Symmetry groups, sums of squares and semidefinite programs

Pablo A. Parrilo
Institut für Automatik
ETH Zürich

Joint work with **Karin Gatermann** (ZIB Berlin)

Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Outline

- Nonnegativity of polynomials.
- Infeasibility of real equations: Positivstellensatz.
- Sums of squares and the P-satz. Finding certificates using SDP.
- Exploiting structure. Groups and symmetries.
- Representation theory and an invariant-theoretic viewpoint.
- Sums of squares on invariant rings.
- Computing with invariants. Symmetric representations.
- An example in geometric theorem proving.

Nonnegativity of polynomials

How to check if a given $F(x_1, \ldots, x_n)$ (of even degree) is globally nonnegative?

$$F(x_1, x_2, \ldots, x_n) \geq 0, \quad \forall x \in \mathbb{R}^n$$

- For $d = 2$, easy (check eigenvalues). What happens in general?
- It is decidable, but NP-hard when $d \geq 4$.
- Possible approaches: Decision algebra, Tarski-Seidenberg, quantifier elimination, etc. Very powerful, but bad complexity properties.
- *Lots* of applications.
- Want "low" complexity, at the cost of possibly being conservative.

A sufficient condition

A "simple" sufficient condition: a sum of squares (SOS) decomposition:

$$F(x) = \sum_i f_i^2(x)$$

If $F(x)$ can be written as above, for some polynomials f_i, then $F(x) \geq 0$.

A purely synctactic, easily verifiable certificate.

Is this condition conservative? Can we quantify this?

- In some cases (for example, polynomials in one variable), it is exact.
- Known counterexamples, but perhaps "rare" (ex. Motzkin, Reznick 99, etc.)

Can we compute it efficiently?

- Yes, using semidefinite programming.

Checking the SOS condition

Given $F(x)$, degree $2d$.

Basic method, the "Gram matrix" (Shor 87, Choi-Lam-Reznick 95, Powers-Wörmann 98, Nesterov, Lasserre, etc.)

Let z be a suitably chosen vector of monomials (in the dense case, all monomials of degree $\leq d$).

Then, F is SOS iff:

$$F(x) = z^T Q z, \qquad Q \succeq 0$$

- Comparing terms, obtain linear equations for the elements of Q.
- Can be solved as a semidefinite program (with equality constraints).
- Factorize $Q = L^T L$. The SOS is given by $f = Lz$.

Example

$$\begin{aligned} F(x,y) &= 2x^4 + 5y^4 - x^2y^2 + 2x^3y \\ &= \begin{bmatrix} x^2 \\ y^2 \\ xy \end{bmatrix}^T \begin{bmatrix} q_{11} & q_{12} & q_{13} \\ q_{12} & q_{22} & q_{23} \\ q_{13} & q_{23} & q_{33} \end{bmatrix} \begin{bmatrix} x^2 \\ y^2 \\ xy \end{bmatrix} \\ &= q_{11}x^4 + q_{22}y^4 + (q_{33} + 2q_{12})x^2y^2 + 2q_{13}x^3y + 2q_{23}xy^3 \end{aligned}$$

An SDP with equality constraints. Solving, we obtain:

$$Q = \begin{bmatrix} 2 & -3 & 1 \\ -3 & 5 & 0 \\ 1 & 0 & 5 \end{bmatrix} = L^T L, \qquad L = \frac{1}{\sqrt{2}} \begin{bmatrix} 2 & -3 & 1 \\ 0 & 1 & 3 \end{bmatrix}$$

And therefore

$$F(x,y) = \frac{1}{2}(2x^2 - 3y^2 + xy)^2 + \frac{1}{2}(y^2 + 3xy)^2$$

Using SOSTOOLS: `[Q,Z]=findsos(2*x^4+5*y^4-x^2*y^2+2*x^3*y)`

Polynomial systems over the reals

- When does a system of equations and inequalities have real solutions?
- A remarkable answer: the Positivstellensatz.
- A fundamental theorem in real algebraic geometry, due to Stengle.
- A common generalization of Hilbert's Nullstellensatz and LP duality.
- Guarantees the existence of infeasibility certificates for real solutions of systems of polynomial equations.
- Sums of squares are a fundamental ingredient.

How does it work?

P-satz and SDP

Given $\{x \in \mathbb{R}^n \mid f_i(x) \geq 0, \quad h_i(x) = 0\}$. Define:

$$\text{Cone}(f_i) = \sum s_i \cdot (\prod_j f_j), \qquad \text{Ideal}(h_i) = \sum t_i \cdot h_i,$$

where the $s_i, t_i \in \mathbb{R}[x]$ and the s_i are sums of squares.

To prove infeasibility, find $f \in \text{Cone}(f_i), h \in \text{Ideal}(h_i)$ such that

$$f + h = -1.$$

- Can find certificates by solving SDPs!
- A complete SDP hierarchy, given by certificate degree (P. 2000).
- Tons of applications:
  optimization, dynamical systems, quantum mechanics...

Exploiting structure

Crucial for good performance. What algebraic properties can we profit of?

- Sparseness: few nonzero coefficients.
  - Newton polytopes techniques.
- Ideal structure: equality constraints.
  - SOS on *quotient rings*.
  - Compute in the coordinate ring. Quotient bases (Gröbner).
- Symmetries: invariance under a group.
  - SOS on *invariant rings*
  - Representation theory and invariant-theoretic methods.
  - Enabling factor in applications.

In this talk, we focus on this last case.

Symmetries

Symmetry is invariance under a group of transformations (*automorphisms*).

General advantages of exploiting symmetries:

- Smaller, more compact representations.
- Eliminates eigenvalue multiplicities.
- Faster, better conditioned, more robust numerically.
- Collapse group-conjugate solutions.

Huge benefits in many areas: dynamical systems, bifurcation theory, PDEs, geometric mechanics, etc...

Exploitation of symmetries is an enabling factor in applications.

What's a symmetry group? What can be done in SDP/SOS?

Symmetry groups

A group is a set G with a binary operation $G \times G \to G$.

Associative, with identity and inverse.

In general, can be finite, or infinite.

Examples: The group operation is matrix multiplication.

- A finite collection $\mathcal{T}$ of matrices $T_i, i = 1, \ldots, n$, satisfying

$$I \in \mathcal{T}, \qquad T_i T_j \in \mathcal{T} \quad \forall i, j, \qquad T_i^{-1} \in \mathcal{T} \quad \forall i.$$

- The group $O(n)$ of unitary matrices $U^T U = I$.

- The set of diagonal matrices $D = \text{diag}(d_1, d_2, \ldots, d_n)$.

The first two groups are compact sets, but the third one is not.

Symmetry reduction

In practice, many problems are invariant under a group of transformations.

$$p(x) = p(Tx), \qquad \forall T \in \mathcal{T}$$

where $\mathcal{T} \subseteq GL(\mathbb{R}^n)$ is a matrix group.

- Ex: $\min x^4 + y^4 + z^4 - 4xyz + x + y + z$.
  Invariant under permutations of x, y, z:

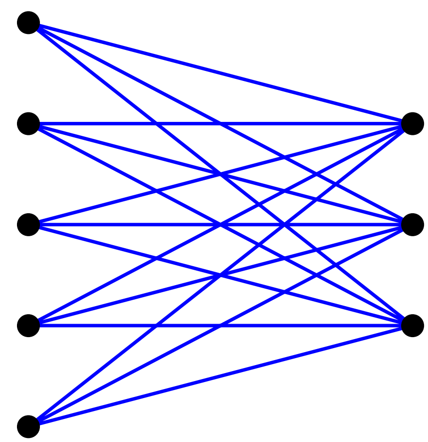
$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}.$$

- Ex: Nonnegativity of even forms (copositivity).

What are the geometric, algebraic, and computational implications?

Example

From Boyd's talk, past Monday. Our thanks to Stephen and Lin Xiao.



The fastest Markov chain in a graph.

An (n, m) complete bipartite graph ($n \geq m$).

The mixing rate depends on the eigenvalues of the associated matrix.
Their question: how to design the transition probs to maximize the rate?

The complete bipartite graph has a $S_n \times S_m$ automorphism group.

Invariant SDPs

If $\mathcal{L}$ is an affine subspace of $\mathcal{S}^n$, and $C, X \in \mathcal{S}^n$, an SDP is given by:

$$\min \langle C, X \rangle \qquad \text{s.t.} \quad X \in \mathcal{L} \cap \mathcal{S}^n_+$$

Definition: Given a finite group G, and associated representation σ, a σ-*invariant SDP* is one where both the feasible set and the cost function are invariant under the group action.

That is:

$$\langle C, X \rangle = \langle C, T(g)X \rangle, \qquad \forall g \in G, \qquad\qquad X \in \mathcal{S} \Rightarrow T(g)X \in \mathcal{S} \qquad \forall g \in G$$

Example:

$$\min a + c, \qquad \text{s.t.} \quad \begin{bmatrix} a & b \\ b & c \end{bmatrix},$$

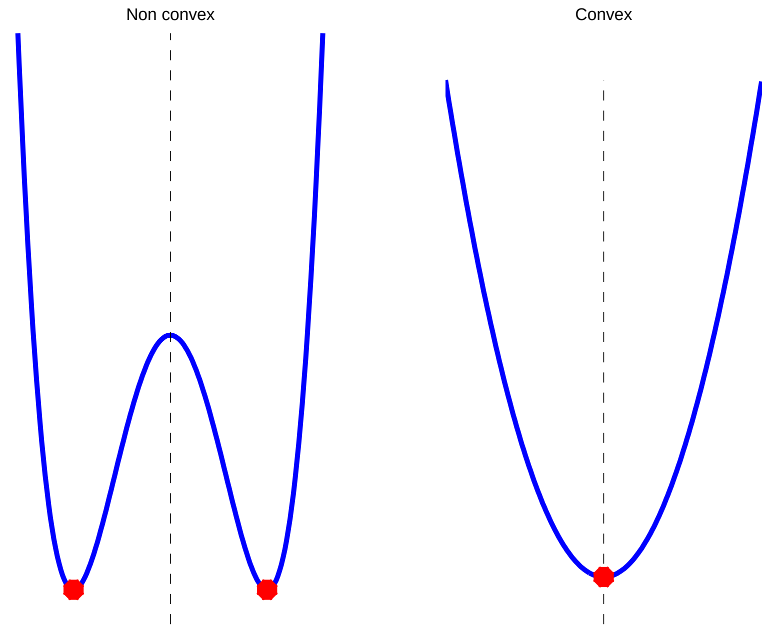
invariant under the Z_2 action generated by: $\begin{bmatrix} X_{11} & X_{12} \\ X_{12} & X_{22} \end{bmatrix} \to \begin{bmatrix} X_{22} & -X_{12} \\ -X_{12} & X_{11} \end{bmatrix}$.

Symmetry and convexity

Key property of symmetric convex sets: the "group average" $\frac{1}{|G|}\sum_{g \in G} \sigma(g)x$ always belongs to the set.

So, in convex optimization we can always restrict the solution to the fixed-point subspace

$$\{x | \sigma(g)x = x, \quad \forall g \in G\}.$$



Instead of looking for solutions in the original space, use the orbit (quotient) space.

The fixed point subspace

Is the set of elements invariant under the group. For convex problems, the solution is always there.

Earlier example:

$$\min a + c, \qquad \text{s.t.} \quad \begin{bmatrix} a & b \\ b & c \end{bmatrix},$$

invariant under the Z_2 action generated by: $\begin{bmatrix} X_{11} & X_{12} \\ X_{12} & X_{22} \end{bmatrix} \to \begin{bmatrix} X_{22} & -X_{12} \\ -X_{12} & X_{11} \end{bmatrix}$.

The fixed point subspace are matrices of the form $\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix}$, so the problem reduces to:

$$\min 2a, \qquad \text{s.t.} \quad 2a \geq 0.$$

A special representation: Let $\rho : G \to GL(\mathbb{R}^n)$ be a representation of the group G, and let $\sigma : G \to GL(\mathcal{S}_n)$ be the induced representation through

$$\sigma(g)M := \rho(g)^T M \rho(g), \quad \forall\, g \in G.$$

Restriction to the fixed point

In SDP, the restriction to the fixed-point subspace takes the form:

$$\sigma(g)M = M \qquad \Longrightarrow \qquad \rho(g)M - M\rho(g) = 0, \quad \forall g \in G. \tag{1}$$

The Schur lemma of representation theory exactly characterizes the matrices that commute with a group action.

Example: circulant matrices.

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & a_4 \\ a_4 & a_1 & a_2 & a_3 \\ a_3 & a_4 & a_1 & a_2 \\ a_2 & a_3 & a_4 & a_1 \end{bmatrix}, \quad Z = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

- A cyclic group $\{Z, Z^2, Z^3, Z^4 = I\}$, and $AZ^k - Z^kA = 0$.
- There exists a change of coordinates (the Fourier matrix) under which *all* matrices A are diagonal (scalar distinct blocks).

Decomposing the problem

In the general case, the blocks are not necessarily scalar, or distinct.

Using Schur's lemma, every group representation decomposes as a direct sum of N irreducible representations:

$$\rho = m_1\vartheta_1 \oplus m_2\vartheta_2 \oplus \cdots \oplus m_N\vartheta_N$$

where $m_1, \ldots, m_N$ are the multiplicities. Therefore, an isotypic decomposition:

$$\mathbb{C}^n = V_1 \oplus \cdots \oplus V_N, \qquad V_i = V_{i1} \oplus \cdots \oplus V_{in_i}.$$

In the symmetry-adapted basis, matrix M in (1) has a block diagonal form:

$$M = (I_{m_1} \otimes M_1) \oplus \ldots \oplus (I_{m_N} \otimes M_N)$$

Not only the SDP block-diagonalizes, but also many blocks are identical!

Reduction

In the new coordinates (for instance),

$$TMT^T = \begin{bmatrix} M_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & M_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & M_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & M_2 & 0 & 0 \\ 0 & 0 & 0 & 0 & M_3 & 0 \\ 0 & 0 & 0 & 0 & 0 & M_3 \end{bmatrix}$$

- The coordinate transformation depends *only on the group*, and not on the problem data.
- Smaller, coupled problems.
- But, instead of checking if a big matrix is PSD, we can just use the M_i.

Example

$$\min c_1 + c_2, \qquad \text{s.t.} \begin{bmatrix} a & b & b \\ b & c_1 & d \\ b & d & c_2 \end{bmatrix} \geq 0 \tag{2}$$

SDP is invariant under permutation of the last two rows and columns. To restrict the problem to the stable subspace, we impose the constraint $c_1 = c_2 = c$, obtaining:

$$\min 2c, \qquad \text{s.t.} \begin{bmatrix} a & b & b \\ b & c & d \\ b & d & c \end{bmatrix} \geq 0 \tag{3}$$

Now, the block diagonalization procedure can be applied, and the constraint simplified to:

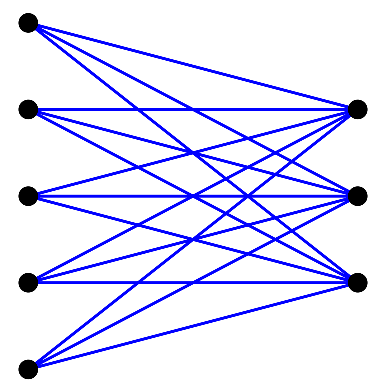
$$\text{minimize } 2c, \qquad \text{s.t.} \begin{bmatrix} a & \sqrt{2}b \\ \sqrt{2}b & c+d \end{bmatrix} \geq 0, \qquad c - d \geq 0 \tag{4}$$

Boyd's example

The fixed-point reduced SDP looks like:

$$\begin{bmatrix} I_n - mp & p\,E_{n\times m} \\ p\,E_{m\times n} & I_m - np \end{bmatrix}$$

Let's decompose it!



Irreps of the symmetric group are well-known, so $S_n \times S_m$ is easy.
Only three appear nontrivially, and after changing coordinates we have:

$$\begin{bmatrix} 1 - np & p\sqrt{nm} \\ p\sqrt{nm} & 1 - mp \end{bmatrix}, \qquad I_{n-1} \otimes (1 - mp), \qquad I_{m-1} \otimes (1 - np).$$

Can easily solve now: $p_{\text{opt}} = \min\left(\frac{1}{n}, \frac{2}{n+2m}\right)$.

SOS and invariant theory

Even more special structure: the representation ρ in $\mathbb{R}^n$ induces another representation τ of G the space of monomials, via $\tau m(x) := m(\rho x)$.

This brings in invariant theory: the study of the ring of invariant polynomials.

What happens with SOS?

Caveat: A “natural” conjecture (sum of invariant polys) is not true.

An S_2 invariant poly: $p(x, y) = p(y, x)$. Take as invariants the elementary symmetric functions $s_1 := x + y$, $s_2 = xy$, so the invariant ring is isomorphic to $\mathbb{R}[s_1, s_2]$. Consider

$$(x_1 - x_2)^2 = s_1^2 - 4s_2$$

is *not* a sum of squares in $\mathbb{R}[s_1, s_2]$.

Reason: “hidden” constraints. Not every real s_1, s_2 map to real x_1, x_2.

Nevertheless, for efficiency reasons, we want to compute on the invariant ring. How, and what’s the right representation?

A detour: SOS matrices

We know about SOS polynomials. What about matrices of polynomials?

Def: A matrix $P(x) \in \mathbb{R}[x]^{n\times n}$ is SOS if $y^T P(x) y$ is a sum of squares in $\mathbb{R}[x,y]$.

Implies that $P(x)$ is positive semidefinite for all x.

Useful in many applications, such as control and quantum mechanics.

Example:

$$M = \begin{bmatrix} x^2 - 2x + 2 & x \\ x & x^2 \end{bmatrix} \text{ is SOS.}$$

Proof:

$$y^T M y = (y_1 + x y_2)^2 + (x-1)^2 y_2^2$$

Symmetric representations

We consider here the simplest case, i.e., when the invariant ring is isomorphic to a polynomial ring (for example, the symmetric group).

That is, we can rewrite every invariant polynomial as $p(\theta_1, \ldots, \theta_n)$.

Thm: Every SOS invariant polynomial can be written as

$$p(\theta) = \sum_{i=1}^{N} \text{trace } S_i \cdot \Pi_i, \qquad S_i, \Pi_i \in \mathbb{R}[\theta]^{n_i \times n_i}.$$

where $S_i(\theta)$ are SOS matrices, and the $\Pi_i(\theta)$ are constructed from the irreducible representations of G.

The matrices Π_i are PSD on the image of $\mathbb{R}^n$ under the θ_i, but not necessarily over the whole space.

Example

Robinson form: invariant under $(x,y) \to (-y,x), \quad (x,y) \to (y,x)$.

$$r(x,y) = x^6 + y^6 - x^4y^2 - y^4x^2 - x^4 - y^4 - x^2 - y^2 + 3x^2y^2 + 1.$$

Dihedral symmetry: group D_4, 8 elements, 5 irr. reps ($4 \cdot 1^2 + 2^2 = 8$).

The primary invariants are: $\theta_1 = x^2 + y^2, \quad \theta_2 = x^2y^2$, so

$$\tilde{r}(\theta_1, \theta_2) = \theta_1^3 - \theta_1^2 - 4\theta_1\theta_2 - \theta_1 + 5\theta_2 + 1.$$

For $r(x,y) - t$ we have $t^* = -\frac{3825}{4096}$, with:

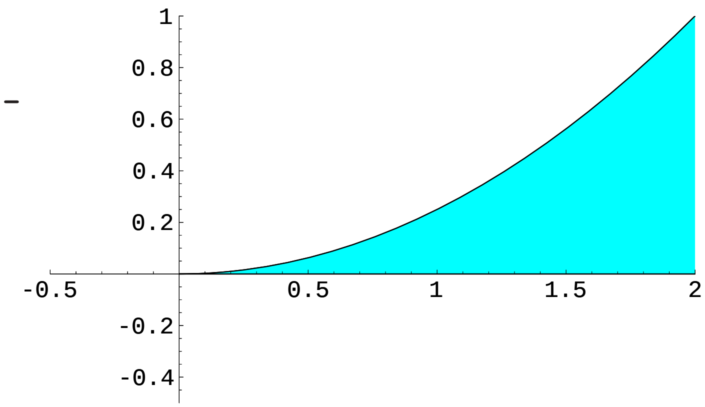
Π_i	1	θ_2	$\theta_1^2 - 4\theta_2$	$\theta_2(\theta_1^2 - 4\theta_2)$	$\begin{bmatrix} \theta_1 & \theta_1^2 - 2\theta_2 \\ \theta_1^2 - 2\theta_2 & \theta_1(\theta_1^2 - 3\theta_2) \end{bmatrix}$
S_i	$\left(-\frac{89}{64} + \frac{\theta_1}{2}\right)^2$	0	0	0	$\begin{bmatrix} (\theta_1 + \frac{5}{8})^2 & -2(\theta_1 + \frac{5}{8}) \\ -2(\theta_1 + \frac{5}{8}) & 4 \end{bmatrix}$

The orbit space

Consider the orbit space, the image of $\mathbb{R}^n$ under the invariants.

$$(x, y) -> (\theta_1, \theta_2) = (x^2 + y^2, x^2 y^2)$$

It is always a semialgebraic set.



For nonnegativity, the following are equivalent:

- $p(x) \geq 0, \quad \forall x \in \mathbb{R}^n.$
- $\tilde{p}(\theta) \geq 0, \quad \forall \theta \in \Theta(\mathbb{R}^n).$

Our representation says something similar, but for SOS.

The matrices Π_i are related to the stratifications of the orbit space.

Remark: Similarities with Schmüdgen, and P-satz representations.

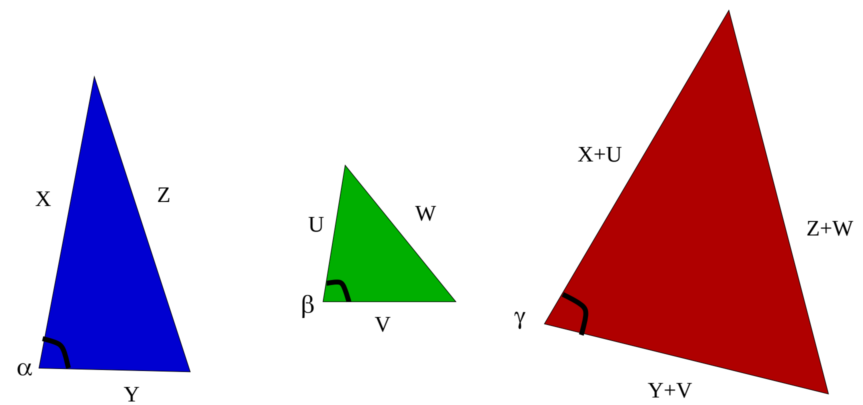
SOS over everything...

Algebraic tools are *essential* to exploit problem structure:

Standard	Equality constraints	Symmetries
polynomial ring $\mathbb{R}[x]$	quotient ring $R[x]/I$	invariant ring $R[x]^G$
monomials (deg $\leq k$)	*standard* monomials	isotypic components
$\frac{1}{(1-\lambda)^n} = \sum_{k=0}^{\infty} \binom{n+k-1}{k} \cdot \lambda^k$	Hilbert series	Molien series
	Finite convergence for zero dimensional ideals	Block diagonalization

Geometric theorem proving

- A geometric inequality arising from circle packings (Ronen Peretz):



$$\alpha \cdot (X + Y - Z) + \beta \cdot (U + V - W) \leq \gamma \cdot ((X + U) + (Y + V) - (Z + W))$$

- Not easy to prove. *Not* semialgebraic, in the standard form.
- The inequality holds if certain polynomial expression is nonnegative.
- Using SOS/SDP, we will obtain a very concise proof.

Geometric theorem proving

The theorem is true if:

$$\begin{aligned} L(a,b,c,d) \quad = \quad & a^2b^2\,(a-b)^2 + (a-b)^2\,c^3d^3 + a^2d^2\,(1-ab)\left(1+ab-2\,b^2\right) - \\ & -adbc\left(2-4\,ab+ba^3+ab^3\right) + b^2c^2\,(1-ab)\left(1+ab-2\,a^2\right) + \\ & +\left(c^2b\,(1-ab)\left(2\,a-b-ab^2\right) - cd\left(a^2+b^2+2\,a^3b^3-4\,a^2b^2\right)\right. \\ & \left. +d^2a\,(1-ab)\left(2\,b-a-a^2b\right)\right) cd \end{aligned}$$

is nonnegative in $[0,1]^4$. Using the nonlinear transformation:

$$t \to \frac{t^2}{1+t^2}$$

that maps $(-\infty,\infty)$ to $[0,1)$, and clearing denominators, we obtain the polynomial

$$P(x,y,z,w) = L(\frac{x^2}{1+x^2},\frac{y^2}{1+y^2},\frac{z^2}{1+z^2},\frac{w^2}{1+w^2})(1+x^2)^4(1+y^2)^4(1+z^2)^3(1+w^2)^3.$$

Big poly

```
P(x,y,z,w) =
x^4*w^4+x^8*y^4+x^8*w^4-2*x^6*y^6-2*z^2*y^2*x^2*w^2+z^4*y^8+2*z^4*y^6+y^4*z^6+2*y^6*z^6
+y^8*z^6+2*x^6*w^6+x^8*w^6+2*x^6*w^4+x^4*y^8+z^4*y^4+x^4*w^6+4*x^6*w^6*z^2+8*x^6*w^6*y^4
+4*x^8*w^6*y^2+8*x^6*w^6*y^2+2*x^8*w^6*z^2+4*x^4*w^6*y^4+4*x^4*w^6*y^2+4*x^8*y^2*w^4
+8*x^6*y^4*w^4+4*x^4*y^4*w^4+8*y^2*x^6*w^4+4*z^4*y^4*x^2+8*z^4*y^6*x^2-4*z^4*y^6*x^6
+6*z^4*y^8*x^4+8*z^4*y^6*x^4+4*z^4*y^4*x^4+2*z^4*y^4*x^8+3*z^4*y^4*w^2+4*z^4*y^6*w^4
+6*z^4*y^6*w^2+2*z^4*y^4*w^4+2*z^4*y^8*w^4+3*z^4*y^8*w^2+4*z^4*y^8*x^2+4*z^6*y^6*w^2
+8*z^6*y^6*x^4+4*z^6*y^8*x^2-6*x^6*y^6*w^2-6*x^6*y^6*z^2+3*y^4*x^8*z^2+3*x^4*y^8*z^2
+3*z^2*w^4*x^8+2*y^8*z^6*w^2+3*z^2*w^4*x^4+6*z^2*w^4*x^6+4*z^4*w^4*x^6+2*z^4*w^4*x^8
+2*z^4*w^4*x^4+3*x^8*y^4*w^2+3*x^4*y^8*w^2+2*x^4*w^4*y^8+6*x^8*w^4*y^4-4*x^6*w^4*y^6
+2*x^4*z^2*w^6+4*x^8*y^4*w^6+4*x^4*y^8*z^6+2*y^4*z^6*w^2+4*x^2*y^4*z^6+4*x^4*y^2*w^4
+4*x^4*y^4*z^6+8*x^2*y^6*z^6-8*z^4*y^6*x^2*w^4-24*z^4*y^6*x^4*w^4-16*z^4*y^6*x^6*w^4
+12*z^4*y^8*x^4*w^2-16*z^4*y^4*x^2*w^4-4*z^4*y^2*x^8*w^2-40*z^4*y^4*x^4*w^4
-12*z^4*y^2*x^4*w^2-8*z^4*y^2*x^2*w^4+8*x^2*y^4*z^6*w^2+16*x^2*y^6*z^6*w^2
+8*x^4*y^4*z^6*w^2+8*x^4*w^6*y^4*z^2+16*x^6*w^6*y^2*z^2+8*x^4*w^6*y^2*z^2
+16*x^6*w^6*y^4*z^2+8*x^8*w^6*y^2*z^2+16*x^4*y^6*z^6*w^2-4*z^4*y^2*x^2*w^2
-12*z^4*y^2*x^6*w^2-16*z^4*y^2*x^4*w^4-16*z^4*y^4*x^4*w^2-20*z^4*y^4*x^6*w^2
+12*z^4*y^6*x^2*w^2+4*z^4*y^6*x^4*w^2-14*x^4*y^4*z^2*w^2-6*x^4*y^2*z^2*w^2
+6*x^4*y^8*z^2*w^2+6*y^4*x^8*z^2*w^2-20*x^6*y^6*z^2*w^2-6*y^2*x^6*z^2*w^2
-16*z^2*w^4*x^6*y^6+12*z^2*w^4*y^2*x^6-12*z^2*w^4*x^2*y^4-16*z^2*w^4*x^4*y^4
+4*z^2*w^4*x^6*y^4-12*z^2*w^4*x^2*y^6+8*z^2*w^4*x^8*y^2-20*z^2*w^4*x^4*y^6
-6*x^2*y^4*z^2*w^2-6*x^2*y^6*z^2*w^2-10*x^4*y^6*z^2*w^2-10*y^4*x^6*z^2*w^2
-2*x^2*y^8*z^2*w^2-2*y^2*x^8*z^2*w^2+12*z^2*w^4*x^8*y^4-4*z^2*w^4*x^2*y^8
-4*x^2*w^4*y^2*z^2+8*x^4*y^8*z^6*w^2+8*x^8*y^4*z^2*w^6-8*z^4*y^2*x^6*w^4
+8*x^2*y^8*z^6*w^2-16*z^4*y^6*x^6*w^2+8*z^4*y^8*x^2*w^2-24*z^4*y^4*x^6*w^4
```

Is $P(x, y, z, w) \geq 0$ for all real values of x, y, z, w?

Properties

- Sparsity:
  - P has degree 20, but only degree 12 in (x, y) and degree 8 in (z, w). Also, quite sparse (123 monomials): A dense $(4, 20)$ poly has 10626 monomials.
- Symmetries:
  - P has many symmetries, some inherited from L, some a result of the transformation.

$$\begin{aligned} (x, y, z, w) &\rightarrow (y, x, w, z) \\ &\rightarrow (\pm x, \pm y, \pm z, \pm w) \end{aligned}$$

    * The first one corresponds to interchange of the triangles.
    * The other ones are byproducts of $t \rightarrow \frac{t^2}{1+t^2}$.
  - A group with 32 elements and 14 irr. reps $(8 \cdot 1^2 + 6 \cdot 2^2 = 32)$.

- No sparsity, no symmetries: 1001×1001, 10626 vars.

- Sparsity, no symmetry: 137×137, 1328 vars.

- Sparsity, symmetry: 14 coupled LMIs, varying dimensions:

Irr. Rep. #	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Multiplicity	1	1	1	1	1	1	1	1	2	2	2	2	2	2
Dim. SDP	9	6	6	4	8	5	3	2	11	7	8	7	8	6

Can easily solve this!

The proof

- It turns out that $P(x, y, z, w)$ is a sum of five squares:

$$P(x, y, z, w) = A^2(z^2 + w^2 + 2z^2w^2) + B^2 + C^2.$$

where

$$A = -y^2z^2 - y^4z^2 + x^2w^2 + 2x^2y^2w^2 - 2x^2y^2z^2 - x^2y^4 - 2x^2y^4z^2 + x^4w^2 + x^4y^2 + 2x^4y^2w^2$$

$$B = (1 + x^2 + y^2)(-x^2w^2 - x^2z^2w^2 - x^2y^2w^2 + x^2y^2z^2 + y^2z^2 + y^2z^2w^2)$$
$$C = (x - y)(x + y)(-x^2z^2w^2 + x^2y^2 + x^2y^2w^2 + x^2y^2z^2 - z^2w^2 - y^2z^2w^2).$$

so P is indeed nonnegative (QED?).

We can also write this in the original variables $a, b, c, d\ldots$

Solution

$$
\begin{aligned}
L(a,b,c,d) &= L_1 + L_2 + L_3 \\
L_1 &= (c+d)(-a^2b + ab^2 - ad + bc - bcd + adc - ab^2c + a^2bd)^2 \\
L_2 &= (1-c)(1-d)(ab-1)^2(ad-bc)^2 \\
L_3 &= (1-c)(1-d)(a-b)^2(ab-cd)^2.
\end{aligned}
$$

From this, stronger conclusions on the sign of L can be derived. Not only it is nonnegative on the open unit hypercube $(0,1)^4$, but the same property holds on the much larger region $\mathbb{R} \times \mathbb{R} \times \{c + d \geq 0, (1-c)(1-d) \geq 0\}$.

An independently verifiably certificate for nonnegativity.

As a consequence, the original geometric inequality is now proved.

SOSTOOLS: sums of squares toolbox

Handles the general problem:

$$\begin{array}{ll} \min_{u_i} & c_1 u_1 + \cdots + c_n u_n \\ \text{s.t} & P_i(x,u) := A_{i0}(x) + A_{i1}(x) u_1 + \cdots + A_{in}(x) u_n \quad \text{are SOS} \end{array}$$

- MATLAB toolbox, freely available.
- Requires MATLAB's symbolic toolbox, and SeDuMi (SDP solver).
- Natural syntax, efficient implementation.
- Developed by Stephen Prajna, Antonis Papachristodoulou, and PP.
- Includes customized functions for several problems.

Get it from: `http://www.aut.ee.ethz.ch/~parrilo/sostools`
`http://www.cds.caltech.edu/sostools`