Computing rational solutions of linear matrix inequalities

Qingdong Guo, Mohab Safey El Din, Lihong Zhi

Computing rational solutions of linear matrix inequalities [*]

Qingdong Guo
Key Laboratory of
Mathematics Mechanization,
Chinese Academy of Sciences
Beijing 100190, China
fguo@mmrc.iss.ac.cn

Mohab Safey El Din
UPMC, Univ Paris 06
INRIA, Paris-Rocquencourt
Center, POLSYS project-team
CNRS LIP6 UMR 7606
Institut Universitaire de France
Mohab.Safey@lip6.fr

Lihong Zhi
Key Laboratory of
Mathematics Mechanization,
Chinese Academy of Sciences
Beijing 100190, China
lzhi@mmrc.iss.ac.cn

ABSTRACT

Consider a $(D \times D)$ symmetric matrix A whose entries are linear forms in $\mathbb{Q}[X_1, \dots, X_k]$ with coefficients of bit size $\leq \tau$. We provide an algorithm which decides the existence of rational solutions to the linear matrix inequality $\mathsf{A} \succeq 0$ and outputs such a rational solution if it exists. This problem is of first importance: it can be used to compute algebraic certificates of positivity for multivariate polynomials. Our algorithm runs within $(k\tau)^{O(1)}2^{O(\min(k,D)D^2)}D^{O(D^2)}$ bit operations; the bit size of the output solution is dominated by $\tau^{O(1)}2^{O(\min(k,D)D^2)}$. These results are obtained by designing algorithmic variants of constructions introduced by Klep and Schweighofer. This leads to the best complexity bounds for deciding the existence of sums of squares with rational coefficients of a given polynomial. We have implemented the algorithm; it has been able to tackle Scheiderer's example of a multivariate polynomial that is a sum of squares over the reals but not over the rationals; providing the first computer validation of this counter-example to Sturmfels' conjecture.

Categories and Subject Descriptors

I.1.2 [**Symbolic and Algebraic Manipulation**]: Algorithms—*algebraic algorithms*; F.2.2 [**Analysis of Algorithms and Problem Complexity**]: Non numerical algorithms and problems—*complexity of proof procedures*

General Terms

Theory, algorithms.

Keywords

effective real algebraic geometry, linear matrix inequality, rational sum of squares, semidefinite programming, convexity, complexity

1. INTRODUCTION

Motivation and problem statement. Let A be a symmetric $(D \times D)$-matrix whose entries are linear forms in $\mathbb{Q}[X_1, \dots, X_k]$ with coefficients of bit size τ. We consider the problem of computing a rational point $\mathbf{x} \in \mathbb{Q}^k$ which is a solution to the linear matrix inequality $\mathsf{A} \succeq 0$ (in other words $\mathsf{A}(\mathbf{x})$ is positive semi-definite, i.e. all its eigenvalues are nonnegative).

This problem can be seen as a variant of integer linear programming or a diophantine version of semi-definite programming. It has become a topical question since semidefinite programming is used to compute sums-of-squares decompositions of polynomials which provide algebraic certificates of positivity [8, 9, 14, 5] and are used in polynomial optimization. In this framework, one issue is to get *rational* solutions to linear matrix inequalities.

This has been formalized through Sturmfels' conjecture asking whether all polynomials with coefficients in $\mathbb{Q}$ and which are sums of squares of polynomials with coefficients in $\mathbb{R}$ can be written as a sum of squares of polynomials with coefficients in $\mathbb{Q}$. More recently, Scheiderer gave an example showing that Sturmfels' conjecture is not true [21]. It is worth to remark that any algorithm designed for grabbing rational solutions to linear matrix inequalities may provide a computer proof to Scheiderer's example.

In [20], an algorithm is given to compute rational points in convex semi-algebraic sets. Linear Matrix Inequalities (LMIs) define convex semi-algebraic sets: these are defined by sign conditions on the coefficients of the characteristic polynomial [15]. As a by-product, [20] provides an algorithmic solution to the problem we consider here. Using the above notations, the algorithm in [20] applied to Linear Matrix Inequalities runs within $\tau^{O(1)}D^{O(k^3)}$.

However, recall that the original motivation for computing rational solutions to Linear Matrix Inequalities is sums of squares decompositions of polynomials. If $f \in \mathbb{Q}[Y_1, \dots, Y_n]$ has degree $2d$, the linear matrix inequality generated to de-

[*] The authors are supported by CNRS and INRIA through the ECCA project at LIAMA and by the EXACTA grant (ANR-09-BLAN-0371-01) of the French National Research Agency (ANR) and the Chinese National Natural Science Foundation under Grant 60911130369. The second author is also supported by the GeoLMI grant (ANR 2011 BS03 011 06) of the French National Research Agency (ANR) and the Institut Universitaire de France. The third author is also supported by NKBRPC 2011CB302400, the Chinese National Natural Science Foundation under Grants 91118001, 60821002/F02.

ISSAC'13, June 26–29, 2013, Boston, Massachusetts, USA.

compose f as a sum of squares is such that $D = \binom{n+d}{n}$ and $k \leq \frac{1}{2}D(D+1) - \binom{n+2d}{n}$. Technical computations show that $\frac{1}{2}D(D+1) - \binom{n+2d}{n}$ lies in $O(\min(n^{2d}, d^{2n}))$ and $\binom{n+d}{n}$ lies in $O(\min(n^d, d^n))$. As a consequence, denoting $\min(n^d, d^n)$ by $\mathsf{M}(d, n)$ [20] yields a complexity $\tau^{O(1)}\mathsf{M}(d,n)^{\mathsf{M}(d,n)^6}$.

The goal of this paper is twofold:

1. improve the above complexity *by exploiting the special structure of LMIs.*
2. by designing an algorithm which is able to provide a "computer-proof" for the non-existence of a sum of squares decomposition over the rationals for Scheiderer's example [21].

Main results. Our study is more restrictive than the one in [20] since we do not consider general convex semi-algebraic sets but only those defined by Linear Matrix Inequalities. Consider a $(D \times D)$ symmetric matrix A whose entries are linear forms in $\mathbb{Q}[X_1, \ldots, X_k]$ with coefficients of bit size $\leq \tau$.

Our main results rely heavily on results obtained by Klep and Schweighofer in [12]. The algorithm we obtain can be seen as an effective variant of the results in [12] which provides some constructions of linear equations S and a linear matrix inequality $\widehat{\mathsf{A}} \succeq 0$ of size $(D-1, D-1)$ such that the set of common rational solutions of S and $\widehat{\mathsf{A}} \succeq 0$ is the same the set of rational solutions of $\mathsf{A} \succeq 0$.

Our algorithm is of recursive nature; it outputs a rational point $\mathbf{x} \in \mathbb{Q}^k$ at which A is positive semi-definite whenever such a point exists else it returns an empty list. It runs within $(k\tau)^{O(1)2^{O(\min(k,D)D^2)}}D^{O(D^2)}$ bit operations and in case of non-emptiness the output point has coordinates of bit size bounded by $\tau^{O(1)2^{O(\min(k,D)D^2)}}$ (see Theorem 4.1 below).

Note that on families of Linear Matrix Inequalities where $k \simeq D^2$ the obtained complexity bounds on runtime and size of output are better than the ones obtained in [20] (we get $k^{1.5}$ in the exponent instead of k^3). For the important application of sums of squares decompositions over the rationals of n-variate polynomials of degree $2d$, using the estimates on binomials which are given above, we obtain as a new bound for the runtime $\tau^{O(1)2^{O(\mathsf{M}(d,n)^3)}}\mathsf{M}(d,n)^{\mathsf{M}(d,n)^2}$ which lies in $\tau^{O(1)2^{O(\mathsf{M}(d,n)^3)}}$ and dramatically improves the one obtained from [20]. The same bound is obtained for the size of the output. This is summarized in the theorem below.

THEOREM 1.1. *Let $f \in \mathbb{Q}[X_1, \ldots, X_n]$ of degree $2d$ with coefficients of bit size $\leq \tau$. There exists an algorithm which decides the existence of a sum of squares decomposition of f over the rationals and computes such a decomposition whenever it exists within $\tau^{O(1)2^{O(\mathsf{M}(d,n)^3)}}$ bit operations where $\mathsf{M}(d,n) = \min(d^n, n^d)$. The bit size of the output is also dominated by $\tau^{O(1)2^{O(\mathsf{M}(d,n)^3)}}$.*

We also implemented our algorithm and ran it on several examples. In particular, our implementation, which uses routines provided by the RAGLIB package [17] has been able to provide the first *computer validation of Scheiderer's result.* The resulting Linear Matrix Inequality to solve over the rationals is rather small: there are 6 variables and the size of the matrix is 6 × 6. But, as far as we know, our implementation is the first one that can handle a non-trivial linear matrix inequality and solve it *over the rationals.*

Related works. Solving Linear Matrix Inequalities over the rationals has been mainly developed in [20]. It is worth to note that these algorithms are actually based on ideas derived by the ones in [10, 11] for solving Linear Matrix Inequalities over the *integers.* This paper mostly relies on results in [12] and it can be seen as an algorithmic variant exploiting some theoretical results in [12] (mostly Theorem 2.3.2 and Proposition 3.2.1). The algorithm makes use of several complexity results in real algebraic geometry mainly due to Basu, Pollack and Roy which are stated and proved in [2, 3]. Our implementation uses [17] which relies on variants of the algorithms presented in [4, 18]. As we explained previously, this paper is motivated by the global polynomial optimization for which computing algebraic certificates is of first importance. It is worth to note that several alternative approaches in Computer Algebra have been developed for polynomial optimizations, let us mention those based on the critical point method (see [1, 6, 19]) and those based on Cylindrical Algebraic Decomposition (see e.g. [1, 7]).

Structure of the paper.. We start in Section 2 with preliminaries, stating some properties of Linear Matrix Inequalities and complexity results in effective real algebraic geometry for solving polynomial systems over the reals. In Section 3, we design the main subroutines on which our main algorithm relies: the first one treats basic cases (univariate inequalities and those whose solution sets have non-empty interior); the other one constructs the aforementioned linear equations using [12]. Finally, we detail how our algorithm runs on Scheiderer's example; providing the first computer validation of the non-existence of rational sums-of-squares decompositions to polynomials with rational coefficients which are sums of squares with real coefficients.

2. PRELIMINARIES

Basic definitions and notations. A symmetric matrix M with entries in $\mathbb{R}$ is said to be positive definite (resp. positive semi-definite) when all its eigenvalues are positive (resp. non-negative). We will write respectively $\mathsf{M} \succ 0$ and $\mathsf{M} \succeq 0$.

In the sequel, given a matrix or a vector M with entries in a ring R, $\mathsf{M}^\star$ denotes the transposition of M.

Let $X_1, \ldots, X_k$ be indeterminates, $\mathsf{A}_0, \ldots, \mathsf{A}_k$ be $(D \times D)$ symmetric matrices with entries in $\mathbb{R}$ and A be the linear matrix $\mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k$. For $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_k) \in \mathbb{R}^k$, we write $\mathsf{A}(\mathbf{x})$ for $\mathsf{A}_0 + \mathbf{x}_1\mathsf{A}_1 + \cdots + \mathbf{x}_k\mathsf{A}_k$. We consider the linear matrix inequality

$$\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k \succeq 0.$$

We denote by $\mathfrak{S}(\mathsf{A}) = \{\mathbf{x} \in \mathbb{R}^k \mid \mathsf{A}(\mathbf{x}) \succeq 0\}$ the feasible region of A. It is a closed convex semi-algebraic set lying in $\mathbb{R}^k$.

We will say that the linear matrix inequality $\mathsf{A} \succeq 0$ is infeasible when $\mathfrak{S}(\mathsf{A}) = \emptyset$, else it is feasible.

Basic properties of Linear Matrix Inequalities. We start with immediate properties of Linear Matrix Inequalities.

LEMMA 2.1. *Let $\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k$ where A_i is a $(D \times D)$ symmetric matrix with entries in $\mathbb{Q}$ (for $0 \leq i \leq k$) and $E \subset \mathbb{R}^k$ be an affine linear subspace defined by a set of linear equations. Assume that the entries of the i-th row* *and column of* A *vanish at all points in* E *and let* $\widehat{\mathsf{A}}$ *be the* $(D-1, D-1)$*-matrix obtained by removing the* i*-th row and column of* A*. Then* $\mathfrak{S}(\widehat{\mathsf{A}}) \cap E = \mathfrak{S}(\mathsf{A}) \cap E$*.*

LEMMA 2.2. *Let* $\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k$ *where* A_i *is a* $(D \times D)$ *symmetric matrix with entries in* $\mathbb{Q}$ *(for* $0 \leq i \leq k$*),* P *be an invertible matrix and* $\mathsf{A}' = \mathsf{P}^\star\mathsf{A}\mathsf{P}$*. If* $\mathbf{x} \in \mathfrak{S}(\mathsf{A})$ *then,* $\mathbf{x} \in \mathfrak{S}(\mathsf{A}')$*.*

Encoding of real algebraic points. Our algorithm will manipulate points which are obtained by algorithms searching for real roots of semi-algebraic sets defined by polynomials with coefficients in $\mathbb{Q}$ (see e.g. [3, Chapter 13]).

The coordinates of these points are real algebraic numbers. As in [20], we will encode such a point $(\alpha_1, \ldots, \alpha_k)$ classically with a 0-dimensional parametrization

$$\mathscr{Q} = (q(T), q_0(T), q_1(T), \ldots, q_k(T))$$

where $q, q_0, \ldots, q_k$ lie in $\mathbb{Q}[T]$, $\mathsf{gcd}(q, q_0) = 1$, q is **irreducible** and such that for some root ϑ of q, $\alpha_i = q_i(\vartheta)/q_0(\vartheta)$ of its coordinates and a Thom-encoding Θ of ϑ (we refer to [3, Chapters 2 and 12] for details about Thom-encodings and univariate representations).

Given the encoding of a real algebraic point $\mathscr{Q}, \Theta$, we will consider the routines MinPol and Param which return respectively q and the vector $(\frac{q_1}{q_0}, \ldots, \frac{q_k}{q_0})$.

Now, consider a 0-dimensional parametrization $\mathscr{U} = (q, q_0, \mathscr{U}_1, \ldots, \mathscr{U}_D) \subset \mathbb{Q}[T]^{2+D\times D}$ of degree δ and a Thom-encoding Θ encoding a point $(\mathbf{u}_1, \ldots, \mathbf{u}_D)$ (with $\mathbf{u}_i \in \mathbb{R}^D$). We will use a routine ExtractFirstEntry$((\mathscr{U}, \Theta), D)$ which returns the encoding $((q, q_0, \mathscr{U}_1), \Theta)$ of $\mathbf{u}_1$.

Decision procedures over the reals. Let Φ be a quantifier-free formula involving s polynomials in k variables of degree $\leq \delta$ and with bit-size bounded by τ and let $\mathfrak{S} \subset \mathbb{R}^k$ be the semi-algebraic set defined by Φ. As in [20], we will consider a subroutine Decision which takes as input Φ and outputs a sample point in $\mathfrak{S}$ iff $\mathfrak{S} \neq \emptyset$ within $\tau s^{k+1}\delta^{O(k)}$ bit-operations, else it returns an empty list (see [3, Chapter 15] or [2]).

In the non-empty situation, such a real point encoded by $(\mathscr{Q}, \Theta)$ where $\mathscr{Q}$ is a 0-dimensional parametrization and Θ is a Thom-encoding of a real root of the minimal polynomial in $\mathscr{Q}$. Moreover, all polynomials in $\mathscr{Q}$ have degree bounded by $O(\delta^k)$ and the bit size of their coefficients is dominated by $\tau\delta^{O(k)}$. As in [20, Section 2.1], using factorization and Euclidean division on univariate polynomials, one can transform $\mathscr{Q}, \Theta$ to $\mathscr{Q}', \Theta'$ where $\mathscr{Q}'$ is a 0-dimensional parametrization and Θ' is a Thom-encoding which encode the same real point as $\mathscr{Q}, \Theta$ within a bit-complexity dominated by $\tau s^{k+1}\delta^{O(k)}$ and such that the minimal polynomial of $\mathscr{Q}'$ is *irreducible.*

We also recall that given a system of s strict inequalities in $\mathbb{Q}[X_1, \ldots, X_k]$ of degree δ and bit size $\leq \tau$ defining a semi-algebraic set $\mathfrak{S} \subset \mathbb{R}^k$, there exists a routine OpenDecision which computes a point with *rational* coordinates in $\mathfrak{S} \cap \mathbb{Q}^k$ within $\tau^{O(1)}s^{k+1}\delta^{O(k)}$ bit operations if and only if $\mathfrak{S} \cap \mathbb{Q}^k \neq \emptyset$ (else it returns an empty list); see [2, Proof of Theorem 4.1.2 pp. 1032]. In case of non-emptiness, the bit-size of the output is dominated by $\tau\delta^{O(k)}$.

For convenience, we summarize these complexity results in the Proposition below.

PROPOSITION 2.3. *[2] Let* Φ *be quantifier-free formula involving* s *polynomials in* k *variables of degree* $\leq \delta$ *and with bit-size bounded by* τ *and* $\mathfrak{S} \subset \mathbb{R}^k$ *be the semi-algebraic set defined by* Φ*. There exists an algorithm* Decision *which takes* Φ *as input and returns an encoding* $(\mathscr{Q}, \Theta)$ *of a point in* $\mathfrak{S}$ *if and only if* $\mathfrak{S} \neq \emptyset$ *else it returns* $\emptyset$ *within* $\tau^{O(1)}s^{k+1}\delta^{O(k)}$ *bit operations. The degrees of the polynomials in* $\mathscr{Q}$ *and the bit size of their coefficients are respectively bounded by* $O(\delta^k)$ *and* $\tau\delta^{O(k)}$*.*

When Φ *contains only strict inequalities, there exists an algorithm* OpenDecision *which returns a rational point in* $\mathfrak{S}$ *if and only if* $\mathfrak{S} \neq \emptyset$ *(else it returns an empty list) within* $\tau^{O(1)}s^{k+1}\delta^{O(k)}$ *bit operations. In case of non-emptiness, the bit-size of the output is dominated by* $\tau\delta^{O(k)}$*.*

Retrieving rational points. Below, we consider a real algebraic number $\vartheta \in \mathbb{R}$ and its minimal polynomial $q \in \mathbb{Q}[T]$ of degree δ. We also consider linear forms

$$\mathscr{L} = g_0(\vartheta) + g_1(\vartheta)X_1 + \cdots + g_k(\vartheta)X_k$$

such that $g_0, \ldots, g_k$ are rational fractions in $\mathbb{Q}(T)$ sharing the same denominator q_0 of degree $\leq \delta - 1$ and whose numerators $n_0, \ldots, n_k$ have also degree $\leq \delta - 1$. We assume that $\mathsf{gcd}(q_0, q) = 1$ and that there exists $0 \leq i \leq k$ such that $n_i \neq 0$.

Consider the linear forms $\ell_0, \ldots, \ell_{\delta-1}$ in $\mathbb{Q}[X_1, \ldots, X_k]$ which are the coefficients of $1, T, \ldots, T^{\delta-1}$ in the polynomial

$$n_0 + n_1X_1 + \cdots + n_kX_k.$$

Since, by assumption, there exists i such that $n_i \neq 0$, then there exists j such that $\ell_j \neq 0$. We denote by ExtractLinForms a routine which takes as input $\mathscr{L}, q$ and returns all linear forms ℓ_j such that $\ell_j \neq 0$.

The following Lemma is extracted from the correctness proof of the algorithm given in [20]. For clarity and completeness, we isolate this statement below and prove it.

LEMMA 2.4. *[20] Let* $\mathfrak{S} \subset \mathbb{R}^k$ *be a semi-algebraic set,* ϑ *be a real algebraic number of degree* δ*,* q *be its minimal polynomial,* τ *be a bound on the bit-size of the coefficients of* q *and* $\mathscr{L}$ *be a linear form in* $\mathbb{Q}(\vartheta)[X_1, \ldots, X_k]$*. Assume that* $\mathscr{L}$ *vanishes at all points in* $\mathfrak{S}$*. Then all linear forms in* $L =$ ExtractLinForms$(\mathscr{L}, q)$ *vanish at all points in* $\mathfrak{S} \cap \mathbb{Q}^k$ *and* L *is obtained within* $O(\tau k\delta^{O(1)})$ *bit operations. The bit size of the coefficients in the output is dominated by* $O(\tau)$*.*

PROOF. Take $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_k) \in \mathfrak{S} \cap \mathbb{Q}^k$; by assumption $\mathscr{L}$ vanishes at $\mathbf{x}$; we conclude that $n_0 + n_1\mathbf{x}_1 + \cdots + n_k\mathbf{x}_k = 0$. Since ϑ is a real algebraic number of degree δ and the n_i's have degree $\leq \delta - 1$ we deduce that all the linear forms $\ell_0, \ldots, \ell_{\delta-1}$ vanish at $\mathbf{x}$. Runtime and bound on the bit size of the output are immediate. □

3. SUBROUTINES

Let $\mathsf{A}_0, \ldots, \mathsf{A}_k$ be symmetric matrices of size $D \times D$ and entries in $\mathbb{Q}$, A be the linear matrix $\mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k$ and $\mathfrak{S}(\mathsf{A}) \subset \mathbb{R}^k$ be the feasible region of the linear matrix inequality $\mathsf{A} \succeq 0$. Recall that $\mathfrak{S}(\mathsf{A})$ is a convex semi-algebraic set. Our algorithm is based on a case distinction:

1. when $k = 1$, then $\mathfrak{S}(\mathsf{A})$ is either empty or a real point or an interval with non-empty interior;

2. when $D = 1$, then A is a linear form and unless $k = 0$ and $\mathsf{A} < 0$, $\mathfrak{S}(\mathsf{A})$ has non-empty interior;
3. when $\mathfrak{S}(\mathsf{A})$ is full dimensional, i.e. $\mathfrak{S}(\mathsf{A})$ has non-empty interior; in this case we say that the linear matrix inequality is strongly feasible.
   These three cases will be tackled by a subroutine BasicCasesLMI.
4. when $\mathfrak{S}(\mathsf{A})$ is *not* full dimensional; if $\mathfrak{S}(\mathsf{A}) = \emptyset$, we say that $\mathsf{A} \succeq 0$ is infeasible, else we say that it is weakly feasible. In this latter case, according to [20, Lemma 3.4], there exists a hyperplane in $\mathbb{R}^k$ which contains $\mathfrak{S}(\mathsf{A})$.
   The routine WeakLMI below constructs linear forms whose coefficients are real algebraic numbers. From Lemma 2.4, this will allow us to deduce other linear forms S with coefficients in $\mathbb{Q}$ whose set of common solutions $\mathsf{Sols}(S) \in \mathbb{R}^k$ contains $\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$. It will also return a $(D-1, D-1)$ symmetric linear matrix $\widehat{\mathsf{A}}$ such that $\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k = \mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(S) \cap \mathbb{Q}^k$.

3.1 Subroutine BasicCasesLMI

Let $\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k$ where $\mathsf{A}_0, \ldots, \mathsf{A}_k$ are $(D \times D)$ symmetric matrices with entries in $\mathbb{Q}$ of bit size bounded by τ. We describe a subroutine BasicCasesLMI which takes as input $\mathsf{A}, [\mathsf{X}_1, \ldots, \mathsf{X}_k]$ and

1. when $k = 1$, it returns a point with rational coordinates in $\mathfrak{S}(\mathsf{A})$ iff $\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q} \neq \emptyset$ else it returns an empty list;
2. a point with rational coordinates in $\mathfrak{S}(\mathsf{A})$ if $\mathfrak{S}(\mathsf{A})$ has a non-empty interior;

else it returns false.

Let $\chi(y) = y^D + m_{D-1}y^{D-1} + \cdots + m_0$ be the characteristic polynomial of A, we denote by Φ the following formula

$$\Phi = \{(-1)^{(i+D)}m_i \geq 0,\ 0 \leq i \leq D-1\}$$

and by Ψ the following formula:

$$\Psi = \{(-1)^{(i+D)}m_i > 0,\ 0 \leq i \leq D-1\}.$$

By [15], the semi-algebraic set $\mathfrak{S}(\mathsf{A})$ is defined by Φ; the interior of $\mathfrak{S}(\mathsf{A})$ is defined by Ψ.

```
BasicCasesLMI($\mathsf{A}, [X_1, \ldots, X_k]$)
  1. If $k = 1$ and if there exists a linear factor $X - a$ of
     $m_i$ (with $a \in \mathbb{Q}$) for some $0 \leq i \leq D-1$ such that
     $(-1)^{(j+D)}m_j(a) \geq 0$ for $j \neq i$ then return $a$.
  2. $\mathscr{U}$ = OpenDecision($\Psi$).
  3. If $\mathscr{U}$ is not empty or $k = 1$ then return $\mathscr{U}$ else return
     false.
```

Proposition 3.1. *Let* $\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k$ *where* $\mathsf{A}_0, \ldots, \mathsf{A}_k$ *are* $(D \times D)$ *symmetric matrices with entries in* $\mathbb{Q}$ *of bit size bounded by* τ*.*

If $k = 1$ *and* $\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q} \neq \emptyset$, BasicCasesLMI($\mathsf{A}, [X_1]$) *returns a rational point in* $\mathfrak{S}(\mathsf{A})$ *else it returns an empty list.*

If $\mathfrak{S}(\mathsf{A}) \subset \mathbb{R}^k$ *is full-dimensional,* BasicCasesLMI($\mathsf{A}, [X_1, \ldots, X_k]$) *returns a rational point in* $\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$ *else it returns* false*.*

It runs within $\tau^{O(1)}D^{O(k)}$ *bit operations, in case of non-empty output, it has bit size bounded by* $\tau^{O(1)}D^{O(k)}$*.*

Proof. Assume that $\mathfrak{S}(\mathsf{A}) \subset \mathbb{R}$ (Step 1). Then, since $\mathfrak{S}(\mathsf{A})$ is convex, it is either empty or a point or an interval with non-empty interior. Suppose that it is a point. Then, it is the unique solution of Φ since $\mathfrak{S}(\mathsf{A})$ is defined by Φ. By assumption, this solution is not a solution of Ψ (else $\mathfrak{S}(\mathsf{A})$ would have a non-empty interior). Then, it can be obtained as the root of linear factors of one m_i for some $0 \leq i \leq D-1$ at which the $(-1)^{j+D}m_j$'s (for $j \neq i$) are positive. Note that in the univariate case, the costs of factorizations and real root isolations are polynomial in τ and D and if a rational point is output at this step it has bit length bounded by $(D\tau)^{O(1)}$ (see [13]).

Now assume that $\mathfrak{S}(\mathsf{A})$ is full-dimensional; it has a non-empty interior. Then, by Proposition 2.3, Step 2 returns a rational point in $\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$ if and only if $\mathfrak{S}(\mathsf{A}) \neq \emptyset$.

Suppose now that $\mathfrak{S}(\mathsf{A})$ is not full dimensional. If $k = 1$, we can conclude that $\mathfrak{S}(\mathsf{A})$ is empty and we are done. Now, assume that $k \geq 2$. Recall that the semi-algebraic set defined by the formula Ψ is the interior of $\mathfrak{S}(\mathsf{A})$; we deduce that it is empty. Then, by Proposition 2.3 $\mathscr{U}$ is empty and we return false.

By Proposition 2.3, runtime and bound on the output are immediate. □

3.2 Subroutine WeakLMI

Let $\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k$ where $\mathsf{A}_0, \ldots, \mathsf{A}_k$ are $(D \times D)$ symmetric matrices with entries in $\mathbb{Q}$ of bit size bounded by τ. We describe a routine WeakLMI which takes as input $\mathsf{A}, [X_1, \ldots, X_k]$ such that the LMI $\mathsf{A} \succeq 0$ is weakly feasible or infeasible and such that there does not exist $\mathbf{u} \in \mathbb{R}^D - \{\mathbf{0}\}$ such that $\mathsf{A}\mathbf{u} = \mathbf{0}$. It returns $S, \widehat{\mathsf{A}}$ such that

1. S is a sequence of linear forms in $\mathbb{Q}[X_1, \ldots, X_k]$ which vanish at all points in $\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$; we let $\mathsf{Sols}(S) \subset \mathbb{R}^k$ be the linear subspace of common solutions of S;
2. $\widehat{\mathsf{A}}$ is a symmetric linear matrix of size $(D-1) \times (D-1)$ with entries in $\mathbb{Q}[X_1, \ldots, X_k]$ such that

$$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(S) \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k.$$

Recall that, as the feasible region of a linear matrix inequality, $\mathfrak{S}(\mathsf{A})$ is convex. Hence, by [20, Lemma 3.4], we already know that there exists a linear form $\mathscr{L} \in \mathbb{R}[X_1, \ldots, X_k]$ which vanishes at all points in $\mathfrak{S}(\mathsf{A})$. In [12, Prop. 3.3.1], Klep and Schweighofer exploited special properties of LMI's to prove that $\mathsf{A} \succeq 0$ is a weak LMI (i.e. $\mathfrak{S}(\mathsf{A})$ has an empty interior) if and only if there exists a non-zero linear form $\mathscr{L} \in \mathbb{R}[X_1, \ldots, X_k]$ and a $(D \times D)$ matrix W with entries in $\mathbb{R}[X_1, \ldots, X_k]$ such that

$$\mathrm{Tr}(\mathsf{A}\mathsf{W}^\star\mathsf{W}) = -\mathscr{L}^2.$$

As noticed in the first line of the proof of [12, Prop. 3.3.1], this implies that $\mathscr{L}$ vanishes at all points in $\mathfrak{S}(\mathsf{A})$. Another stronger result was given in the proof of [12, Lemma. 4.3.5]: there exist linear forms $\mathscr{L}_1, \ldots, \mathscr{L}_D$ in $\mathbb{R}[X_1, \ldots, X_k]$ and $(D \times D)$ matrices $\mathsf{W}_1, \ldots, \mathsf{W}_D$ such that

$$\mathrm{Tr}(\mathsf{A}\mathsf{W}_i^\star\mathsf{W}_i) = -\mathscr{L}_i^2, \text{ for } 1 \leq i \leq D.$$

In the proof of [12, Lemma. 4.3.5], the matrices $\mathsf{W}_1, \ldots, \mathsf{W}_D$ are constructed from points in the semi-algebraic sets

$$G_1 = \{\mathbf{u} \in \mathbb{R}^D - \{\mathbf{0}\} \mid \mathbf{u}^\star\mathsf{A}\mathbf{u} = 0\}$$

$$G_2 = \{(\mathbf{u}_1, \ldots, \mathbf{u}_D) \in \mathbb{R}^{D \times D} \mid \sum_{i=1}^{D} \mathbf{u}_i^\star\mathsf{A}\mathbf{u}_i = 0, \mathbf{u}_1, \mathbf{u}_2 \neq \mathbf{0}\}$$

The algorithm described below can be seen as an effective counterpart and variant of the constructions in the proof of [12, Lemma. 4.3.5] to construct $\mathscr{L}_1, \ldots, \mathscr{L}_D$. These are obtained from the encodings of points in the aforementioned semi-algebraic sets. Finally, according to Lemma 2.4 (see also [20]), one can deduce from $\mathscr{L}_i$ linear equations with rational coefficients that must be satisfied by all elements in $\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$.

We denote by $\mathsf{ConstructFormula1}$, $\mathsf{ConstructFormula2}$ routines that take as input A and return the following formulas defining respectively G_1, G_2:

$$||\mathbf{U}||^2 > 0, \mathbf{U}^\star \mathsf{A}_i \mathbf{U} = 0, \text{ for } 0 \leq i \leq k$$

$$||\mathbf{U}_1||^2 > 0, ||\mathbf{U}_2||^2 > 0, \sum_{i=1}^{D} \mathbf{U}_i^\star \mathsf{A}_j \mathbf{U}_i^\star = 0, \text{ for } 0 \leq j \leq k$$

where $\mathbf{U} = [U_1, \ldots, U_D]^\star$ is a vector of new indeterminates and $\mathbf{U_1}, \ldots, \mathbf{U}_D$ are vectors of new indeterminates $[U_{1,i}, \ldots, U_{D,i}]^\star$ for $1 \leq i \leq D$. We can now describe the algorithm $\mathsf{WeakLMI}$.

```
WeakLMI(A, $[X_1, \ldots, X_k]$)
  1. Let $\mathscr{U}$ = Decision(ConstructFormula1(A))
  2. If $\mathscr{U}$ is not empty then
     (a) Let $i$ be the smallest index of the non-null coordinates of the point encoded by $\mathscr{U}$
     (b) Let P be the matrix $[\mathsf{Param}(\mathscr{U}), (\mathbf{e}_j)_{1 \leq j \neq i \leq D}]$ and $\mathsf{A}' = \mathsf{P}^\star \mathsf{A} \mathsf{P}$
     (c) Let $\mathscr{L}_1, \ldots, \mathscr{L}_D$ be the entries of element of $\mathsf{A}'\mathbf{e}_1$ and let $\widehat{\mathsf{A}}$ be the $(D-1, D-1)$ matrix obtained by removing the 1-st row and column in $\mathsf{A}'$
     (d) Return
         $(\mathsf{ExtractLinForms}(\mathscr{L}_i, \mathsf{MinPol}(\mathscr{U})), 1 \leq i \leq D), \widehat{\mathsf{A}}$.
  3. Let $\mathscr{V} = (\mathfrak{V}, \Theta)$ = Decision(ConstructFormula2(A))
  4. Let $\mathscr{U}$ = ExtractFirstEntry($\mathscr{V}, D$)
     (a) Let $i$ be the smallest index of the non-null coordinates of the point encoded by $\mathscr{U}$
     (b) Let P be the matrix $[\mathsf{Param}(\mathscr{U}), (\mathbf{e}_j)_{1 \leq j \neq i \leq D}]$ and $\mathsf{A}' = \mathsf{P}^\star \mathsf{A} \mathsf{P}$
     (c) Let $\mathscr{L}_1, \ldots, \mathscr{L}_D$ be the entries of $\mathsf{A}'\mathbf{e}_1$ and let $\widehat{\mathsf{A}}$ be the $(D-1, D-1)$ matrix obtained by removing the 1-st row and column in $\mathsf{A}'$
     (d) Return
         $(\mathsf{ExtractLinForms}(\mathscr{L}_i, \mathsf{MinPol}(\mathscr{U})), 1 \leq i \leq D), \widehat{\mathsf{A}}$.
```

PROPOSITION 3.2. *Let $\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k$ where $\mathsf{A}_0, \ldots, \mathsf{A}_k$ are $(D \times D)$ symmetric matrices with entries in $\mathbb{Q}$ of bit size bounded by τ. Assume that $\mathsf{A} \succeq 0$ is either weakly feasible or infeasible and that there does not exist $\mathbf{u} \in \mathbb{R}^D - \{\mathbf{0}\}$ such that $\mathsf{A}\mathbf{u} = \mathbf{0}$.*

Then $\mathsf{WeakLMI}(\mathsf{A}, [X_1, \ldots, X_k])$ returns $S, \widehat{\mathsf{A}}$ where S is a sequence of linear forms in $\mathbb{Q}[X_1, \ldots, X_k]$ which vanishes at all points in $\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$ and $\widehat{\mathsf{A}}$ is a $(D-1, D-1)$ symmetric linear matrix with entries en $\mathbb{Q}[X_1, \ldots, X_k]$ such that $\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(S) \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$.

It runs within $\tau^{O(1)} 2^{O(D^2)} D^{O(D^2)}$ bit operations; the bit size of the coefficients of forms in S is bounded by $\tau 2^{O(D^2)}$ and the bit size of coefficients of the entries of $\widehat{\mathsf{A}}$ is bounded by $O(\tau)$.

Proof of correctness. We briefly sketch the construction in [12, Lemma. 4.3.5]. The construction in the proof of [12, Lemma. 4.3.5] is based on the following case distinction:

Case 1. Assume first that there exists a *non-null* vector $\mathbf{u} = (u_1, \ldots, u_D)^\star \in \mathbb{R}^D - \{0\}$ such that $\mathbf{u}^\star \mathsf{A} \mathbf{u} = 0$. Step 1 computes such a vector. In the proof of [12, Lemma. 4.3.5] it is shown that if $\mathbf{u} = \mathbf{e}_1$ then any non null element $\mathscr{L}$ of $\mathsf{A}\,\mathbf{e}_1$ vanishes at all points in $\mathfrak{S}(\mathsf{A})$; moreover since we have assumed that $\{\mathbf{u} \mid \mathsf{A}\mathbf{u} = \mathbf{0}\} = \{\mathbf{0}\}$ there exists such a non null element $\mathscr{L}$.

We denote by i the smallest index such that $u_i \neq 0$. Here, to retrieve a similar situation where $\mathbf{u} = \mathbf{e}_1$, Step 2 substitutes A by $\mathsf{A}' = \mathsf{P}^\star \mathsf{A} \mathsf{P}$ where P is the $(D \times D)$-matrix whose first column is $\mathbf{u}$ and next columns are the vectors $\mathbf{e}_j$ for $j \in \{1, \ldots, D\} - \{i\}$ (see Step 2b). Note that P is invertible and consider the matrix A' in Step 2b; Lemma 2.2 implies that $\mathfrak{S}(\mathsf{A}') = \mathfrak{S}(\mathsf{A})$. Moreover, following the proof of [12, Lemma. 4.3.5], all entries of $\mathsf{A}'\mathbf{e}_1$ (Step 2c) vanish at all points in $\mathfrak{S}(\mathsf{A}')$.

Let S be the set of linear forms obtained at Step 2d and $\mathsf{Sols}(S) \subset \mathbb{R}^k$ the affine linear subspace defined by their common solutions. Lemma 2.4 implies that

$$\mathfrak{S}(\mathsf{A}') \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}') \cap \mathsf{Sols}(S) \cap \mathbb{Q}^k.$$

Moreover, note that, by construction of S, the first row and column of A' is $\mathbf{0}$ at all points in $\mathsf{Sols}(S)$. Lemma 2.1 implies that $\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(S) = \mathfrak{S}(\mathsf{A}') \cap \mathsf{Sols}(S)$; we deduce that $\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(S) \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$ since we previously observed that $\mathfrak{S}(\mathsf{A}') = \mathfrak{S}(\mathsf{A})$.

Case 2. We assume that there doesn't exist $\mathbf{u} \in \mathbb{R}^D - \{\mathbf{0}\}$ such that $\mathbf{u}^\star \mathsf{A} \mathbf{u} = 0$. By [12], this implies that there exist vectors $\mathbf{u}_1, \ldots, \mathbf{u}_D$ in $\mathbb{R}^D$ such that $\sum_{i=1}^D \mathbf{u}_i^\star \mathsf{A} \mathbf{u}_i = 0$ and $\mathbf{u}_1 \neq \mathbf{0}, \mathbf{u}_2 \neq \mathbf{0}$. Step 3 computes $\mathscr{V}$ which encodes the concatenation of such vectors $\mathbf{u}_1, \ldots, \mathbf{u}_D$. Step 4 extracts from $\mathscr{V}$ the encoding $\mathscr{U}$ of the vector $\mathbf{u}_1 \in \mathbb{R}^D - \{\mathbf{0}\}$; note that $\mathbf{u}_1^\star \mathsf{A} \mathbf{u}_1 \neq 0$. In the proof of [12, Lemma. 4.3.5], when $\mathbf{u}_1 = \mathbf{e}_1$ it is proved that the entries of the first row and column of A vanish at all points in $\mathfrak{S}(\mathsf{A})$.

We retrieve such a situation when we substitute A with A' (Step 4b): here we have $\mathbf{e}_1^\star \mathsf{A}' \mathbf{e}_1 \neq 0$; note that $\mathfrak{S}(\mathsf{A}') = \mathfrak{S}(\mathsf{A})$ by Lemma 2.2. Also the linear forms $\mathscr{L}_1, \ldots, \mathscr{L}_D$ constructed at Step 4c correspond to the one constructed in the proof of [12, Lemma. 4.3.5] (Case 2) which vanish at all points in $\mathfrak{S}(\mathsf{A}') = \mathfrak{S}(\mathsf{A})$.

Now, consider

1. $\widehat{\mathsf{A}}$ is the matrix defined at Step 4c;
2. S be the set of linear forms obtained at Step 4d and $\mathsf{Sols}(S) \subset \mathbb{R}^k$ the affine linear subspace defined by their common solutions.

As in Case 1, note that by the construction of S, the first row and column of A' is $\mathbf{0}$ at $\mathsf{Sols}(S)$. Then, using the same reasoning based on Lemmas 2.1 and 2.4 as in Case 1, we conclude that

$$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(S) = \mathfrak{S}(\mathsf{A}') \cap \mathsf{Sols}(S)$$

and that $\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(S) \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$ since we previously observed that $\mathfrak{S}(\mathsf{A}') = \mathfrak{S}(\mathsf{A})$. □

Complexity analysis. Proposition 2.3 implies that Step 1 requires $\tau^{O(1)} k^{O(D)} 2^{O(D)}$ bit operations. Moreover, if $\mathscr{U}$ is not an empty list, it encodes a real point in G_1 using a 0-dimensional parametrization of degree $\leq O(2^D)$ and coefficients of bit size $\leq \tau 2^{O(D)}$.

Assume that $\mathscr{U}$ is not empty. Step 2a requires only gcd operations on univariate polynomials in this parametrization; the cost is polynomial in $\tau k^D 2^D$. Steps 2b-2c do not induce an extra cost. Finally, Step 2d is negligible in terms of bit operations and it returns linear forms of bit size $\leq \tau 2^{O(D)}$ (Lemma 2.4).

Assume now that $\mathscr{U}$ is empty. Then, Proposition 2.3 implies that Step 3 requires $\tau^{O(1)}D^{O(D^2)}2^{O(D^2)}$ bit operations; in case of non-emptiness, the output 0-dimensional parametrization has degree $\leq O(2^{D^2})$ and the bit size of its coefficients is bounded by $\tau 2^{O(D^2)}$. Step 4 runs within a negligible cost and as in the previous paragraph Steps 4a-4d do not induce extra cost and, by Lemma 2.4, the bit size of the output linear equations in Step 4d is bounded by $\tau 2^{O(D^2)}$.

Estimates on the bit size of the coefficients in the entries of the matrices $\widehat{\mathsf{A}}$ (Steps 2c and 4c) are immediate. □

4. MAIN ALGORITHM

Let $\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k$ where $\mathsf{A}_0, \ldots, \mathsf{A}_k$ are $(D \times D)$ symmetric matrices with entries in $\mathbb{Q}$ of bit size bounded by τ. We describe now the main algorithm RationalLMI of this paper. It takes as input A, $[X_1, \ldots, X_k]$, and returns $\mathbf{x} = (\mathbf{x}_1, \ldots, \mathbf{x}_k) \in \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$ encoded by the sequence $(X_1 - \mathbf{x}_1, \ldots, X_k - \mathbf{x}_k)$ if A has rational solutions; otherwise returns $\emptyset$.

At the beginning of the algorithm, we consider the following semi-algebraic set:

$$G = \{\mathbf{u} \in \mathbb{R}^D - \{\mathbf{0}\} \mid \mathsf{A}\mathbf{u} = \mathbf{0}\}.$$

We denote by ConstructFormula routine that takes as input A and returns the formula defining G.

We will also use several other basic subroutines:

1. LinearSolve: it takes a set of linear forms with coefficients in $\mathbb{Q}$ and returns a rational point in the set of their common solutions if it is not empty, else it returns an empty list.
2. GaussianElimination: it takes as input a set of linear forms in $\mathbb{Q}[X_1, \ldots, X_k]$ and performs Gaussian elimination to return $\mathcal{X}, \mathcal{H}, \mathcal{V}$ where $\mathcal{X}$ is a list of variables $X_{i_1}, \ldots, X_{i_\ell}$, $\mathcal{V}$ is the list of variables in $\{X_1, \ldots, X_k\} - \{X_{i_1}, \ldots, X_{i_\ell}\}$ and $\mathcal{H}$ is a list of linear forms $h_{i_1}, \ldots, h_{i_\ell}$ in $\mathbb{Q}[\mathcal{V}]$ such that the relations of the form $X_{i_r} = h_{i_r}(\mathcal{V})$ are generated by the input.
3. Substitute: it takes as input a list of variables $[X_1, \ldots, X_r]$, a list of linear forms $[h_1, \ldots, h_r]$ and a linear matrix A with entries depending on variables $X_1, \ldots, X_k$ and which substitutes X_i by h_i in A for $1 \leq i \leq r$.
4. Evaluate: it takes as input a list of variables $\mathcal{X} = [X_1, \ldots, X_r]$, a list of polynomials $\mathcal{H} = [h_1, \ldots, h_r]$ in $\mathbb{Q}[Y_1, \ldots, Y_p]$ and a sequence of rational numbers $q = (q_1, \ldots, q_p)$; it returns the sequence $(X_i - h_i(q), 1 \leq i \leq r)$.

```
RationalLMI($\mathsf{A}, [X_1, \ldots, X_k]$)
1. $\mathscr{U}$ = BasicCasesLMI($\mathsf{A}, [X_1, \ldots, X_k]$)
2. If $\mathscr{U} \neq$ false is not empty then, denoting by $(\mathbf{x}_1, \ldots, \mathbf{x}_k)$ the point encoded by $\mathscr{U}$ return $X_1 - \mathbf{x}_1, \ldots, X_k - \mathbf{x}_k$
3. Let $\mathscr{U}$ = LinearSolve(ConstructFormula($\mathsf{A}$))
4. If $\mathscr{U}$ is not empty then
   (a) compute an invertible matrix $\mathsf{P}$ with entries in $\mathbb{Q}$ such that $\mathsf{P}\mathbf{e}_1 = \mathbf{u}$ and let $\mathsf{A}' = \mathsf{P}^\star\mathsf{A}\mathsf{P}$ and $\widehat{\mathsf{A}}$ be the $(D-1, D-1)$-matrix obtained by removing the first row and column from $\mathsf{A}'$
   (b) return RationalLMI($\widehat{\mathsf{A}}, [X_1, \ldots, X_k]$)
5. $S, \widehat{\mathsf{A}}$ = WeakLMI($\mathsf{A}, [X_1, \ldots, X_k]$)
6. If LinearSolve($S$) is empty then return $\emptyset$
7. $\mathcal{X}, \mathcal{H}, \mathcal{V}$ = GaussianElimination($S$)
8. $\widetilde{\mathsf{A}}$ = Substitute($\mathcal{X}, \mathcal{H}, \widehat{\mathsf{A}}$) and $R$ = RationalLMI($\widetilde{\mathsf{A}}, \mathcal{V}$)
9. If $R$ is not empty then return $R$, Evaluate($\mathcal{X}, \mathcal{H}, R$) else return $\emptyset$
```

THEOREM 4.1. *Let $\mathsf{A} = \mathsf{A}_0 + X_1\mathsf{A}_1 + \cdots + X_k\mathsf{A}_k$ where $\mathsf{A}_0, \ldots, \mathsf{A}_k$ are $(D \times D)$ symmetric matrices with entries in $\mathbb{Q}$ of bit size bounded by τ. Then* RationalLMI$(\mathsf{A}, [X_1, \ldots, X_k])$ *returns a point in $\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$ iff $\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k \neq \emptyset$ else it returns an empty list. It runs within*

$$(k\tau)^{O(1)}2^{O(\min(k,D)D^2)}D^{O(D^2)}$$

bit operations and in case of non-emptiness the output point has coordinates of bit size bounded by $\tau^{O(1)}2^{O(\min(k,D)D^2)}$.

Proof of correctness. Assume for the moment that either $k = 1$ or $\mathfrak{S}(\mathsf{A})$ is full dimensional (note that if $D = 1$ and $k \geq 1$ $\mathfrak{S}(\mathsf{A})$ is full dimensional). Then, correctness follows from Proposition 3.1. The rest of the proof is by induction on D: our induction assumption is that for any linear symmetric matrix B of size $D - 1$ with linear entries in $\mathbb{Q}[X_1, \ldots, X_p]$, RationalLMI$(\mathsf{B}, [X_1, \ldots, X_p])$ outputs a rational point in $\mathfrak{S}(\mathsf{B}) \cap \mathbb{Q}^p$ if and only if $\mathfrak{S}(\mathsf{B}) \cap \mathbb{Q}^p$ is not empty.

Suppose first that there exists a vector $\mathbf{u} \in \mathbb{R}^D - \{0\}$ such that $\mathsf{A}.\mathbf{u} = \mathbf{0}$, then Step 3 computes such a vector. Lemma 2.2 ensures that $\mathfrak{S}(\mathsf{A}')$ (where A' is the symmetric matrix considered at Step 4a) equals $\mathfrak{S}(\mathsf{A})$. Moreover, by construction, we have $\mathsf{A}'\mathbf{e}_1 = \mathbf{0}$; then the first column (and row) of A' is $\mathbf{0}$. Then, by Lemmas 2.1 and 2.2, we conclude that $\mathfrak{S}(\widehat{\mathsf{A}}) = \mathfrak{S}(\mathsf{A}') = \mathfrak{S}(\mathsf{A})$. By the induction assumption applied to $\widehat{\mathsf{A}}$, we conclude that the call to RationalLMI at Step 4b outputs a rational point in $\mathfrak{S}(\mathsf{A})$ if $\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k \neq \emptyset$ else it returns $\emptyset$.

Now assume that there is no vector $\mathbf{u} \in \mathbb{R}^D - \{0\}$ such that $\mathsf{A}.\mathbf{u} = \mathbf{0}$; we are at Step 5. Proposition 3.2 implies that:

1. all linear forms in S vanish at all points in $\mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$ and at least one of them is not identically null; we denote by $\mathsf{Sols}(S) \subset \mathbb{R}^k$ the set of common solutions of the forms in S;
2. the $(D-1, D-1)$-matrix $\widehat{\mathsf{A}}$ is a symmetric linear matrix with entries in $\mathbb{Q}[X_1, \ldots, X_k]$ such that

$$\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(S) \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k.$$

If S has no solution then $\mathfrak{S}(\mathsf{A})$ is empty (Step 6). In steps (7-8), the linear forms in S are used to eliminate variables in $\widehat{\mathsf{A}}$; this provides the symmetric linear matrix $\widetilde{\mathsf{A}}$ of size $(D-1, D-1)$ (Step 8). The induction assumption applied to $\widetilde{\mathsf{A}}$ allows us to conclude that, through the call to RationalLMI in Step 8, the last step returns a point in $\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(S) \cap \mathbb{Q}^k$ if this set is non-empty else it returns $\emptyset$. Now recall that we previously observed that $\mathfrak{S}(\widehat{\mathsf{A}}) \cap \mathsf{Sols}(S) \cap \mathbb{Q}^k = \mathfrak{S}(\mathsf{A}) \cap \mathbb{Q}^k$; which concludes the proof. □

Complexity analysis. Let $\mathcal{A}$ be the set of symmetric linear matrices A of size D with entries in $\mathbb{Q}[X_1, \ldots, X_k]$ the coefficients of which have bit size bounded by τ. We denote by $\mathsf{C}(\tau, D, k)$ an upper bound on the runtime of the execution of RationalLMI for all possible inputs $\mathsf{A} \in \mathcal{A}$ and $[X_1, \ldots, X_k]$; we also denote by $\mathsf{T}(\tau, D, k)$ an upper bound on the bit size of the coordinates of the output of RationalLMI for all possible inputs $\mathsf{A} \in \mathcal{A}$.

By Propositions 3.1 and 3.2, there exist constants A and B large enough, independent of τ, D, k, such that

(A) Step 1 is performed within $A\tau^B D^{Bk}$ bit operations and if $\mathscr{U}$ is not empty then the returned point (Step 2) has coordinates of bit size bounded by $\tau^B D^{Bk}$;

(B) Step 3 (which consists of solving k linear systems of size $D \times D$ with coefficients of bit size $\le \tau$), is performed within $A\tau^B D^B$ operations and the coefficients in $\mathscr{U}$ have bit size bounded by τD^B;

(C) Steps (4a-4b), which again consists of linear algebra operations, builds the matrix P in $A\tau^B D^B$ operations and the elements in the matrix P have bit size bounded by τD^B;

(D) Step 5 requires at most $\tau^B 2^{BD^2} D^{BD^2}$ bit operations and the bit size of the coefficients of forms in S is bounded by $\tau 2^{BD^2}$, and using elementary complexity results in linear algebra the bit size of coefficients of the entries of $\widetilde{\mathsf{A}}$ (in Step 8) is bounded by $\tau 2^{BD^2}$.

We let $m_{k,D} = \min(k, D)$ and prove below that

$$\mathsf{C}(\tau, D, k) \le Ak\tau^B 2^{B^2 m_{k,D} D^2} D^{B^2 D^2}$$

$$\mathsf{T}(\tau, D, k) \le A\tau^B 2^{B^2 m_{k,D} D^2}$$

by decreasing induction on D and k. More precisely, we will assume that for $D' < D$ and $k' \le k$

$$\mathsf{C}(\tau, D', k') \le Ak'\tau^B 2^{B^2 m_{k',D'} D'^2} D^{B^2 D'^2}$$

$$\mathsf{T}(\tau, D', k') \le A\tau^B 2^{B^2 m_{k',D'} D'^2}$$

and that for $D' \le D$ and $k' < k$

$$\mathsf{C}(\tau, D', k') \le Ak'\tau^B 2^{B^2 m_{k',D'} D'^2} D^{B^2 D'^2}$$

$$\mathsf{T}(\tau, D', k') \le A\tau^B 2^{B^2 m_{k',D'} D'^2}$$

This induction is easily initialized for $k = 1$ or $D = 1$ at Steps 1-2 using Proposition 3.1.

We consider now the general case. Using the observations **(A)**, **(B)**, **(C)** and **(D)**, the worst case complexity is attained if $\mathscr{U}$ (computed in Step 1) is false and when the execution goes through Step 5. The cost of Step 3 is negligible compared to the cost of Step 1. In case of non-emptiness of $\mathscr{U}$ the recursive call at Step 4b requires to check that

$$\begin{aligned}
\mathsf{C}(\tau, D, k) &\le A\tau^B D^B + \mathsf{C}(\tau D^B, D-1, k) \\
&\le A\tau^B D^B + \\
&\quad Ak\tau^B D^{B^2} 2^{B^2 m_{k,D-1}(D-1)^2} D^{B^2 (D-1)^2} \\
&\le Ak\tau^B 2^{B^2 m_{k,D} D^2} D^{B^2 D^2} \text{ by induction} \\
\mathsf{T}(\tau, D, k) &\le \mathsf{T}(\tau D^B, D-1, k) \\
&\le A\tau^B (D-1)^{B^2} 2^{B^2 m_{k,D-1}(D-1)^2} \text{ (induction)} \\
&\le A\tau^B 2^{B^2 m_{k,D} D^2}
\end{aligned}$$

Now, we need to check the worst case bound when the execution of $\mathsf{RationalLMI}$ goes through Step 5. By observation **(D)**, we get

$$\begin{aligned}
\mathsf{C}(\tau, D, k) &\le A\tau^B D^{BD^2} + \mathsf{C}(\tau 2^{BD^2}, D-1, k-1) \\
&\le A\tau^B D^{BD^2} + \\
&\quad A(k-1)\tau^B 2^{B^2(D^2 + m_{k-1,D-1}(D-1)^2)} D^{B^2(D-1)^2} \\
&\le Ak\tau^B 2^{B^2 m_{k,D} D^2} D^{BD^2} \text{ by induction} \\
\mathsf{T}(\tau, D, k) &\le \mathsf{T}(\tau 2^{BD^2}, D-1, k-1) \\
&\le A\tau^B 2^{B^2 D^2} 2^{B^2 m_{k-1,D-1}(D-1)^2} \text{ by induction} \\
&\le A\tau^B 2^{B^2 m_{k,D} D^2}
\end{aligned}$$

Finally, $\mathsf{C}(\tau, D, k)$ lies in $(k\tau)^{O(1)} 2^{O(m_{k,D} D^2)} D^{O(D^2)}$; we also have $\mathsf{T}(\tau, D, k)$ lies in $\tau^{O(1)} 2^{O(m_{k,D} D^2)}$. □

5. SCHEIDERER'S EXAMPLE

In [21], Scheiderer constructed explicit polynomials with rational coefficients which are sums of squares of polynomials with real coefficients, but not sums of squares of polynomials with rational coefficients.

By [21, Theorem 2.2] The polynomial

$$f = x^4 + x\,y^3 + y^4 - 3\,x^2\,y\,z - 4\,x\,y^2\,z + 2\,x^2\,z^2 + x\,z^3 + y\,z^3 + z^4$$

can be written as a sum of two polynomials with real coefficients but has no sos decomposition over rational numbers.

Suppose

$$f = [x^2, xy, y^2, xz, yz, z^2]\,\mathsf{A}\,[x^2, xy, y^2, xz, yz, z^2]^\star,$$

where the Gram matrix A is a 6×6 symmetric matrix

$$\begin{bmatrix}
1 & 0 & X_1 & 0 & -\frac{3}{2} - X_2 & X_3 \\
0 & -2\,X_1 & \frac{1}{2} & X_2 & -2 - X_4 & -X_5 \\
X_1 & \frac{1}{2} & 1 & X_4 & 0 & X_6 \\
0 & X_2 & X_4 & -2\,X_3 + 2 & X_5 & \frac{1}{2} \\
-\frac{3}{2} - X_2 & -2 - X_4 & 0 & X_5 & -2\,X_6 & \frac{1}{2} \\
X_3 & -X_5 & X_6 & \frac{1}{2} & \frac{1}{2} & 1
\end{bmatrix}$$

with six variables: $X_1, X_2, X_3, X_4, X_5, X_6$ corresponding to seven symmetric matrices $\mathsf{A}_0, \mathsf{A}_1, \mathsf{A}_2, \mathsf{A}_3, \mathsf{A}_4, \mathsf{A}_5, \mathsf{A}_6$.

- Apply the routine $\mathsf{HasRealSolutions}$ in RAGLib [17] to compute

  $$\mathscr{U} = \mathsf{OpenDecision}(\Psi).$$

  The set $\mathscr{U}$ is empty, hence A is not strongly feasible.

- In step 5 of $\mathsf{RationalLMI}$, by $\mathsf{WeakLMI}(\mathsf{A}, [X_1, \cdots, X_6])$,

  1. Use the routine $\mathsf{RationalUnivariateRepresentation}$ [16], we get an encoding of a real algebraic solution

     $$\mathbf{u} = \begin{bmatrix}
     -1 + \frac{1}{2}\,\vartheta + \frac{1}{2}\,\vartheta^4 \\
     \frac{\vartheta^3}{2} + \frac{1}{2} \\
     \vartheta^2 \\
     -2\,\vartheta + \frac{1}{2}\,\vartheta^2 + \frac{1}{2}\,\vartheta^5 \\
     \vartheta \\
     1
     \end{bmatrix},$$

     where ϑ is a real algebraic number satisfying

     $$\vartheta^6 - 4\,\vartheta^2 - 1 = 0.$$

  2. $\mathscr{U}$ is not empty then

     (a) $i = 1$.

     (b) $P = [\mathsf{Param}(\mathscr{U}), e_2, \ldots, e_6]$ and $\mathsf{A}' = \mathsf{P}^\star \mathsf{A}\mathsf{P}$.

(c) $\mathscr{L}_1, \ldots, \mathscr{L}_6$ in the first column of A' are

$$\begin{bmatrix} 0 \\ \frac{1}{2}\,X_2\,\vartheta^5 - X_1\vartheta^3 + \cdots - X_1 - X_5 \\ \frac{1}{2}\,X_4\,\vartheta^5 + \frac{1}{2}\,X_1\,\vartheta^4 + \cdots - X_1 + X_6 + \frac{1}{4} \\ (1 - X_3)\,\vartheta^5 + \frac{1}{2}\,X_2\,\vartheta^3 + \cdots + \frac{1}{2} + \frac{1}{2}\,X_2 \\ \frac{1}{2}\,X_5\,\vartheta^5 + \cdots + 1 + X_2 - \frac{1}{2}\,X_4 \\ \frac{1}{4}\vartheta^5 + \frac{1}{2}\,X_3\,\vartheta^4 + \cdots - X_3 + 1 - \frac{1}{2}\,X_5 \end{bmatrix}$$

As $i = 1$, $\widehat{\mathsf{A}}$ is equivalent to the 5×5 matrix obtained by removing the 1-st row and column in A.

(d) The sequence of coefficients of $\vartheta^5, \ldots, \vartheta^1, 1$ in $\mathscr{L}_1, \ldots, \mathscr{L}_6$ is denoted as S, return $S, \widehat{\mathsf{A}}$.

- In step 6 of RationalLMI, the coefficient vector of ϑ^5 in $\mathscr{L}_1, \ldots, \mathscr{L}_6$ is

$$S_5 = \left[0, \frac{1}{2}\,X_2, \frac{1}{2}\,X_4, 1 - X_3, \frac{1}{2}\,X_5, \frac{1}{4}\right]^\star.$$

The last entry of S_5 is $\frac{1}{4}$, the linear system $S_5 = \mathsf{0}$ has no solutions. Therefore, LinearSolve(S) returns an empty set.

$\mathfrak{S}(\mathsf{A})$ has no rational solutions. The Maple worksheet can be downloaded from http://www.mmrc.iss.ac.cn/~lzhi/Research/hybrid/RaLMI

6. REFERENCES

[1] H. Anai. Solving lmi and bmi problems by quantifier elimination. In R. Liska, editor, *The 4th International IMACS Conference on Applications of Computer Algebra*, volume 98 of *Proc. of IMACS-ACA*, 1998.

[2] S. Basu, R. Pollack, and M.-F. Roy. On the combinatorial and algebraic complexity of quantifier elimination. *J. ACM*, 43(6):1002–1045, November 1996.

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

[4] J.C. Faugère, G. Moroz, F. Rouillier, and M. Safey El Din. Classification of the perspective-three-point problem, discriminant variety and real solving polynomial systems of inequalities. In D. Jeffrey, editor, *Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*, ISSAC '08, pages 79–86, New York, NY, USA, 2008. ACM.

[5] A. Greuet, F Guo, M. Safey El Din, and L. Zhi. Global optimization of polynomials restricted to a smooth variety using sums of squares. *Journal of Symbolic Computation*, 47(5):503 – 518, 2012.

[6] A. Greuet and M. Safey El Din. Deciding reachability of the infimum of a multivariate polynomial. In É. Schost and I. Z. Emiris, editors, *Proceedings of the 36th international symposium on Symbolic and algebraic computation*, ISSAC '11, pages 131–138, New York, NY, USA, 2011. ACM.

[7] H. Iwane, H. Yanami, H. Anai, and K. Yokoyama. An effective implementation of a symbolic-numeric cylindrical algebraic decomposition for quantifier elimination. In H. Kai and H. Sekigawa, editors, *Proceedings of the 2009 conference on Symbolic numeric computation*, pages 55–64. ACM, 2009.

[8] E. Kaltofen, B. Li, Z. Yang, and L. Zhi. Exact certification of global optimality of approximate factorizations via rationalizing sums-of-squares with floating point scalars. In D. Jeffrey, editor, *Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*, ISSAC '08, pages 155–164, New York, NY, USA, 2008. ACM.

[9] E. Kaltofen, B. Li, Z. Yang, and L. Zhi. Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients. *J. Symb. Comput.*, 47(1):1–15, January 2012.

[10] L. Khachiyan and L. Porkolab. Computing integral points in convex semi-algebraic sets. In *Proceedings of the 38th Annual Symposium on Foundations of Computer Science*, FOCS '97, pages 162–171, Washington, DC, USA, 1997. IEEE Computer Society.

[11] L. Khachiyan and L. Porkolab. Integer optimization on convex semialgebraic sets. *Discrete and Computational Geometry*, 23(2):207–224, 2000.

[12] I. Klep and M. Schweighofer. An exact duality theory for semidefinite programming based on sums of squares. *ArXiv e-prints*, July 2012.

[13] A.K. Lenstra, H.W. Lenstra, and L. Lovàsz. Factoring polynomials with rational coefficients. *Mathematische Annalen*, 261:515–534, 1982.

[14] H. Peyrl and P. A. Parrilo. Computing sum of squares decompositions with rational coefficients. *Theor. Comput. Sci.*, 409(2):269–281, December 2008.

[15] V. Powers and T. Wörmann. An algorithm for sums of squares of real polynomials. *Journal of Pure and Applied Algebra*, 127:99–104, 1998.

[16] F. Rouillier. Solving zero-dimensional systems through the rational univariate representation. *Applicable Algebra in Engineering, Communication and Computing*, 9:433–461, 1999.

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

[18] M. Safey El Din. Testing sign conditions on a multivariate polynomial and applications. *Mathematics in Computer Science*, 1(1):177–207, 2007.

[19] M. Safey El Din. Computing the global optimum of a multivariate polynomial over the reals. In D. Jeffrey, editor, *Proceedings of the twenty-first international symposium on Symbolic and algebraic computation*, ISSAC '08, pages 71–78, New York, NY, USA, 2008. ACM.

[20] M. Safey El Din and L. Zhi. Computing rational points in convex semialgebraic sets and sum of squares decompositions. *SIAM J. on Optimization*, 20(6):2876–2889, September 2010.

[21] C. Scheiderer. Descending the ground field in sums of squares representations. *eprint arXiv:1209.2976v2*, 09/2012.