

$$f \in \Sigma \mathbb{R}[X]^2 \implies f \in \Sigma \mathbb{Q}[X]^2$$

Rational Sums of Squares

Christopher Hillar
(Texas A&M University)

Motivational Problem

In 1975, Bessis, Moussa, and Villani (BMV) introduced a positivity conjecture while studying partition functions of quantum mechanical systems.

Fix A, B to be $n \times n$ positive semidefinite matrices (symmetric, nonnegative eigenvalues)

Conjecture [BMV]: For each m , the polynomial in t

$$p(t) = \text{tr}[(A+tB)^m]$$

has nonnegative coefficients

Example: If $m = 2$, then conjecture BMV asserts

$$\text{tr}[(A+tB)^2] = \text{tr}[B^2] t^2 + \text{tr}[AB+BA] t + \text{tr}[A^2]$$

Sums of Squares

Definition: Focusing on individual coefficients, we define matrices

$$S_{m,k}(A,B) = [t^k] (A + tB)^m,$$

the sum of all length m words in A and B with k B s.

$$S_{2,1}(A,B) = AB + BA$$

$$S_{3,2}(A,B) = ABB + BAB + BBA$$

Assuming A, B positive semidefinite is the same as having $A = X^2$, $B = Y^2$ for symmetric matrices X, Y

Sums of Squares

Example: $\text{Tr}[S_{3,2}(X^2, Y^2)] = 3\text{Tr}[(XY^2)(XY^2)^T]$

This turns the problem into one of noncommutative algebra

Defintion: $f(X, Y)$ is *cyclically equivalent* to $g(X, Y)$ if one can go from f to g by cycling monomials

E.g. $XY^2 + XY \sim YXY + XY \sim YYX + YX$

Question: Is $S_{m,k}(X^2, Y^2)$ cyclically equivalent to a noncommutative sum of squares?

If so, then $\text{Tr}[S_{m,k}] \geq 0$ for all PSD matrices X, Y

Gram matrices and SOS

Example [Haegele 07]: $S_{7,3}$ is cyclically equivalent to $7(YX^4Y^2)(YX^4Y^2)^T + 7(X^2Y^2X^2Y + X^4Y^3)(X^2Y^2X^2Y + X^4Y^3)^T$

In general, this question can be solved by a semidefinite program (Schor, Parrilo, Helton,...)

Idea: Find a vector V of monomials in X, Y and a positive semidefinite (Gram) matrix G such that

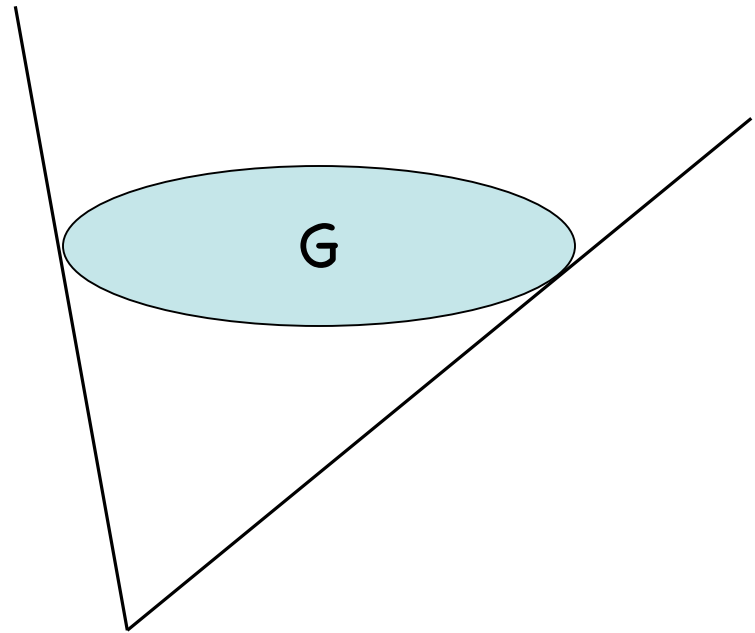
$$f \sim V^T G V$$

This is a system of linear equalities and a PSD condition on G .

SDP and SOS

$$f \sim V^T G V$$

This is a set of linear equations in the entries of G along with a PSD condition on G



There are fast numerical interior point Semidefinite Program solvers (SeDumi) that can find this G (numerically)

SDP and SOS

Problem: Need **exact** (rational) certificates, but SDP solvers are numerical.

Theorem [Klep, Schweighofer 08]: The BMV conjecture is true for $m = 13$ (also, there are **no certificates** whatsoever for $m = 6, k = 3$)

Theorem [H07]: If the BMV conjecture is true for a power m , then it is true for all $m' < m$

Corollary: BMV is true for all $m \leq 13$

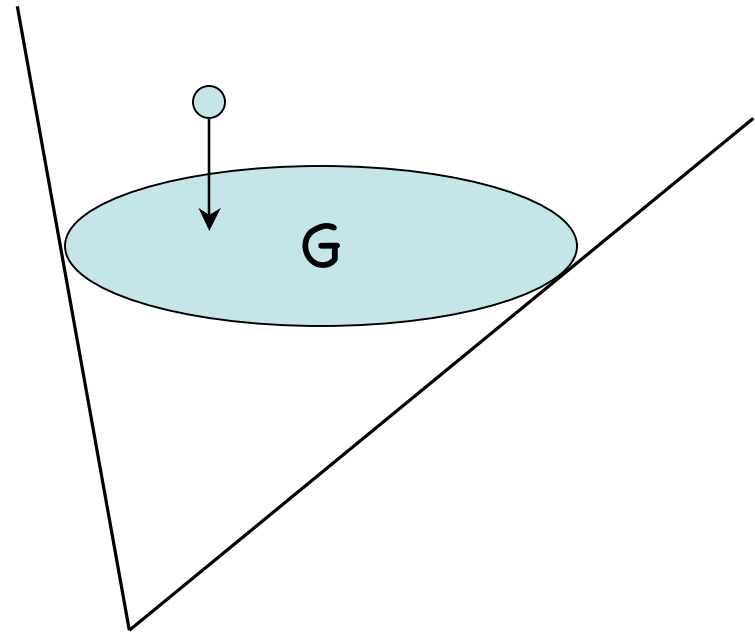
- Any new certificates give the current best result (and works for all sizes of matrices)

Rational SDP

Parillo and Peyrl have a package in Macaulay 2 that tries to find rational SOS SDP solutions

The idea is to find a numerical solution, round it to a rational one, then project back onto the linear space of equations

In general, need a theorem guaranteeing a rational solution always exists (if set of G has no interior)



Commutative Example

Problem: Is the following polynomial nonnegative:

$$f = 3 - 12y - 6x^3 + 18y^2 + 3x^6 + 12x^3y - 6xy^3 + 6x^2y^4$$

Maybe SDP says **yes** it is an SOS numerically:

$$\begin{aligned} f = & (x^3 + 3.53y + .347xy^2 - 1)^2 \\ & + (x^3 + .12y + 1.53xy^2 - 1)^2 \\ & + (x^3 + 2.35y + -1.88xy^2 - 1)^2 \end{aligned}$$

But $(f - \text{RHS})$ has terms like $-.006xy^2$ which are small but nonzero

We need **exact** certificates for an algebraic proof

Rational sum of squares

It turns out that we are approximating an SOS:

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

where a, b, c are real and roots of the equation
 $u(x) = x^3 - 3x + 1$

Question [Sturmfels]: If f is a polynomial with rational coefficients that is a real nonnegative sum of squares, then is f a rational sum of squares?

In our example, it turns out that f equals

$$(x^3 + xy^2 + 3y/2 - 1)^2 + (x^3 + 2y - 1)^2 + (x^3 - xy^2 + 5y/2 - 1)^2 \\ + (2y - xy^2)^2 + 3y^2/2 + 3x^2y^4$$

Known Results

- It follows from Artin's solution of Hilbert's 17th problem that f is a sum of rational functions with rational entries
- The result is true in the univariate case (Landau, Pourchet, Schweighofer) and 5 squares suffice
- For more variables, it is known that no fixed number of squares suffice (Choi, Dai, Lam, Reznick)
- It is enough to assume that f is a sum of squares over some real finite algebraic extension of \mathbb{Q} (quantifier elimination for real closed fields)

Totally Real SOS

Let K be a finite algebraic field extension of \mathbb{Q} .

Definition: K is called *totally real* if all its complex embeddings are real.

Equivalently, K is a field generated by a root of an irreducible polynomial $u(x) \in \mathbb{Q}[x]$, all of whose zeroes are real.

Example: $K = \mathbb{Q}(a,b,c)$ where $x^3+3x-1 = (x-a)(x-b)(x-c)$

Example: Any field generated by square roots of positive rational numbers

Totally Real SOS

Although the general case is still open, when K is a totally real field extension of Q , we have

Theorem [H08]: If $f \in Q[x_1, \dots, x_n]$ is a sum of squares over $K[x_1, \dots, x_n]$, then it is a sum of squares over $Q[x_1, \dots, x_n]$

In fact, if f is a sum of m squares over K , then it is a sum of

$$4m \cdot 2^{[K:Q]+1} \binom{[K:Q]+1}{2}$$

squares over Q

Proof Ideas

Step 1: Assume that K is a Galois extension of \mathbb{Q}

- A Galois closure of a totally real field is also totally real

Step 2: Sum f over all actions σf for σ in

$G = \text{Gal}(K/\mathbb{Q})$, the Galois group of K over \mathbb{Q}

- Reduces the problem to finding a rational SOS of the trace form of a polynomial $p \in K[x_1, \dots, x_n]$:

$$f = \sum_{\sigma \in G} (\sigma p)^2$$

Proof Ideas

Step 3: Vandermonde factorization

Set $K = \mathbb{Q}(u)$, then trace form may be written as

$$f = V^T M^T M V$$

for vector of rational polynomials V and a Vandermonde matrix M in the numbers σu , where σ runs over the Galois group G of K

Using ideas of Ilyusheckin, we can factor M as

$$M = C^T C$$

for a matrix C with entries in $\mathbb{Q}(\sqrt{r_1}, \dots, \sqrt{r_s})$ for positive integers r_i

Proof Ideas

Note: this already shows that f is a sum of squares over the field $\mathbb{Q}(\sqrt{r_1}, \dots, \sqrt{r_s})$

Step 4: (Special case) totally real field $\mathbb{Q}(\sqrt{r_1}, \dots, \sqrt{r_s})$

- this is done inductively on the integer s

For example, if $f = (p + q\sqrt{2})^2$ for some $p, q \in \mathbb{Q}[x_1, \dots, x_n]$, then

$$2f = f + \sigma f = p^2 + 2q^2$$

Example revisited

Example: $K = Q(a,b,c)$ where $x^3+3x-1 = (x-a)(x-b)(x-c)$

$$f = V^T C^T C V = (C V)^T C V$$

$$C^T = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 0 \\ -1/2 & 0 & 1/2 & -1 & -\sqrt{6}/2 & -\sqrt{3} \\ 3/2 & 2 & 5/2 & 2 & \sqrt{6}/2 & 0 \end{bmatrix}$$

$$V^T = [x^3+2xy^2-1, -xy^2, y-xy^2]$$

$$f = (x^3+xy^2+3y/2-1)^2 + (x^3+2y-1)^2 + (x^3-xy^2+5y/2-1)^2 \\ + (2y-xy^2)^2 + 3y^2/2 + 3x^2y^4$$

Open Problems

1. Try to work out the case of algebraic extensions with abelian Galois group (class field theory)
2. Find a smaller bound for the number of squares over \mathbb{Q}
3. The general case?

The End

(of talk)