Hilbert's 17th Problem

to

Semidefinite Programming

&

Convex Algebraic Geometry

Rekha R. Thomas

University of Washington, Seattle

References

Monique Laurent, Sums of squares, moment matrices and optimization over polynomials, IMA Volume, to appear

Murray Marshall, Positive polynomials and sums of squares, AMS 2008

João Gouveia, Pablo Parrilo, Rekha Thomas, Theta bodies for polynomial ideals, preprint 2008.

Polynomial Optimization: $p^* := \inf\{p(\mathbf{x}) : \mathbf{x} \in K\}$ $(*)$

- $K = \{\mathbf{x} \in \mathbb{R}^n : g_1 \geq 0, \ldots, g_m \geq 0, h_1 = 0, \ldots, h_s = 0\}$

  (basic semialgebraic set), $p, g_i, h_j \in \mathbb{R}[\mathbf{x}] := \mathbb{R}[x_1, \ldots, x_n]$
- $K = \mathbb{R}^n \longrightarrow$ unconstrained polynomial optimization
- $m = 0 \longrightarrow K = \mathcal{V}_{\mathbb{R}}(I)$ real variety of $I = \langle h_1, \ldots, h_m \rangle \subseteq \mathbb{R}[\mathbf{x}]$
- non-convex optimization problem
- NP-hard even when $\deg(p) = 4$ and $K = \mathbb{R}^n$.

GOAL: Find a sequence of relaxations of $(*)$ by convex optimization problems that converges to $(*)$.

Examples (all NP complete)

Partition problem: Given $a_1, \ldots, a_n \in \mathbb{Z}_+$, does there exist $\mathbf{x} \in \{\pm 1\}^n$ s.t. $\sum a_i x_i = 0$? Yes $\Leftrightarrow p^* = 0$ for $p := \left(\sum_{i=1}^n a_i x_i\right)^2 + \sum_{i=1}^n (x_i^2 - 1)^2$.

Distance realization: Given distances $\mathbf{d} := (d_{ij}) \in \mathbb{R}^E$, $\mathbf{d}$ is realizable in $\mathbb{R}^k$ if there exists $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{R}^k$ such that $d_{ij} = ||\mathbf{v}_i - \mathbf{v}_j||$ for all $ij \in E$.
$\mathbf{d}$ realizable in $\mathbb{R}^k \Leftrightarrow p^* = 0$ for $p := \sum_{ij \in E} \left(d_{ij}^2 - \sum_{h=1}^k (x_{ih} - x_{jh})^2\right)^2$.

$0/1$ Integer programming: $\min\{\mathbf{c} \cdot \mathbf{x} : A\mathbf{x} \leq \mathbf{b},\ x_i^2 = x_i \ \forall\ i \in [n]\}$

Semidefinite programming

- vector space: Symm$(\mathbb{R}^{n\times n})$
- trace product: $A, B \in$ Symm$(\mathbb{R}^{n\times n})$, $\quad A \cdot B :=$ trace(AB)
- positive semidefinite: $\quad A \succeq 0$

$$\begin{aligned} &\Leftrightarrow \quad \text{all eigenvalues of } A \text{ are non-negative} \\ &\Leftrightarrow \quad \mathbf{v}^t A \mathbf{v} \geq 0 \text{ for all } \mathbf{v} \in \mathbb{R}^n \\ &\Leftrightarrow \quad A = BB^t \quad \text{for some} \quad B \in \mathbb{R}^{n\times m} \end{aligned}$$

semidefinite program (sdp):

$$\sup\{C \cdot X \,:\, A_j \cdot X = b_j,\ j = 1, \ldots, m,\ X \succeq 0\}$$

- convex optimization, polynomial time algorithms
- Linear programming is SDP over diagonal matrices

Hilbert's 17th problem

$\mathcal{P}_n := \{p \in \mathbb{R}[\mathbf{x}] : p(\mathbf{x}) \geq 0, \forall\, \mathbf{x} \in \mathbb{R}^n\}$ non-negative polynomials

$\Sigma_n := \{\sum h_j^2 : h_j \in \mathbb{R}[\mathbf{x}]\}$ sum of squares (sos) of polynomials

$\mathcal{P}_{n,d}, \Sigma_{n,d}$ polynomials of degree at most d in $\mathcal{P}_n$ and Σ_n

$\Sigma_n \subseteq \mathcal{P}_n$ and $\Sigma_{n,d} \subseteq \mathcal{P}_{n,d}$ cones in $\mathbb{R}[\mathbf{x}]$

Hilbert 1888: $\Sigma_{n,d} = \mathcal{P}_{n,d} \Leftrightarrow n = 1$ or $d = 2$ or $(n,d) = (2,4)$.

Hilbert's 17th problem: Is every $p \in \mathcal{P}_n$ a sos of rational functions?

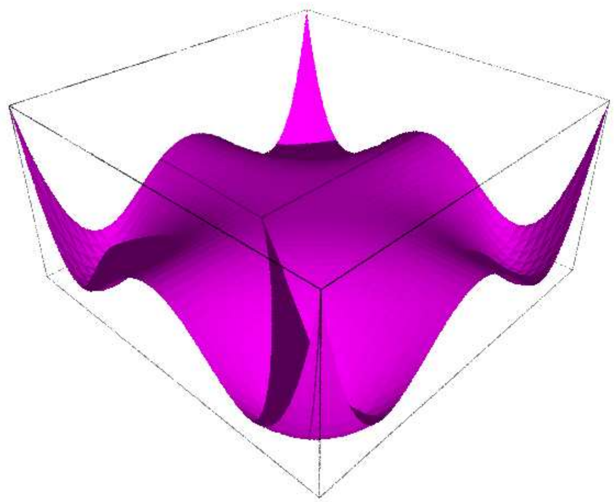
Yes! Artin 1927 using Tarski's transfer principle and orderings on fields

Motzkin (1967):

$s(x,y) := 1 - 3x^2y^2 + x^2y^4 + x^4y^2$

- $s(x,y) \in \mathcal{P}_{2,6} \setminus \Sigma_{2,6}$
- $\frac{a+b+c}{3} \geq \sqrt[3]{abc} \ \forall \ a,b,c \geq 0,$

  $a := 1,\ b := x^2y^4,\ c := x^4y^2$



Blekherman (2006): for d fixed, many more nonnegative forms than sos forms as $n \to \infty$

Lasserre (2006): for n fixed, any nonnegative polynomial can be approximated arbitrarily closely by sos polynomials.

Testing for sos representations via SDP

$p = x^4 + 2x^3y + 3x^2y^2 + 2xy^3 + 2y^4$ sos

$$\Leftrightarrow \quad \exists\, A \succeq 0 \text{ s.t. } p = (x^2, xy, y^2) \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{pmatrix} \begin{pmatrix} x^2 \\ xy \\ y^2 \end{pmatrix}$$

$\Leftrightarrow$ the sdp $\{A \succeq 0 : a_{11} = 1, a_{12} = 1, a_{22} + 2a_{13} = 3, a_{23} = 1, a_{33} = 2\}$ is feasible

ex: $A = B^t B$ for $B = \begin{pmatrix} 1 & 1 & -1 \\ 0 & 2 & 1 \end{pmatrix}$ or $B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & \sqrt{3/2} & \sqrt{3/2} \\ 0 & \sqrt{1/2} & -\sqrt{1/2} \end{pmatrix}$

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

Sos relaxations for $p^* := \inf\{p(\mathbf{x}) : \mathbf{x} \in K\}$

$$p^* := \sup\{\rho : p - \rho \geq 0 \text{ on } K\} = \sup\{\rho : p - \rho > 0 \text{ on } K\}$$

- $K = \mathbb{R}^n$: $p^{\text{sos}} := \sup\{\rho : p - \rho \text{ is sos}\}$

CAUTION Motzkin polynomial: $p^{\text{sos}} = -\infty < p^* = 0$

- $K = \{\mathbf{x} \in \mathbb{R}^n : g_1 \geq 0, \ldots, g_m \geq 0\}$:

$$p^{\text{sos}} := \sup\{\rho : p - \rho = s_0 + \sum_{i=1}^m s_i g_i, \ s_i \text{ sos}\}$$

to get sdps we look at successive truncations:

$$p_t^{\text{sos}} := \sup\{\rho : p - \rho = s_0 + \sum_{i=1}^m s_i g_i, \ s_i \text{ sos}, \ \deg(s_0), \deg(s_i g_i) \leq 2t\}$$

$$p_t^{\text{sos}} \leq p_{t+1}^{\text{sos}} \leq p^{\text{sos}} \leq p^*, \quad \lim_{t\to\infty} p_t^{\text{sos}} = p^{\text{sos}}$$

Positivstellensatz (Krivine 1964, Stengle 1974)

$T := \{\sum s_i (g_1^{i_1} g_2^{i_2} \cdots g_m^{i_m}) : (i_1, \ldots, i_m) \in \{0,1\}^m, \ s_i \text{ sos}\}$ preorder

non-negativity set of $K = \{\mathbf{x} \in \mathbb{R}^n : g_1 \geq 0, \ldots, g_m \geq 0\}$.

Positivstellensatz: Given $p \in \mathbb{R}[\mathbf{x}]$,

(i) $p > 0$ on $K \Leftrightarrow pf = 1 + g, \ f, g \in T$

(ii) $p \geq 0$ on $K \Leftrightarrow pf = p^{2k} + g, \ f, g \in T$ (solves Hilbert's 17th prob)

(iii) $p = 0$ on $K \Leftrightarrow -p^{2k} \in T$

(iv) $K = \emptyset \Leftrightarrow -1 \in T$ (compare: Hilbert's weak Nullstellensatz)

Real Nullstellensatz: p vanishes on $\{\mathbf{x} \in \mathbb{R}^n : h_1 = \cdots = h_s = 0\} \Leftrightarrow$
$p^{2k} + s = \sum_{j=1}^{s} u_j h_j$ for $u_j \in \mathbb{R}[\mathbf{x}], s$ sos. (Hilbert's strong NS)

Schmüdgen's & Putinar's refinements

$p^* := \sup\{\rho : p - \rho > 0 \text{ on } K\} = \sup\{\rho : (p-\rho) f = 1 + g,\ \ f, g \in T\}.$

Schmüdgen 1991: If K is compact then $p > 0$ on $K \Rightarrow p \in T$.

$$p_t^{\text{Schm}} = \sup\{\rho : (p-\rho) = \sum s_i (g_1^{i_1} g_2^{i_2} \cdots g_m^{i_m}),\ s_i \text{ sos},\ \deg(**) \leq t\}$$

(sdp, $\lim_{t\to\infty} p_t^{\text{Schm}} = p^*$, involves 2^m terms !)

Putinar 1993: If K is Archimedean then $p > 0$ on $K \Rightarrow p \in M$.

$M := \{s_0 + \sum_{i=1}^m s_i g_i : s_0, s_i \text{ sos}\}$ quadratic module

$$p_t^{\text{Put}} = \sup\{\rho : (p-\rho) = s_0 + \sum s_i g_i,\ s_0, s_i \text{ sos},\ \deg(**) \leq t\}$$

(sdp, $\lim_{t\to\infty} p_t^{\text{Put}} = p^*$, only $m+1$ terms !)

Moments of probability measures

μ probability measure on $\mathbb{R}^n$:

- $y_\alpha := \int \mathbf{x}^\alpha d\mu$ moment of order α
- $y := (y_\alpha : \alpha \in \mathbb{N}^n)$ moment sequence of μ

K-moment problem: Characterize moment sequences of measures supported on $K \subseteq \mathbb{R}^n$.

$y \in \mathbb{R}^{\mathbb{N}^n}$ moment sequence:

- moment matrix: $M(y) \in \mathbb{R}^{\mathbb{N}^n \times \mathbb{N}^n}$: $M(y)_{(\alpha,\beta)} := y_{\alpha+\beta}$
- truncated moment matrix: $M_t(y)$ – principal submatrix of $M(y)$ indexed by $\mathbb{N}^n_t$

Moment relaxations for $p^* := \inf\{p(\mathbf{x}) : \mathbf{x} \in K\}$

$y \in \mathbb{R}^{\mathbb{N}^n_{2t}}$ (truncated) moment sequence of μ on $K \Rightarrow \forall t \geq d_K$,

$$M_t(y) \succeq 0, \;\; M_{t-d_K}(g_i y) \succeq 0, \; i = 1, \ldots, m$$

$$p^* \;=\; \inf\{\textstyle\int_K p(\mathbf{x}) d\mu : \mu \text{ prob measure on } K\}$$

$$= \;\inf\{p^t y : y_0 = 1, y \text{ mom seq of } \mu \text{ on } K\}$$

$$p^{\text{mom}} := \inf\{p^t y : y_0 = 1, \; M(y) \succeq 0, \; M(g_i y) \succeq 0, \; i = 1, \ldots, m\}$$

to get sdps we look at successive truncations:

$$p_t^{\text{mom}} := \inf\{p^t y : y_0 = 1, \; M_t(y) \succeq 0, \; M_{t-d_K}(g_i y) \succeq 0, \; \forall\, i, \; y \in \mathbb{R}^{\mathbb{N}^n_{2t}}\}$$

$$p_t^{\text{mom}} \leq p_{t+1}^{\text{mom}} \leq p^{\text{mom}} \leq p^*, \quad \lim_{t\to\infty} p_t^{\text{mom}} = p^{\text{mom}}$$

Duality

Recall: $\mathcal{P}$ = $\{p : p(\mathbf{x}) \geq 0, \forall\, \mathbf{x} \in \mathbb{R}^n\}$, Σ = $\{\sum h_j^2 : h_j \in \mathbb{R}[\mathbf{x}]\}$.

Define $\mathcal{M} := \{y \in \mathbb{R}^{\mathbb{N}^n}$: y mom seq of μ on $\mathbb{R}^n\} \subseteq \mathbb{R}[\mathbf{x}]^*$

$\mathcal{M}_{\succeq} := \{y \in \mathbb{R}^{\mathbb{N}^n} : M(y) \succeq 0\} \subseteq \mathbb{R}[\mathbf{x}]^*$

Haviland 1935 $\mathcal{P} = \mathcal{M}^*$, $\mathcal{P}^* = \mathcal{M}$

Berg,Christensen,Jensen 1979: $\Sigma = \mathcal{M}_{\succeq}^*$, $\Sigma^* = \mathcal{M}_{\succeq}$

Corollary: $(n = 1) \Rightarrow \mathcal{M} = \mathcal{M}_{\succeq}$ Hamburger's theorem

$\exists\ K$-versions of these dual cones

sdp duality $\Rightarrow p_t^{\text{sos}} \leq p_t^{\text{mom}} \leq \cdots \leq p^{\text{sos}} \leq p^{\text{mom}} \leq p^*$

Theta Body of a Graph

$G = ([n], E)$ undirected graph

$$\text{STAB}(G) := \text{conv}\{\chi^S : S \text{ stable set in } G\}$$

max stable set problem: $\max\{\sum x_i : \mathbf{x} \in \text{STAB}(G)\}$ (NP-hard)

$$I_G := \langle x_i : i \in [n],\ x_i x_j : ij \in E\rangle \Rightarrow \mathcal{V}(I_G) = \{\chi^S : S \text{ stable set in } G\}$$

Lovász 1980

- $\text{TH}(G) := \{\mathbf{x} \in \mathbb{R}^n : f(\mathbf{x}) \geq 0\ f \text{ linear},\ f \text{ 1-sos mod } I_G\} \supseteq \text{STAB}(G)$
- G perfect $\Leftrightarrow \text{STAB}(G) = \text{TH}(G)$
- stable set problem solved in poly time if G perfect:

  $\max\{\sum x_i : \mathbf{x} \in \text{TH}(G)\}$ is an sdp

Lovász 1994: Which ideals $I \subseteq \mathbb{R}[\mathbf{x}]$ are perfect?

$$(\forall\ f \text{ linear, } f \geq 0 \text{ on } \mathcal{V}_{\mathbb{R}}(I) \Rightarrow f \text{ is 1-sos mod } I) \qquad .$$

- $f \in \mathbb{R}[\mathbf{x}]$ k-sos mod I if $f \equiv \sum h_j^2$ mod I, $\deg(h_j) \leq k$
- I is k-perfect if every linear $f \geq 0$ mod I is k-sos mod I
- $TH_k(I) := \{\mathbf{x} \in \mathbb{R}^n : f(\mathbf{x}) \geq 0, \forall\ f \text{ linear } f\ k\text{-sos mod } I\}$
- $\mathrm{TH}_1(I) \supseteq \mathrm{TH}_2(I) \supseteq \cdots \supseteq \overline{\mathrm{conv}(\mathcal{V}_{\mathbb{R}}(I))}$ theta bodies for ideals

Gouveia, Parrilo, T. 2008

- $TH_k(I)$ is the closure of the projection of a spectrahedron
- $I = I(S)$, $S \subset \mathbb{R}^n \Rightarrow I$ k-perfect $\Leftrightarrow \overline{\mathrm{conv}(\mathcal{V}_{\mathbb{R}}(I))} = \mathrm{TH}_k(I)$
- $I = I(S)$, S finite $\Rightarrow I$ perfect $\Leftrightarrow$ for every facet inequality $g(\mathbf{x}) \geq 0$ of conv(S), $S \subseteq \{g(\mathbf{x}) = 0\} \cup \{g(\mathbf{x}) = c_g\}$
- In this case, # facets, # vertices $\leq 2^n$ (both sharp)

Convex Algebraic Geometry

$$\mathrm{TH}_1(I) \supseteq \mathrm{TH}_2(I) \supseteq \cdots \supseteq \overline{\mathrm{conv}(\mathcal{V}_{\mathbb{R}}(I))}$$

Theta bodies approximate convex hulls of real varieties

Compute theta bodies via sdp, convergence in many cases

Gouveia, Parrilo, T. 2008

For $I \subseteq \mathbb{R}[\mathbf{x}]$, $\mathrm{TH}_1(I) = \cap\{\mathrm{conv}(\mathcal{V}_{\mathbb{R}}(F)) : F$ convex quadric in $I\}$

Ex. $S = \{(0,0),(1,0),(0,1),(2,2)\}$