to appear in Eur. J. O.R.

Products of positive forms, linear matrix inequalities, and Hilbert 17-th problem for ternary forms

Etienne de Klerk* Dmitrii V. Pasechnik*†

November 2, 2001

Abstract

A form p on $\mathbb{R}^n$ (homogeneous n-variate polynomial) is called positive semidefinite (p.s.d.) if it is nonnegative on $\mathbb{R}^n$. In other words, the zero vector is a global minimizer of p in this case. The famous $17th$ conjecture of Hilbert [9] (later proven by Artin [1]) is that a form p is p.s.d. if and only if it can be decomposed a sum of squares of rational functions.

In this paper we give an algorithm to compute such a decomposition for ternary forms ($n = 3$). This algorithm involves the solution of a series of systems of linear matrix inequalities (LMI's). In particular, for a given p.s.d. ternary form p of degree $2m$, we show that the abovementioned decomposition can be computed by solving at most $m/4$ systems of LMI's of dimensions polynomial in m. The underlying methodology is largely inspired by the original proof of Hilbert, who had been able to prove his conjecture for the case of ternary forms.

1 Introduction

Usually, mathematical programming is used in operations research and engineering. In this text, however, the application domain is primarily pure mathematics, or, to be more precise, real algebra. The algorithm described here, however, can be applied to check efficiently whether a ternary form

*Faculty of Information Technology and Systems, Department of Technical Mathematics and Informatics, Delft University of Technology, P.O. Box 5031, 2600 GA Delft, The Netherlands.

†*Corresponding author*; e-mail: d.pasechnik@its.tudelft.nl

(or, equivalently, a bivariate polynomial) is nonnegative. This can be used in stability analysis of dynamic systems, in global optimization, etc.

The question on whether a positive semidefinite (p.s.d.) n-ary form p can be represented as a finite sum of squares (s.o.s.) of rational functions, i.e.

$$p = \sum_{j=1}^{N} \frac{q_j^2}{r_j^2}, \tag{1}$$

was listed by Hilbert in his address to the first International Congress of Mathematicians in 1900 [9]. It became later known as the 17-th Hilbert problem, and was affirmatively solved in full generality by E. Artin [1, pp. 273-88], albeit in a rather non-constructive way.

It was already established by Hilbert that the r_j's in (1) cannot in general be constants. The following example is due to Motzkin [10, p. 217] (see also [20]). The form

$$M(x, y, z) = z^6 + x^4y^2 + x^2y^4 - 3x^2y^2z^2 \tag{2}$$

is p.s.d., but not s.o.s. of forms.

Hilbert himself was able to give a solution for the 17-th problem in the case of ternary forms [8], that is, when the number n of variables equals 3. More on the topic of the 17-th Hilbert problem can be found in e.g. in [20, 14, 15]. Hilbert's approach also appears to be, at first sight, a non-constructive one. However, as we will show, a slight modification leads to an algorithm. Namely, the main ingredient in his approach, finding a p.s.d. form p_1 of degree $\deg p_1 = \deg p - 4 = 2m - 4$ such that

$$p = \frac{\sum_{j=1}^{N} q_j^2}{p_1}, \tag{3}$$

can be restated as a semidefinite feasibility problem[1], at least when Hilbert's extra condition $N = 3$ is replaced by a weaker one, $N < \infty$. Once such p_1 and the set of $q_j = q_{0j}$ is found, (3) can be applied to p_1 in place of $p = p_0$, and some p_2 on place of p_1. Repeating this sufficiently many times, say k, one arrives at the situation when $\deg p_k \leq 4$. It is known that a ternary p.s.d. form of degree at most 4 can be decomposed in a s.o.s. of forms, using the method that is known to algebraic geometers as Gram matrix method.

[1] Given a system of LMI's, the problem of deciding whether a solution exists is known as the semidefinite feasibility problem.

It is then easy to construct a sum (1) from p_i and q_{ij}. We will give details in the proof of Theorem 1.

For instance, for $p = M(x,y,z)$ in (2), $k = 1$ step suffices, and the following decomposition of M as in (1), with $p_1 = x^2+y^2+z^2$, can be found (see [11]).

$$M(x,y,z) = \frac{p_1(x^2yz-yz^3)^2}{p_1^2} + \frac{p_1(xy^2z-xz^3)^2}{p_1^2} + \frac{p_1(x^2y^2-z^4)^2}{p_1^2} + \tag{4}$$
$$+\frac{p_1(xy^3-x^3y)^2}{4p_1^2} + \frac{\sqrt{3}^2 p_1(xy^3+x^3y-2xyz^2)^2}{4p_1^2}.$$

Specifically, we obtain the following.

Theorem 1. A p.s.d. ternary form p of degree $2m$ can be decomposed as in (1) via solving a sequence of at most $m/4$ systems of linear matrix inequalities of dimensions polynomial in m. The degrees of the denominators in (1) will be bounded from above by $3m^2/2$.

We must mention that the complexity status of the semidefinite feasibility problem is not known, but it cannot be an NP-complete problem unless NP = co-NP (see [16, 17, 12]). In particular, we can state the following result.

Corollary 1. The complexity of computing the decomposition (1) in the real number model (see [2]) is in $\mathrm{NP} \cap \mathrm{co}-\mathrm{NP}$.

For further remarks concerning complexity, see Section 4.

Remark 1. The degree bound in Theorem 1 is the sharpest known, and optimal for $m \leq 4$. In fact, this is the only bound known to us on those degrees for forms with real roots, that is, p.s.d., but no positive definite. The bounds for the latter, such as [13, 19, 18] all involve the minimal value taken by the form on the unit sphere.

The main work in proving Theorem 1 lies in proving the following.

Theorem 2. For a p.s.d. ternary form p of degree $2m$, a p.s.d. form p_1 of degree $2m-4$ satisfying (3) can be found by solving an LMI of dimensions polynomial in m.

The existence of a decomposition just mentioned was proved in [8]. Thus, one needs to demonstrate how to compute one using LMIs. We defer this task to the following Sections.

Let us show how to derive Theorem 1 from Theorem 2. Denote $Q_i = \sum_{j=1}^{N_i} q_{ij}^2$. We also abuse notation by assuming $\prod_{i=i_0}^{i=i_t} Q_i = 1$ whenever $i_0 > i_t$. Then repeated application of (3) gives

$$p_0 = p = \frac{Q_0}{p_1} = \frac{p_2 Q_0}{Q_1} = \frac{Q_0 Q_2}{p_3 Q_1} = \cdots = f \frac{\prod_{i=0}^{k-1} Q_{2i}}{\prod_{i=0}^{k-s} Q_{2i+1}}, \tag{5}$$

where $f = p_{2k}$, $s = 1$ for $m = 4k+1$ or $4k+2$, and $f = 1/p_{2k-1}$, $s = 2$ for $m = 4k-1$ or $4k$.

Note that for odd m the degree of f (respectively, of $1/f$) is two, while for even m the degree of f (respectively, of $1/f$) is four. Such an f (respectively, $1/f$) can always be decomposed as a s.o.s. of forms. This is well-known for degree 2. For degree 4 it was first proved by Hilbert [7], and an easy modern proof can be found in [3].

Multiplying both the numerator and the denominator D (it will include f when $m = 4k-1$ or $4k$) in (5) by D presents p as a sum of squares of rational functions with the same denominator D.

This allows one to compute the degree of D^2 in (5), using the fact that $\deg Q_i = 4m - 8i - 4$. Namely, one gets

m	$4k-1$	$4k$	$4k+1$	$4k+2$
$\deg D^2$	$12k^2 - 12k + 2$	$12k^2 - 8k$	$12k^2$	$12k^2 + 4k$

This completes the proof of Theorem 1.

2 Preliminaries

2.1 Linear matrix inequalities

The notation we use here is fairly standard and taken largely from [21, 12].

Denote the space of symmetric $k \times k$ matrices by $\mathcal{S}_k$. A matrix $A \in \mathcal{S}_k$ is p.s.d. is the associated quadratic form $x^T A x$ is p.s.d., that is, $x^T A x \geq 0$ for all $x \in \mathbb{R}_k$. Write $A \succeq 0$ if A is p.s.d., and $A \succeq B$ if $A - B \succeq 0$. The elements of the standard basis of $\mathbb{R}^k$ are denoted e_i, for $1 \leq i \leq k$. For a vector v, we denote $\mathrm{diag}(v)$ the diagonal matrix with the entries specified by v, and for a square matrix A we denote by $\mathrm{Diag}(A)$ the vector of diagonal entries of A. For a subset $\mathcal{U} \subseteq \mathbb{R}^k$, we denote $\mathcal{U}_+ = \{x \in \mathcal{U} \mid x \geq 0\}$.

In what follows we are concerned with certain convex subsets $\mathcal{T}$ of the cone of the p.s.d. matrices $\{A \in \mathcal{S}_k \mid A \succeq 0\}$. We need the definition of the

relative interior $\mathrm{ri}(\mathcal{T})$ of $\mathcal{T}$. Namely, $\mathrm{ri}(\mathcal{T})$ consists of $A \in \mathcal{T}$ such that for any $B \in \mathcal{T}$ there exists $\epsilon > 0$ satisfying $(\epsilon + 1)A - \epsilon B \in \mathcal{T}$.

Then, $\mathrm{Tr}(A) = \sum_i A_{ii}$ denotes the *trace* of A. Equip $\mathcal{S}_k$ with the inner product $\langle A, B \rangle = \mathrm{Tr}(AB)$. A *linear matrix inequality* (LMI, for short) on $\mathcal{S}_k$ is specified by a K-tuple of matrices $(A_i, \ldots, A_K)$, where $A_i \in \mathcal{S}_k$, and $c \in \mathbb{R}^K$, as follows.

$$\langle A_i, X \rangle = c_i \quad \text{for } 1 \leq i \leq K \tag{6}$$

$$X \succeq 0 \tag{7}$$

We say that the LMI (6)-(7) is *feasible* if there exists $X \in \mathcal{S}_k$ satisfying (6)-(7), and we denote the set of such X by $\mathcal{T}(A_1, \ldots, A_K, c)$. The numbers k and K are called the *dimensions* of the LMI here.

In fact, the feasible set of a system of LMI's is sometimes called a *spectrahedron* which is a generalization of the concept of a polytope. Just as for linear programming, that is, linear optimization on polytopes, there is rich theory and practice of solving linear optimization problems on spectrahedra, known as *semidefinite programming* (see e.g. [22]). In particular, the semidefinite feasibility problem can be solved by interior point methods (see e.g. [5, 6]). This can be done by embedding (6)-(7) into a larger semidefinite programming problem that is strictly feasible (has positive definite feasible solutions) and is its own dual problem (i.e. is self-dual). Thus the so-called *central path* of the embedding problem exists, and interior point methods 'follow' the central path approximately to reach the optimal set of the embedding problem. An optimal solution of the embedding problem tells us whether (6)-(7) has a solution or not. Moreover, if $\mathcal{T}(A_1, \ldots, A_K, c) \neq \emptyset$, the limit point of the central path of the embedding problem yields a solution in the relative interior of $\mathcal{T}(A_1, \ldots, A_K, c)$. The only difficulty is that the limit point of the central path can only be approximated to within ϵ-accuracy in time polynomial in k, K and $\log(1/\epsilon)$ for each $\epsilon > 0$, and it is not known if it can be computed exactly (in the real number model); for a detailed discussion of these issues, see [5, 6].

For future reference, we summarize the above as follows.

Lemma 1. There is an iterative algorithm that either produces iterates that converge to an $X \in \mathrm{ri}(\mathcal{T})$, where $\mathcal{T} = \mathcal{T}(A_1, \ldots, A_K, c)$, or certifies that $\mathcal{T} = \emptyset$.

We shall need a slight extension of (6)-(7), where c is not fixed, but rather given by an affine linear map C from $\mathbb{R}^{L'} \times \mathbb{R}^L_+$ to $\mathbb{R}^K$, so that

$$c_i = d_i + C_i^T y + C'^T_i y', \quad y \in \mathbb{R}^L_+, \quad y' \in \mathbb{R}^{L'}, \quad d_i \in \mathbb{R}. \tag{8}$$

First of all, there is no loss in generality in assuming $L' = 0$, as any y' in (8) can be written as $y' = y^+ - y^-$, with $y^+ \geq 0$ and $y^- \geq 0$, and adjusting C_i accordingly (there are other ways of dealing with y' that require less extra dimensions added). Now we have to consider just

$$c_i = d_i + C_i^T y, \quad y \in \mathbb{R}_+^L, \quad d_i \in \mathbb{R}. \tag{9}$$

It is well-known that this problem can be converted into (6)-(7) by adding L diagonal 1×1 blocks to X. Namely, one replaces X by $X \oplus \mathrm{diag}(y_1, \ldots, y_L)$, c_i by d_i and A_i by $A_i \oplus \mathrm{diag}(-C_i)$, where $\oplus$ is the operation that constructs the matrix

$$A \oplus B = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

from matrices A and B, and constraints ensuring that the extra off-diagonal entries of X are 0.

2.2 Forms

We introduce the following standard notation for writing multivariate polynomials. We write $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$. The vector space of n-ary f forms of degree d is denoted $H_d(\mathbb{R}^n)$. In what follows we restrict ourselves to polynomials with coefficients in $\mathbb{R}$ and write $H_d(n)$ instead of $H_d(\mathbb{R}^n)$.

An $f \in H_d(n)$ can be written as

$$f(x) = \sum_{||\alpha||_1 = d, \alpha \in \mathbb{Z}_+^n} a_\alpha x^\alpha. \tag{10}$$

with $a = (a_{\alpha_1} \ldots a_{\alpha_N}) =\in \mathbb{R}^N$ being the N-tuple of coefficients of f. Note that $N = \binom{n+d-1}{n-1}$. The *Newton polytope* of f is the convex closure $C(f) = \mathrm{Conv}(\alpha_1, \ldots, \alpha_N)$.

Further, one easily checks that for $f = \sum_\alpha a_\alpha x^\alpha \in H_d(n)$ and $g = \sum_\beta b_\beta x^\beta \in H_{d'}(n)$, the product as given as follows.

$$fg = \sum_{\gamma \in \mathbb{Z}_+^n} \left(\sum_{\gamma = \alpha + \beta} a_\alpha b_\beta \right) x^\gamma. \tag{11}$$

That is, coefficients c_γ of fg are as follows.

$$c_\gamma = \sum_{\substack{\gamma = \alpha + \beta; ||\alpha||_1 = d, ||\beta||_1 = d' \\ \alpha, \beta \in \mathbb{Z}_+^n}} a_\alpha b_\beta. \tag{12}$$

By definition, a form $f \in H_d(n)$ is p.s.d. if $f(x) \geq 0$ for all $x \in \mathbb{R}^n$. Note that $d = 2m$ is necessarily even here, unless $f = 0$. Then, f is s.o.s. of forms (we will simply write s.o.s. in what follows) if

$$f = \sum_{j=1}^{M} h_j^2, \quad \text{for } h_j \in H_m(n), \quad M < \infty. \tag{13}$$

If f is s.o.s. then f is p.s.d., but the converse only holds for $(n, m) = (2, m)$, $(n, m) = (n, 1)$ and $(n, m) = (3, 2)$.

Let $h_j = \sum_\beta u_\beta^{(j)} x^\beta$ for h_j in (13), and let

$$U_\beta = \left(u_\beta^{(1)}, \ldots, u_\beta^{(M)}\right)^T \in \mathbb{R}^M. \tag{14}$$

Then

$$f = \sum_{j=1}^{M} (\sum_\beta u_\beta^{(j)} x^\beta)(\sum_{\beta'} u_{\beta'}^{(j)} x^{\beta'}) = \sum_{\beta,\beta'} (U_\beta^T U_{\beta'}) x^{\beta+\beta'}. \tag{15}$$

The equation (16) shows U and the corresponding monomials involved in the decomposition (4) for $f = M(x, y, z)(x^2+y^2+z^2)$, where M is defined in (2).

$$U = \begin{pmatrix} 0 & 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -2 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \qquad C(h_j) \cap \mathbb{Z}^3 = \begin{Bmatrix} (0,0,4) \\ (0,1,3) \\ (1,0,3) \\ (1,1,2) \\ (1,2,1) \\ (1,3,0) \\ (2,1,1) \\ (2,2,0) \\ (3,1,0) \end{Bmatrix} \tag{16}$$

Comparing coefficients a_α of f at both sides of (15), one gets

$$a_\alpha = \sum_{\beta+\beta'=\alpha} U_\beta^T U_{\beta'}.$$

This observation reduces testing whether f is s.o.s. to checking feasibility of the LMI, where $G = UU^T$,

$$\begin{aligned} a_\alpha &= \sum_{\beta+\beta'=\alpha} G_{\beta\beta'} \quad \text{for } \alpha \in \mathbb{Z}_+^n, \quad ||\alpha||_1 = d \\ G &\succeq 0. \end{aligned} \tag{17}$$

This is called *Gram matrix method* in [4, 20]. In particular, one sees that, $M \leq \dim H_m(n) = \binom{n+m-1}{n-1}$ in (13), as $G \in H_m(n)$. Obviously, M equals the rank of G obtained from (17).

Further refinements to this can be found, for instance in [20]. E.g., as the Newton polytopes $C(h_j)$ of the forms h_j from (13) must be contained in $\frac{1}{2}C(f)$, not all the monomials from $H_m(n)$ are allowed in h_j's. For instance, for $f = M(x,y,z)(x^2+y^2+z^2)$ only the 9 monomials on the righthand side of (16) are allowed, and $G \in H_{m'}(n)$ with $m' < m$.

3 LMIs and products of forms

As we already mentioned, a p.s.d. f need not be a s.o.s. One can try to find $g = \sum_\mu b_\mu x^\beta \in H_{m'}(n)$, for $m' < m$, such that the product fg is a s.o.s., and $f = (\sum_j h_j^2)/g$. The former is easy to accomplish by plugging (12) into (17).

$$\sum_{\alpha+\mu=\gamma} a_\alpha b_\mu = \sum_{\beta+\beta'=\gamma} G_{\beta\beta'} \quad \text{for } \gamma \in \mathbb{Z}_+^n, \quad ||\gamma||_1 = 2(m+m') \tag{18}$$

$$G \succeq 0. \tag{19}$$

Obviously, this is an LMI of the form (6)-(8). Not always a solution (g,G) of (18)-(19) would satisfy the second requirement, that $f = (\sum_j h_j^2)/g$. Indeed, $(0,G)$ is always a trivial solution of (18)-(19). More precisely, to satisfy $f = (\sum_j h_j^2)/g$, one needs to ensure that the set of real roots $V_{\mathbb{R}}(g)$ of g is contained in $V_{\mathbb{R}}(f)$. However, noting that the solutions (g,G) to (18)-(19) form a convex set, and observing that all g appearing in solutions (g,G) are p.s.d., one sees that $V_{\mathbb{R}}((g+g')/2) = V_{\mathbb{R}}(g) \cap V_{\mathbb{R}}(g')$. That means that a "generic" solution (g,G) has $V_{\mathbb{R}}(g)$ as small as possible. This is made precise in Lemma 3 below.

Finally, we should make sure that g obtained from (18)-(19) is p.s.d.. This will always be the case as long as f and fg are not identically 0 and p.s.d.. Indeed, assume $g(x^*) = g_0 < 0$ for some x^*. Then $f(x^*) = 0$. Applying a nondegenerate linear transformation, one can assume that $x^* = e_1$. This means that g has a term $x^{\deg g}$ with negative coefficient, and thus for any x there exists $\mu_0 > 0$ such that $g(y) < 0$ for $y = x - (\mu - x_1)e_1$ and any $\mu \geq \mu_0$. Hence f vanishes on every such y, clearly a nonsense. To summarize, we have proved the following.

Lemma 2. Let (g,G) be a solution of (18)-(19) for a p.s.d. form $f = \sum_\alpha a_\alpha x^\alpha \in H_d(n)$. Then g is p.s.d. If g satisfies $V_{\mathbb{R}}(g) \subseteq V_{\mathbb{R}}(f)$ then $f = (\sum_j h_j^2)/g$, with the coefficients $u^{(j)}$ of h_j obtained from $G = UU^T$ using (14).

If g^* corresponds to a solution (g^*, G^*) in the relative interior of the feasible set of (18)-(19), then $V_{\mathbb{R}}(g^*) \subseteq V_{\mathbb{R}}(g)$ for *any* solution (g, G) of (18)-(19). (Recall that the iterates of a suitable interior point algorithm converge to a solution in the relative interior.)

Lemma 3. Let $\mathcal{T}$ be the feasibility set of (18)-(19) and let $(g, G) \in \mathrm{ri}(\mathcal{T})$ and $(g', G') \in \mathcal{T}$. Then $V_{\mathbb{R}}(g) \subseteq V_{\mathbb{R}}(g')$. Furthermore, if $(g', G') \in \mathrm{ri}(\mathcal{T})$ then $V_{\mathbb{R}}(g) = V_{\mathbb{R}}(g')$.

Proof. Let $(g'', G'') = \frac{1}{2}(g, G) + \frac{1}{2}(g', G'')$. Then $(g'', G'') \in \mathcal{T}$ and $V_{\mathbb{R}}(g'') = V_{\mathbb{R}}(g) \cap V_{\mathbb{R}}(g')$. On the other hand, by definition of the relative interior, there exists $0 < \epsilon < 1$ such that $\epsilon(g'', G'') + (1-\epsilon)(g, G) \in \mathcal{T}$. Thus $V_{\mathbb{R}}(g) \subseteq V_{\mathbb{R}}(g'')$. By a similar argument, $V_{\mathbb{R}}(g') \subseteq V_{\mathbb{R}}(g'')$ when also $(g', G') \in \mathrm{ri}(\mathcal{T})$. Hence the lemma. □

To complete the proof of Theorem 2, we use the following result of Hilbert.

Theorem 3. (Hilbert [8], cf. [20].) Let $p \in H_{2m}(3)$ be p.s.d., $m \geq 3$. Then there exists $p_1 \in H_{2m-4}(3)$ such that $p = (\sum_{j=1}^{N} h_j^2)/p_1$ for $N = 3$ and some $h_j \in H_{2m-2}(3)$, $j = 1, 2, 3$.

We will not use the $N = 3$ part of Hilbert's result. As observed above, without assuming $N = 3$, the corresponding p_1 and h_j can be computed using an interior point method for SDP on the system of LMIs (18)-(19). This completes the proof of Theorem 2.

To summarize, we state our algorithm concisely (Algorithm 1).

4 Discussion

The main result of the paper gives an algorithm to find a decomposition of a p.s.d. ternary form of degree $2m$ into a s.o.s. of rational functions with degrees of denominators bounded from above by $O(m^2)$. For a given p.s.d. ternary form p of degree $2m$, the algorithm requires the solution of at most $m/4$ systems of LMI's of dimensions polynomial in m.

The $O(m^2)$ bound for the degrees of the denominators appears to be close to being the best possible.

The number of terms in (1) is however far from optimal, for Hilbert [8] has shown that $N = 4$ terms suffice. The obstacle here lies probably in (18)-(19), as the number of terms in the intermediate s.o.s. obtained equals the rank of G; if $p(x) > 0$ for all $x \in \mathbb{R}^3$ then G can be of full rank. Reducing the number of terms in the decomposition remains a topic for future research.

Algorithm 1 Computing s.o.s. of rational functions decomposition of p

INPUT: a ternary form p
$i := 1$; $p_1 := p$
while $\deg p_i > 4$ **do**
  compute g of degree $\deg p_i - 4$ such that $p_i g$ is s.o.s. and $V_{\mathbb{R}}(g)$ is minimal by solving the LMI's (18)-(19).
  if $g = 0$ **then**
    STOP — p is not p.s.d.
  end if
  $p_{i+1} := g$; $Q_i := p_{i+1} p_i$.
  $i \leftarrow i + 1$
end while
compute $f :=$ (resp. $1/f :=$) s.o.s.(p_i).
OUTPUT: p given by (5).

Another intriguing question is when, for a given n-ary p.s.d. form p, there exists a form p_1, $\deg p_1 < \deg p$, such that p admits a decomposition as in (3). This cannot be the case for *all* n, unless P = NP.

A last remark concerns the complexity of our algorithm. A practical (polynomial-time) implementation of the algorithm would use ϵ-approximations of a relatively interior solution of the system of LMI's (18)-(19), instead of an exact solution in the relative interior. Such a polynomial-time implementation can probably still detect nonnegativity of positive definite ternary forms (i.e. ternary forms positive on the unit sphere in $\mathbb{R}^n$). In this case one would choose ϵ as a function of the minimum value of the form on the unit sphere. It is of practical interest to prove rigorous results along these lines.

References

[1] E. Artin. *The collected papers of Emil Artin.* Addison–Wesley Publishing Co., Inc., Reading, Mass.-London, 1965.

[2] L. Blum, M. Shub, and S. Smale. On a theory of computation and complexity over the real numbers: NP-completeness, recursive functions and universal machines. *Bull. Amer. Math. Soc. (N.S.)*, 21(1):1–46, 1989.

[3] M. D. Choi and T. Y. Lam. Extremal positive semidefinite forms. *Math. Ann.*, 231(1):1–18, 1977/78.

[4] M. D. Choi, T. Y. Lam, and B. Reznick. Sums of squares of real polynomials. In *K-theory and algebraic geometry: connections with quadratic forms and division algebras (Santa Barbara, CA, 1992)*, pages 103–126. Amer. Math. Soc., Providence, RI, 1995.

[5] E. de Klerk, C. Roos, and T. Terlaky. Initialization in semidefinite programming via a self–dual, skew–symmetric embedding. *OR Letters*, 20:213–221, 1997.

[6] E. de Klerk, C. Roos, and T. Terlaky. Infeasible–start semidefinite programming algorithms via self–dual embeddings. In P. M. Pardalos and H. Wolkowicz, editors, *Topics in Semidefinite and Interior-Point Methods*, volume 18 of *Fields Institute Communications Series*, pages 215–236. American Mathematical Society, 1998.

[7] D. Hilbert. Über die darstellung definiter formen als summe von formenquadraten. *Math. Ann.*, 32:342–350, 1888.

[8] D. Hilbert. Über ternäre definite Formen. *Acta Math.*, 17:169–197, 1893.

[9] D. Hilbert. Mathematical problems. *Bull. Amer. Math. Soc. (N.S.)*, 37(4):407–436 (electronic), 2000. Reprinted from Bull. Amer. Math. Soc. **8** (1902), 437–479.

[10] T. S. Motzkin. The arithmetic-geometric inequality. In *Inequalities (Proc. Sympos. Wright-Patterson Air Force Base, Ohio, 1965)*, pages 205–224. Academic Press, New York, 1967.

[11] P. A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. Technical report, CalTech, 2001. submitted, available at `http://www.cds.caltech.edu/~pablo/pubs/SDPrelaxations.ps`.

[12] L. Porkolab and L. Khachiyan. On the complexity of semidefinite programs. *J. Global Optim.*, 10(4):351–365, 1997.

[13] V. Powers and B. Reznick. A new bound for Pólya's Theorem with applications to polynomials positive on polyhedra. *J. Pure Appl. Alg.*, to appear. available online at `http://www.math.uiuc.edu/~reznick/11200.pdf`.

[14] A. Prestel and C. N. Delzell. *Positive polynomials.* Springer-Verlag, Berlin, 2001. From Hilbert's 17th problem to real algebra.

[15] A. R. Rajwade. *Squares.* Cambridge University Press, Cambridge, 1993.

[16] M. V. Ramana. An exact duality theory for semidefinite programming and its complexity implications. *Math. Programming*, 77(2, Ser. B):129–162, 1997.

[17] M. V. Ramana and P. M. Pardalos. Semidefinite programming. In *Interior point methods of mathematical programming*, pages 369–398. Kluwer Acad. Publ., Dordrecht, 1996.

[18] B. Reznick. Sums of even powers of real linear forms. *Mem. Amer. Math. Soc.*, 96(463):viii+155, 1992.

[19] B. Reznick. Uniform denominators in Hilbert's seventeenth problem. *Math. Z.*, 220(1):75–97, 1995.

[20] B. Reznick. Some concrete aspects of Hilbert's 17th Problem. In *Real algebraic geometry and ordered structures (Baton Rouge, LA, 1996)*, pages 251–272. Amer. Math. Soc., Providence, RI, 2000.

[21] R. Rockafellar. *Convex analysis.* Princeton University Press, Princeton, New Jersey, 1970.

[22] H. Wolkowicz, R. Saigal, and L. Vandenberghe, editors. *Handbook of semidefinite programming.* Kluwer Academic Publishers, Norwell, MA, 2000.