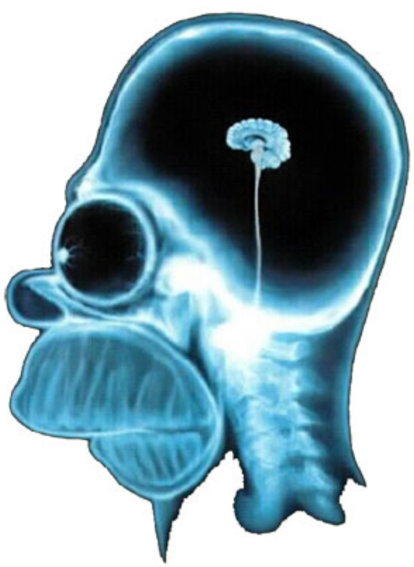
$$f \in \Sigma\mathbb{R}[X]^2 \quad \Longrightarrow \quad f \in \Sigma\mathbb{Q}[X]^2$$

Rational Sums of Squares and Applications

Christopher Hillar
(MSRI & Berkeley)



A 2008 study found that adding a picture of a brain
scan to a scientific argument about human nature
made the general public more likely to be believe it
even if brain activity wasn't relevant to the point being made.

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

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

has nonnegative coefficients

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

$$\mathrm{Tr}[(A+tB)^2] = \mathrm{Tr}[B^2]\, t^2 + \mathrm{Tr}[AB+BA]\, t + \mathrm{Tr}[A^2] \quad \in \mathbb{R}_+[t]$$

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 Bs.

$$S_{2,1}(A,B) = AB + BA$$
$$S_{3,2}(A,B) = ABB + BAB + BBA$$

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

Sums of Squares

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

Turns problem into one of noncommutative algebra

Defintion: Noncommutative polynomial f(X,Y) is *cyclically equivalent* to g(X,Y) if one can go from f to g by cycling monomials (then Tr[f(A,B)] = Tr[g(A,B)])

E.g. XYY + XY ~ YXY + XY ~ YYX + YX

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

If so, $\mathrm{Tr}[S_{m,k}(A,B)] \geq 0$ for all PSD **matrices** A,B (and any size n!)

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 (Parrilo, Helton,...)

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

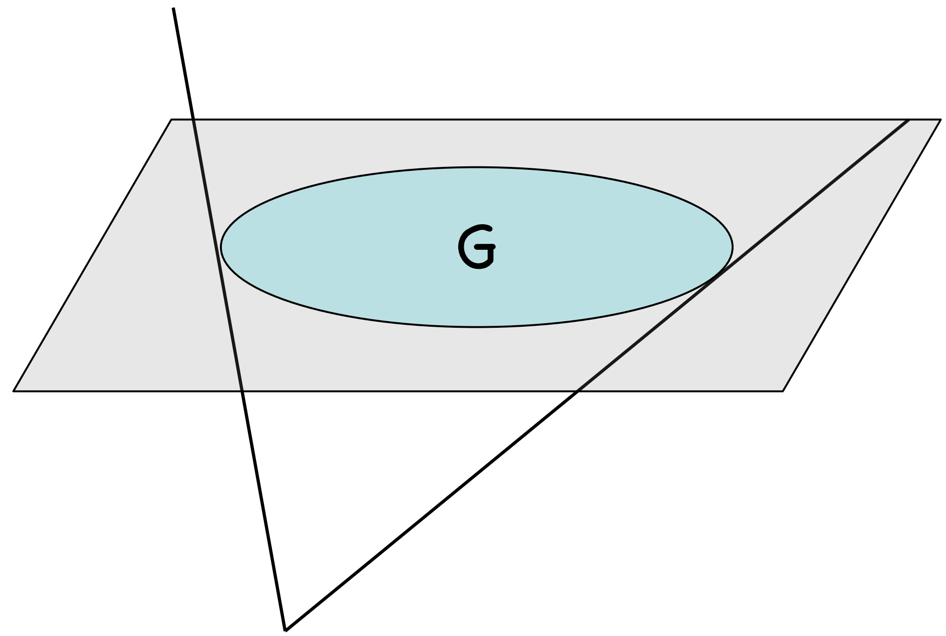
$$f \sim V^T G V$$

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 (e.g. 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 $m \leq 13$

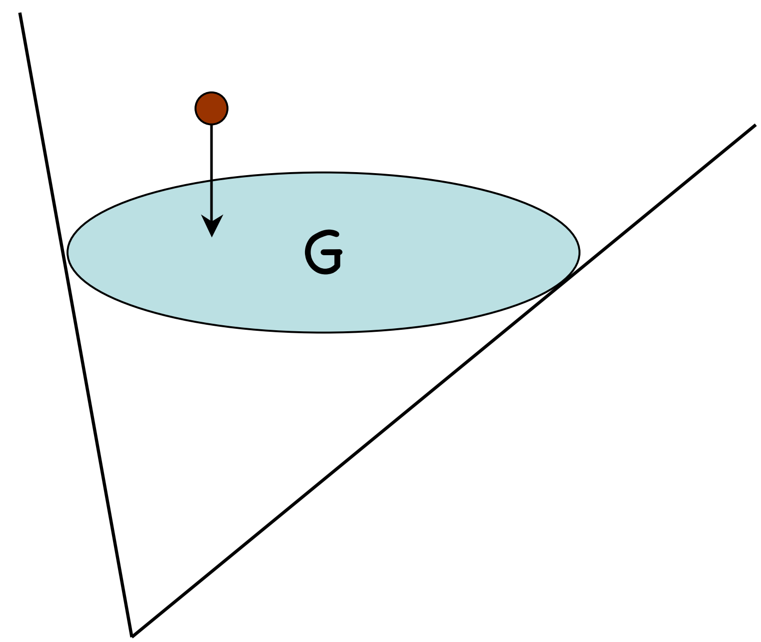
- Any new certificates give the current best result (and works for all sizes of matrices)

(Closed) Problem: Find SOS for $S_{m,k}$ with both m,k even
[Collins,Dykema,Torres-Ayala 09]: No SOS m > 16 ;(

Rational SDP

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

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)

Other algorithms for rational SOS: [Zhi,Ei Din 09], [Monniaux 10]

Rational SDP

Example Gram matrix certificate

$$
\begin{bmatrix}
\frac{5}{2} & \frac{5}{2} & \frac{13}{3} & \frac{23}{2} & 0 & \frac{14}{3} & \frac{14}{3} & -\frac{5}{2} & -\frac{1}{2} & 0 & \frac{14}{3} & \frac{14}{3} & 0 & \frac{14}{3} & \frac{14}{3} & \frac{14}{3} & -\frac{16}{3} & -5 & 28 \\
-\frac{77}{90} & -\frac{77}{90} & -\frac{7}{6} & \frac{9}{5} & 1 & -2 & -2 & 1 & -\frac{10}{3} & -2 & -2 & -2 & -2 & -2 & -2 & -2 & 1 & \frac{7}{2} & \frac{14}{3} \\
-\frac{77}{90} & -\frac{77}{90} & -\frac{7}{6} & \frac{9}{5} & 1 & -2 & -2 & 1 & -\frac{10}{3} & -2 & -2 & -2 & -2 & -2 & -2 & -2 & 1 & \frac{7}{2} & \frac{14}{3} \\
-\frac{77}{90} & -\frac{77}{90} & -\frac{7}{6} & \frac{9}{5} & 1 & -2 & -2 & 1 & -\frac{10}{3} & -2 & -2 & -2 & -2 & -2 & -2 & -2 & 1 & \frac{7}{2} & \frac{14}{3} \\
0 & 0 & -1 & -1 & -\frac{13}{4} & -2 & -2 & 1 & -\frac{31}{27} & -2 & -2 & -2 & -2 & -2 & -2 & -2 & \frac{11}{2} & -\frac{1}{4} & 0 \\
-\frac{77}{90} & -\frac{77}{90} & -\frac{7}{6} & \frac{9}{5} & 1 & -2 & -2 & 1 & -\frac{10}{3} & -2 & -2 & -2 & -2 & -2 & -2 & -2 & 1 & \frac{7}{2} & \frac{14}{3} \\
-\frac{77}{90} & -\frac{77}{90} & -\frac{7}{6} & \frac{9}{5} & 1 & -2 & -2 & 1 & -\frac{10}{3} & -2 & -2 & -2 & -2 & -2 & -2 & -2 & 1 & \frac{7}{2} & \frac{14}{3} \\
0 & 0 & -1 & -1 & -\frac{13}{4} & -2 & -2 & 1 & -\frac{31}{27} & -2 & -2 & -2 & -2 & -2 & -2 & -2 & \frac{11}{2} & -\frac{1}{4} & 0 \\
-\frac{28829}{4480} & -\frac{28829}{4480} & -\frac{55591}{20007} & -8 & 0 & -\frac{10}{3} & -\frac{10}{3} & \frac{7}{2} & -\frac{757}{81} & -\frac{31}{27} & -\frac{10}{3} & -\frac{10}{3} & -\frac{31}{27} & -\frac{10}{3} & -\frac{10}{3} & -\frac{10}{3} & 6 & 4 & -\frac{1}{2} \\
0 & 0 & \frac{9}{2} & -\frac{229}{81} & -\frac{1327}{972} & 1 & 1 & \frac{109987}{10080} & \frac{7}{2} & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 18 & \frac{3}{2} & -\frac{5}{2} \\
-\frac{77}{90} & -\frac{77}{90} & -\frac{7}{6} & \frac{9}{5} & 1 & -2 & -2 & 1 & -\frac{10}{3} & -2 & -2 & -2 & -2 & -2 & -2 & -2 & 1 & \frac{7}{2} & \frac{14}{3} \\
-\frac{77}{90} & -\frac{77}{90} & -\frac{7}{6} & \frac{9}{5} & 1 & -2 & -2 & 1 & -\frac{10}{3} & -2 & -2 & -2 & -2 & -2 & -2 & -2 & 1 & \frac{7}{2} & \frac{14}{3} \\
0 & 0 & \frac{99031}{13440} & -\frac{44}{3} & -\frac{1240243}{162000} & 1 & 1 & -\frac{1327}{972} & 0 & -\frac{13}{4} & 1 & 1 & -\frac{13}{4} & 1 & 1 & 1 & \frac{85}{27} & 7 & 0 \\
-\frac{413}{180} & -\frac{413}{180} & \frac{1369}{180} & -\frac{195323}{22050} & -\frac{44}{3} & \frac{9}{5} & \frac{9}{5} & -\frac{229}{81} & -8 & -1 & \frac{9}{5} & \frac{9}{5} & -1 & \frac{9}{5} & \frac{9}{5} & \frac{9}{5} & \frac{22}{9} & 2 & \frac{23}{2} \\
1 & 1 & 6 & \frac{1369}{180} & \frac{99031}{13440} & -\frac{7}{6} & -\frac{7}{6} & \frac{9}{2} & -\frac{55591}{20007} & -1 & -\frac{7}{6} & -\frac{7}{6} & -1 & -\frac{7}{6} & -\frac{7}{6} & -\frac{7}{6} & 2 & 4 & \frac{13}{3} \\
-\frac{2246}{315} & -\frac{2246}{315} & 1 & -\frac{413}{180} & 0 & -\frac{77}{90} & -\frac{77}{90} & 0 & -\frac{28829}{4480} & 0 & -\frac{77}{90} & -\frac{77}{90} & 0 & -\frac{77}{90} & -\frac{77}{90} & -\frac{77}{90} & 0 & 0 & \frac{5}{2} \\
-\frac{2246}{315} & -\frac{2246}{315} & 1 & -\frac{413}{180} & 0 & -\frac{77}{90} & -\frac{77}{90} & 0 & -\frac{28829}{4480} & 0 & -\frac{77}{90} & -\frac{77}{90} & 0 & -\frac{77}{90} & -\frac{77}{90} & -\frac{77}{90} & 0 & 0 & \frac{5}{2}
\end{bmatrix}
$$

Other Applications SOS

- Copositivity of matrices
- Global optimization of polynomial functions

(and generally, optimization over semialgebraic sets)

- Control of Nonlinear Systems via Lyapunov Functions
- Inequalities in probability theory
- Mixed continuous-discrete optimization
- Distinguishing separable from entangled states in quantum systems
- Geometric theorem proving
- SOS modulo Gradient Ideals (Nie, Demmel, Sturmfels)

...

Commutative Example

Problem: Is the polynomial globally 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 - 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 (Pourchet)

- 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 Q (quantifier elimination for real closed fields)

Known Results

- If there is a positive definite gram matrix for f, then there is a rational SOS for f

$$f = v^T G v = v^T S v \qquad (S = S^T)$$

$$S = \{S_0 + t_1 S_1 + \dots t_k S_k : t_i \text{ real}\}$$

- The real Nullstellensatz has rational certificates (essentially Artin's original proof)

- [Powers 09] There are rational analogues of Putinar and Schmudgen's theorems

Totally Real SOS

Let K be a finite algebraic field extension of 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 $u(x) \in Q[x]$, all of whose zeroes are real.

Example: $K = Q(a,b,c)$ 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 $f \in Q[x_1,\ldots,x_n]$ is a sum of squares over $K[x_1,\ldots,x_n]$, then it is a sum of squares over $Q[x_1,\ldots,x_n]$

Remark: Recenly, Kaltofen, Scheiderer, Quarez have found another proof of this fact that gives better bounds for the number of squares needed.

Open Problem: algebraic extensions with abelian Galois group (class field theory)? General case?

Spectrahedron

Definition: Spectrahedron is the feasiblity set of a semidefinite program: Let $A_0,\ldots,A_n$ real m x m symmetric

$$\{ (x_1,\ldots,x_n) : A_0 + x_1A_1 + \cdots + x_nA_n \geq 0 \}$$

Open Problem: Determine those real algebraic numbers that can be given as a finite spectrahedron with n variables. Even for $n = 1$ not known:

What algebraic numbers are given as the unique element of some set with A being a symmetric matrix:

$$S = \{ (x,y) : x + yA \text{ is positive semidefinite } \}$$

Known [Laurent,…]: All real algebraic (as m,n vary)

Spectrahedron

Definition: Spectrahedron is the feasiblity set of a semidefinite program: $A_0,\ldots,A_n$ rational m x m symmetric

$$\{ (x_1,\ldots,x_n) : A_0 + x_1A_1 + \cdots + x_nA_n \geq 0 \}$$

Open Problem: Determine those real algebraic numbers that can be given as a finite spectrahedron with n variables. Even for n = 1 not known:

What algebraic numbers are given as the unique element of some set with A being a symmetric matrix:

$$S = \{ (x,y) : x + yA \text{ is positive semidefinite } \}$$

Known [Laurent,...]: All real algebraic (as m,n vary)

The End

(of talk)