num}(q')$ by $\text{num}(q)$.

Lemma 19. *Let $P, Q \in \mathbb{Q}[\mathbf{y}][T]$ be polynomials in T , with coefficients in $\mathbb{Q}[\mathbf{y}]$. Denote by $M = \max(\deg_{\mathbf{y}}(P), \deg_{\mathbf{y}}(Q))$. Then,*

$$\deg_{\mathbf{y}}(\text{Res}(P, Q)) \leq M(\deg_T(P) + \deg_T(Q)),$$

$$\deg_{\mathbf{y}}(\text{Prem}_T(P, Q)) \leq M \max(\deg_T(P) - \deg_T(Q) + 2, 1)$$

Moreover, there exists $A, B \in \mathbb{Q}[\mathbf{y}][T]$, with $\deg_T(A) \leq \deg_T(Q)$, $\deg_T(B) \leq \deg_T(P)$, such that $AP + BQ = \text{Res}(P, Q)$, and

$$\max(\deg_{\mathbf{y}}(A), \deg_{\mathbf{y}}(B)) \leq M(\deg_T(P) + \deg_T(Q)).$$

Finally, all the items above can be computed in $O(\deg_T(P) \deg_T(Q))$ operations in $\mathbb{Q}[\mathbf{y}]$.

Proof. Suppose w.l.o.g. that $\deg_T(P) \geq \deg_T(Q)$. From Basu et al. (2016, Eq. 4.3, Not. 8.55), using the notations of Basu et al. (2016), we have

$$\text{Res}(P, Q) = \varepsilon_{\deg_T(P)} \text{sRes}_0(P, Q),$$

$$\text{Prem}(P, Q) = \varepsilon_{\deg_T(P) - \deg_T(Q) + 1} \text{sRes}_{\deg_T(Q) - 1}(P, Q),$$

where $\varepsilon_i = (-1)^{i(i-1)/2}$. The degree bounds then follow from Basu et al. (2016, Prop. 8.71). Moreover, Basu et al. (2016, Prop. 8.64) gives

$$\text{sRes}_0(P, Q) = \text{sRemU}_0(P, Q)P + \text{sRemV}_0(P, Q)Q,$$

with sRemU_0 and sRemV_0 satisfying the same degree bounds as sRes_0 . Finally, all the items can be computed in Basu et al. (2016, Alg. 8.81), hence the complexity. $\square$

As a direct consequence, $\deg_T(b) \leq \delta$, $\deg_{\mathbf{y}}(b) \leq 2\Delta(2\delta - 1)$, and $\deg(c) \leq 2\Delta(2\delta - 1)$. We then factor out the denominator from the sum in Equation (4), and hence deduce a degree bound on the entries of Hermite matrices and their principal minors.

Proposition 20. *For $\alpha \in \{0, 1, 2\}^s$, there exists $\rho \in \mathbb{Q}[\mathbf{y}]$, with*

$$\deg(\rho) \leq |\alpha| \Delta(6\delta - 3 + \deg(\mathbf{g})) + \Delta(2\delta - 2),$$

where $|\alpha| := \sum_{i=1}^s \alpha_i$, such that for all $i, j \in \llbracket 0, \delta - 1 \rrbracket$, $\rho M_{T^{i+j} \mathbf{g}^\alpha}$ is a matrix with entries in $\mathbb{Q}[\mathbf{y}]_{\leq \mathcal{D}(|\alpha|)}$, where

$$\begin{aligned} \mathcal{D}(|\alpha|) &:= 2\Delta(2\delta - 1) \max(1, |\alpha|(|\alpha| + 1)(2\delta - 1 + \deg(\mathbf{g}))) \\ &\quad + \Delta(3\delta - 3) + |\alpha| \Delta \in O(|\alpha|^2(\delta + m\delta)\delta\Delta). \end{aligned}$$

Proof. We rewrite the remainder as

$$\begin{aligned} \text{Rem}_T(T^{i+j+k} \mathbf{g}^\alpha, q) &= \text{Rem}_T(T^{i+j+k} \tilde{\mathbf{g}}^\alpha, q) \\ &= \frac{\text{denom}(q')^{|\alpha|}}{c^{|\alpha|} \text{denom}(p)} \frac{\text{Prem}_T(T^{i+j+k} \text{num}(p), \text{num}(q))}{\text{denom}(q)^{\max(i+j+k+\deg_T(p)-\deg_T(q)+1, 0)}}, \end{aligned}$$

where $p = b^{|\alpha|} \tilde{v}^\alpha \in \mathbb{Q}(\mathbf{y})[T]$, with the degree bounds

$$\begin{aligned} \deg_T(p) &\leq |\alpha| (2\delta - 1), \\ \deg_{\mathbf{y}}(\text{num}(p)) &\leq 2|\alpha| \Delta(2\delta - 1 + \deg(\mathbf{g})), \\ \deg(\text{denom}(p)) &\leq |\alpha| \Delta \deg(\mathbf{g}), \end{aligned}$$

so that

$$\begin{aligned} &\deg_{\mathbf{y}}(\text{Prem}(T^{i+j+k} \text{num}(p), \text{num}(q))) \\ &\leq 2\Delta \max(|\alpha| (2\delta - 1 + \deg(\mathbf{g})), 1) \max(i + j + k + |\alpha| (2\delta - 1) - \delta + 2, 1) \\ &\leq 2\Delta(2\delta - 1) \max(1, |\alpha| (|\alpha| + 1)(2\delta - 1 + \deg(\mathbf{g}))). \end{aligned}$$

It suffices then to take

$$\rho = c^{|\alpha|} \text{denom}(p) \text{denom}(q)^{\max(3\delta - 2 + \deg_T(p) - \deg_T(q), 0)},$$

hence the degree bound on ρ .

Moreover, suppose w.l.o.g. that $\deg_T(p) \geq \deg_T(q)$ holds. Then, for $k \in \llbracket 0, \delta - 1 \rrbracket$, we have

$$\begin{aligned} &\text{cof}(T^k, \text{Rem}_T(T^{i+j+k} \mathbf{g}^\alpha, q)) \\ &= \rho^{-1} \text{cof}(T^k, \text{Prem}_T(T^{i+j+k} \text{num}(p), \text{num}(q))) \\ &\quad \text{denom}(q)^{3\delta - 3 - i - j - k} \text{denom}(q')^{|\alpha|}, \end{aligned} \tag{7}$$

hence the degree bound on the entries of $\rho M_{T^{i+j} \mathbf{g}^\alpha}$. $\square$

Hence, the numerator of each $(\mathcal{H}_{\mathbf{g}^\alpha})_{i,j}$ has degree $\leq \mathcal{D}(|\alpha|)$, and the numerator of each minor of $\mathcal{H}_{\mathbf{g}^\alpha}$ has degree $\leq \delta \mathcal{D}(|\alpha|)$.

6.3. Arithmetic complexity

Recall that one can evaluate a multivariate polynomial P in k variables at any point within $O(\mathcal{M}_{\deg(P),k})$ arithmetic operations, using (Canny et al., 1989, Sec. 3a, 3b). Similarly, with $O(\mathcal{M}_{k,\deg(P)})$ interpolation points and the value of P at these points, one can recover P within $\tilde{O}(\mathcal{M}_{k,\deg(P)})$ arithmetic operations. Below, we don't use $\mathcal{M}_{\deg(P),k}$ and $\mathcal{M}_{k,\deg(P)}$ interchangeably, even though they are equal.

Proposition 21. Each call to Gaillard and Safey El Din (2024, Alg. 2) with input $\mathbf{f} = (f_1, \dots, f_p)$, $\mathbf{g} = (g_1, \dots, g_s)$ takes

$$\tilde{O}(s \mathcal{M}_{t,\delta \mathcal{D}(2s)} (2\delta s \beta)^{t+1} 2^{3t} (\delta \mathcal{D}(2s))^{2t+1}) \tag{8}$$

arithmetic operations in $\mathbb{Q}$, where β is the number of realizable signs of $\mathbf{g}$ on $V(\mathbf{f})$, and outputs at most $(4\delta s \beta \mathcal{D}(2s))^t$ formulas that consist of $O(\delta s \beta)$ polynomials of degree at most $\delta \mathcal{D}(2s)$.

Proof. By Gaillard and Safey El Din (2024, Prop. 4.11), each call to SAMPLEPOINTS involves at most $2\delta s \beta$ polynomials, and hence outputs a set of at most $(4\delta^2 s \beta \mathcal{D}(2s))^t$ points using at most $\tilde{O}(\mathcal{M}_{t,\delta \mathcal{D}(2s)} (2\delta s \beta)^{t+1} 2^{3t} (\delta \mathcal{D}(2s))^{2t+1})$ arithmetic operations in $\mathbb{Q}$. There are at most s calls to SAMPLEPOINTS, hence the complexity in Equation (8).

We show that the complexity of computing the minors (Lines 9 - 13) and evaluating the signatures (Lines 16, 25) is dominated by the complexity of computing sample points; as observed in Gaillard and Safey El Din (2024, Sec. 4.3), the other steps are simply linear algebra and negligible.

Lines 9 - 13. For $\mathcal{H}_{g^\alpha}$ with $|\alpha| \geq 1$, the numerator of $(\mathcal{H}_{g^\alpha})_{i,j}$, denoted by P , is given by Equation (4). Suppose w.l.o.g. that $\deg_T(p) \leq \deg_T(q) - 1$, so that the coefficients are given by Equation (7).

To compute P , we need $\mathcal{M}_{t, \deg(P)}$ interpolation points, where $\deg(P) \leq \mathcal{D}(|\alpha|)$. For each interpolation point $y \in \mathbb{Q}^t$, we first compute $\text{num}(p)(y)$, $\text{num}(q)(y)$, $\text{denom}(q)(y)$, and $\text{denom}(q')(y)$, in $O(\mathcal{M}_{\deg(\text{num}(p)), t+1})$ operations; then, for each $k \in \llbracket 0, \delta - 1 \rrbracket$, we compute $\text{Prem}_T(T^{i+j+k} \text{num}(p), \text{num}(q))(y)$ in $O(|\alpha| \delta^2)$ operations; finally, we compute $P(y)$ in $O(\delta)$ operations. Hence, we need $\tilde{O}(\mathcal{M}_{t, \mathcal{D}(|\alpha|)}(\mathcal{M}_{\deg(\text{num}(p)), t+1} + |\alpha| \delta^3))$ operations.

Consequently, computing $\mathcal{H}_{g^\alpha}$ takes the same complexity as P , as we can take the same points for all traces, and computing ρ has a negligible cost in front of P . Also, there are at most $2\delta\beta$ principal minors to compute, and computing each takes at most

$$\tilde{O}(\mathcal{M}_{t, \delta \mathcal{D}(2s)}(\mathcal{M}_{4s\Delta(2\delta-1+\deg(g))+2s(2\delta-1), t+1} + 2s\delta^3))$$

arithmetic operations in $\mathbb{Q}$, as it takes at most $O(\delta^3)$ operations for $\mathcal{H}_{g^\alpha}(y)$, and $O(\delta^\omega)$ operations for the determinant. However, all the above bounds are negligible in front of the complexity of computing sample points, as

$$\begin{aligned} & \mathcal{M}_{4s\Delta(2\delta-1+\deg(g))+2s(2\delta-1), t+1} \\ & < 2(4s\Delta(2\delta-1+\deg(g)) + 2s(2\delta-1))^{t+1} \\ & \ll (2s+1)(2\delta-1)(4s\Delta(2\delta-1+\deg(g)))^{t+1} \\ & < (\delta \mathcal{D}(2s))^{t+1} \ll (\delta \mathcal{D}(2s))^{2t+1}. \end{aligned}$$

Lines 16, 25. For the evaluation of the signatures, we recall that there are $3\delta\beta$ minors, whose numerators have degree at most $\delta \mathcal{D}(2s)$, to evaluate at at most $(4\delta^2 s \beta \mathcal{D}(2s))^t$ points. This is then in

$$O(\mathcal{M}_{t, \delta \mathcal{D}(2s)} \delta \beta (4\delta^2 s \beta \mathcal{D}(2s))^t)$$

arithmetic operations in $\mathbb{Q}$. $\square$

Proof of Theorem 1 (generic inputs, algorithmic complexity). For all $\mathbf{f} = \mathbf{f}_{r,t,i} \in \tilde{\mathcal{R}}[\mathbf{u}, \lambda]$, we have $s \leq m$, $\mathcal{D}(2s) \leq 32(m+1)^2(\delta + md + m)\delta\Delta$, and $\beta \leq 3^m$, so that the complexity of each call to CLASSIFICATION, given by Equation (8) in Proposition 21, is in

$$\tilde{O}\left(2^{3t} m (3^m 2m\delta)^{t+1} (32m^2(\delta + md)\delta^2\Delta)^{3t+1}\right)$$

operations in $\mathbb{Q}$. As REALDET gives at most $\sum_{r=0}^{m-1} \binom{m}{r} (n - \binom{m-r+1}{2}) = 2^{m-3}(8n - m^2 - 3m + 8) - n - 1$ polynomial systems, computing real root classifications for all $\mathbf{f}$ then take the complexity in Equation (2).

By Henrion et al. (2016a, Th. 5.6), REALDET is in $n^{O(m^2)} 2^{O(m)} (n + m^2)^{O(1)}$ arithmetic operations in $\mathbb{Q}[\mathbf{y}]$, which is negligible compared to the terms of Equation (2) without Δ^* , let alone the complexity in $\mathbb{Q}$ by interpolation. The same argument holds for PSDMATRIXCOND and CHANGEVARS. Finally, the complexity of computing each parametric geometric resolution, given by Equation (5), is in $2^{O(t+m)} (nt)^{O(1)} (md)^{O(t)} \delta^{\star t} \delta^{\star t}$ arithmetic operations in $\mathbb{Q}$, which is also negligible compared to the terms of Equation (2). $\square$

7. Handling degeneracies

So far, we have worked under the standing *genericity assumption* that $\mathbf{f}_{r,t}$ satisfies $P(t+n - \binom{m-r+1}{2})$, as is the case for *generic* parametric linear matrices $A \in \mathbb{S}_m(\tilde{\mathcal{R}}_{\leq 1})$. Here, the genericity stands on the coefficients of the entries of A . The aim of this section is to outline a standard strategy for dealing with *degenerate* cases, via a deformation technique. As we will see, this deformation operates on the constant coefficients of the entries of A only. The core strategy is to deform these coefficients

with the product of some rational number with formal parameter, say ε , to recover the genericity properties we use in the previous sections, solve the problem with this parameter in our base field and then let the parameter tend to 0. Hence, such a parameter encodes an infinitesimal. In this setting, which is quite classical in effective real algebraic geometry (see, e.g., Grigor'ev and Vorobjov, 1988; Heintz et al., 1990; Basu et al., 1996), all solutions have coordinates in the Puiseux series field $\mathbb{R}\langle\varepsilon\rangle$. Before proceeding, we recall some basic notions on infinitesimals and Puiseux series.

Puiseux series Let ε be an infinitesimal, i.e., a positive transcendental element smaller than any positive element in the base field. We denote by $\mathbb{R}\langle\varepsilon\rangle$ the field of Puiseux series in ε with real coefficients: each element is of the form $x = \sum_{i \geq i_0} a_i \varepsilon^{i/q}$, where $a_i \in \mathbb{R}$, $q \in \mathbb{N} \setminus \{0\}$ and $i_0 \in \mathbb{Z}$. We call x bounded if $i_0 \geq 0$. In this case, $a_0 \in \mathbb{R}$ is called the limit of x , and we denote it by $a_0 = \lim_{\varepsilon} x$. We extend $\lim_{\varepsilon}$ component-wise to vectors. For a set $Q \subset \mathbb{R}\langle\varepsilon\rangle^n$, we define $\lim_{\varepsilon} Q \subset \mathbb{R}^n$ to be the set of limits of all bounded elements of Q .

7.1. Finding minimizers via deformation

In Henrion et al. (2021), the authors address the problem of minimizing a linear functional $\ell : \mathbb{R}^n \rightarrow \mathbb{R}$ over a spectrahedron defined by a linear matrix $A \in \mathbb{S}_m(\mathbb{Q}[\mathbf{x}]_{\leq 1})$, using a deformation approach. They consider the perturbed matrix $A + \varepsilon B$, where $B \in \mathbb{S}_m(\mathbb{Q})$ and ε is an infinitesimal. (By abuse of notation, when ε is instead taken to be a small positive real number, we work over $\mathbb{R}$ rather than $\mathbb{R}\langle\varepsilon\rangle$.) We write $\mathbf{f}_{r,l}^{(\varepsilon)}$ for the polynomial system $\mathbf{f}_{r,l}$ associated with $A + \varepsilon B$, and similarly for $\mathbf{f}_{r,l,i}^{(\varepsilon)}$. We now recall the result of Henrion et al. (2021, Th. 11).

Proposition 22 (Henrion et al., 2021, Th. 11). *Let $A \in \mathbb{S}_m(\mathbb{Q}[\mathbf{x}]_{\leq 1})$ be a linear matrix. There exists a non-empty Zariski open set $\mathcal{B} \subset \mathbb{S}_m(\mathbb{C})$ such that for all $B \in \mathcal{B} \cap \mathbb{S}_m(\mathbb{Q})$, there exists a non-empty Zariski open set $\mathcal{M}_B \subset \text{GL}_n(\mathbb{C})$ such that for all $M \in \mathcal{M}_B \cap \text{GL}_n(\mathbb{Q})$, the set $\bigcup_{r,l} \lim_{\varepsilon} \pi_{\mathbf{x}}(V(\mathbf{f}_{r,l,1}^{(\varepsilon)M}))$ is finite. Moreover, if the minimum of π_1 on $\text{spec}(A)^M$ is attained, then this set contains a minimizer of π_1 on $\text{spec}(A)^M$.*

The idea of the proof is simple to state. If $B \in \mathbb{S}_m(\mathbb{Q})$, $M \in \text{GL}_n(\mathbb{Q})$ and $\varepsilon \in (0, 1]$ are chosen generically enough, one has that

1. $\pi_1(\text{spec}(A))^M$ and $\pi_1(\text{spec}(A + \varepsilon B))^M$ are Euclidean closed intervals of $\mathbb{R}$. Consequently, a minimizer $x \in \mathbb{R}^n$ of π_1 on $\text{spec}(A)^M$, if it exists, can be obtained as the limit of a sequence of minimizers $x^{(\varepsilon)} \in \mathbb{R}^n$ of π_1 on $\text{spec}(A + \varepsilon B)^M$;
2. Each $\mathbf{f}_{r,l}^{(\varepsilon)}$ satisfies $P(n - \binom{m-r+1}{2})$. Moreover, each minimizer $x^{(\varepsilon)}$ is contained in the finite set $\bigcup_{r,l} \pi_{\mathbf{x}}(V(\mathbf{f}_{r,l,1}^{(\varepsilon)M}))$, so that x is contained in the finite limit set $\bigcup_{r,l} \lim_{\varepsilon} \pi_{\mathbf{x}}(V(\mathbf{f}_{r,l,1}^{(\varepsilon)M}))$.

With these two ingredients, the result follows. One subtle point is that the genericity assumptions on B , M and ε enforce dependencies between these elements. The corresponding non-empty Zariski open sets that account for these dependencies are constructed in Henrion et al. (2021, Lem. 2, Cor. 3, Prop. 7, 8).

To design an algorithm based on Proposition 22, we must be able to represent points in $\mathbb{R}\langle\varepsilon\rangle^n$, and be able to compute their limits. Following Henrion et al. (2021), a set $Q \in \mathbb{R}\langle\varepsilon\rangle^n$ is encoded by a one-dimensional parametric geometric resolution in which ε is treated as a parameter. The limit set $\lim_{\varepsilon} Q$ can then be computed by applying Algorithm 2 below, adapted from Safey El Din and Schost (2018, Lem. 12, Sec. 3.5). As shown in Safey El Din and Schost (2018, Alg. 1), when $\mathbb{K} = \mathbb{Q}$, the algorithm takes quasi-linear time in the degree of the input and linear time in the number of variables.

7.2. From finding minimizers to finding boundary points

Proposition 22 shows that, for a suitable change of variables $M \in \text{GL}_n(\mathbb{Q})$, if $\pi_1(\text{spec}(A)^M)$ is a Euclidean closed interval with at least one finite endpoint, then the non-emptiness of $\text{spec}(A)$ can be

Algorithm 2 CUT.

Input: A one-dimensional parametrization given by $\hat{q}, \hat{v}_1, \dots, \hat{v}_n \in \mathbb{K}[\varepsilon, T]$ of an algebraic set $Q \subset \overline{\mathbb{K}}^{n+1}$, where $\mathbb{K}$ is a field of characteristic zero

Output: A zero-dimensional parametrization given by $q_1, y_1, \dots, y_n \in \mathbb{K}[T]$ of the limit set $\lim_{\varepsilon} \pi_{\mathbf{x}}(Q) \subset \overline{\mathbb{K}}^n$

```

1:  $e = -v(\hat{q})$ 
2:  $\hat{q}^* = \varepsilon^e \hat{q}(\varepsilon, T)$ 
3: for all  $i \in \llbracket 1, n \rrbracket$  do
4:    $\hat{v}_i^* = \varepsilon^e \hat{v}_i(\varepsilon, T)$ 
5: end for
6:  $q_0 = \text{lc}_T(\hat{q}^*)$ 
7:  $q = \hat{q}^*(0, T)/q_0$ 
8:  $\tilde{q} = q / \gcd(q, q')$ 
9:  $q_1 = \tilde{q} / \gcd(\tilde{q}, q')$ 
10:  $q_{\geq 2} = q/q_1$ 
11: for all  $i \in \llbracket 1, n \rrbracket$  do
12:    $y_i = \hat{v}_i^*(0, T)/q_0 q_{\geq 2} \bmod q_1$ 
13: end for
14: return  $q_1, y_1, \dots, y_n$ 

```

certified by computing a minimizer of π_1 on $\text{spec}(A)^M$. However, one cannot in general choose M such that $\pi_1(\text{spec}(A)^M)$ has a finite endpoint. How, then, can we decide whether or not $\text{spec}(A)$ is empty in this situation?

To address this, we extend the above strategy by seeking a boundary point of $\text{spec}(A)^M$ for a suitable M , provided the boundary is non-empty. The guiding idea is analogous to that of critical point methods: we apply the procedure of Proposition 22 recursively to spectrahedra obtained by specializing $x_1, \dots, x_{n-1}$ to real values $\tau_1, \dots, \tau_{n-1} \in \mathbb{R}$. This guarantees the existence of an index $i \in \llbracket 1, n \rrbracket$ such that $\pi_{x_i}(S \cap \pi_{i-1}^{-1}(\tau_{[1, i-1]}))$ is a Euclidean closed interval with at least one finite endpoint. The next two lemmas establish that such an index exists for a generic choice of M , and for every choice of τ .

Lemma 23. *Let $\mathbf{R}$ be a real closed field, and $\mathbf{C}$ be an algebraic closure of $\mathbf{R}$. Let S be a Euclidean closed, convex, non-empty proper semi-algebraic subset of $\mathbf{R}^n$. Suppose that for all $i \in \llbracket 1, n \rrbracket$, the set $\pi_i(S)$ is Euclidean closed in $\mathbf{R}^i$. Then, for all $\tau \in \mathbf{R}^n$, there exists $i \in \llbracket 1, n \rrbracket$ such that the Euclidean closed interval $\pi_{x_i}(S \cap \pi_{i-1}^{-1}(\tau_{[1, i-1]}))$ is a non-empty proper subset of $\mathbf{R}$.*

Proof. Suppose on the contrary that for all $i \in \llbracket 1, n \rrbracket$, $\pi_{x_i}(S \cap \pi_{i-1}^{-1}(\tau_{[1, i-1]}))$ is either empty or equal to $\mathbf{R}$. As S is non-empty, a simple induction shows that these sets are all non-empty, hence equal to $\mathbf{R}$. By convexity of S , this implies that $S = \mathbf{R}^n$, contradicting the assumption. $\square$

Lemma 24. *Let $\mathbf{R}$ be a real closed field, $\mathbf{C}$ be an algebraic closure of $\mathbf{R}$, and $S \subset \mathbf{R}^n$ be a Euclidean closed semi-algebraic set. Then, there exists a non-empty Zariski open set $\mathcal{M} \subset \text{GL}_n(\mathbf{C})$ such that for all $M \in \mathcal{M} \cap \text{GL}_n(\mathbf{R})$, $i \in \llbracket 1, n \rrbracket$, $\pi_i(S^M)$ is Euclidean closed.*

Proof. The proof is by induction on the dimension of S . When S has dimension 0, the result is immediate: the projections have dimension 0 as well. Suppose now that S has dimension $d \geq 1$. By Bochnak et al. (1998, Th. 2.3.6), S is the disjoint union of finitely many Euclidean closed, semi-algebraically connected semi-algebraic sets $S_1, \dots, S_k$. We show that for all $i \in \llbracket 1, n \rrbracket$ and $j \in \llbracket 1, k \rrbracket$, there exists a non-empty Zariski open set $\mathcal{M}_{i,j} \subset \text{GL}_n(\mathbf{C})$ such that for all $M \in \mathcal{M}_{i,j} \cap \text{GL}_n(\mathbf{R})$, $\pi_i(S_j^M)$ is Euclidean closed. Then, taking $\mathcal{M}$ as the intersection of those finite many $\mathcal{M}_{i,j}$ concludes the proof.

Let $j \in \llbracket 1, k \rrbracket$. If S_j has dimension less than d , we conclude by the induction hypothesis. Otherwise, S_j has dimension d , so that by Bochnak et al. (1998, Prop. 2.8.13), its boundary T_j has dimension at most $d - 1$. By induction hypothesis, there exists a non-empty Zariski open set $\mathcal{M}_{1,j} \subset \text{GL}_n(\mathbf{C})$ such that for all $M \in \mathcal{M}_{1,j} \cap \text{GL}_n(\mathbf{R})$, $\pi_1(T_j^M)$ is Euclidean closed. Furthermore, let $V \subset \mathbf{C}^n$ be the Zariski closure of S_j , and $C \subset \mathbf{R}^n$ be the semi-algebraically connected component of $V \cap \mathbf{R}^n$ containing S_j . By

Henrion et al. (2016b, Prop. 17), there exists a non-empty Zariski open set $\mathcal{M}_{2,j} \subset \mathrm{GL}_n(\mathbf{C})$ such that for all $M \in \mathcal{M}_{2,j} \cap \mathrm{GL}_n(\mathbf{R})$, $\pi_i(C^M)$ is Euclidean closed. It suffices then to take $\mathcal{M}_j = \mathcal{M}_{1,j} \cap \mathcal{M}_{2,j}$.

To see why $\pi_i(S_j^M)$ is Euclidean closed for $M \in \mathcal{M}_j \cap \mathrm{GL}_n(\mathbf{R})$, we show that each boundary point of $\pi_i(S_j^M)$, if any, is contained in $\pi_i(S_j^M)$. Let $a \in \mathbf{R}^i$ be such a point, and denote by $B(a, \eta) \subset \mathbf{R}^i$ the open ball of radius $\eta > 0$ centered at a . If for all $\eta > 0$, $\pi_i^{-1}(B(a, \eta)) \cap T_j^M \neq \emptyset$, then there exists $x \in T_j^M \subset S_j^M$ such that $a = \pi_i(x) \in \pi_i(S_j^M)$. Otherwise, there exists $\eta > 0$ such that $\pi_i^{-1}(B(a, \eta)) \cap T_j^M = \emptyset$, so that $\pi_i^{-1}(B(a, \eta)) \cap C^M = \pi_i^{-1}(B(a, \eta)) \cap S_j^M$. As $\pi_i(C^M)$ is Euclidean closed, there exists $x \in C^M$ such that $a = \pi_i(x)$. Hence, $x \in S_j^M$, and $a \in \pi_i(S_j^M)$. $\square$

Corollary 25. Let $A \in \mathcal{S}_m(R_{\leq 1})$ be a linear matrix, and $B \in \mathcal{S}_m(\mathbb{Q})$ be a positive definite matrix. Then, there exists a non-empty Zariski open set $\mathcal{M} \subset \mathrm{GL}_n(\mathbf{C})$ such that for all $M \in \mathcal{M} \cap \mathrm{GL}_n(\mathbb{Q})$, $i \in \llbracket 1, n \rrbracket$, $\pi_i(\mathrm{spec}(A)^M)$ and $\pi_i(\mathrm{spec}(A + \varepsilon B)^M)$ are both Euclidean closed.

Proof. Let $\mathcal{M}_1 \subset \mathrm{GL}_n(\mathbf{C})$ and $\mathcal{M}_2 \subset \mathrm{GL}_n(\mathbf{C}(\varepsilon))$ be the non-empty Zariski open sets given by Lemma 24 for $S = \mathrm{spec}(A)$ and $S = \mathrm{spec}(A + \varepsilon B)$, respectively. Then, $\mathcal{M}_2$ contains a non-empty Zariski open set $\mathcal{M}'_2 \subset \mathrm{GL}_n(\mathbf{C})$. We take $\mathcal{M} = \mathcal{M}_1 \cap \mathcal{M}'_2$. $\square$

Now, suppose that the boundary of $\mathrm{spec}(A) \subset \mathbb{R}^n$ is non-empty. Then, for a generic choice of $B \in \mathcal{S}_m(\mathbb{Q})$ that is positive definite, and for a generic choice of $M \in \mathrm{GL}_n(\mathbb{Q})$, both $\mathrm{spec}(A)^M$ and $\mathrm{spec}(A + \varepsilon B)^M$ satisfy the assumptions of Lemma 24. Denote by I_i the interval $\pi_{x_i}(\mathrm{spec}(A)^M \cap \pi_{i-1}^{-1}(\tau_{[1,i-1]}))$ for $\mathrm{spec}(A)^M$ that is proper in $\mathbb{R}$, and $I_i^{(\varepsilon)}$ the corresponding interval for $\mathrm{spec}(A + \varepsilon B)^M$.

Let $x \in \mathrm{spec}(A)^M \cap \pi_{i-1}^{-1}(\tau_{[1,i-1]})$ be a point that attains an endpoint of I_i . Clearly, x lies on the boundary of $\mathrm{spec}(A)^M$. Moreover, by Henrion et al. (2021, Lem. 5), there exists a sequence of points $x^{(\varepsilon)}$, each attaining an endpoint of $I_i^{(\varepsilon)}$, such that $\lim_{\varepsilon} x^{(\varepsilon)} = x$. In the propositions below, we show that each $x^{(\varepsilon)}$ belongs to the finite set $\bigcup_{r,i} \pi_{\mathbf{x}}(V(\mathbf{f}_{r,i}^{(\varepsilon)}))$. Taking limits then recovers x , which in turn allows us to decide whether $\mathrm{spec}(A)$ is empty or not.

Proposition 26. Let $A \in \mathcal{S}_m(\tilde{R}_{\leq 1})$ be a linear matrix. Then, there exists a non-empty Zariski open set $\mathcal{B} \subset \mathcal{S}_m(\mathbf{C})$ such that for all $B \in \mathcal{B} \cap \mathcal{S}_m(\mathbb{Q})$, there exists a non-empty Zariski open set $\mathcal{T}_B \subset \mathbf{C}^n$ such that for all $\tau \in \mathcal{T}_B \cap \mathbb{Q}^n$, and $\varepsilon \in (0, 1]$ out of a finite set, the following holds:

For all $r \in \llbracket 0, m-1 \rrbracket$, $\iota \in \llbracket 1, m \rrbracket$ with $|\iota| = m-r$, $i \in \llbracket 1, n \rrbracket$, $\mathbf{f}_{r,i}^{(\varepsilon)}(\tau_{[1,i-1]}, \cdot)$ satisfies $P(n - \binom{m-r+1}{2} - i)$.

Proof. Let $\mathfrak{B}$ be an unknown $m \times m$ symmetric matrix, and $\tilde{x} = (\tau_{[1,i-1]}, x_{[i,n]})$. For the perturbed parametric linear matrix $A + \varepsilon \mathfrak{B}$, given fixed r, ι, i , we consider the map

$$\mathbf{f}_i^{(\varepsilon)} : \mathbf{C}^{n+m(m-r)} \times \mathbf{C}^{\binom{m+1}{2}} \rightarrow \mathbf{C}^{m(m-r) + \binom{m-r+1}{2}},$$

$$(\tilde{x}, u, \mathfrak{B}) \mapsto \mathbf{f}_{r,i}^{(\varepsilon)}.$$

By Henrion et al. (2021, Prop. 7), 0 is a regular value of $\mathbf{f}_i^{(1)}$. Thom's weak transversality theorem (Safey El Din and Schost, 2017, Prop. B.3) then gives a non-empty Zariski open set $\mathcal{O}_{r,\iota,i} \subset \mathcal{S}_m(\mathbf{C}) \times \mathbf{C}^n$ such that for all $(B, \tau) \in \mathcal{O}_{r,\iota,i}$, 0 is a regular value of the map $(x_{[i,n]}, u) \mapsto \mathbf{f}_i^{(1)}(\tilde{x}, u, B)$. Taking $\mathcal{O}$ as the intersection of those finitely many $\mathcal{O}_{r,\iota,i}$, we can construct $\mathcal{B}$ and $\mathcal{T}_B$ for all $B \in \mathcal{B}$ stated in the proposition.

We now show why this implies that $\mathbf{f}_{r,i}^{(\varepsilon)}(\tau_{[1,i-1]}, \cdot)$ satisfies $P(n - \binom{m-r+1}{2} - i)$. Let F be the generator of the ideal of all polynomials vanishing on the complement of $\mathcal{O}$. Let $B \in \mathcal{B}$ and $\tau \in \mathcal{T}_B$. As $F(B, \tau) \neq 0$, $t \mapsto F(\varepsilon B, \tau)$ vanishes a finite number of times, i.e., $(\varepsilon B, \tau) \in \mathcal{O}$ except for a finite number of $\varepsilon \in (0, 1]$. Thus, for all such ε , 0 is a regular value of the map $(x_{[i,n]}, u) \mapsto \mathbf{f}_i^{(\varepsilon)}(\tilde{x}, u, B)$, which concludes the proof. $\square$

Proposition 27. *There exists a non-empty Zariski open set $\mathcal{B} \subset \mathbb{S}_m(\mathbb{C})$ such that for all $B \in \mathcal{B} \cap \mathbb{S}_m(\mathbb{Q})$, there exists a non-empty Zariski open set $\mathcal{M}_B \subset \text{GL}_n(\mathbb{C})$ such that for all $M \in \mathcal{M}_B \cap \text{GL}_n(\mathbb{Q})$, there exists a non-empty Zariski open set $\mathcal{T}_{B,M} \subset \mathbb{C}^n$ such that for all $\tau \in \mathcal{T}_{B,M} \cap \mathbb{Q}^n$, and $\varepsilon \in (0, 1]$ out of a finite set, the following holds:*

If $\pi_{x_i}(\text{spec}(A + \varepsilon B)^M \cap \pi_{i-1}^{-1}(\tau_{[1, i-1]}))$ has a minimum or a maximum attained at $x_\varepsilon^ \in \text{spec}(A + \varepsilon B)^M$, then $\bigcup_i \pi_{\mathbf{x}}(V(\mathbf{f}_{r, \iota, i}^{(\varepsilon)M}))$ is finite and contains x_ε^* , where r is the rank of $A + \varepsilon B$ at x_ε^* .*

Proof. As in the proof of Proposition 26, given fixed r, ι, i , we consider the map $\mathbf{g}_i^{(\varepsilon)} = \lambda^T \text{jac}(\mathbf{f}_i^{(\varepsilon)}) - (1, 0, \dots, 0)$. By the same argument as in Henrion et al. (2021, Prop. 8), the Jacobian matrix of $(\mathbf{f}_i^{(1)}, \mathbf{g}_i^{(1)})$ has full rank at every point in $V(\mathbf{f}_i^{(1)}, \mathbf{g}_i^{(1)})$ such that $A + \varepsilon B$ has rank r . Hence, for generic choices of B, M and τ , $\pi_{\mathbf{x}}(V(\mathbf{f}_{r, \iota, i}^{(1)M}))$ is finite, and the same holds for $\bigcup_i \pi_{\mathbf{x}}(V(\mathbf{f}_{r, \iota, i}^{(1)M}))$. Repeating the argument from the proof of Proposition 26 then yields that $\bigcup_i \pi_{\mathbf{x}}(V(\mathbf{f}_{r, \iota, i}^{(\varepsilon)M}))$ is finite for all $\varepsilon \in (0, 1]$ out of a finite set. Finally, Naldi (2016, Lem. 2) implies that $x_\varepsilon^* \in \bigcup_i \pi_{\mathbf{x}}(V(\mathbf{f}_{r, \iota, i}^{(\varepsilon)M}))$, if such a point exists. $\square$

7.3. Extending to parametric linear matrices

We now apply the same strategy to parametric linear matrices $A \in \mathbb{S}_m(\tilde{R}_{\leq 1})$. The following proposition is the analogue of Proposition 7 in this setting, and it does not require any genericity assumptions on A .

Proposition 28. *Let $A \in \mathbb{S}_m(\tilde{R}_{\leq 1})$ be a parametric linear matrix. There exists a non-empty Zariski open set $\mathcal{B} \subset \mathbb{S}_m(\mathbb{C})$ such that for all $B \in \mathcal{B} \cap \mathbb{S}_m(\mathbb{Q})$, there exists a non-empty Zariski open set $\mathcal{M}_B \subset \text{GL}_n(\mathbb{C})$ such that for all $M \in \mathcal{M}_B \cap \text{GL}_n(\mathbb{Q})$, there exists a non-empty Zariski open set $\mathcal{T}_{B,M} \subset \mathbb{C}^n$ such that for all $\tau \in \mathcal{T}_{B,M} \cap \mathbb{Q}^n$, there exists a non-empty Zariski open set $\mathcal{Y}_{B,M,\tau} \subset \mathbb{C}^t$ such that for all $y \in \mathcal{Y}_{B,M,\tau} \cap \mathbb{R}^t$, the set $\bigcup_{r, \iota, i} \lim_{\varepsilon} \pi_{\mathbf{x}}(V(\mathbf{f}_{r, \iota, i}^{(\varepsilon)M}(y, \cdot)))$ is finite. Moreover, if the boundary of $\text{spec}(A(y, \cdot))^M$ is non-empty, then this set contains a point on the boundary.*

The proof of Proposition 28 follows immediately from the proof of Proposition 22 together with the propositions stated below. Collectively, these results extend Lemma 24, Corollary 25 and Propositions 26, 27 to the parametric case.

Lemma 29. *Let $\mathbf{R}$ be a real closed field, $\mathbf{C}$ be an algebraic closure of $\mathbf{R}$, and $S \subset \mathbf{R}^{t+n}$ be a Euclidean closed semi-algebraic set. Then, there exists a non-empty Zariski open set $\mathcal{M} \subset \text{GL}_n(\mathbf{C})$ such that for all $M \in \mathcal{M} \cap \text{GL}_n(\mathbf{R})$, there exists a non-empty Zariski open set $\mathcal{Y}_M \subset \mathbf{C}^t$ such that for all $y \in \mathcal{Y}_M \cap \mathbf{R}^t$, $i \in [1, n]$, $\pi_i(S^M(y, \cdot))$ is Euclidean closed.*

Proof. The proof is verbatim as in Lemma 24, using induction on $\dim(S)$; we therefore only outline the differences. In the induction step, when S_j has dimension d , we construct $\mathcal{M}$ and, for all $M \in \mathcal{M} \cap \text{GL}_n(\mathbf{R})$, the corresponding set $\mathcal{Y}_M$ as follows. First, we take $\mathcal{M}_1$ and $\mathcal{Y}_{M,1}$ for all $M \in \mathcal{M}_1 \cap \text{GL}_n(\mathbf{R})$ by applying the induction hypothesis to T_j , so that for all $y \in \mathcal{Y}_{M,1} \cap \mathbf{R}^t$, $\pi_i((T_j^M)_y)$ is Euclidean closed. Next, we take $\mathcal{M}_2$ and $\mathcal{Y}_{M,2}$ for all $M \in \mathcal{M}_2 \cap \text{GL}_n(\mathbf{R})$ by applying (Henrion et al., 2016b, Prop. 17) over $\overline{\mathbf{C}}(\mathbf{y})$ as in Le and Safey El Din (2021, Prop. 6), so that for all $y \in \mathcal{Y}_{M,2} \cap \mathbf{R}^t$, $\pi_i((S_j^M)_y)$ is Euclidean closed. Finally, we set $\mathcal{M} = \mathcal{M}_1 \cap \mathcal{M}_2$ and $\mathcal{Y}_M = \mathcal{Y}_{M,1} \cap \mathcal{Y}_{M,2}$ for all $M \in \mathcal{M} \cap \text{GL}_n(\mathbf{R})$. $\square$

Corollary 30. *Let $A \in \mathbb{S}_m(\tilde{R}_{\leq 1})$ be a parametric linear matrix, and $B \in \mathbb{S}_m(\mathbb{Q})$ be a positive definite matrix. Then, there exists a non-empty Zariski open set $\mathcal{M} \subset \text{GL}_n(\mathbb{C})$ such that for all $M \in \mathcal{M} \cap \text{GL}_n(\mathbb{Q})$, there exists a non-empty Zariski open set $\mathcal{Y}_M \subset \mathbb{C}^t$ such that for all $y \in \mathcal{Y}_M \cap \mathbb{R}^t$, $i \in [1, n]$, $\pi_i(\text{spec}(A_y)^M)$ and $\pi_i(\text{spec}(A_y + \varepsilon B)^M)$ are both Euclidean closed.*

Proof. As in Corollary 25, it suffices to apply the previous lemma to $\text{spec}(A)$ and $\text{spec}(A + \varepsilon B)$, then for the latter, extract the non-empty Zariski open sets in $\text{GL}_n(\mathbb{C})$ and $\mathbb{C}^t$ from those in $\text{GL}_n(\mathbb{C}(\varepsilon))$ and $\mathbb{C}(\varepsilon)^t$, respectively. $\square$

Proposition 31. Let $A \in \mathbb{S}_m(\tilde{R}_{\leq 1})$ be a parametric linear matrix. Then, there exists a non-empty Zariski open set $\mathcal{B} \subset \mathbb{S}_m(\mathbb{C})$ such that for all $B \in \mathcal{B} \cap \mathbb{S}_m(\mathbb{Q})$, there exists a non-empty Zariski open set $\mathcal{T}_B \subset \mathbb{C}^n$ such that for all $\tau \in \mathcal{T}_B \cap \mathbb{Q}^n$, there exists a non-empty Zariski open set $\mathcal{Y}_{B,\tau} \subset \mathbb{C}^t$ such that for all $y \in \mathcal{Y}_{B,\tau} \cap \mathbb{R}^t$, and $\varepsilon \in (0, 1]$ out of a finite set, the following holds:

For all $r \in \llbracket 0, m-1 \rrbracket$, $\iota \in \llbracket 1, m \rrbracket$ with $|\iota| = m-r$, $i \in \llbracket 1, n \rrbracket$, $\mathbf{f}_{r,\iota}^{(\varepsilon)}(y, \tau_{\llbracket 1, i-1 \rrbracket}, \cdot)$ satisfies $P(n - \binom{m-r+1}{2}) - i$.

Proof. The proof is verbatim as in Proposition 26, except that for fixed r, ι, i , we consider the map

$$\mathbf{f}_i^{(\varepsilon)} : \mathbb{C}^{t+n+m(m-r)} \times \mathbb{C}^{\binom{m+1}{2}} \rightarrow \mathbb{C}^{m(m-r) + \binom{m-r+1}{2}},$$

$$(y, \tilde{x}, u, \mathfrak{B}) \mapsto \mathbf{f}_{r,\iota}^{(\varepsilon)}.$$

As 0 is still a regular value of $\mathbf{f}_i^{(1)}$, Thom's weak transversality theorem (Safey El Din and Schost, 2017, Prop. B.3) gives $\mathcal{B} \subset \mathbb{S}_m(\mathbb{C})$, $\mathcal{T}_B \subset \mathbb{C}^n$ for all $B \in \mathcal{B}$ and $\mathcal{Y}_{B,\tau}$ for all $\tau \in \mathcal{T}_B$, such that for all $B \in \mathcal{B}$, $\tau \in \mathcal{T}_B$, $y \in \mathcal{Y}_{B,\tau}$, 0 is a regular value of the map $(x_{\llbracket i, n \rrbracket}, u) \mapsto \mathbf{f}_i^{(1)}(y, \tilde{x}, u, B)$. Taking union over all r, ι, i and applying the same argument as in Proposition 26 for ε then concludes the proof. $\square$

Proposition 32. There exists a non-empty Zariski open set $\mathcal{B} \subset \mathbb{S}_m(\mathbb{C})$ such that for all $B \in \mathcal{B} \cap \mathbb{S}_m(\mathbb{Q})$, there exists a non-empty Zariski open set $\mathcal{M}_B \subset \text{GL}_n(\mathbb{C})$ such that for all $M \in \mathcal{M}_B \cap \text{GL}_n(\mathbb{Q})$, there exists a non-empty Zariski open set $\mathcal{T}_{B,M} \subset \mathbb{C}^n$ such that for all $\tau \in \mathcal{T}_{B,M} \cap \mathbb{Q}^n$, there exists a non-empty Zariski open set $\mathcal{Y}_{B,M,\tau} \subset \mathbb{C}^t$ such that for all $y \in \mathcal{Y}_{B,M,\tau} \cap \mathbb{R}^t$, and $\varepsilon \in (0, 1]$ out of a finite set, the following holds:

If $\pi_{x_i}(\text{spec}(A_y + \varepsilon B)^M \cap \pi_{i-1}^{-1}(\tau_{\llbracket 1, i-1 \rrbracket}))$ has a minimum or a maximum attained at $x_\varepsilon^* \in \text{spec}(A_y + \varepsilon B)^M$, then $\bigcup_\iota \pi_x(V(\mathbf{f}_{r,\iota,i}^{(\varepsilon)M}(y, \cdot)))$ is finite and contains x_ε^* , where r is the rank of $A(y) + \varepsilon B$ at x_ε^* .

Proof. The proof is verbatim as in Proposition 27, with the same adaptation as in the previous proposition. $\square$

7.4. Algorithm for the degenerate case

We are now ready to outline how Algorithm 1 can be modified to handle degeneracies. We first choose a random matrix $B \in \mathbb{S}_m(\mathbb{Q})$ that is positive definite. Then, in place of parametric geometric resolutions of $\mathbf{f}_{r,\iota,i}^M$, we work with the limits of the parametric geometric resolutions of $\mathbf{f}_{r,\iota,i}^{(\varepsilon)M}$, in which ε is treated as an additional parameter. The complete procedure is given in Algorithm 3.

Algorithm 3 PARAMETRICSOLVELMI2.

Input: $A \in \mathbb{S}_m(\tilde{R}_{\leq 1})$

Output: A semi-algebraic formula Φ in $\mathbb{Q}[y]$ defining a dense subset of the set $\{y \in \mathbb{R}^t \mid A(y, \cdot) \geq 0\}$.

```

1: choose  $B \in \mathbb{S}_m(\mathbb{Q})$  positive definite
2: choose  $M \in \text{GL}_n(\mathbb{Q})$ 
3: choose  $\tau \in \mathbb{Q}^n$ 
4:  $\mathbf{F}^{(\varepsilon)M} \leftarrow \text{REALDET}(A + \varepsilon B, M, \tau)$ 
5:  $\mathbf{g}^M \leftarrow \text{CHANGEVARS}(\text{PSDMATRIXCOND}(A), M)$ 
6:  $\Phi \leftarrow \text{PSDMATRIXCOND}(A(\cdot, 0)) > 0$ 
7: for all  $\mathbf{f}_{r,\iota,i}^{(\varepsilon)M} \in \mathbf{F}^{(\varepsilon)M}$  do
8:    $\Phi_{r,\iota,i} \leftarrow \text{CLASSIFICATION}(\text{CUT}(\mathbf{f}_{r,\iota,i}^{(\varepsilon)M}), \mathbf{g}^M)$ 
9:    $\Phi \leftarrow \Phi \vee \bigvee_{j: x_j > 0} \Phi_{r,\iota,i,j}$ 
10: end for
11: return  $\Phi$ 
```

Proof of Theorem 1 (degenerate inputs, algorithmic correctness)

Theorem 33. Let $A \in \mathbb{S}_m(\tilde{R}_{\leq 1})$ be a parametric linear matrix. Assume that all parameters chosen in Algorithm 3 satisfy the assumptions of Proposition 28. Then, Algorithm 3 is correct.

Proof. Algorithm 2 uses only finitely many algebraic operations in the coefficient field of the input polynomials (e.g., taking leading coefficients, computing GCDs, and inverses modulo suitable polynomials). Such operations commute with specialization at parameters $y \in \mathbb{C}^t$, as long as no denominator, leading coefficient, or relevant resultant or discriminant vanishes at y . Hence, for all y outside a proper Zariski closed subset of $\mathbb{C}^t$, we have

$$\text{CUT}(\mathbf{f}_{r,t,i}^{(\varepsilon)M})(y, \cdot) = \text{CUT}(\mathbf{f}_{r,t,i}^{(\varepsilon)M}(y, \cdot)).$$

With this commutation in place, the rest of the proof proceeds exactly as in Proposition 8: it suffices to replace Proposition 7 by Proposition 28, which ensures that for a generic choice of y , if $\partial \text{spec}(A(y, \cdot)) \neq \emptyset$, then there exists r, t, i such that $\text{CUT}(\mathbf{f}_{r,t,i}^{(\varepsilon)M}(y, \cdot))$ is finite and meets $\text{spec}(A_y)^M$. This yields the correctness of our approach. $\square$

Arithmetic complexity of Algorithm 3 Theorem 1 asserts that Algorithm 3 has the same asymptotic complexity bound as in the generic case. We now establish this result.

Proof of Theorem 1 (degenerate inputs, algorithmic complexity). We prove that the asymptotic degree bounds Δ^* and δ^* from Proposition 20 remain valid for $\mathbf{f}_{r,t,i}^{(\varepsilon)}$. Moreover, applying Algorithm 2 to the parametric geometric resolutions of $\mathbf{f}_{r,t,i}^{(\varepsilon)M}$ increases polynomial degrees by at most a factor $\Delta^{O(1)}\delta^{O(1)}$. As this growth does not change the asymptotic complexity bounds stated in Theorem 1, the result then follows.

The first claim is straightforward. As in Henrion et al. (2021, Prop. 9), the linear matrix $A + \varepsilon B$ can be seen as linear in the $n + 1$ variables $\mathbf{x}$ and ε , so that the asymptotic bounds Δ^* and δ^* for $\mathbf{f}_{r,t,i}$ also apply to $\mathbf{f}_{r,t,i}^{(\varepsilon)}$ when replacing n by $n + 1$. In particular, the asymptotic forms of these bounds are unchanged.

The second claim is more delicate. Assume that the inputs $\hat{q}, \hat{w}_1, \dots, \hat{w}_n$ to Algorithm 2 satisfy the degree bounds in Proposition 20, and let $q, w_1, \dots, w_n$ be the polynomials produced by the algorithm. The degrees in T of the polynomials $\gcd_T(q, q')$, $\tilde{q}$, $\gcd_T(\tilde{q}, q')$, q_1 , $q_{\geq 2}$ and y_i appearing in the algorithm are clearly bounded by δ^* . We now bound the degrees in $\mathbf{y}$ of the numerators and denominators of these polynomials. We write

$$\tilde{q} = \frac{\text{num}(q) / \gcd(\text{num}(q), \text{num}(q'))}{\text{denom}(q) \text{lc}_T(\gcd(\text{num}(q), \text{num}(q')))},$$

so that $\deg(\text{denom}(\tilde{q})) \leq 3\Delta$ and $\deg_{\mathbf{y}}(\text{num}(\tilde{q})) \leq 2\Delta$. Replacing q by $\tilde{q}$, we obtain analogously that

$$\deg(\text{denom}(q_1)) \leq 4\Delta, \quad \deg_{\mathbf{y}}(\text{num}(q_1)) \leq 2\Delta.$$

Consequently, $\deg(\text{denom}(q_{\geq 2})) \leq \Delta$ and $\deg_{\mathbf{y}}(\text{num}(q_{\geq 2})) \leq 6\Delta$. To bound the degrees in $\mathbf{y}$ of y_i , we use the same approach as in Section 6.2. Let $c = \text{Res}(\text{num}(q_1), \text{num}(q_{\geq 2})) \in \mathbb{Q}[\mathbf{y}]$, $a, b \in \mathbb{Q}[\mathbf{y}][T]$ of degree at most $\deg_T(q)$ such that $a \text{num}(q_1) + b \text{num}(q_{\geq 2}) = c$, and $p = bw_i$. Then,

$$y_i = \frac{\text{denom}(q_0 q_{\geq 2})}{c \text{num}(q_0) \text{denom}(p)} \frac{\text{Prem}_T(\text{num}(p), \text{num}(q_1))}{\text{denom}(q_1)^{\max(\deg_T(p) - \deg_T(q_1) + 1, 0)}}.$$

Carrying out the same degree estimates as in Proposition 20 yields

$$\begin{aligned} \deg(\text{denom}(y_i)) &\in O(\Delta(\delta + \deg(\text{denom}(w_i)))), \\ \deg_{\mathbf{y}}(\text{num}(y_i)) &\in O(\Delta\delta(\delta + \deg_{\mathbf{y}}(\text{num}(w_i)))). \end{aligned}$$

We therefore conclude that, in the output of Algorithm 2, the degrees in $\mathbf{y}$ of the numerators and denominators increase by at most a factor $O(\Delta\delta)$. This concludes the proof. $\square$

8. Implementation details

In this section, we report on the implementation details of our algorithm that allowed us to carry out the experiments in Section 9. The implementation is written in Julia, using Nemo.jl (Fieker et al., 2017) as a binding to FLINT (The FLINT team, 2025) for polynomial arithmetic, AlgebraicSolving.jl (or internally msolve Berthomieu et al., 2021) to compute reduced Gröbner bases over $\mathbb{Q}$ with *graded reverse lexicographical* orderings, and optionally RAGlib (Safey El Din, 2007) for sampling points in a semi-algebraic set. All our code is available upon request, and is expected to be integrated into AlgebraicSolving.jl.

Evaluation-interpolation scheme In our implementation, we use evaluation-interpolation techniques to speed up computations involving polynomials or rational functions in $\mathbb{Q}(\mathbf{y})$. These methods were originally proposed in Cuyt and Lee (2011, Sec. 2.2) and later extended to projective coordinates in Peraro (2016, Sec. 3.5) and van der Hoeven and Lecerf (2021, Sec. 3.3). In short, we regard the target rational function $f \in \mathbb{Q}(\mathbf{y})$ as a blackbox that can be evaluated at integer points in $\mathbb{Z}^t$. After evaluating f at sufficiently many points, we reconstruct f by interpolating the numerator and denominator separately.

For best performance, we call `fmpq_poly_interpolate_fmpz_fmpq_vec` from FLINT 3.4 for univariate interpolation with integer points, thus requiring Nemo.jl 0.53.0 or higher.

Computing parametric Gröbner bases Given $\mathbf{f} \subset \mathbb{Q}[\mathbf{y}, \mathbf{x}]$, we aim to compute the reduced Gröbner basis $\mathcal{G}$ of the ideal $\langle \mathbf{f} \rangle_{\mathbb{Q}(\mathbf{y})}$ with respect to a monomial ordering. In our implementation, the default approach is an evaluation-interpolation scheme:

1. We first identify the monomial support of each element of $\mathcal{G}$ by computing reduced Gröbner bases of the specialized ideals $\langle \mathbf{f}(y, \cdot) \rangle$ at random points $y \in \mathbb{Z}^t$, using AlgebraicSolving.jl.
2. Next, for every monomial occurring in each basis element, we recover its coefficient by interpolation from evaluations at sufficiently many points. This entails computing reduced Gröbner bases of $\langle \mathbf{f}(y, \cdot) \rangle$ at all interpolation points. For each computed basis, we check that its monomial structure agrees with that determined in the first step; if it does not, we discard that point.

Alternatively, if the property that $\mathcal{G}$ is reduced is not essential, we can compute a parametric Gröbner basis by computing the reduced Gröbner basis of $\langle \mathbf{f} \rangle$ with respect to a block monomial ordering that eliminates $\mathbf{x}$, and then extracting $\mathcal{G}$ via post-processing. This is the approach taken in Naldi et al. (2025); however, it is significantly more memory-consuming, and makes it impractical to handle large examples in our experiments.

Computing parametric Hermite matrices To compute Hermite matrices with entries in $\mathbb{Q}(\mathbf{y})$, the default approach of our implementation follows exactly the definition in Section 4.2:

1. We compute the reduced Gröbner basis of the input ideal over $\mathbb{Q}(\mathbf{y})$ with respect to the graded reverse lexicographical ordering. This is done via evaluation-interpolation as described above.
2. Then, we can construct the Hermite matrices by computing multiplication matrices with normal form computation, using the `divrem` function from Nemo.jl, and then taking traces. To accelerate the process, we precompute the Hermite matrix $\mathcal{H}_1$, as well as the multiplication matrices $\mathcal{M}_b$ for all monomials b in the monomial basis $\mathcal{B}$, so that for g with normal form $\sum_{b \in \mathcal{B}} c_b b$, we have $\mathcal{M}_g = \sum_{b \in \mathcal{B}} c_b \mathcal{M}_b$, and hence $\mathcal{H}_g = \mathcal{H}_1 \mathcal{M}_g$.

This approach serves as an alternative to the parametric geometric resolution algorithm for constructing our Hermite matrices due to better performance in practice (see Gaillard and Safey El Din, 2024). Aside from this default approach, one may instead compute Hermite matrices directly by

evaluation-interpolation via an optional setting in our implementation. On the instances we considered, however, this variant can be up to an order of magnitude slower: for example, for the instance GRD24 in Section 9, the runtime increases from 8.5 minutes to 1.2 hours.

Computing sample points To compute sample points in the non-vanishing of a set of polynomials $f_1, \dots, f_s \in \mathbb{Q}[\mathbf{y}]$, we use the following approach:

1. When $t = 1$, we compute a real root isolation of the product $\prod_{i=1}^s f_i$ using AlgebraicSolving.jl, and then select sample points in each interval between two consecutive real roots.
2. When $t = 2$, we compute sample points in the non-vanishing of the product of leading coefficients in y_2 , discriminants with respect to y_2 , and pairwise resultants with respect to y_2 , for all f_i (Collins, 1975). The discriminants and resultants are computed using evaluation-interpolation techniques. Then, for each sample point in y_1 , we compute sample points in the non-vanishing of the univariate polynomials obtained by specializing y_1 .

When $t \geq 3$, the strategy depends on s and degrees of the input polynomials. If they are small enough, we use the same approach as in the case $t = 2$, by eliminating one variable at a time. Otherwise, we use the RAGlib library (Safey El Din, 2007) to compute sample points in the non-vanishing of $f_1, \dots, f_s$, which behaves better in practice for larger examples.

Computing real root classifications To compute real root classifications of parametric polynomial systems, we implement (Gaillard and Safey El Din, 2024, Alg. 2) with optimizations from Gaillard and Safey El Din (2024, Sec. 5) to reduce the cost of computing sample points when all the Hermite matrices are of full rank. The performance of our implementation is comparable to the results reported in Table 1 of Gaillard and Safey El Din (2024), despite using a different programming language and libraries.

Example 2 (continued). For the parametric linear matrix A of Example 1, we obtained in Section 1 the set of polynomials $\mathbf{f}, \mathbf{g} \subset \mathbb{Q}(\mathbf{y})[\mathbf{x}, \mathbf{u}, \lambda]$, where $\mathbf{g}$ is independent of $\mathbf{u}$ and λ . Eliminating the auxiliary variables from $\mathbf{f}$ via Gröbner basis computation yields the parametric Gröbner basis $\mathcal{G}$ generated by

$$\mathbf{g} = x^2 + (-a + 2c)x - b + c^2.$$

As $\mathbf{g} = -g_0$, it suffices to identify the sign of g_1 at the real solutions of $\mathbf{g} = 0$. For the monomial basis $B = (1, x)$ of $\mathbb{Q}(\mathbf{y})[\mathbf{x}] / \langle \mathcal{G} \rangle_{\mathbb{Q}(\mathbf{y})}$, the Hermite matrix associated with 1 is exactly

$$H = \begin{bmatrix} 2 & a - 2c \\ a - 2c & a^2 - 4ac + 2b + 2c^2 \end{bmatrix},$$

and the multiplication matrix of g_1 is

$$M = \begin{bmatrix} b + 1 & ab - ac^2 \\ a & a^2 - 2ac + b + 1 \end{bmatrix}.$$

We then sample one point in each connected component of the non-vanishing of $\det(H)\det(M)$, and compute the possible signs of g_1 for each sample point. This yields the following classification:

- Either $\mathbf{g} = 0$ has two distinct real solutions (i.e., H is positive definite), and $g_1 > 0$ at all these solutions (i.e., A is positive semidefinite);
- Or $\mathbf{g} = 0$ has no real solution (i.e., H has eigenvalues of opposite signs), so that g_1 has no realizable sign.

Hence the conclusion in Section 1.

9. Practical experiments

We present practical experiments with our implementation on LMIs with background in multiple domains. Due to their large size, we refer to <https://weijia.perso.lip6.fr/generic-param-lmi/> for the exact form of the LMIs. In the following, we denote by PRB t n the LMI for the problem labeled PRB, with t parameters and n variables.

Sum-of-squares problem A polynomial $P \in \mathbb{Q}[\mathbf{x}]$ with real coefficients is a sum of squares (SOS) if and only if it can be written as $P = \beta^\top W \beta$, where β is a vector of monomials (typically monomials with exponent vectors in the Newton polytope of P) and W is a positive semidefinite matrix. Expanding the right-hand side and matching coefficients with P yields a set of linear equality constraints on the entries of W . The SOS condition is therefore equivalent to the feasibility of an LMI in the entries of W . When the coefficients of the input polynomial depend on some parameters, one obtains a parametric LMI.

Example 3. For $P = z^6 - 3x^2y^2z^2 + x^2y^4 + x^4y^2 + \xi(x^2 + y^2 + z^2)^3$, with ξ considered as a parameter, one can choose $\beta = (x^3, xy^2, y^3, x^2z, y^2z, z^3)^\top$, and hence obtain the following parametric LMI in the variable w :

$$\begin{bmatrix} \xi & \frac{1}{2} + \frac{3}{2}\xi & 0 & 0 & w & 0 \\ \frac{1}{2} + \frac{3}{2}\xi & 1 + 3\xi & 0 & -w & 0 & 0 \\ 0 & 0 & \xi & 0 & 0 & 0 \\ 0 & -w & 0 & 3\xi & 3\xi - \frac{3}{2} & \frac{3}{2}\xi \\ w & 0 & 0 & 3\xi - \frac{3}{2} & 3\xi & \frac{3}{2}\xi \\ 0 & 0 & 0 & \frac{3}{2}\xi & \frac{3}{2}\xi & 1 + \xi \end{bmatrix} \geq 0.$$

For a detailed derivation of the LMI from the sum-of-squares condition, the reader is referred to the webpage mentioned above.

In the following, MKN11 is extracted from a perturbation of Motzkin's polynomial (Motzkin, 1967), and RBN11 from Robinson's polynomial (Robinson, 1973).

Algorithm analyses We also consider LMIs extracted from the analysis of classical first-order optimization algorithms. In the following, GRD12 to GRD24 correspond to different choices of parameters and specializations of the same LMI of size $m = 3$, with 2 parameters and 4 free variables, generated from the gradient descent method. Similarly, PPM21 and PPM31 are generated from the proximal point method, LGD34 from Lyapunov analysis of gradient descent, and GRD34 from an alternative LMI for gradient descent. DRS32 to DRS43 come from Ryu et al. (2020, SM3.1.1, SM3.2.1) in the analysis of the Douglas-Rachford splitting, and SGD32 from Taylor and Bach (2019, App. E.7) in the analysis of stochastic gradient descent.

Example 4. Ryu et al. (2020, Thm. 4.1) gives the tight contraction factor ρ of the DRS operator $I - \theta J_B + \theta J_A(2J_B - I)$ under the assumptions of μ -strong monotonicity and β -cocoercivity. The analysis is based on the feasibility of the following parametric LMI in the variables λ_μ^A and λ_β^B :

$$\begin{bmatrix} \rho^2 + \beta\lambda_\beta^B - 1 & -\theta + \frac{\lambda_\mu^A}{2} & \theta - (\frac{1}{2} + \beta)\lambda_\beta^B \\ -\theta + \frac{\lambda_\mu^A}{2} & -\theta^2 + (1 + \mu)\lambda_\mu^A & \theta^2 - \lambda_\mu^A \\ \theta - (\frac{1}{2} + \beta)\lambda_\beta^B & \theta^2 - \lambda_\mu^A & -\theta^2 + (1 + \beta)\lambda_\beta^B \end{bmatrix} \geq 0.$$

A detailed derivation of the LMI is given in Ryu et al. (2020, SM3).

Experimental setup Timings are given in days (d.), hours (h.), minutes (min.) and seconds (s.). All computations were performed single-threaded on an Intel Xeon Gold 6246R server with 1.5 TB of RAM. Columns O1 and O2 give the runtimes for the first two options described in Section 4.3, using our implementation with Julia 1.12, Nemo.jl 0.53.0 and AlgebraicSolving.jl 0.10.2. Column Ob reports the runtime for computing one point in each connected component of $\pi_Y(\text{spec}(A))$. These points are obtained by collecting the determinants of the Hermite matrices produced by two successive runs of O1 (with different choices of M and τ), and then computing sample points where neither the denominators nor the common factor of the numerators vanishes. Columns QE1 and QE2 report quantifier elimination runtimes in Maple 2025 (Chen and Moreno Maza, 2016) and Wolfram 14.3 (Strzeboński, 2006), respectively; both solvers are based on variants of cylindrical algebraic decomposition algorithms.

	O1	Ob	O2	QE1	QE2
MKN11	0.2 s	0.5 s	0.4 s	9.2 s	0.2 s
RBN11	0.2 s	0.5 s	0.4 s	12 s	0.2 s
GRD12	1.0 s	2.6 s	1.2 s	2.1 h	0.7 s
GRD13	11 s	30 s	17 s	∞	∞
GRD14	1.1 min	2.3 min	1.5 min	∞	∞
GRD21	0.6 s	1.3 s	1.0 s	1.3 s	0.3 s
GRD22	3.6 s	8.1 s	11 s	∞	1.1 h
GRD23	2.3 min	5.9 min	1.5 h	∞	∞
GRD24	8.5 min	17 min	8.5 h	∞	∞
PPM21	0.2 s	0.4 s	0.5 s	0.08 s	0.07 s
PPM31	1.1 s	2.4 s	2.0 s	0.2 s	0.07 s
SGD32	1.0 min	3.7 min	∞	∞	∞
DRS32	22 min	46 min	∞	∞	∞
DRS42	8.3 h	17.2 h	∞	∞	∞
DRS33	1.0 h	2.1 h	∞	∞	∞
DRS43	21 h	1.8 d	∞	∞	∞
GRD34	3.9 h	7.8 h	∞	∞	∞
LGD34	1.2 s	2.8 s	1.7 s	∞	∞

In the table, the symbol ∞ indicates that the computation is unfortunately intractable either because no result was obtained within 7 days or due to lack of memory.

When $t \geq 2$ or $n \geq 2$, our implementation succeeds for examples where quantifier elimination in Maple and Wolfram either fails due to lack of memory or does not terminate within 7 days. This illustrates the benefit of our approach on this range of problems compared to general-purpose solvers for quantifier elimination. In addition, the examples GRD14, GRD23 and DRS43, which were previously out of reach in Naldi et al. (2025), can now be solved within a reasonable time frame thanks to the evaluation-interpolation techniques and other improvements in our implementation.

CRedit authorship contribution statement

Simone Naldi: Writing – review & editing, Writing – original draft, Project administration, Methodology, Conceptualization. **Mohab Safey El Din:** Writing – review & editing, Writing – original draft, Project administration, Methodology, Conceptualization. **Adrien Taylor:** Writing – review & editing, Writing – original draft, Project administration, Methodology, Conceptualization. **Weijia Wang:** Writing – review & editing, Writing – original draft, Methodology, Conceptualization.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests: Mohab Safey El Din is an Editorial Board Member for this journal and was not involved in the editorial review or the decision to publish this article. Simone

Naldi, Adrien Taylor and Weijia Wang declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

Simone Naldi is supported by the ANR Project ANR-21-CE48-0006-01 “HYPERSPACE”. Adrien Taylor is supported by the European Union (ERC grant CASPER 101162889). The French government also partly funded this under the management of Agence Nationale de la Recherche as part of the “France 2030” program, reference ANR-23-IACL-0008 “PR[AI]RIE-PSAI”. Mohab Safey El Din and Weijia Wang are supported by the ANR Project ANR-22-CE91-0007 “EAGLES” and by grant FA8655-25-1-7469 of the European Office of Aerospace Research and Development of the Air Force Office of Scientific Research (AFOSR). This collaboration started during the workshop *Conic Linear Optimization for Computer-Assisted Proofs* in April 2022 at the Mathematisches Forschungsinstitut Oberwolfach (MFO), organized by Etienne de Klerk, Didier Henrion, Frank Vallentin and Angelika Wiegele. Special thanks to Didier Henrion for his stimulating and helpful discussions as well as his encouragements to develop this research track. Views and opinions expressed are however those of the authors only.

Data availability

No data was used for the research described in the article.

References

- Anjos, M.F., Lasserre, J.B., 2011. *Handbook on Semidefinite, Conic and Polynomial Optimization*. Springer New York, New York, NY, USA.
- Bank, B., Giusti, M., Heintz, J., Safey El Din, M., Schost, É., 2010. On the geometry of polar varieties. *Appl. Algebra Eng. Commun. Comput.* 21 (1), 33–83.
- Basu, S., Pollack, R., Roy, M.-F., 1996. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM* 43 (6), 1002–1045.
- Basu, S., Pollack, R., Roy, M.-F., 2016. *Algorithms in Real Algebraic Geometry*. Springer Berlin Heidelberg, Berlin, Heidelberg.
- Berthomieu, J., Eder, C., Safey El Din, M., 2021. Msolve: a library for solving polynomial systems. In: *Proceedings of the 2021 on International Symposium on Symbolic and Algebraic Computation*. Association for Computing Machinery, New York, NY, USA, pp. 51–58.
- Bochnak, J., Coste, M., Roy, M.-F., 1998. *Real Algebraic Geometry*. Springer Berlin Heidelberg, Berlin, Heidelberg.
- Boyd, S., Vandenberghe, L., 2004. *Convex Optimization*. Cambridge University Press, Cambridge, UK.
- Bruns, W., Vetter, U., 2006. *Determinantal Rings*, vol. 1327. Springer Berlin Heidelberg, Berlin, Heidelberg.
- Canny, J.F., Kaltofen, E., Yagati, L., 1989. Solving systems of nonlinear polynomial equations faster. In: *Proceedings of the ACM-SIGSAM 1989 International Symposium on Symbolic and Algebraic Computation*. Association for Computing Machinery, New York, NY, USA, pp. 121–128.
- Chen, C., Moreno Maza, M., 2016. Quantifier elimination by cylindrical algebraic decomposition based on regular chains. In: *Special Issue on the Conference ISSAC 2014: Symbolic Computation and Computer Algebra*. *J. Symb. Comput.* 75, 74–93.
- Collins, G.E., 1975. Quantifier elimination for real closed fields by cylindrical algebraic decomposition. In: *Lecture Notes in Computer Science*. Springer Berlin Heidelberg, Berlin, Heidelberg, pp. 134–183.
- Cuyt, A., Lee, W.-S., 2011. Sparse interpolation of multivariate rational functions. *Theor. Comput. Sci.* 412 (16), 1445–1456.
- Drori, Y., Teboulle, M., 2014. Performance of first-order methods for smooth convex minimization: a novel approach. *Math. Program.* 145 (1), 451–482.
- Eisenbud, D., 2013. *Commutative Algebra: with a View Toward Algebraic Geometry*. Springer Science & Business Media, New York, NY, USA.
- Elliott, J., Giesbrecht, M., Schost, É., 2023. Bit complexity for computing one point in each connected component of a smooth real algebraic set. *J. Symb. Comput.* 116, 72–97.
- Fieker, C., Hart, W., Hofmann, T., Johansson, F., 2017. Nemo/Hecke: computer algebra and number theory packages for the Julia programming language. In: *Proceedings of the 2017 ACM International Symposium on Symbolic and Algebraic Computation*. Association for Computing Machinery, New York, NY, USA, pp. 157–164.
- Gaillard, L., Safey El Din, M., 2024. Solving parameter-dependent semi-algebraic systems. In: *Proceedings of the 2024 International Symposium on Symbolic and Algebraic Computation*. Association for Computing Machinery, New York, NY, USA, pp. 447–456.
- Grigor'ev, D.Yu., 1988. Complexity of deciding Tarski algebra. *J. Symb. Comput.* 5 (1), 65–108.
- Grigor'ev, D.Yu., Vorobjov Jr., N.N., 1988. Solving systems of polynomial inequalities in subexponential time. *J. Symb. Comput.* 5 (1–2), 37–64.
- Heintz, J., 1983. Definability and fast quantifier elimination in algebraically closed fields. *Theor. Comput. Sci.* 24 (3), 239–277.
- Heintz, J., Roy, M.-F., Solernó, P., 1990. Sur la complexité du principe de Tarski-Seidenberg. *Bull. Soc. Math. Fr.* 118 (1), 101–126.

- Henrion, D., Naldi, S., Safey El Din, M., 2016a. Exact algorithms for linear matrix inequalities. *SIAM J. Optim.* 26 (4), 2512–2539.
- Henrion, D., Naldi, S., Safey El Din, M., 2016b. Real root finding for determinants of linear matrices. *J. Symb. Comput.* 74, 205–238.
- Henrion, D., Naldi, S., Safey El Din, M., 2021. Exact algorithms for semidefinite programs with degenerate feasible set. *J. Symb. Comput.* 104, 942–959.
- Hermite, C., 1856. Extrait d'une lettre de Mr. Ch. Hermite de Paris à Mr. Borchardt de Berlin sur le nombre des racines d'une équation algébrique comprises entre des limites données.
- Hong, H., Safey El Din, M., 2009. Variant real quantifier elimination: algorithm and application. In: *Proceedings of the 2009 International Symposium on Symbolic and Algebraic Computation*. Association for Computing Machinery, New York, NY, USA, pp. 183–190.
- Hong, H., Safey El Din, M., 2012. Variant quantifier elimination. *J. Symb. Comput.* 47 (7), 883–901.
- Kalkbrener, M., 1997. On the stability of Gröbner bases under specializations. *J. Symb. Comput.* 24 (1), 51–58.
- Le, H.P., Safey El Din, M., 2021. Faster one block quantifier elimination for regular polynomial systems of equations. In: *Proceedings of the 2021 International Symposium on Symbolic and Algebraic Computation*. Association for Computing Machinery, New York, NY, USA, pp. 265–272.
- Le, H.P., Safey El Din, M., 2022. Solving parametric systems of polynomial equations over the reals through Hermite matrices. *J. Symb. Comput.* 112, 25–61.
- Motzkin, T.S., 1967. The arithmetic-geometric inequality. In: *Inequalities*. Proc. Sympos. Wright-Patterson Air Force Base, Ohio, 1965, vol. 205, p. 54.
- Naldi, S., 2016. Solving rank-constrained semidefinite programs in exact arithmetic. In: *Proceedings of the 2016 ACM International Symposium on Symbolic and Algebraic Computation*. Association for Computing Machinery, New York, NY, USA, pp. 357–364.
- Naldi, S., Safey El Din, M., Taylor, A., Wang, W., 2025. Solving generic parametric linear matrix inequalities. In: *Proceedings of the 2025 International Symposium on Symbolic and Algebraic Computation*. Association for Computing Machinery, New York, NY, USA, pp. 267–276.
- Peraro, T., 2016. Scattering amplitudes over finite fields and multivariate functional reconstruction. *J. High Energy Phys.* 12, 1–46.
- Robinson, R.M., 1973. Some definite polynomials which are not sums of squares of real polynomials. In: *Selected Questions of Algebra and Logic (a Collection Dedicated to the Memory of A. I. Malcev)*. Izdat. Nauka Sibirsk. Otdel, Novosibirsk, pp. 264–282.
- Ryu, E.K., Taylor, A.B., Bergeling, C., Giselsson, P., 2020. Operator splitting performance estimation: tight contraction factors and optimal parameter selection. *SIAM J. Optim.* 30 (3), 2251–2271.
- Safey El Din, M., 2007. RAGLib: A Library for Real Solving Polynomial Systems of Equations and Inequalities.
- Safey El Din, M., Schost, É., 2003. Polar varieties and computation of one point in each connected component of a smooth real algebraic set. In: *Proceedings of the 2003 International Symposium on Symbolic and Algebraic Computation*. Association for Computing Machinery, New York, NY, USA, pp. 224–231.
- Safey El Din, M., Schost, É., 2017. A nearly optimal algorithm for deciding connectivity queries in smooth and bounded real algebraic sets. *J. ACM* 63 (6), 1–37.
- Safey El Din, M., Schost, É., 2018. Bit complexity for multi-homogeneous polynomial system solving—application to polynomial minimization. *J. Symb. Comput.* 87, 176–206.
- Schost, É., 2003. Computing parametric geometric resolutions. *Appl. Algebra Eng. Commun. Comput.* 13 (5), 349–393.
- Shafarevich, I.R., Reid, M., 1994. *Basic Algebraic Geometry*. Springer Berlin Heidelberg, Berlin, Heidelberg.
- Strzeboński, A.W., 2006. Cylindrical algebraic decomposition using validated numerics. *J. Symb. Comput.* 41 (9), 1021–1038.
- Tarski, A., 1951. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, Berkeley, CA, USA.
- Taylor, A., Bach, F., 2019. Stochastic first-order methods: non-asymptotic and computer-aided analyses via potential functions. In: *Proceedings of the Thirty-Second Conference on Learning Theory (Proceedings of Machine Learning Research, vol. 99)*. PMLR, Phoenix, AZ, USA, pp. 2934–2992.
- Taylor, A.B., Hendrickx, J.M., Glineur, F., 2017a. Exact worst-case performance of first-order methods for composite convex optimization. *SIAM J. Optim.* 27 (3), 1283–1313.
- Taylor, A.B., Hendrickx, J.M., Glineur, F., 2017b. Smooth strongly convex interpolation and exact worst-case performance of first-order methods. *Math. Program.* 161, 307–345.
- The FLINT team, 2025. FLINT: fast library for number theory. Version 3.4.0. <https://flintlib.org>.
- van der Hoeven, J., Lecerf, G., 2021. On sparse interpolation of rational functions and gcds. *ACM Commun. Comput. Algebra* 55 (1), 1–12.