Certificates of Impossibility of Hilbert-Artin Representations of a Given Degree for Definite Polynomials and Functions*

Feng Guo
Key Laboratory of Mathematics Mechanization, AMSS
Beijing 100190, China
fguo@mmrc.iss.ac.cn

Erich L. Kaltofen
Dept. of Mathematics, NCSU
Raleigh, North Carolina
27695-8205, USA
kaltofen@math.ncsu.edu
http://www.kaltofen.us

Lihong Zhi
Key Laboratory of Mathematics Mechanization, AMSS
Beijing 100190, China
lzhi@mmrc.iss.ac.cn
http://www.mmrc.iss.ac.cn/~lzhi/

ABSTRACT

We deploy numerical semidefinite programming and conversion to exact rational inequalities to certify that for a positive semidefinite input polynomial or rational function, any representation as a fraction of sums-of-squares of polynomials with real coefficients must contain polynomials in the denominator of degree no less than a given input lower bound. By Artin's solution to Hilbert's 17th problems, such representations always exist for some denominator degree. Our certificates of infeasibility are based on the generalization of Farkas's Lemma to semidefinite programming.

The literature has many famous examples of impossibility of SOS representability including Motzkin's, Robinson's, Choi's and Lam's polynomials, and Reznick's lower degree bounds on uniform denominators, e.g., powers of the sum-of-squares of each variable. Our work on exact certificates for positive semidefiniteness allows for non-uniform denominators, which can have lower degree and are often easier to convert to exact identities. Here we demonstrate our algorithm by computing certificates of impossibilities for an arbitrary sum-of-squares denominator of degree 2 and 4 for some symmetric sextics in 4 and 5 variables, respectively. We can also certify impossibility of base polynomials in the denominator of restricted term structure, for instance as in Landau's reduction by one less variable.

Categories and Subject Descriptors: I.1.2 [Symbolic and Algebraic Manipulation]: Algorithms; G.1.6 [Numerical Analysis]: Global optimization

General Terms: algorithms, experimentation

*This material is based on work supported in part by the National Science Foundation under Grants CCF-0830347 and CCF-1115772 (Kaltofen), and by NCSU as host for Guo's Study Abroad Program. Guo and Zhi are supported by NKBRPC 2011CB302400 and the Chinese National Natural Science Foundation under Grants 91118001, 60821002/F02, 60911130369 and 10871194.

ISSAC'12, July 22–25, 2012, Grenoble, France.

Keywords: certificates of infeasibility of semidefinite programs, sum-of-squares denominators in Artin's Theorem for definite polynomials, Farkas Lemma in semidefinite programming, exact solution to semidefinite programs

1. INTRODUCTION

The Farkas Lemma of linear programming can be employed to construct certificates of infeasibility, in its simplest form of an inconsistent system of linear equations [8], in linear programming of a system of linear inequalities, and in semidefinite programming of a system of linear equations with semidefiniteness constraints on the solution. A polynomial is not a sum-of-squares of polynomials (SOS) if the corresponding semidefinite program is infeasible. Thus the Farkas Lemma produces a certificate that a polynomial is not an SOS, the separating hyperplane [1].

Motivated by our SOS certificates for global optima of polynomials and rational functions [13, 15, 16] (see also [10, 21, 22] for earlier work), we extend those impossibility certificates to Hilbert-Artin representations of a given denominator degree: by Emil Artin's Theorem [3], every real positive semidefinite rational function is a fraction of two sums-of-squares of polynomials. We write for an $f(X_1,\ldots,X_n) \in K(X_1,\ldots,X_n)$, where K is a subfield of the real numbers,

$$f \succeq 0 \quad \text{if} \quad \forall \xi_1,\ldots,\xi_n \in \mathbb{R}\colon f(\xi_1,\ldots,\xi_n) \not< 0.$$

Note that at a real root of the denominator of f its value is undefined, hence $\not< 0$. Artin's original theorem stipulates that

$$\forall f \succeq 0\colon \exists u_1,\ldots,u_l, w \in K[X_1,\ldots,X_n]\colon f = \frac{1}{w^2}\sum_{i=1}^{l} u_i^2. \quad (1)$$

If f is a polynomial $\in K[X_1,\ldots,X_n]$, one may eliminate one variable from the denominator w, that is, construct from (1) a representation with $w_{\text{new}} \in K[X_1,\ldots,X_{n-1}]$, which Artin in his 1927 paper attributes to Edmund Landau. The reduction can be accomplished with the same number of $l_{\text{new}} = l$ squares, which in [25] is attributed to J. W. S. Cassels. In both constructions the degree of w_{new} is substantially larger than that of w. As is customary, if a positive semidefinite polynomial f allows a representation (1) with $w = 1$, we shall call f a *sum-of-squares* (SOS). In general, however, as already David Hilbert has shown in 1888 [11], positive semidefinite polynomials are not SOS (see also [4, 5]).

In order to minimize the numerator and denominator degrees, we seek

$$u_1,\ldots,u_l,v_1,\ldots,v_{l'} \in \mathbb{R}[X_1,\ldots,X_n] \text{ s. t. } f = \frac{\sum_{i=1}^{l} u_i^2}{\sum_{j=1}^{l'} v_j^2}. \quad (2)$$

We shall call (2) a *Hilbert-Artin representation* of f, which constitutes an SOS proof for $f \succeq 0$. By allowing an SOS as the denominator polynomial, one then can construct such proofs with a possibly smaller degree than the common denominator w^2 in (1). For instance, for the Motzkin polynomial $\max_j\{\deg(v_j)\} \le 1$ suffices in (2), but $\deg(w) \le 1$ is impossible in (1) [16, Section 1].

It is not known if minimal degree denominator SOSes can always have coefficients in K, as is the case in Artin's original theorem (1). A special case is when f is an SOS of polynomials ($w = 1$), and the existence of u_i with all coefficients in K for all i is conjectured (Sturmfels; cf. [12, 14, 24, 29]). Our method can certify "absolute" impossibility by SOSes, that is, for coefficients from all possible subfields of $\mathbb{R}$. Our certificates are rational, that is, they have their scalars in $\mathbb{Q}$. The problem of whether there exists a representation of a given degree with coefficients in $\mathbb{Q}$ appears to be decidable [28].

As in [16], we compute our certificates, the separating hyperplanes in Farkas's Lemma, by first computing a numerical approximation using a numerical semidefinite program solver and then converting the numerical scalars to exact rational numbers. For ill-posed polynomials (see Example 5.4 below), high-accuracy semidefinite program solver [9] is needed. The separating hyperplane is the strictly feasible solution to a semidefinite program whose objective function tends to $-\infty$. We compute such a strictly feasible solution by the Big-M method [31]. The semidefinite programs in [1] and ours certify infeasibility of SOSes, which has been generalized to infeasibility of arbitrary linear matrix inequalities [17].

We have tested our method on polynomials from the literature. In particular, we show that the SOS proofs of positive semidefiniteness in [15] indeed require denominators for three polynomials. The *ArtinProver* program [16] successfully introduced denominators not only for purpose of handling inequalities that do not allow a polynomial SOS proof, but also for avoiding possible non-rational SOSes, to which the semidefinite program solvers may have converged in the case where the Gram matrix is intrinsically rank deficient (our "hard case" [16]). Our impossibility certificates show that for the proof of the Monotone Column Permanent conjecture in dimension 4, actually the former is the case.

A final problem is to explicitly construct a positive semidefinite polynomial for which the Hilbert-Artin representation (2) must have $\deg(\sum_j v_j^2) \ge 4$. Bruce Reznick in 2009 has kindly provided us with the challenges raised in [6, Section 7]: how large must r be such that the even symmetric sextics in n variables multiplied by uniform denominators, i.e., $(x_1^2 + \cdots + x_n^2)^r f_{n,k}$ (see Example 5.3 below), are SOS? In [6] it is proven that for $f_{4,2}$ one has $r = 2$. We can compute certificates that show that for $f_{4,2}$, $f_{5,2}$, $f_{6,2}$, the degree lower bound ≥ 4 and for $f_{5,3}$, $f_{6,4}$, the lower bound ≥ 6 even hold for *any* denominator $\sum_j v_j^2$ in (2).

Notation: Throughout this paper, $\mathbb{N}$ denotes the set of nonnegative integers and we set $\mathbb{N}_t^n = \{\alpha \in \mathbb{N}^n \mid |\alpha| = \sum_{i=1}^n \alpha_i \le t\}$ for $t \in \mathbb{N}$. $\mathbb{R}[X] = \mathbb{R}[X_1,\ldots,X_n]$ denotes the ring of polynomials in variables $X = (X_1,\ldots,X_n)$ with real coefficients. Given a polynomial $f = \sum_\alpha f_\alpha X_1^{\alpha_1}\ldots X_n^{\alpha_n} \in \mathbb{R}[X]$, let $\operatorname{supp}(f) = \{X_1^{\alpha_1}\ldots X_n^{\alpha_n} \mid c_\alpha \ne 0\}$, i.e., the set of the support terms of f. Denote by $\deg(f)$ the total degree of f. Given $n \ge 1$ and $e \ge 0$, let $\mathrm{Terms}[X;\deg{\le}e] = \{X_1^{e_1}\ldots X_n^{e_n} \mid \sum_{i=1}^n e_i \le e\}$, i.e., the set of all terms of total degree $\le e$ in the n variables X. For a given subset $\mathcal{T} \subseteq \mathrm{Terms}[X;\deg{\le}e]$, we introduce the following notation for a term-restricted SOS, $\mathrm{SOS}_\mathcal{T} = \{\sum v_j^2 \mid v_j \in \mathbb{R}[X], \operatorname{supp}(v_j) \subseteq \mathcal{T}\}$, and the following notation for a denominator term-restricted Hilbert-Artin representation,

$$\mathrm{SOS}/\mathrm{SOS}_\mathcal{T} = \Big\{ \sum u_i^2 \Big/ \sum v_j^2 \;\Big|\; u_i, v_j \in \mathbb{R}[X], \; \forall j\colon \operatorname{supp}(v_j) \subseteq \mathcal{T} \Big\}.$$

Finally, we write the shorthand

$$\mathrm{SOS}/\mathrm{SOS}_{\deg\le 2e} = \mathrm{SOS}/\mathrm{SOS}_{\mathrm{Terms}[X;\deg\le e]}.$$

By $\mathbb{SR}^{k\times k}$ we denote the subspace of real symmetric $k \times k$ matrices. For a matrix $W \in \mathbb{SR}^{k\times k}$, $W \succeq 0$ means W is positive semidefinite. The bold number zero $\mathbf{0}$ denotes the zero matrix, and I denotes the identity matrix.

2. HILBERT-ARTIN REPRESENTATION OF POSITIVE SEMIDEFINITE POLYNOMIALS

2.1 Rational Function Sum-of-Squares and Semidefinite Programming

For a given subset $\mathcal{T} \subseteq \mathrm{Terms}[X;\deg{\le}e]$, note that $f \in \mathrm{SOS}/\mathrm{SOS}_\mathcal{T}$ if and only if

$$0 = \sum_i^l u_i(X)^2 + (-f)\sum_j^{l'} v_j(X)^2,$$

for some polynomials $u_i(X), v_j(X) \in \mathbb{R}[X]$ with $\operatorname{supp}(v_j) \in \mathcal{T}$. Consider the following set:

$$\Big\{[W^{[1]}, W^{[2]}] \;\Big|\; m_{\mathrm{Terms}[X;\deg\le d]}{}^T W^{[1]} m_{\mathrm{Terms}[X;\deg\le d]} = f(X)\cdot(m_\mathcal{T}{}^T W^{[2]} m_\mathcal{T}), \; W^{[1]}\succeq 0,\; W^{[2]}\succeq 0,\; \mathrm{Trace}(W^{[2]})=1\Big\}, \quad (3)$$

where $m_\mathcal{T}$ and $m_{\mathrm{Terms}[X;\deg\le d]}$ denote the column vectors which consist of the elements in $\mathcal{T}$ and $\mathrm{Terms}[X;\deg{\le}d]$, respectively. Here and hereafter, we let $d = \lceil e + \deg(f)/2 \rceil$, and therefore,

$$\Big\{X^{\alpha+\beta} \mid X^\alpha, X^\beta \in \mathrm{Terms}[X;\deg{\le}d]\Big\} \supseteq \Big\{X^{\alpha+\beta+\gamma} \mid X^\gamma \in \operatorname{supp}(f), X^\alpha, X^\beta \in \mathcal{T}\Big\}.$$

The last constraint $\mathrm{Tr}(W^{[2]}) = 1$ is added to enforce that $W^{[2]} \ne \mathbf{0}$.

Proposition 2.1. *We have $f \notin \mathrm{SOS}/\mathrm{SOS}_\mathcal{T}$ if and only if the set (3) is empty.*

Now we review the following standard *Semidefinite Program* (SDP) (see [31]),

$$\begin{array}{llll} \sup\limits_{W\in\mathbb{SR}^{k\times k}} & -C\bullet W & \inf\limits_{y\in\mathbb{R}^l} & b^T y \\ s.t. & A_i\bullet W=b_i, & s.t. & C+\sum_{i=1}^l y_iA_i\succeq 0. \\ & i=1\cdots l, & & \\ & W\succeq 0. & & \end{array} \quad (4)$$

For symmetric matrices C, W, the scalar product in $\mathbb{R}^{n\times n}$ space is defined as

$$C\bullet W=\langle C,W\rangle=\sum_{i=1}^{n}\sum_{j=1}^{n}c_{i,j}w_{i,j}=\mathrm{Tr}CW.$$

Let

$$m_{\mathrm{Terms}[X;\deg\le d]}{}^T W^{[1]} m_{\mathrm{Terms}[X;\deg\le d]}=\sum_{\alpha}(G^{[\alpha]}\bullet W^{[1]})X^{\alpha},$$

where $G^{[\alpha]}$ are scalar symmetric matrices and X^{α} are all possible terms appearing in the polynomial of degree $\le 2d$. Similarly, let

$$(-f(X))\cdot m_{\mathcal{T}}{}^T W^{[2]} m_{\mathcal{T}}=\sum_{\beta}(H^{[\beta]}\bullet W^{[2]})X^{\beta},$$

where $H^{[\beta]}$ are symmetric matrices and X^{β} are all possible terms appearing in the product of $(-f(X))$ with a polynomial of degree $\le 2e$. Now we consider the following block SDP:

$$\begin{array}{ll} \sup\limits_{W\in\mathbb{SR}^{k\times k}} & -C\bullet W \\ s.t. & \begin{bmatrix} \vdots \\ A^{[\alpha]}\bullet W \\ \vdots \\ A\bullet W \end{bmatrix} = \begin{bmatrix} \vdots \\ 0 \\ \vdots \\ 1 \end{bmatrix}, \quad W\succeq 0. \end{array} \quad (5)$$

where $k=\binom{n+d}{d}+\binom{n+e}{e}$,

$$\begin{array}{l} C:=\begin{bmatrix} \mathbf{0} & \\ & \mathbf{0} \end{bmatrix},\quad W:=\begin{bmatrix} W^{[1]} & * \\ * & W^{[2]} \end{bmatrix}, \\ A^{[\alpha]}:=\begin{bmatrix} G^{[\alpha]} & \\ & H^{[\alpha]} \end{bmatrix},\quad A:=\begin{bmatrix} \mathbf{0} & \\ & I \end{bmatrix} \end{array} \quad (6)$$

and α ranges over $\mathbb{N}^n_{2d}$. The matrix C can be chosen as a random symmetric matrix. We set it to be a zero matrix only for the convenience of discussions below (see Proposition 3.2). For all block positive semidefinite matrices appearing in the present paper, we use the symbol $*$ to indicate that the associated elements could be any real numbers such that the whole matrices are still positive semidefinite and leave some positions blank to indicate that the associated blocks are zero matrices.

Proposition 2.2. *We have $f\notin \mathrm{SOS}/\mathrm{SOS}_{\mathcal{T}}$ if and only if SDP (5) is infeasible.*

2.2 Dual Problem and Certification

Before we consider the dual problem of (5), let us review some definitions about moment matrices and localizing moment matrices. Given a sequence $y=(y_\alpha)_{\alpha\in\mathbb{N}^n}\in\mathbb{R}^{\mathbb{N}^n}$, its *moment matrix* is the (infinite) real symmetric matrix $M(y)$ indexed by $\mathbb{N}^n$, with (α,β)th entry $y_{\alpha+\beta}$, for $\alpha,\beta\in\mathbb{N}^n$. Given an integer $t\ge 1$ and a truncated sequence $y=(y_\alpha)_{\alpha\in\mathbb{N}^n_{2t}}\in\mathbb{R}^{\mathbb{N}^n_{2t}}$, its *moment matrix of order* t is the matrix $M_t(y)$ with (α,β)th entry $y_{\alpha+\beta}$, for $\alpha,\beta\in\mathbb{N}^n_t$. For a given polynomial $q\in\mathbb{R}[X]$, if the (i,j)th entry of $M_t(y)$ is y_β, then the tth *localizing moment matrix* of q is defined by

$$M_t(qy)(i,j):=\sum_{\alpha}q_\alpha y_{\alpha+\beta}.$$

More details about moment matrices, see [18, 19, 20].

According to (4), the dual problem of (5) is

$$\begin{array}{ll} s^*:=\inf\limits_{(y,s)\in\mathbb{R}^{m+1}} & s \\ & s.t.\ M(y,s)\succeq 0, \end{array} \quad (7)$$

where

$$M(y,s):=\begin{bmatrix} M_d(y) & \\ & M_e((-f)y)+sI \end{bmatrix}, \quad (8)$$

$y:=(y_\alpha)_{\alpha\in\mathbb{N}^n_{2d}}\in\mathbb{R}^{\mathbb{N}^n_{2d}}$ and $m=\binom{n+2d}{2d}$, $M_d(y)$ is a truncated moment matrix of order d and $M_e((-f)y)$ is the eth localizing moment matrix.

The next lemma shows that the problem (7) is strictly feasible. The proof is similar to the one given in [18, Proposition 3.1].

Lemma 2.3. *There exists $(\tilde y,\tilde s)\in\mathbb{R}^{m+1}$ such that $M_d(\tilde y)\succ 0$ and $M_e(-f\tilde y)+\tilde sI\succ 0$.*

Proof. Let μ be a probability measure on $\mathbb{R}^n$ with a *strictly positive* density h with respect to Lebesgue measure such that

$$\tilde y_\alpha:=\int X^\alpha d\mu<\infty.$$

For any $q(X)\in\mathbb{R}[X]$ with $\mathrm{supp}(q)\in \mathrm{Terms}[X;\deg\le d]$, let $\mathrm{vec}(q)$ denote its sequence of coefficients in the monomial basis $\mathrm{Terms}[X;\deg\le d]$. We have

$$\begin{aligned}\langle \mathrm{vec}(q)^T, M_d(\tilde y)\mathrm{vec}(q)\rangle &= \int q(x)^2\mu(dx)\\ &=\int q(x)^2 h(x)dx\\ &>0 \text{ whenever } q\neq 0,\end{aligned}$$

which implies $M_d(\tilde y)\succ 0$. Take $\tilde s>-\lambda_{\min}(M_e((-f)\tilde y))$, then $M_e(-f\tilde y)+\tilde sI\succ 0$. $\square$

For standard SDPs in (4), we have the following important duality fact.

Lemma 2.4. [2, Lemma 2.3; Semidefinite Farkas Lemma] *Let $A_i\in\mathbb{SR}^{k\times k}$ for all $i=1,\ldots,l$ and let $b\in\mathbb{R}^l$. Suppose there exists a vector $y\in\mathbb{R}^l$ such that $\sum_{i=1}^l y_iA_i\succ 0$. Then exactly one of the following is true:*

1. *There exists a positive semidefinite symmetric matrix $W\in\mathbb{SR}^{k\times k}$, $W\succeq 0$, such that $A_i\bullet W=b_i$ for all $i=1,\ldots,l$;*
2. *There exists a vector $\hat y\in\mathbb{R}^l$ such that $\sum_{i=1}^l \hat y_iA_i\succeq 0$ and $b^T\hat y<0$.*

We call the vector $\hat y$ *Farkas's certificate vector of infeasibility.* For other forms of the Farkas Lemma, see [7, Section 4.2].

Note that Lemma 2.3 implies that the assumption in the Farkas Lemma 2.4 is satisfied in SDPs (5) and (7). Then we have our main result:

Theorem 2.5. *Given a polynomial $f \in \mathbb{Q}[X]$ and an integer $e \geq 0$, let $d = \lceil e + \deg(f)/2 \rceil$, then for any subset $\mathcal{T} \subseteq \mathrm{Terms}[X; \deg \leq e]$, the following are equivalent:*

1. $f \notin \mathrm{SOS}/\mathrm{SOS}_{\mathcal{T}}$,
2. *There exists a rational vector $\hat{y} = (\hat{y}_\alpha) \in \mathbb{Q}^m$ with $m = \binom{n+2d}{2d}$ such that $M_d(\hat{y}) \succeq 0$ and $M_e(f\hat{y}) \prec 0$.*

PROOF. By employing the Farkas Lemma 2.4 to SDPs (5) and (7), we have that $f \notin \mathrm{SOS}/\mathrm{SOS}_{\mathcal{T}}$ if and only if there exists $p' = (y', s') \in \mathbb{R}^{m+1}$ for (7) such that $M(y', s') \succeq 0$ and $s' < 0$. Now we prove that p' can be chosen to be rational.

Let $\tilde{p} = (\tilde{y}, \tilde{s})$ be the strictly feasible point constructed in Lemma 2.3. For $0 < t \leq 1$, let $\bar{y} = (1-t)y' + t\tilde{y}$ and $\bar{s} = (1-t)s' + t\tilde{s}$, then $M(\bar{y}, \bar{s}) \succ 0$. Denote $\bar{p} = (\bar{y}, \bar{s})$. Since $s' < 0$, it is always possible to choose a rational number t such that $\bar{s} < 0$. Then there exists $\varepsilon > 0$ such that for all $p = (y, s) \in B_{\bar{p}}(\varepsilon)$ where $B_{\bar{p}}(\varepsilon)$ is a ball with center $\bar{p}$ and radius ε, we have $M(y, s) \succeq 0$. Taking $\varepsilon < \frac{1}{2}|\bar{s}|$, there always exists a point $\hat{p} = (\hat{y}, \hat{s}) \in B_{\bar{p}}(\varepsilon)$ such that $\hat{p} \in \mathbb{Q}^{m+1}$, $M_d(\hat{y}) \succeq 0$, $M_e(-f\hat{y}) + \hat{s}I \succeq 0$ and $\hat{s} < 0$ which implies $M_e(f\hat{y}) \prec 0$. □

2.3 Moment matrices and linear forms on $\mathbb{R}[X]$

In this section, we give an interpretation of our infeasibility certification using linear forms on $\mathbb{R}[X]$.

Given $y \in \mathbb{R}^{\mathbb{N}^n}$, we define the linear form $L_y \in (\mathbb{R}[X])^*$ by

$$L_y(f) := y^T \mathrm{vec}(f) = \sum_\alpha y_\alpha f_\alpha \text{ for } f = \sum_\alpha f_\alpha X^\alpha \in \mathbb{R}[X], \tag{9}$$

where $\mathrm{vec}(f)$ denotes its sequence of coefficients.

Lemma 2.6. [20, Lemma 4.1] *Let $y \in \mathbb{R}^{\mathbb{N}^n}$, $L_y \in (\mathbb{R}[X])^*$ the associated linear form, and let $f, g, h \in \mathbb{R}[X]$.*

1. *$L_y(fg) = vec(f)^T M(y) vec(g)$; in particular, $L_y(f^2) = vec(f)^T M(y) vec(f)$, $L_y(f) = vec(1)^T M(y) vec(f)$.*
2. *$L_y(fgh) = vec(f)^T M(y) vec(gh) = vec(fg)^T M(y) vec(h) = vec(f)^T M(hy) vec(g)$.*

Now we have the following statement which is equivalent to Theorem 2.5:

Theorem 2.7. *Given a polynomial $f \in \mathbb{Q}[X]$ and an integer $e \geq 0$, let $d = \lceil e + \deg(f)/2 \rceil$, then for any subset $\mathcal{T} \subseteq \mathrm{Terms}[X; \deg \leq e]$, the following are equivalent:*

1. $f \notin \mathrm{SOS}/\mathrm{SOS}_{\mathcal{T}}$,
2. *There exists a rational vector $\hat{y} \in \mathbb{Q}^m$ with $m = \binom{n+2d}{2d}$, and the associated linear form $L_{\hat{y}} \in (\mathbb{R}[X]_{2d})^*$ such that for any polynomials $v, u \in \mathbb{R}[X]$ with $supp(v) \in \mathcal{T}$ and $supp(u) \in \mathrm{Terms}[X; \deg \leq d]$, we have $L_{\hat{y}}(fv^2) < 0$ and $L_{\hat{y}}(u^2) \geq 0$.*

PROOF. By (7) and Theorem 2.5, $f \notin \mathrm{SOS}/\mathrm{SOS}_{\mathcal{T}}$ if and only if there exists $\hat{y} \in \mathbb{Q}^m$ such that $M_d(\hat{y}) \succeq 0$ and $M_e(f\hat{y}) \prec 0$. According to Lemma 2.6, the conclusion follows. □

Now one has a better understanding that the existence of a certificate $\hat{y}$ in Theorem 2.5 implies $f \notin \mathrm{SOS}/\mathrm{SOS}_{\mathcal{T}}$. In fact if $f = \sum u_i^2 / \sum v_j^2$ with $\mathrm{supp}(u_i) \in \mathrm{Terms}[X; \deg \leq d]$ and $\mathrm{supp}(v_j) \in \mathcal{T}$, then $0 \leq L_{\hat{y}}(\sum u_i^2) = \sum L_{\hat{y}}(f v_j^2) < 0$ which is a contradiction.

Remark 2.1. One special case is $e = 0$, i.e. we certify that f can not be written as a rational SOS. According to Theorem 2.7, f is not an SOS if and only if there is $\hat{y} \in \mathbb{Q}^m$ and the associated linear form $L_{\hat{y}}$, such that $\forall u \in \mathbb{R}[X]$ with $\mathrm{supp}(u) \in \mathrm{Terms}[X; \deg \leq \lceil \deg(f)/2 \rceil]$, $L_{\hat{y}}(u^2) \geq 0$ and $L_{\hat{y}}(f) < 0$. This special case has also been studied in [1], in which $\hat{y}$ is referred as the *separating hyperplane*.

3. COMPUTATIONAL ASPECTS OF THE CERTIFICATION

3.1 Finding $\hat{y}$ by Big-M method

Given a polynomial $f \in \mathbb{Q}[X]$ and an integer $e \geq 0$, note that $f \notin \mathrm{SOS}/\mathrm{SOS}_{\mathcal{T}}$ if and only if (5) is infeasible. From the proof of Theorem 2.5, we have

Lemma 3.1. *$f \notin \mathrm{SOS}/\mathrm{SOS}_{\mathcal{T}}$ if and only if $s^* = -\infty$ in (7).*

To find a certificate $\hat{y}$ in Theorem 2.5, we need find a feasible point of the dual problem (7) at which the value of its objective function s is negative. We employ the Big-M method [31] to (5) and (7), and solve the following two modified SDPs

$$\begin{aligned} r^*_{\mathcal{M}} := \sup_{W \in \mathbb{S}\mathbb{R}^{k \times k}, w \in \mathbb{R}} \quad & -C \bullet (W - w) - \mathcal{M}w \\ s.t. \quad & \begin{bmatrix} \vdots \\ A^{[\alpha]} \bullet (W - w) \\ \vdots \\ A \bullet (W - w) \end{bmatrix} = \begin{bmatrix} \vdots \\ 0 \\ \vdots \\ 1 \end{bmatrix}, \\ & W \succeq 0, w \geq 0, \end{aligned} \tag{10}$$

$$\begin{aligned} s^*_{\mathcal{M}} := \inf_{(y,s) \in \mathbb{R}^{m+1}} \quad & s \\ s.t. \quad & M(y, s) \succeq 0, \\ & \mathrm{Tr} M(y, s) \leq \mathcal{M}, \end{aligned} \tag{11}$$

where matrices C, $A^{[\alpha]}$, A, $M(y, s)$ in (10) and (11) are defined as in (6) and (8).

Proposition 3.2. *If $f \notin \mathrm{SOS}/\mathrm{SOS}_{\mathcal{T}}$, then for any real number $\mathcal{M} > 0$, SDPs (10), (11) are strictly feasible and $s^*_{\mathcal{M}} < 0$ in (11).*

PROOF. By Lemma 2.3, (11) is strictly feasible for some $\mathcal{M} \in \mathbb{R}$. For any real number $\mathcal{M} > 0$, denote the feasible set of (11) by

$$\mathcal{F}_{\mathcal{M}} = \{(y, s) \in \mathbb{R}^{m+1} \mid M(y, s) \succeq 0,\ \mathrm{Tr} M(y, s) \leq \mathcal{M}\}.$$

Since $C = \mathbf{0}$ in (6), for any two real numbers $\mathcal{M}_1 > 0, \mathcal{M}_2 > 0$, we have

$$\mathcal{F}_{\mathcal{M}_1} = \frac{\mathcal{M}_1}{\mathcal{M}_2} \cdot \mathcal{F}_{\mathcal{M}_2} \tag{12}$$

which means $(y,s) \in \mathbb{R}^{m+1} \in \mathcal{F}_{\mathcal{M}_2}$ if and only if $\frac{\mathcal{M}_1}{\mathcal{M}_2}(y,s) \in \mathcal{F}_{\mathcal{M}_1}$. Thus (11) is strictly feasible for any real $\mathcal{M} > 0$. As shown in [31], (10) is also strictly feasible for any $\mathcal{M} > 0$ and $r^*_{\mathcal{M}} = s^*_{\mathcal{M}} \to -\infty$ as $\mathcal{M} \to \infty$. Hence, there exists a real $\mathcal{M} > 0$ such that $s^*_{\mathcal{M}} < 0$. Again, by (12), we have that $s^*_{\mathcal{M}} < 0$ for any real number $\mathcal{M}$. □

Remark 3.1. To find a certificate $\hat{y}$ in Theorem 2.5, rather than the optimizer of the dual problem (7), we only need to find a feasible point of (7) at which the value of its objective function s is negative. Note that any feasible point of (11) is also feasible to (7). Then by Proposition 3.2, we can fix any real $\mathcal{M} > 0$ (need not increase it) and obtain a certificate $\hat{y}$ by solving (10) and (11) using interior-point methods. Thus large numbers and numerical difficulties would not appear in the Big-M method. Since it might cause numerical error when $\mathcal{M}$ is too small, we in practice fix a moderately large number $\mathcal{M}$ (for example, 10 times the largest coefficient of f).

Algorithm 3.1.
Input: *$f \in \mathbb{Q}[X]$, $e \in \mathbb{Z}_{\geq 0}$ and a subset $\mathcal{T} \subseteq$ Terms$[X;\deg{\leq}e]$.*
Output: *If $f \notin$ SOS/SOS$_{\mathcal{T}}$, return a certificate $\hat{y} \in \mathbb{Q}^m$.*

I. *Reduce the problem to SDPs (5) and (7).*

II. *Fix a big $\mathcal{M} \in \mathbb{Z}$ and modify (5), (7) to (10), (11).*

III. *Solve (10) and (11) by interior-point methods to get a solution $p_k = (y^k, s^k)$ with $s^k < 0$.*

IV. *Find a strictly feasible point $\tilde{p} = (\tilde{y}, \tilde{s})$ of (7).*

V. *Fix $0 < t \leq 1$ and $\bar{p} = (1-t)p_k + t\tilde{p} = (\bar{y}, \bar{s})$ such that $\bar{s} < 0$.*

VI. *Choose a rational point $\hat{p} = (\hat{y}, \hat{s}) \in B_\varepsilon(\bar{p})$ where $\varepsilon < \frac{1}{2}|\bar{s}|$.*

Remark 3.2. In Step III, provided that the problem is of large size and not ill-conditioned, we can solve (10) and (11) using SDP solvers in Matlab like SeDuMi [30] which is very efficient. If the problem has small size and an accurate solution is needed, Maple package *SDPTools* [9] is a better choice. *SDPTools*, in which the above algorithm has been implemented, is a high precision SDP solver based on the potential reduction method in [31].

Remark 3.3. In practice, if the SDPs (10) and (11) in Step III are precisely computed by interior-point methods, then the floating-point solution (y^k, s^k) is a highly accurate approximation of a strictly feasible point of (7). Hence, without Step IV, V, VI, one can expect that an exact certificate can be obtained by simply rounding (y^k, s^k) to a rational feasible solution to (7).

3.2 Exploiting the Newton polytope

To reduce computation cost, we can replace $m_{\text{Terms}[X;\deg\leq d]}$ in (3), i.e. the vector of all terms with degree $\leq d$ by a vector containing part of $m_{\text{Terms}[X;\deg\leq d]}$ due to the following theorem:

Theorem 3.3. [26, Theorem 1] *For a polynomial $p(x) = \sum_\alpha p_\alpha x^\alpha$, we define $C(p)$ as the convex hull of $\{\alpha|\ p_\alpha \neq 0\}$, then we have $C(p^2) = 2C(p)$; for any positive semidefinite polynomials f and g, $C(f) \subseteq C(f+g)$; if $f = \sum_j g_j^2$ then $C(g_j) \subseteq \frac{1}{2}C(f)$.*

The polytope $C(p)$ in the above theorem is usually called the *Newton polytope* which is used in many different areas.

Definition 1. *Given a polynomial $f \in \mathbb{R}[X]$, an integer $e \geq 0$ and a subset $\mathcal{T} \subseteq$ Terms$[X;\deg{\leq}e]$, let $\mathcal{C}_{f,\mathcal{T}}$ be the convex hull of $\{\alpha \in \mathbb{N}^n \mid \alpha = \beta + \gamma_1 + \gamma_2, X^\beta \in supp(f), X^{\gamma_1}, X^{\gamma_2} \in \mathcal{T}\}$. We define $\mathcal{G}_{f,\mathcal{T}} = \{X^\alpha |\ 2\alpha \in \mathcal{C}_{f,\mathcal{T}}\}$. We write the shorthand $\mathcal{G}_{f,\deg\leq e}$ if $\mathcal{T} =$ Terms$[X;\deg{\leq}e]$.*

By Theorem 3.3, we have $m_{\mathcal{G}_{f,\mathcal{T}}} \subseteq m_{\text{Terms}[X;\deg\leq d]}$ and that $f \in$ SOS/SOS$_{\mathcal{T}}$ if and only if there exist $W^{[1]} \succeq 0$ and $W^{[2]} \succeq 0$ with $\text{Tr}(W^{[2]}) = 1$ such that

$$0 = m_{\mathcal{G}_{f,\mathcal{T}}}{}^T W^{[1]} m_{\mathcal{G}_{f,\mathcal{T}}} + (-f(X)) \cdot m_{\mathcal{T}}{}^T W^{[2]} m_{\mathcal{T}}.$$

Thus the sizes of the SDPs (5) and (7) decrease. We show below another version of Theorem 2.7 employing the Newton polytope.

Corollary 3.4. *Given a polynomial $f \in \mathbb{Q}[X]$ and an integer $e \geq 0$, let $d = \lceil e + \deg(f)/2 \rceil$, then for any subset $\mathcal{T} \subseteq$ Terms$[X;\deg{\leq}e]$, the following are equivalent:*

1. *$f \notin$ SOS/SOS$_{\mathcal{T}}$,*
2. *There exists a rational vector $\hat{y} \in \mathbb{Q}^m$ and the associated linear form $L_{\hat{y}} \in (\mathbb{R}[X]_{2d})^*$ such that for any polynomials $v, u \in \mathbb{R}[X]$ with $supp(v) \in \mathcal{T}$ and $supp(u) \in \mathcal{G}_{f,\mathcal{T}}$, we have $L_{\hat{y}}(fv^2) < 0$ and $L_{\hat{y}}(u^2) \geq 0$,*

where m is the number of elements in the set $\{X^{\alpha+\beta} \mid X^\alpha, X^\beta \in \mathcal{G}_{f,\mathcal{T}}\}$.

4. HILBERT-ARTIN REPRESENTATION OF POSITIVE SEMIDEFINITE RATIONAL FUNCTIONS

We generalize our method for solving the following problem: Given a rational function $f/g \in \mathbb{Q}(X)$ with $g(X) \succeq 0$ an integer $e \geq 0$ and $\mathcal{T} \subseteq$ Terms$[X;\deg{\leq}d]$, certify $f/g \notin$ SOS/SOS$_{\mathcal{T}}$.

Consider the following set

$$\Big\{[W^{[1]}, W^{[2]}] \ \Big|\ g(x) \cdot m_{\text{Terms}[X;\deg\leq d]}{}^T W^{[1]} m_{\text{Terms}[X;\deg\leq d]} = f(X) \cdot (m_{\mathcal{T}}{}^T W^{[2]} m_{\mathcal{T}}), \quad W^{[1]} \succeq 0,\ W^{[2]} \succeq 0,\ \text{Trace}(W^{[2]}) = 1\Big\}, \qquad (13)$$

where $d = e + (\lceil \deg(f) - \deg(g) \rceil)/2$.

Proposition 4.1. *We have $f/g \notin$ SOS/SOS$_{\mathcal{T}}$ if and only if the set (13) is empty.*

Let

$$\left.\begin{aligned} \Gamma_1 &:= \Big\{X^{\alpha+\beta+\gamma} \ \Big|\ X^\gamma \in \text{supp}(g), X^\alpha, X^\beta \in \text{Terms}[X;\deg\leq d]\Big\}, \\ \Gamma_2 &:= \Big\{X^{\alpha+\beta+\gamma} \ \Big|\ X^\gamma \in \text{supp}(f), X^\alpha, X^\beta \in \mathcal{T}\Big\}. \end{aligned}\right\} \quad (14)$$

We assume that $\Gamma_1 \supseteq \Gamma_2$, otherwise $f/g \notin \text{SOS}/\text{SOS}_{\mathcal{T}}$. The following analysis is similar to the one given in Section 2.

The primal block SDP considered here has the same form as (5) but we use

$$g(X) \cdot m_{\text{Terms}[X;\deg\leq d]}{}^T W^{[1]} m_{\text{Terms}[X;\deg\leq d]} = \sum_{\alpha} (G^{[\alpha]} \bullet W^{[1]}) X^{\alpha} \quad (15)$$

to define matrices $G^{[\alpha]}$. Its dual problem is

$$s^* := \inf_{(y,s)\in\mathbb{R}^{m+1}} s \quad s.t.\ M(y,s) \succeq 0, \quad (16)$$

where

$$M(y,s) := \begin{bmatrix} M_d(gy) & \\ & M_e((-f)y) + sI \end{bmatrix},$$

$y := (y_\alpha)_{\alpha\in\mathbb{N}^n_{2d}} \in \mathbb{R}^{\mathbb{N}^n_{2d}}$ and m is the number of elements in the set Γ_1. $M_d(gy)$ and $M_e((-f)y)$ are localizing moment matrices. Similar to Lemma 2.3, we have

Lemma 4.2. *There exists $\tilde{p} = (\tilde{y}, \tilde{s})$ such that $M_d(g\tilde{y}) \succ 0$ and $M_e(-f\tilde{y}) + \tilde{s}I \succ 0$.*

Proof. Taking $\tilde{y}_\alpha$ to be the one defined in the proof of Lemma 2.3, since $g(X)$ is nonnegative, for any polynomial $q(X) \in \mathbb{R}[X]$ with $\text{supp}(q) \in \text{Terms}[X;\deg\leq d]$, we have

$$\begin{aligned}\langle \text{vec}(q)^T, M_d(g\tilde{y})\text{vec}(q)\rangle &= \int g(x)q(x)^2\mu(dx) \\ &= \int g(x)q(x)^2 h(x)dx \\ &> 0 \text{ whenever } q \neq 0,\end{aligned}$$

which implies $M_d(g\tilde{y}) \succ 0$. Take

$$\tilde{s} > -\lambda_{\min}(M_e((-f)\tilde{y})),$$

then $M_e(-f\tilde{y}) + \tilde{s}I \succ 0$. $\square$

Based on the Farkas Lemma 2.4 and Lemma 4.2, similar to Theorem 2.5 and Theorem 2.7, we have the following results.

Theorem 4.3. *Given a rational function $f/g \in \mathbb{Q}(X)$ with $g(X) \succeq 0$ and an integer $e \geq 0$, let $d = e + (\lceil \deg(f) - \deg(g)\rceil)/2$, then for any subset $\mathcal{T} \subseteq \text{Terms}[X;\deg\leq e]$, the following are equivalent:*

1. *$f/g \notin \text{SOS}/\text{SOS}_{\mathcal{T}}$,*
2. *$\Gamma_1 \not\supseteq \Gamma_2$ in (14), or there exists a rational vector $\hat{y} = (\hat{y}_\alpha) \in \mathbb{Q}^m$ such that $M_d(g\hat{y}) \succeq 0$ and $M_e(f\hat{y}) \prec 0$ in (16),*

where m is the number of elements in the set Γ_1.

With a view towards linear forms in $\mathbb{R}[X]$, Theorem 4.3 is equivalent to

Theorem 4.4. *Given a rational function $f/g \in \mathbb{Q}(X)$ with $g(X) \succeq 0$ and an integer $e \geq 0$, let $\mathbb{R}[X]_{2d+\deg(g)} := \{p \in \mathbb{R}[X] \mid supp(p) \in \text{Terms}[X;\deg\leq 2d+\deg(g)]\}$ where $d = e + (\lceil \deg(f) - \deg(g)\rceil)/2$, then for any subset $\mathcal{T} \subseteq \text{Terms}[X;\deg\leq e]$, the following are equivalent:*

1. *$f/g \notin \text{SOS}/\text{SOS}_{\mathcal{T}}$,*
2. *$\Gamma_1 \not\supseteq \Gamma_2$ in (14), or there exists a rational vector $\hat{y} \in \mathbb{Q}^m$ and the associated linear form $L_{\hat{y}} \in (\mathbb{R}[X]_{2d+\deg(g)})^*$, such that for any polynomials $v, u \in \mathbb{R}[X]$ with $supp(v) \in \mathcal{T}$ and $supp(u) \in \text{Terms}[X;\deg\leq d]$, we have $L_{\hat{y}}(fv^2) < 0$ and $L_{\hat{y}}(gu^2) \geq 0$,*

where m is the number of elements in the set Γ_1.

5. EXAMPLES AND EXPERIMENTS

Example 5.1. We prove that the well known Motzkin polynomial

$$f(X_1, X_2) = X_1^4X_2^2 + X_1^2X_2^4 + 1 - 3X_1^2X_2^2$$

is not an SOS. Set $n = 2$, $e = 0$ and $d = 3$. By Definition 1, we have $\mathcal{G}_{f,\deg\leq 0} = \{1, X_1X_2, X_1^2X_2, X_1X_2^2\}$. According to Corollary 3.4, $m = 10$ and we need to find a rational sequence $\hat{y} \in \mathbb{Q}^{10}$ or its associated linear form $L_{\hat{y}} \in (\mathbb{R}[X]_6)^*$ such that for any polynomial $u \in \mathbb{R}[X]$ with $\text{supp}(u) \in \mathcal{G}_{f,\deg\leq 0}$, we have $L_{\hat{y}}(u^2) \geq 0$ and $L_{\hat{y}}(f) < 0$. The certificate we obtained is

$$\begin{aligned}\hat{y} = (&\hat{y}_{0,0} = \hat{y}_{1,1} = \hat{y}_{1,2} = 0, \hat{y}_{2,2} = 300, \\ &\hat{y}_{3,2} = \hat{y}_{2,3} = \hat{y}_{4,2} = \hat{y}_{3,3} = \hat{y}_{2,4} = 0).\end{aligned}$$

Its associated linear form $L_{\hat{y}}$ satisfies

$$L_{\hat{y}}(u^2) = 300u_{1,1}^2 \geq 0 \text{ and } L_{\hat{y}}(f) = -3\times 300 = -900 < 0,$$

which implies f can not be written as an SOS.

Example 5.2. In [15], the monotone column permanent (MCP) conjecture has been proven for dimension 4 via certifying polynomials $p_{1,1}, p_{1,2}$, $p_{1,3}, p_{2,2}, p_{2,3}, p_{3,3}$ of degree 8 in 8 variables to be positive semidefinite, see [15] for the explicit forms of these polynomials. Among them, the polynomials $p_{1,1}, p_{3,3}$ are perfect squares. Applying the hybrid symbolic-numeric algorithm in [16], they proved that the polynomial $p_{1,3}$ can be written as an SOS and the polynomials $p_{1,2}, p_{2,2}, p_{2,3}$ can be written as an SOS divided by weighted sums of squares of variables. We certify that all polynomials $p_{1,2}, p_{2,2}, p_{2,3}$ can not be written as an SOS via finding the corresponding certificates $\hat{y} \in \mathbb{Q}^m$ and the associated linear forms $L_{\hat{y}} \in (\mathbb{R}[X]_8)^*$. By exploiting the Newton polytope, for $p_{1,2}$, the matrices W, $M(y,s)$ in (5), (7) are of dimension 24×24 and $m = 189$. For $p_{2,2}$, W and $M(y,s)$ are of dimension 29×29 and $m = 255$. For $p_{2,3}$, W and $M(y,s)$ are of dimension 39×39 and $m = 372$.

Example 5.3. This example comes from the even symmetric sextics in [6]. Let

$$M_{n,r}(X) = \sum_{i=1}^{n} X_i^r,$$

for integers k, $0 \leq k \leq n-1$, we define polynomials $f_{n,k}$ by

$$f_{n,0} = -nM_{n,6} + (n+1)M_{n,2}M_{n,4} - M_{n,2}^3,$$

and

$$f_{n,k} = (k^2+k)M_{n,6} - (2k+1)M_{n,2}M_{n,4} + M_{n,2}^3,\ 1 \leq k \leq n-1.$$

Some interesting results about these polynomials have been given in [6].

Proposition 5.1. *For $n \geq 3$,*

(1) *all $f_{n,k}$, $0 \leq k \leq n-1$, are positive semidefinite polynomials;*

(2) *the polynomials $f_{n,0}$ and $f_{n,1}$ are SOS;*

(3) *the polynomials $f_{n,2}, \ldots, f_{n,n-1}$ are not SOS;*

(4) *$M_{3,2} \cdot f_{3,2}$ is an SOS [27]; $M_{4,2}^2 \cdot f_{4,2}$ is an SOS;*

(5) *for $n \geq 4$, $M_{n,2} \cdot f_{n,n-1}$ is an SOS.*

For $n \geq 4$ and $2 \leq i \leq n-2$, we wish to know whether $M_{n,2} \cdot f_{n,i}$ is an SOS. We have the following results.

1). For $n = 4$, we can certify that the polynomial

$$\boxed{f_{4,2} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \leq 2}.}$$

By exploiting the Newton polytope, in (5), $W^{[1]}$ has dimension 55×55 and $W^{[2]}$ has dimension 5×5. We have $m = 369$ in (7).

2). For $n = 5$, we can certify the following:

$$\boxed{f_{5,2} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \leq 2} \text{ and } f_{5,3} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \leq 4}.}$$

By exploiting the Newton polytope, for $f_{5,2}$, $W^{[1]}, W^{[2]}$ have dimension $105 \times 105, 6 \times 6$, respectively and $m = 1036$. For $f_{5,3}$, $W^{[1]}, W^{[2]}$ have dimension $231 \times 231, 21 \times 21$, respectively and $m = 2751$.

3). For $n = 6$, we can certify the following:

$$\boxed{f_{6,2} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \leq 2} \text{ and } f_{6,3}, f_{6,4} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \leq 4}.}$$

By exploiting the Newton polytope, for $f_{6,2}$, $W^{[1]}, W^{[2]}$ have dimension $182 \times 182, 7 \times 7$, respectively and $m = 2541$. For $f_{6,3}$ and $f_{6,4}$, $W^{[1]}, W^{[2]}$ have dimension $434 \times 434, 28 \times 28$, respectively and $m = 7546$.

Example 5.4. Consider the polynomial $f(X_1, X_2) = X_1^2 + X_2^2 - 2X_1X_2 = (X_1 - X_2)^2$. Its minimum is 0. However, for any small perturbation $\varepsilon > 0$, the polynomial $f_\varepsilon(X_1, X_2) = (1-\varepsilon^2)X_1^2 + X_2^2 - 2X_1X_2$ is not an SOS. Indeed, $f_\varepsilon(C, C) = -\varepsilon^2 C^2$ which implies that the infimum of f_ε is $-\infty$. Hence f is an *ill-posed* polynomial [13]. For $\varepsilon = 10^{-1}, \ldots, 10^{-5}$, we can use Matlab SDP solver SeDuMi in Step III in Algorithm 3.1 to certify that f_ε is not SOS. But for $\varepsilon < 10^{-5}$, Step III does not work out and we are not able to obtain a rational solution at which $s_k < 0$. If we use the command findsos in SOSTOOLS [23], it outputs a wrong SOS decomposition. Our method implemented in *SDPTools* in Maple can give exact certificates for f_ε being not an SOS for $\varepsilon = 10^{-8}$ or smaller! Take $\varepsilon = 10^{-8}$ for instance. By exploiting the Newton polytope, we have $\mathcal{G}_{f_\varepsilon, \deg \leq 0} = \{X_1, X_2\}$. Setting *Digits* $= 45$ in Maple, the certificate we obtained is $\hat{y} = (\hat{y}_{2,0}, \hat{y}_{1,1}, \hat{y}_{0,2})$ where

$$\hat{y}_{2,0} = \frac{4663536264238733709698 6}{1731626131338905851065},$$
$$\hat{y}_{1,1} = \frac{5347000107337789029026 7}{1985404333861113854675},$$
$$\hat{y}_{0,2} = \frac{1992641423885484771552 5}{739891310902398542446}.$$

For any $u \in \mathbb{R}[X]$ with $\mathrm{supp}(u) \in \mathcal{G}_{f_\varepsilon, \deg \leq 0}$, we have

$$\begin{aligned} L_{\hat{y}}(u^2) &= \frac{46635362642387337096986}{1731626131338905851065} u_{1,0}^2 \\ &\quad + \frac{19926414238854847715525}{739891310902398542446} u_{0,1}^2 \\ &\quad + 2 \times \frac{53470001073377890290267}{1985404333861113854675} u_{1,0}u_{0,1} \\ &\geq |2u_{1,0}u_{0,1}| \left(\left(\frac{46635362642387337096986}{1731626131338905851065} \right. \right. \\ &\quad \left. \times \frac{19926414238854847715525}{739891310902398542446} \right)^{\frac{1}{2}} \\ &\quad \left. - \frac{53470001073377890290267}{1985404333861113854675} \right) \\ &\geq 0. \end{aligned}$$

However,

$$\begin{aligned} L_{\hat{y}}(f_\varepsilon) &= \frac{9999999999999999}{10000000000000000} \times \frac{46635362642387337096986}{1731626131338905851065} \\ &\quad + \frac{19926414238854847715525}{739891310902398542446} \\ &\quad - 2 \times \frac{53470001073377890290267}{1985404333861113854675} \\ &< 0, \end{aligned}$$

which implies f_ε is not SOS.

Example 5.5. In this example, we consider some rational functions.

1). For Motzkin polynomial in Example 5.1, we can certify that

$$\frac{X_1^4X_2^2 + X_1^2X_2^4 + 1 - 3X_1^2X_2^2}{X_1^2 + 1} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \leq 2}.$$

2). For the even symmetric sextics in Example 5.3, we can certify that

$$\frac{f_{n,2}}{M_{n,2}}, \ldots, \frac{f_{n,n-1}}{M_{n,2}} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \leq 2}, \quad n = 4, 5, 6.$$

Those constitute our largest certificates. For $n = 4$, the certificate for each $\frac{f_{n,i}}{M_{n,2}} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \leq 2}$ has size $m = 480$; For $n = 5$, $m = 1256$; For $n = 6$, $m = 2940$.

The correctness of the above result is guaranteed by the following proposition.

Proposition 5.2. *Let $f/g \in \mathbb{R}(X)$ be a multivariate rational function where $f, g \in \mathbb{R}[X]$ with $\mathrm{GCD}(f, g) = 1$. If $f, -f \notin \mathrm{SOS}$ then $f/g \notin \mathrm{SOS}/\mathrm{SOS}_{\deg \leq \deg(g)}$.*

Proof. Assume the contrary, namely that

$$\frac{f}{g} = \frac{\sum_{i=1}^{l} u_i(X)^2}{\sum_{j=1}^{l'} v_j(X)^2}, \quad \deg(v_j) \leq \deg(g)/2. \tag{17}$$

where $u_i(X), v_j(X) \in \mathbb{R}[X]$. Thus the right-side of (17) constitutes the reduced fraction f/g, which means $g(X) = c\sum_j^{l'} v_j(X)^2$ for some non-zero constant $c \in \mathbb{R}$, making $f/c = \sum_{i=1}^{l} u_i(X)^2$, a contradiction. □

Furthermore, for the polynomials in Example 5.3, we can compute the certificates for the following result:

$$\left.\begin{aligned} &\frac{f_{n,2}}{M_{n,2}} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg\le 4}, \quad n = 4,5,6 \\ &\frac{f_{5,3}}{M_{5,2}} \notin \mathrm{SOS}/\mathrm{SOS}_{\deg\le 6}. \end{aligned}\right\} \qquad (18)$$

We have no generalization of Proposition 5.2 to $\pm f \notin \mathrm{SOS}/\mathrm{SOS}_{\deg\le 2e}$, and the impossibilities (18) may hint at new unknown properties of the even symmetric sextics in [6].

Acknowledgments: We thank Bruce Reznick for kindly pointing us to the even symmetric sextics in Example 5.3, and the reviewers for their comments. Feng Guo thanks the Study Abroad Program staff at AMSS and the staff at NCSU for their assistance with his 2011 study visit at NCSU. Feng Guo is especially grateful to Erich and Hoang Kaltofen for their warm hospitality and kind help during his stay in Raleigh Feb. 2011–Jan. 2012.

6. REFERENCES

[1] Ahmadi, A. A., and Parrilo, P. A. A convex polynomial that is not SOS-convex. *Mathematical Programming* (2011).

[2] Alizadeh, F. Interior point methods in semidefinite programming with applications to combinatorial optimization. *SIAM Journal on Optimization 5* (1995), 13–51.

[3] Artin, E. Über die Zerlegung definiter Funktionen in Quadrate. *Abhandlungen Math. Seminar Univ. Hamburg 5*, 1 (1927), 100–115.

[4] Blekherman, G. Dimensional difference between nonnegative polynomials and sums of squares. *Computing Research Repository abs/0907.1339* (2009). URL http://arxiv.org/abs/0907.1339.

[5] Chesi, G. On the gap between positive polynomials and SOS of polynomials. *IEEE Trans. Automatic Control 52*, 6 (June 2007), 1066–1072.

[6] Choi, M. D., Lam, T. Y., and Reznick, B. Even symmetric sextics. *Mathematische Zeitschrift 195* (Dec. 1987), 559–580.

[7] Dattorro, J. *Convex Optimization & Euclidean Distance Geometry*. Meboo Publishing, USA, 2011.

[8] Giesbrecht, M., Lobo, A., and Saunders, B. D. Certifying inconsistency of sparse linear systems. In *ISSAC 98 Proc. 1998 Internat. Symp. Symbolic Algebraic Comput.* (New York, N. Y., 1998), O. Gloor, Ed., ACM Press, pp. 113–119.

[9] Guo, F. SDPTools: High precision SDP solver in Maple. *MM-Preprints 28* (2009), 66–73. URL: http://www.mmrc.iss.ac.cn/pub/mm28.pdf/05-guofeng.pdf.

[10] Harrison, J. Verifying nonlinear real formulas via sums of squares. In *Proceedings of the 20th International Conference on Theorem Proving in Higher Order Logics, TPHOLs 2007* (Kaiserslautern, Germany, 2007), K. Schneider and J. Brandt, Eds., vol. 4732 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 102–118. URL http://www.cl.cam.ac.uk/~jrh13/papers/sos.pdf.

[11] Hilbert, D. Über die Darstellung definiter Formen als Summe von Formenquadraten. *Math. Ann. 32*, 3 (1888), 342–350.

[12] Hillar, C. Sums of polynomial squares over totally real fields are rational sums of squares. *Proc. American Math. Society 137* (2009), 921–930. URL: http://www.math.tamu.edu/~chillar/files/totallyrealsos.pdf.

[13] Hutton, S. E., Kaltofen, E. L., and Zhi, L. Computing the radius of positive semidefiniteness of a multivariate real polynomial via a dual of Seidenberg's method. In *Proc. 2010 Internat. Symp. Symbolic Algebraic Comput. ISSAC 2010* (New York, N. Y., July 2010), S. M. Watt, Ed., Association for Computing Machinery, pp. 227–234. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/10/HKZ10.pdf.

[14] Kaltofen, E. A short proof of C. Hillar's totally real SOS theorem. Email to Bernd Sturmfels and Chris Hillar, Jan. 2009. URL http://www.math.ncsu.edu/~kaltofen/bibliography/09/totallyreal.pdf.

[15] Kaltofen, E., Yang, Z., and Zhi, L. A proof of the Monotone Column Permanent (MCP) Conjecture for dimension 4 via sums-of-squares of rational functions. In *SNC'09 Proc. 2009 Internat. Workshop on Symbolic-Numeric Comput.* (New York, N. Y., 2009), H. Kai and H. Sekigawa, Eds., ACM Press, pp. 65–69. URL: http://www.math.ncsu.edu/~kaltofen/bibliography/09/KYZ09.pdf.

[16] Kaltofen, E. L., Li, B., Yang, Z., and Zhi, L. Exact certification in global polynomial optimization via sums-of-squares of rational functions with rational coefficients. *J. Symbolic Comput. 47*, 1 (Jan. 2012), 1–15. In memory of Wenda Wu (1929–2009). URL: http://www.math.ncsu.edu/~kaltofen/bibliography/09/KLYZ09.pdf.

[17] Klep, I., and Schweighofer, M. Infeasibility certificates for linear matrix inequalities, 2011. URL http://www.math.uni-konstanz.de/~schweigh/publications/infeasible.pdf.

[18] Lasserre, J. B. Global optimization with polynomials and the problem of moments. *SIAM Journal on Optimization 11* (2001), 796–817.

[19] Lasserre, J. B. *Moments, Positive Polynomials and Their Applications*. Imperial College Press, 2009.

[20] Laurent, M. Sums of squares, moment matrices and optimization over polynomials. In *Emerging Applications of Algebraic Geometry of IMA Volumes in Mathematics and its Applications* (2009), vol. 149, Springer, pp. 157–270.

[21] Peyrl, H., and Parrilo, P. A. Computing sum of squares decompositions with rational coefficients. *Theoretical Computer Science 409* (2008), 269–281.

[22] Powers, V., and Wörmann, T. An algorithm for sums of squares of real polynomials. *Journal of Pure and Applied Algebra 6*, 1 (1998), 99–104.

[23] Prajna, S., Papachristodoulou, A., and Parrilo, P. A. SOSTOOLS: Sum of squares optimization toolbox for MATLAB. http://www.cds.caltech.edu/sostools.

[24] Quarez, R. Bounding the rational sums of squares over totally real fields. *Computing Research Repository abs/0907.2336* (2009). URL http://arxiv.org/abs/0907.2336.

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

[26] Reznick, B. Extremal PSD forms with few terms. *Duke Mathematical Journal 45*, 2 (1978), 363–374.

[27] Robinson, R. M. Some definite polynomials which are not sums of squares of real polynomials. In *Selected questions of algebra and logic* (1973), pp. 264–282. Abstract in Notices Amer. Math. Soc. 16 (1969), p. 554.

[28] Safey El Din, M., and Zhi, L. Computing rational points in convex semi-algebraic sets and SOS decompositions. *SIAM J. Optimization 20*, 6 (2010), 2876–2889. URL http://arxiv.org/abs/0910.2973.

[29] Scheiderer, C. A remark on descending sums of squares representations, July 2009. Manuscript, 2 pages.

[30] Sturm, J. F. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization Methods and Software 11/12* (1999), 625–653.

[31] Vandenberghe, L., and Boyd, S. Semidefinite programming. *SIAM Review 38*, 1 (1996), 49–95.