

RATIONAL LMI AND SUMS OF SQUARES

CHRISTOPHER J. HILLAR

ABSTRACT. Do rational certificates always exist? This is an especially important question given the rise of numerical and seminumerical algorithms. We discuss some open problems, questions, and conjectures that arise naturally in the context of semidefinite programming and sums of squares.

1. INTRODUCTION

I will introduce two problems that are very related. The first deals with what I will call *rational LMI realizations* and involves the exploration of which real algebraic numbers can be realized as rational LMI's. The second general problem deals with rational certificates to nonnegative polynomials being sums of squares. Whether one can find such certificates is a very important question in the SOS semidefinite relaxation theory of optimization.

While the second problem on rational sums of squares seems very difficult, the first one is wide open, and it should be possible to obtain nice results in finite time.

2. RATIONAL LMI REPRESENTATIONS

Fix a positive integer n and real symmetric $m \times m$ matrices $A = (A_0, \dots, A_n)$. Consider the following set of real vectors:

$$S_{A,n} = \left\{ (x_1, \dots, x_n) \in \mathbb{R}^n : A_0 + \sum_{i=1}^n x_i A_i \succeq 0 \right\}.$$

Here $M \succeq 0$ signifies that M is a positive semidefinite matrix. Such sets, called *spectrahedron*, are related to what are called *LMI's* (*linear matrix inequalities*) in the literature, and they are ubiquitous these days in convex optimization and related fields.

The set $S_{A,n}$ is said to be *zero-dimensional* if $|S_{A,n}| < \infty$; in this case, $S_{A,n}$ consists of a single point (since it is convex). We would like to determine which algebraic numbers can be realized as coordinates of elements of some $S_{A,n}$, in which the symmetric matrices A_i have rational entries.

Definition 2.1. *A real algebraic number $\alpha \in \overline{\mathbb{Q}} \cap \mathbb{R}$ is said to be rationally (m, n) LMI-realizable (or simply rationally realizable) if there exists a positive integer n and rational symmetric matrices $A_0, \dots, A_n \in \mathbb{Q}^{m \times m}$ such that $S_{A,n}$ is zero-dimensional and α is a coordinate of some element of $S_{A,n}$.*

It seems to be a new and open-ended problem to study which real algebraic numbers are realizable in this sense (even for $n = 1$). As a simple example, we show the following.

Lemma 2.2. *Every number of the form $\sqrt[t]{t}$ with $0 \leq t \in \mathbb{Q}$ is rationally $(4, 1)$ LMI-realizable.*

Supported under an NSA Young Investigator Grant.

Proof. One simply checks that the following matrix is positive semidefinite if and only if $x = \sqrt{t}$:

$$\begin{bmatrix} t & x & 0 & 0 \\ x & t & 0 & 0 \\ 0 & 0 & tx & t \\ 0 & 0 & t & x \end{bmatrix}.$$

□

Remark 2.3. *Can one do this with 3×3 matrices still with $n = 1$?*

In general, nothing else seems to be known about which algebraic numbers are realizable for a fixed n , and a characterization for $n = 1$ is open (although very little work has been done so far on this problem it seems).

Problem 2.4 (Solved = yes). *Is $\alpha = \sqrt[3]{2}$ rationally realizable?*

Here are some open problems in this regard. We begin with the following general questions.

Problem 2.5. *Fix n and m . Characterize those real $m \times m$ symmetric matrices which give rise to zero-dimensional sets $S_{A,n}$.*

Problem 2.6. *For $n = 1$, determine all the rationally LMI-realizable algebraic numbers (m is allowed to vary).*

If the answer to the previous problem is not all of $\overline{\mathbb{Q}} \cap \mathbb{R}$, then we may ask the following.

Problem 2.7. *For a fixed $n > 1$, determine all the rationally LMI-realizable algebraic numbers (m is allowed to vary).*

It appears that the following problem can be solved using some ideas in <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.5.4181>.

Problem 2.8 (Solved = $\overline{\mathbb{Q}} \cap \mathbb{R}$?). *Determine all the rationally LMI-realizable algebraic numbers (both m and n are allowed to vary).*

In answering the previous problem, it would be interesting to have a bound on the m and n required that depends some way on the real algebraic number α that is desired.

Problem 2.9. *If α is a rationally LMI-realizable algebraic number, what are explicit m and n realizing this number? (Or bounds on them in terms of the algebraic degree/height of α).*

Recall that a *totally real number field* is a finite algebraic extension of \mathbb{Q} all of whose complex embeddings lie entirely in \mathbb{R} . An equivalent definition of a totally real number field K is that it is a field generated by a root of an irreducible polynomial $u(x) \in \mathbb{Q}[x]$, all of whose zeroes are real. For instance, the field $\mathbb{Q}(\sqrt{t})$ is totally real for positive, integral t .

Given the results in [5], the following conjecture seems natural.

Conjecture 2.10. *Any totally real algebraic number (that is, an element of some totally real number field) is rationally LMI-realizable with $n = 1$.*

I believe that this conjecture is quite tractable given the techniques of [5].

Another related problem is the rational symmetric eigenvalue realizability problem.

Problem 2.11. *Given a monic polynomial $f \in \mathbb{Q}[x]$ with all real roots, determine if there exists a rational symmetric matrix with characteristic polynomial equal to f .*

In general, there are rational polynomials that are not realizable in this sense. For instance, $f(x) = x^2 - 3$ is not the characteristic polynomial of any rational symmetric matrix (see [5] for a proof). However, a result of Fiedler says that (again, see [5] for an exposition of his proof):

Theorem 2.12 (Fiedler). *If $f(x) \in \mathbb{Q}[x]$ is monic of degree r and has r distinct real roots, then there are positive rational numbers l_1, \dots, l_r and a symmetric matrix A with entries in $\mathbb{Q}(\sqrt{l_1}, \dots, \sqrt{l_r})$ such that the eigenvalues of A are the roots of $f(x)$.*

This fact was an important ingredient in the proof of Theorem 3.2 below.

An interesting question that might help solve the main problem of the next section was suggested by Dustin Cartwright.

Problem 2.13. *Given a monic polynomial $f \in \mathbb{Q}[x]$ with all real roots, does there always exist a rational symmetric matrix A and a polynomial $g \in \mathbb{Q}[x]$ such that the characteristic polynomial of A is equal to $f(x)g(x)$?*

It seems as though this problem is solved (constructively even) in the affirmative in the following paper by Krakowski [9] (thanks to Claus Scheiderer for this reference).

A related problem which will probably be an important ingredient of the $n = 1$ rational LMI realization problem is the following:

Problem 2.14. *Given a rational symmetric matrix A that is invertible and diagonalizable, does there exist a pair of symmetric rational matrices R, S such that $A = RS$?*

Of course, the situation we are interested in is when A is the companion matrix of a univariate polynomial $f(x)$ with rational coefficients. This corresponds to finding a representation $f(x) = \det(xE + F)$ for rational symmetric matrices E and F , and thus is clearly related to Problem 2.6.

3. RATIONAL SUMS OF SQUARES

In recent years, techniques from semidefinite programming have produced numerical algorithms for expressing positive semidefinite polynomials as sums of squares. These algorithms have many applications in optimization, control theory, quadratic programming, and matrix analysis [14, 15, 16, 17, 18]. Moreover, such representations aid in the computation of the real locus of a polynomial. For a noncommutative application of these techniques to a famous trace conjecture (the BMV conjecture in statistical mechanics), see the papers [1, 4, 6, 8, 12, 21].

One major drawback with these algorithms is that their output is, in general, numerical. For many applications, however, exact polynomial identities are needed. In this regard, Sturmfels has asked the following question.

Question 3.1 (Sturmfels). *If $f \in \mathbb{Q}[x_1, \dots, x_n]$ is a sum of squares in $\mathbb{R}[x_1, \dots, x_n]$, then is f also a sum of squares in $\mathbb{Q}[x_1, \dots, x_n]$?*

This question has a positive answer in the univariate case due to results of Landau [11] and Pourchet [19] (and algorithmically by Schweighofer [21]). It follows from a famous theorem of Artin [20] that if $f \in \mathbb{Q}[x_1, \dots, x_n]$ is a sum of squares of rational functions in $\mathbb{R}(x_1, \dots, x_n)$, then it is a sum of squares in $\mathbb{Q}(x_1, \dots, x_n)$. Moreover, from the work of Voevodsky on the Milnor conjectures, it is known that 2^{n+2} such squares suffice [10]. However, the transition from rational functions to polynomials is often a very delicate one. For instance, not every polynomial that is a sum of squares of rational functions is a sum of squares of polynomials [20].

More generally, Sturmfels is interested in the algebraic degree [13] of maximizing a linear functional over the space of all sum of squares representations of a given polynomial that is a sum of squares. In the special case of Question 3.1, a positive answer signifies an algebraic degree of 1 for this optimization problem.

General theory (quantifier elimination for real closed fields) reduces Question 3.1 to one involving real algebraic numbers. Recently, progress was made in the multivariate case when the coefficients lie in a totally real number field K . The main theorem in [5] is the following.

Theorem 3.2. *Let K be a totally real number field with Galois closure L and let R be a commutative \mathbb{Q} -algebra. If $f \in R$ is a sum of m squares in $R \otimes_{\mathbb{Q}} K$, then f is a sum of $4m \cdot 2^{\lfloor L:\mathbb{Q} \rfloor} \binom{\lfloor L:\mathbb{Q} \rfloor + 1}{2}$ squares in R .*

The proof of Theorem 3.2 in [5] is constructive. We remark that it is known [2] that arbitrarily large numbers of squares are necessary to represent any sum of squares over $\mathbb{R}[x_1, \dots, x_n]$, $n > 1$, making a fixed bound (for a given n) as in the rational function case impossible.

A generalization of this result to arbitrary field extensions will settle the very important question of how much limitation one has in using semidefinite techniques for finding algebraic certificates of nonnegativity.

Problem 3.3. *Let K be a finite algebraic extension of \mathbb{Q} . If $f \in \mathbb{Q}[x_1, \dots, x_n]$ is a sum of squares in $K[x_1, \dots, x_n]$, then is f also a sum of squares in $\mathbb{Q}[x_1, \dots, x_n]$?*

As a start, it might be interesting to work with special classes of field extensions K other than totally real fields.

Problem 3.4. *Let K be a finite abelian extension of \mathbb{Q} (its Galois group is abelian). If $f \in \mathbb{Q}[x_1, \dots, x_n]$ is a sum of squares in $K[x_1, \dots, x_n]$, then is f also a sum of squares in $\mathbb{Q}[x_1, \dots, x_n]$?*

REFERENCES

- [1] S. Burgdorf, *Notes on $S_{m,4}(X \cdot Y^2)$* , preprint.
- [2] M. D. Choi, Z. D. Dai, T. Y. Lam, B. Reznick, *The Pythagoras number of some affine algebras and local algebras*. *J. Reine Angew. Math.* **336** (1982), 45–82.
- [3] M. Drton, B. Sturmfels, S. Sullivant, *Algebraic factor analysis: Tetrads, pentads and beyond*, *Probability Theory and Related Fields*, **138** (2007) 463–493.
- [4] D. Hägele, *Proof of the cases $p \leq 7$ of the Lieb-Seiringer formulation of the Bessis-Moussa-Villani conjecture*, *J. Stat. Phys.* **127** (2007), 1167–1171.
- [5] C. Hillar, *Sums of polynomial squares over totally real fields are rational sums of squares*, *Proc. Amer. Math. Soc.*, **137** (2009), 921–930.

- [6] C. Hillar, *Advances on the Bessis-Moussa-Villani Trace Conjecture*, Lin. Alg. Appl., **426** (2007), 130–142.
- [7] C. Hillar, J. Nie, *An elementary and constructive solution to Hilbert’s 17th problem for matrices*, Proc. Amer. Math. Soc., **136** (2008), 73–76.
- [8] I. Klep and M. Schweighofer, *Sums of Hermitian squares and the BMV conjecture*, preprint.
- [9] F. Krakowski, *Eigenwerte und Minimalpolynome symmetrischer Matrizen in kommutativen Körpern*, Comm. Math. Helvetici 32, 224–240 (1958).
- [10] T. Y. Lam, *Introduction To Quadratic Forms Over Fields*, American Mathematical Society, 2004.
- [11] E. Landau, *Über die Darstellung definiter Funktionen durch Quadrate*, Math Ann., **62** (1906), 272–285.
- [12] P. Landweber and E. Speer, *On D. Hägeles approach to the Bessis-Moussa-Villani conjecture*, preprint.
- [13] J. Nie, K. Ranestad, B. Sturmfels, *The algebraic degree of semidefinite programming*, Mathematical Programming, to appear, math.CO/0611562.
- [14] A. Papachristodoulou, P. A. Parrilo, S. Prajna, *Introducing SOSTOOLS: A General Purpose Sum of Squares Programming Solver*. Proceedings of the IEEE Conference on Decision and Control (CDC), Las Vegas, NV. 2002.
- [15] A. Papachristodoulou, P. A. Parrilo, S. Prajna, *New Developments in Sum of Squares Optimization and SOSTOOLS*. Proceedings of the American Control Conference (ACC), Boston, MA. 2004.
- [16] P. Parrilo, *Semidefinite programming relaxations for semialgebraic problems*. Math. Program., Ser. B **96** (2003), 293–320.
- [17] P. Parrilo, *Exploiting algebraic structure in sum of squares programs*, Positive polynomials in Control, Lecture Notes in Control and Information Sciences, Vol. 312, pp. 181–194, Springer, 2005.
- [18] P. Parrilo, B. Sturmfels, *Minimizing polynomial functions*, Algorithmic and quantitative real algebraic geometry, DIMACS Series in Discrete Mathematics and Theoretical Computer Science, Vol. 60, pp. 83–99, AMS.
- [19] Y. Pourchet, *Sur la représentation en somme de carrés des polynômes à une indéterminée sur un corps de nombres algébriques*, Acta Arith. **19** (1971), 89–104.
- [20] A. Prestel, C. N. Delzell, *Positive Polynomials: From Hilbert’s 17th Problem to Real Algebra*, Springer, 2001.
- [21] M. Schweighofer, *Algorithmische Beweise für Nichtnegativ- und Positivstellensätze*, Diplomarbeit an der Universität Passau, 1999.

MSRI, 17 GAUSS WAY, BERKELEY, CA 94120
E-mail address: `chillar@msri.org`