Rational Certificates of Positivity

Vicki Powers

Dept. of Mathematics and Computer Science
Emory University, Atlanta, USA

ECCAD 2011, University of Waterloo, Ontario
April 9, 2011
In theory, theory and practice are the same. But in practice, they are different.
Certificates of positivity

Throughout we work in $\mathbb{R}[X] := \mathbb{R}[x_1, \ldots, x_n]$. For any ring $R$,

$$
\sum R^2 = \{ r_1^2 + \cdots + r_k^2 \mid r_i \in R \},
$$

the set of sums of squares in $R$.

For $S \subseteq \mathbb{R}^n$, $f \geq 0$ on $S$ means $f(x) \geq 0$ for all $x \in S$. Similarly for $f > 0$ on $S$.

Suppose $S \subseteq \mathbb{R}^n$, $f \in \mathbb{R}[X]$, and $f \geq 0$ on $S$. By a certificate of positivity for $f$ on $S$ we mean an algebraic expression for $f$, usually involving elements in $\sum \mathbb{R}[X]^2$, from which one can deduce the positivity condition immediately.
For example, I claim $f \geq 0$ on $\mathbb{R}^2$:

$$f(x, y) := x^4 + 4y^4 - 4xy^2 + 2x^2y - x^2 + y^2 - 2y + 1$$

The following certificate of positivity for $f$ proves the claim:

$$f = (x^2 + y - 1)^2 + (2y^2 - x)^2$$
We are interested in the following (vague!) questions:

- If a certificate of positivity exists for \( f \) in theory, does one exist in practice?
- If a certificate of positivity exists for \( f \) in practice, does one exist in theory?
Sums of squares - Background and history

- $f \in \mathbb{R}[X]$ is positive semi-definite, or \textbf{psd} if $f(\alpha) \geq 0$ for all $\alpha \in \mathbb{R}^n$. $f$ is a sum of squares, or \textbf{sos} if $f \in \sum \mathbb{R}[X]^2$.

- Obviously, $f$ sos implies $f$ is psd – squares in $\mathbb{R}$ are non-negative! Writing $f$ as a sum of squares gives us a certificate of positivity for $f$ on $\mathbb{R}^n$.

- If $n = 1$, it’s easy to show that every psd $f$ is sos (use the Fundamental Theorem of Algebra).

- If $\deg f = 2$ and $f$ is psd, then $f$ is sos by completing the square (Sylvester, 1850s)
In 1888, Hilbert proved two remarkable theorems (in one paper!)

**Theorem (Hilbert)**

- Suppose $f$ is psd of degree 4 in two variables, then $f$ is sos.
- For all other cases, there exist psd $f$ which are not sos.

Hilbert did not give an explicit example of a psd, non-sos polynomial. The first published examples did not appear until the 1960s, the most famous is the Motzkin polynomial

$$x^4 y^2 + x^2 y^4 - 3x^2 y^2 + 1$$
In 1893, Hilbert proved that for $n = 2$ every psd polynomial in $\mathbb{R}[X]$ can be written as a sum of squares of rational functions, equivalently, as a quotient $g/h$ with $g \in \sum \mathbb{R}[X]^2$ and $h \in \mathbb{R}[X]^2$.

Unable to prove that this holds for all psd polynomials, it became the 17th problem on Hilbert’s list of 23 problems he gave in his address to the International Congress of Mathematicians in 1900.
E. Artin settled the question:

**Theorem (Artin 1927)**

Suppose $f \in \mathbb{R}[X]$ is psd. Then there is a nonzero $h \in \mathbb{R}[X]$ such that $h^2 f$ is sos.

Note that an identity $h^2 f = g_1^2 + \cdots + g_k^2$ is a certificate of positivity for $f$ on $\mathbb{R}^n$.

Artin (along with Schreier) developed the theory of ordered fields in order to solve the 17th problem. And thus the subject of Real Algebra was born (more or less).
Finding SOS decompositions

For a given sos $f \in \mathbb{R}[X]$, thanks to the magic of linear algebra, there are effective algorithms for writing $f$ as a sum of squares.

Suppose $\deg f = 2d$ and

$$f = \sum_{i=1}^{k} g_i(x)^2$$  \hfill (1)

The linear algebra version of (1) is

$$f(X) = V \cdot BB^T \cdot V^T,$$

$V$ = monomials of $\deg \leq d$, and $B$ is the matrix with $i$-th column the coefficients of $g_i$.

$A = B \cdot B^T$ is psd symmetric matrix, called a **Gram matrix** for $f$ corresponding to (1).
“$f$ is sos” is equivalent to the existence of a Gram matrix for $f$, i.e., a psd symmetric matrix $A$ such that

$$f(X) = V^T \cdot A \cdot V,$$

(2)

$A$ is an $N \times N$ matrix, where $N = \binom{n+d}{d}$. The set of $N \times N$ matrices $A$ such that (2) holds is an affine subset $\mathcal{L}$ of the space of $N \times N$ symmetric matrices.

$f$ is sos iff $\mathcal{L} \cap P_N \neq \emptyset$, where $P_N$ is the convex cone of psd symmetric $N \times N$ matrices over $\mathbb{R}$.

Finding this intersection is a **semidefinite program** (SDP). There are good numerical algorithms – and software! – for solving semidefinite programs.
A **semialgebraic set** in $\mathbb{R}^n$ is a subset defined by finitely many polynomial inequalities.

For $G = \{g_1, \ldots, g_r\} \subseteq \mathbb{R}[X]$, $S(G)$ denotes the **basic closed semialgebraic set generated by** $G$:

$$S(G) = \{ \alpha \in \mathbb{R}^n \mid g_1(\alpha) \geq 0, \ldots, g_r(\alpha) \geq 0 \}.$$  

Question: Suppose $f \geq 0$ or $f > 0$ on $S(G)$, does there exist a certificate of positivity for $f$ on $S(G)$?

Answer: If $S(G)$ is compact and $f > 0$ on $S(G)$, yes!
Fix $S = S(G)$, there are two algebraic objects associated to $G$:

The **quadratic module** generated by $G$,

$$M(G) := \{s_0 + s_1 g_1 + \cdots + s_r g_r \mid \text{each } s_i \text{ is sos} \}.$$  

The **preorder** generated by $G$,

$$PO(G) := \{ \sum_{\epsilon \in \{0,1\}^n} s_{\epsilon} g_{1}^{\epsilon_1} \cdots g_{r}^{\epsilon_r} \mid s_{\epsilon} \text{ is sos} \}.$$  

A representation of $f$ in either $M(G)$ or $PO(G)$ yields a certificate of positivity for $f$ on $K$.  

**Rational Certificates of Positivity**
Fix a basic closed semialgebraic set $S = S(G)$, the corresponding quadratic module $M = M(G)$, and the corresponding preorder $P = PO(G)$.

$M$ is **archimedean** if there is $N \in \mathbb{N}$ such that $N - \sum X_i^2 \in M$. A similar definition holds for $P$.

If $M$ is archimedean, then $S$ must be compact, and $N - \sum X_i^2 \in M$ is a “certificate of compactness” for $S$. The converse is not true in general.

However, $S$ compact implies that $P$ is archimedean. This follows from work of Schmüdgen; there is a nice algebraic proof due to Wörmann.
We have the following (beautiful!) theorems:

**Theorem (Putinar)**

*If $M$ is archimedean and $f > 0$ on $S$, then $f \in M$.*

**Theorem (Schm"udgen)**

*If $S$ is compact, then $f > 0$ on $S$ implies $f \in P$.*

This means that if $S$ is compact, then there exists a certificate of positivity for every $f > 0$ on $S$. 
As in the global (sum of squares) case, the problem of finding a representation of $f$ in $P$ or in $M$ can be implemented as a semidefinite programming problem.

The quadratic module $M$ is computationally simpler than using the preorder $P$. If we know an $N \in \mathbb{N}$ such that $N - \sum X_i^2 \geq 0$ on $S$, then we can add $N - \sum X_i^2$ to our generators $G$ and $M$ is now archimedean.

The point is that finding a certificate of positivity for $f > 0$ on a compact $S(G)$ can be done using software.
Applications of certificates of positivity

Why find certificates of positivity?

There are many applications!

- Optimization of polynomials.
- Graph theoretic problems: MAXCUT, MAX CLIQUE.
- Robotics and trajectory planning.
- Geometric theorem proving
- Control of nonlinear systems via Lyapunov functions
- BMV positivity conjecture related to Quantum Mechanics
**Problem**: Given $f \in \mathbb{R}[X]$, find the minimum of $f$ on $\mathbb{R}^n$ (if it exists).

Equivalent to finding the minimum of $\{\lambda \in \mathbb{R} | f - \lambda \geq 0 \text{ on } \mathbb{R}^n\}$. We can look for the smallest $\lambda$ so that $f - \lambda \in \sum \mathbb{R}^n$. This will give a lower bound for the minimum of $f$. In other words, find the minimum $\lambda$ so that a certificate of positivity for $f$ exists.

This idea generalizes to certificates of positivity on $S \subseteq \mathbb{R}^n$. Lasserre has used this to develop an algorithm for minimizing polynomials on compact semialgebraic sets.
Rational sums of squares

Consider the following example, due to C. Hillar:

Is \( f = 3 - 12x - 6x^3 + 18y^2 + 3x^6 + 12x^3y - 6xy^3 + 6x^2y^4 \) sos?

Our SDP program might say \textbf{yes} and return a certificate:

\[
f = (x^3 + 3.53y + .347xy^2 - 1)^2 + (x^3 + .12y + 1.53xy^2 - 1)^2 + (x^3 + 2.35y - 1.88xy^2 - 1)^2
\]

Note that \( f - \text{RHS} \) has terms such as \(-.006xy^2\) which are nonzero.

Is \( f \) really a sum of squares?

It turns out that our SDP program has approximated an sos decomposition for \( f \) of the form

\[
(x^3 + a^2y + bxy^2 - 1)^2 + (x^3 + b^2y + cxy^2 - 1)^2 + (x^3 + c^2y + axy^2 - 1)^2,
\]

where \( a, b, c \) are real roots of the equation \( u(x) = x^3 - 3x + 1 \).
For many applications of certificates of positivity, we need exact certificates, but SDP’s are numerical.

In theory, SDP problems can be solved purely algebraically, e.g., using quantifier elimination. In practice, this is impossible for all but trivial problems.

Work by J. Nie, K. Ranestand, and B. Sturmfels shows that optimal solutions of relatively small SDP’s can have minimum defining polynomials of huge degree.

Much more promising are recent hybrid symbolic-numeric approaches.
**Problem:** Given a numerical (approximate) certificate \( f = \sum g_i^2 \) (via SDP software, say) find an exact rational solution.

Peyrl and Parrilo gave an algorithm for solving this problem, in some cases. The idea: We want to find a symmetric psd matrix \( A \) with rational entries so that

\[
f = V \cdot A \cdot V^T
\]  

The SDP software will produce a psd matrix \( A \) which only \textit{approximately} satisfies (3). The idea is to project \( A \) onto the affine space of solutions to (3) in such a way that the projection remains in the cone of psd symmetric matrices.
The Peyrl-Parrilo method is (theoretically!) guaranteed to work IF there exists a rational solution and the underlying SDP is strictly feasible, i.e., there is a solution with full rank.

E. Kaltofen, B. Li, Z. Yang, and L. Zhi have generalized the technique of Peyrl and Parrilo and used these ideas to find sos certificates certifying rational lower bounds for several well-known problems.
Rational sums of squares decompositions

The above algorithms assume that there is a rational sos certificate for \( f \). But maybe one doesn’t exist, even if \( f \) has rational coefficients.

Suppose \( f \in \mathbb{Q}[X] \) is in \( \sum \mathbb{R}[X]^2 \).

Sturmfels asked: Is \( f \in \sum \mathbb{Q}[X]^2 \)?

A trivial, but illustrative example:

\[
2x^2 = (\sqrt{2}x)^2 \in \sum \mathbb{R}[x]^2
\]

\[
2x^2 = x^2 + x^2 \in \sum \mathbb{Q}[x]^2
\]
Recall the Hillar example

\[ f = 3 - 12x - 6x^3 + 18y^2 + 3x^6 + 12x^3y - 6xy^3 + 6x^2y^4, \]

which is in \( \sum \mathbb{R}[X]^2 \).

It turns out that \( f \in \sum \mathbb{Q}[X]^2: \)

\[ f = (x^3 + xy^2 + \frac{3}{2}y - 1)^2 + (x^3 + 2y - 1)^2 + \\
(x^3 - xy^2 + \frac{5}{2}y - 1)^2 + (2y - xy^2)^2 + \frac{3}{2}y^2 + 3x^2y^4 \]

In both of these examples, the sos decompositions in \( \sum \mathbb{Q}[X]^2 \) use more squares than the ones in \( \sum \mathbb{R}[X]^2 \).
Known results on Sturmfel’s question:

- In the univariate case, the answer is “yes” (Landau, Porchet, Schweighofer) and at most 5 squares are needed (Porchet).

- C. Hillar showed that the answer to Sturmfel’s question is “yes” if $f \in \sum K^2$, where $K$ is a totally real extension of $\mathbb{Q}$, and he gave bounds for the number of squares needed.

- There is a simple proof of a slightly more general result with a better bound given (independently) by Kaltofen, Scheiderer, and Quarez.
**Theorem (Scheiderer)**

Let $K/k$ be an extension of real fields of finite degree $d$, and assume that every ordering of $k$ extends to $d$ different orderings of $K$. For every $k$-algebra $A$ and every $f \in A$ which is a sum of $m$ squares in $A_K = A \otimes K$, $f$ is a sum of $dmp$ squares in $A$, where $p$ is the Pythagoras number of $k$, i.e., the smallest number $p$ such that every sum of squares in $k$ is a sum of $p$ squares in $k$.

Note: The Pythagoras number of $\mathbb{Q}$ is 4, i.e., every positive rational can be written as a sum of 4 or fewer squares of rationals.

The general question is still open.
Even assuming that $\mathbb{Q}[X] \cap \sum \mathbb{R}[X]^2 = \sum \mathbb{Q}[X]^2$, there is still a problem: As Hilbert proved, $f \geq 0$ on $\mathbb{R}^n$ does not imply that $f$ is sos. So there might not exist any certificate of positivity for $f$ if we insist on sums of squares of polynomials.

But recall Artin’s Theorem: Every psd $f$ can be written as a quotient $g/h$ where $g, h \in \sum \mathbb{R}[X]^2$.

Even better, Artin’s proof shows that if $f \in \mathbb{Q}[X]$ is psd, then there always exist $g, h \in \sum \mathbb{Q}[X]^2$ such that $f = g/h$. The rationality question is not an issue!
Recent work of Kaltofen, Li, Yang, and Zhi turns Artin’s theorem into a symbolic-numeric algorithm for finding certificates of positivity for any psd \( f \in \mathbb{Q}[X] \).

The algorithm finds a numerical representation of \( f \) as a quotient \( g/h \), where \( g \) and \( h \) are sos, and then converts this to an exact rational identity.

There is even software! ArtinProver.

The authors have used their techniques and the software to settle the dimension 4 case of the Monotone Column Permanent Conjecture.
What can we say about rational certificates of positivity in the compact semialgebraic set case?

Fix $G = \{g_1, \ldots, g_k\} \subseteq \mathbb{R}[X]$ and let $S = S(G)$, the basic closed semialgebraic set generated by $G$, $M = M(G)$, the quadratic module generated by $G$, and $P = PO(G)$, the preorder generated by $G$.

Question: Suppose $G \subseteq \mathbb{Q}[X], f \in \mathbb{Q}[X]$, and $f > 0$ on $S$. Does there exist a rational certificate of positivity for $f$ on $S$?
Theorem

Given $G \subseteq \mathbb{Q}[X]$ and suppose $S = S(G)$ is compact. Then for any $f \in \mathbb{Q}[X]$ such that $f > 0$ on $S$, there is a representation of $f$ in the preordering $PO(G)$,

$$f = \sum_{e \in \{0,1\}^s} \sigma_e g_1^{e_1} \cdots g_s^{e_s},$$

with all $\sigma_e \in \sum \mathbb{Q}[X]^2$.

The proof follows from an algebraic proof of Schmüdgen’s Theorem, due to T. Wörmann, which uses the Abstract Positivstellensatz.
For Putinar’s Theorem, we have:

**Theorem**

Suppose $G = \{g_1, \ldots, g_s\} \subseteq \mathbb{Q}[X]$ and $N - \sum X_i^2 \in M$ for some $N \in \mathbb{N}$. Then given any $f \in \mathbb{Q}[X]$ such that $f > 0$ on $S$, there exist $\sigma_0 \ldots \sigma_s, \sigma \in \sum \mathbb{Q}[X]^2$ so that

$$f = \sigma_0 + \sigma_1 g_1 + \cdots + \sigma_s g_s + \sigma(N - \sum X_i^2).$$

This follows by carefully analyzing an algorithmic proof of Putinar’s Theorem due to Schweighofer, which involves reducing to Pólya’s Theorem for forms positive on the standard simplex. We follow the proof, making sure each step preserves rationality.
**Open question:** If $G \subseteq \mathbb{Q}[X]$ and $N - \sum X_i^2 \in M$, can we find a certificate of positivity for $N - \sum X_i^2$ in $M$ with so that the sos’s are in $\sum \mathbb{Q}[X]^2$?
In theory, rational certificates of positivity exist for globally positive polynomials and for polynomials strictly positive on compact basic semialgebraic sets.

There are many interesting applications of certificates of positivity.

Using hybrid symbolic-numeric algorithms, certificates of positivity can be found in practice.

Thanks for listening!