What is Hilbert's 17th Problem

2026/06/16 OSU What Is...? Seminar

Q: Can every nonnegative integer n be written as a sum of squares??

A: Yes: $\underbrace{1^2 + 1^2 + \cdots + 1^2}_{n \text{ times}}$

A [Lagrange's Four Square Theorem 1770]: Yes, using ≤ 4 squares

(Minimality question leads us to Waring's Problem)

What is the analogous question for polynomials??

Defn: A homogeneous polynomial ("form") $p(x_1, \ldots, x_n) \in \mathbb{R}[x_1, \ldots, x_n]$ is positive semidefinite if if $\forall\ \bar{x} \in \mathbb{R}^n$, $p(\bar{x}) \geq 0$

Q: Can every positive semidefinite (PSD) polynomial be expressed as a sum of squares? (SOS)

Rmk: We can restrict our attention to homogeneous polynomials.

$f(x_1, \ldots, x_n) \xrightarrow{\text{homogenization}} y^d f(x_1/y, \ldots, x_n/y)$ any $d \geq \deg(f)$ even

$p(x_1, \ldots, x_n, 1) \xleftarrow[\text{dehomogenization}]{} p(x_1, \ldots, x_n, y)$

These operations preserve PSD & SOS.

Pf: Say $f(x_1, \ldots, x_n)$ is PSD. Let $d \geq \deg(f)$ even. Then $\forall\ (x_1, \ldots, x_n, y) \in \mathbb{R}^{n+1}$

$\Rightarrow \underbrace{y^d}_{\geq 0 \text{ } d \text{ even}} \underbrace{f(x_1/y, \ldots, x_n/y)}_{\bar{x}/y \in \mathbb{R}^n,\ f \text{ PSD}} \geq 0$

Conversely say $p(x_1, \ldots, x_n, y)$ is PSD, then so is $p(x_1, \ldots, x_n, 1)$

Say $f(x_1, \dots, x_n)$ is SOS, $f(\bar{x}) = \sum_k h_k(\bar{x})^2$. Let $d \geq \deg(f)$ even, $d = 2e$

$$y^{2e} f(x_1/y, \dots, x_n/y) = \sum_k y^{2e} h_k(x_1/y, \dots, x_n/y)^2 = \sum_k \left(y^e h_k(x_1/y, \dots, x_n/y) \right)^2$$

Conversely say $p(x_1, \dots, x_n, y)$ is SOS, then so is $p(x_1, \dots, x_n, 1)$

Defn: $H_m(\mathbb{R}^n) :=$ set of degree-m forms in $\mathbb{R}[x_1, \dots, x_n]$

$P_{n,m} :=$ set of PSD forms in $H_m(\mathbb{R}^n)$

$\Sigma_{n,m} :=$ set of SOS forms in $H_m(\mathbb{R}^n)$

These are both closed, convex cones in $\mathbb{R}^N$ $N = \binom{n+m-1}{n-1}$

Goal: study $\Delta_{n,m} := P_{n,m} \setminus \Sigma_{n,m}$ $\Sigma_{n,m} \subseteq P_{n,m}$ immediate

- If $n' \geq n$, $\Delta_{n,m} \subseteq \Delta_{n',m}$
- If $m' \geq m$ even, $p \in \Delta_{n,m} \Rightarrow x_1^{m'-m} p \in \Delta_{n,m'}$

Q [Hilbert's 17th Question]: Can every positive semidefinite polynomial be expressed as a sum of squares of rational functions?

If $p \in P_{n,m}$, are there polynomials $q, h_1, \dots, h_k$ and $\lambda_1, \dots, \lambda_k \in \mathbb{R}$ s.t.

$$p \cdot q^2 = \sum_{i=1}^{k} \lambda_i h_i^2$$

A [Artin 1927]: Yes (Lead to modern real AG & theory of ordered fields)

We will not dive into the proof of Artin's result (Artin-Schreier Theory). Instead, we will ask:

Q: How do we find polynomial examples in $\Delta_{n,m}$?

Here is a fun application of caring about PSD vs SOS.

Ex: We can prove some fundamental inequalities by showing some polynomials are PSD

AM-GM:

$$\frac{x_1 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \cdots x_n} \quad \Leftrightarrow \quad AG := \frac{x_1^{2n} + \cdots + x_n^{2n}}{n} - x_1^2 \cdots x_n^2 \geq 0$$

$x_i \geq 0$

Cauchy-Schwartz:

$$\sum_{i=1}^n x_i y_i \leq \sqrt{\left(\sum_{i=1}^n x_i^2\right) \cdot \left(\sum_{i=1}^n y_i^2\right)} \Leftrightarrow CS := \left(\sum_{i=1}^n x_i^2\right) \cdot \left(\sum_{i=1}^n y_i^2\right) - \left(\sum_{i=1}^n x_i y_i\right)^2 \geq 0$$

Minkowski's Inequality (Superadditivity of Geometric Mean):

$$\left(\prod_{i=1}^n (x_i + y_i)\right)^{1/n} \geq \left(\prod_{i=1}^n x_i\right)^{1/n} + \left(\prod_{i=1}^n y_i\right)^{1/n} \Leftrightarrow M := \prod_{i=1}^n (x_i^{2n} + y_i^{2n}) - \left(\prod_{i=1}^n x_i^2 + \prod_{i=1}^n y_i^2\right)^n$$

To get a flavor for this, Lagrange gives the following SOS expression for CS

$$CS = \sum_{1 \leq i < j \leq n} (x_i y_j - x_j y_i)^2$$

Note: This makes case of equality immediate

So asking about PSD vs SOS is asking about the existance of such proofs.

We first consider some basic cases.

Prop: $P_{n,2} = \Sigma_{n,2}$

Pf: Say $p(x_1, \dots, x_n) = \sum_{1 \le i \le j \le n} p_{i,j}\, x_i x_j \in P_{n,2}$

Let $a_{i,i} = p_{i,i}$, $1 \le i \le n$

$a_{i,j} = \frac{1}{2} p_{i,j}$, $1 \le i < j \le n$, $p_{i,j} = p_{j,i}$

$A = (a_{i,j})_{1 \le i,j \le n}$

Then $p(\bar{x}) = \bar{x}^T A \bar{x}$, A symmetric $\Rightarrow$ A orthogonally diagonalizable

Say $A = P^T D P$, $D = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$, $\lambda_i \ge 0$ (say v is eigenvector for λ_i: $0 \le p(v) = v^T A v = v^T \lambda_i v = \lambda_i \cdot \|v\|^2$)

Then $p(\bar{x}) = \bar{x}^T P^T D P \bar{x} = (P\bar{x})^T D (P\bar{x})$

Say $f_i(\bar{x})$ is i-th row of $P\bar{x}$, $\deg f_i(\bar{x}) = 1$

$$p(\bar{x}) = (P\bar{x})^T D (P\bar{x}) = \sum_{i=1}^{n} \lambda_i f_i(\bar{x})^2 = \sum_{i=1}^{n} \left(\lambda_i f_i(\bar{x})\right)^2 \in \Sigma_{n,2}$$

So $P_{n,2} = \Sigma_{n,2}$

Prop: $P_{2,m} = \Sigma_{2,m}$

Pf: Say $p(x,y) \in P_{2,m}$. Then $f(x) = p(x,1)$ is also PSD.
$\Rightarrow$ $f(x)$ has some real roots of multiplicity two and some complex roots, which appear in conjugate pairs. Then

$$f(x) = c^2 \prod_{i=1}^{t} (x - t_i)^{2a_i} \cdot \prod_{j=1}^{s} (x - (\alpha_j + i \cdot \beta_j)) \cdot \prod_{j=1}^{s} (x - (\alpha_j - i \cdot \beta_j))$$

$$= A(x)^2 \cdot (B(x) + i \cdot C(x)) \cdot (B(x) - i \cdot C(x))$$

$$= A(x)^2 (B(x)^2 + C(x)^2) = (A(x)B(x))^2 + (A(x)C(x))^2 \in \Sigma_{2,m}$$

So $f(x) = p(x,1)$ is SOS. Homogenization $\Rightarrow$ $p(x,y)$ is SOS

So $P_{2,m} = \Sigma_{2,m}$.

Thm [Hilbert 1888]: $P_{3,4} = \Sigma_{3,4}$ and $\Delta_{n,m} = P_{n,m} \setminus \Sigma_{n,m}$ is nonempty for $n \ge 3$ and $m \ge 6$ or $n \ge 4$ and $m \ge 4$.

Ex [Lax-Lax 1978, 1971 IMO #1]: Let $A_n(\bar{x}) = \sum_{i=1}^{n} \prod_{j \neq i} (x_i - x_j)$. For which n is A_n PSD?

- If n even, $\deg(A_n)$ odd $\Rightarrow$ not PSD
- Say n odd, $n \geq 7$, set $x_1 = x_2 = x_3 = 0$, $x_4 = 1$, $x_5 = \cdots = x_n = 2$. Then all terms except $i = 4$ are zero, so

$$A_n(\bar{x}) = \prod_{j \neq 4} (1 - x_j) = (-1)^{n-4} = -1$$

- If $n = 3$, $A_3(\bar{x}) = \frac{1}{2}\left[(x_1 - x_2)^2 + (x_1 - x_3)^2 + (x_2 - x_3)^2\right]$

Thm [Lax, Lax 1978]: $A_5(\bar{x}) \in \Delta_{5,4}$

Proof uses symmetry of A_5 to argue $x_1 \geq \cdots \geq x_5$, then check term by term

Ex [Robinson 1969]: Robinson used ideas of Hilbert to make explicit examples

$\phi(x,y) = x^3 - x$ & $\psi(x,y) = y^3 - y$ have common zeroes $\{-1, 0, 1\}^2$

Using Hilbert's method, Robinson derived the following

$$R(x,y,z) = x^6 + y^6 + z^6 - (x^4y + x^2y^4 + x^4z^2 + x^2z^4 + y^4z^2 + y^2z^4) + 3x^2y^2z^2$$

We can see that $R(x,y,z) \geq 0$ via

Lem [Schur]: For $r, u, v, w \geq 0$

$$u^r(u-v)(u-w) + v^r(v-u)(v-w) + w^r(w-u)(w-v) \geq 0$$

To recover $R(x,y,z) \geq 0$, take $r = 1$, $(u,v,w) = (x^2, y^2, z^2)$.

Suppose $R = \sum_k h_k(x,y,z)^2$, each h_k a cubic.

R vanishes on $\{(1, \pm 1, \pm 1), (1, \pm 1, 0), (1, 0, \pm 1), (0, 1, \pm 1)\}$

Each h_k also vanishes on this set.
This gives 10 linearly independent equations on the coeffs of the h_k
$\Rightarrow h_k = 0$ $\forall k$. Contradiction.

Hilbert constructed examples in $\Delta_{3,6}$ by homogenizing the following construction. We will describe Hilbert's general construction [Hilbert 1888] from which Robinson derived his example.

Let $\phi(x,y)$, $\psi(x,y)$ (x^3-x, y^3-y) be two coprime cubics w/ common zeroes $\{P_1,\dots,P_9\} \subseteq \mathbb{R}^2$

Choose quadratic $f(x,y)$ vanishing at $P_1,\dots,P_4$
quartic $g(x,y)$ vanishing at $P_1,\dots,P_5$, singular at P_6, P_7, P_8

Such f, g exist by constant counting: f has 6 coeffs, 4 constraints
g has 16 coeffs, 5 + 3·3 constraints

Hilbert then showed $\exists \lambda \in \mathbb{R}$ s.t.

$$F(x,y) = \phi(x,y)^2 + \psi(x,y)^2 + \lambda f(x,y)\, g(x,y) \geq 0$$

and $F(P_i) = 0 \quad \forall\, 1 \leq i \leq 8$ and $F(P_9) \neq 0$.

Suppose $F(x,y) = \sum_k h_k(x,y)^2$. Then $\forall\, 1 \leq i \leq 8$, $F(P_i) = 0 \Rightarrow h_k(P_i) = 0$.

Thm [Cayley-Bacharach]: Say two coprime cubic curves have common zeroes $\{P_1,\dots,P_9\}$. Then any cubic curve passing through 8 points must pass through the ninth.

So $h_k(P_9) = 0 \ \forall k \Rightarrow F(P_9) = 0$, contradiction.

Ex [Motzkin '1967]: $(x_1^2 + \cdots + x_{n-1}^2 - n y^2)\, x_1^2 \cdots x_{n-1}^2 + y^{2n} \in \Delta_{n,2n}$

Pf: Consider the case of $n=3$:

$$M(x,y,z) = (x^2+y^2-3z^2)\,x^2y^2 + z^6 = x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2$$

Why is $M(x,y,z)$ PSD? Apply AM-GM to (x^4y^2, x^2y^4, z^6)

$$\frac{x^4y^2 + x^2y^4 + z^6}{3} \geq (x^4y^2 \cdot x^2y^4 \cdot z^6)^{1/3}$$

Suppose $M(x,y,z) = \sum_k h_k(x,y,z)^2$. We derive a contradiction via coefficients

$$h_k(x,y,z) = A_k x^3 + B_k x^2 y + C_k x y^2 + D_k y^3 + E_k x^2 z + F_k xyz + G_k y^2 z + H_k x z^2 + I_k y z^2 + J_k z^3$$

$[x^6]M = 0 \Rightarrow \sum A_k^2 = 0 \Rightarrow A_k = 0 \ \forall k$

$[x^4z^2]M = 0 \Rightarrow \sum E_k^2 + 2A_kH_k = \sum E_k^2 = 0 \Rightarrow E_k = 0 \ \forall k$

$[x^2z^4]M = 0 \Rightarrow \sum 2E_kJ_k + H_k^2 = \sum H_k^2 = 0 \Rightarrow H_k = 0 \ \forall k$

$D_k, G_k, I_k = 0$ via similar argument to y^6, y^4z^2, y^2z^4

So

$$x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2 = \sum_k (B_k x^2y + C_k xy^2 + F_k xyz + J_k z^3)^2$$

$M(1,\pm1,\pm1) = 0 \Rightarrow \forall k,\ h_k(1,\pm1,\pm1) = 0$. So

$$B_k + C_k + F_k + J_k = B_k + C_k - F_k - J_k = -B_k + C_k - F_k + J_k = -B_k + C_k + F_k - J_k = 0$$

$\Rightarrow B_k = C_k = F_k = J_k$ by linear independance.

$\Rightarrow h_k = 0 \ \forall k$, contradicting M is SOS.

How can we generalize the above? This is the Gram Matrix Method

Defn: For a polynomial $f(\bar{x}) = \sum_{\bar{\alpha}} c_{\bar{\alpha}} \bar{x}^{\bar{\alpha}}$, it's Newton Polytope is

$$N(f) = \text{conv}\{\bar{\alpha} \mid c_{\bar{\alpha}} \neq 0\}$$

Lem: If $f(\bar{x}) = \sum_k h_k^2$, then $\frac{1}{2} N(f) \supseteq N(h_k)$ $\forall k$.

For example,

$$M(x,y,z) = (x^2+y^2-3z^2)x^2y^2 + z^6 = x^4y^2 + x^2y^4 + z^6 - 3x^2y^2z^2$$

$N(M)$ is the triangle w/ vertices $\{(4,2,0), (2,4,0), (0,0,6)\}$. $(2,2,2)$ is int. point.
Then if $M = \sum_k h_k^2$, $N(h_k)$ has lattice points $\{(2,1,0), (1,2,0), (0,0,3), (1,1,1)\}$

This recovers the fact that each h_k can only have monomials x^2y, xy^2, z^3, xyz.
This "automates" the first portion of Motzkin's example.

To automate the rest, say $f(\bar{x}) = \sum c_{\bar{\alpha}} \bar{x}^{\bar{\alpha}} \in P_{n,2d}$ and $f(\bar{x}) = \sum_k h_k(\bar{x})^2$

Write $h_k = \sum_{\bar{\beta}} u_{\bar{\beta}}^{(k)} \bar{x}^{\bar{\beta}}$, $u_{\bar{\beta}} := (u_{\bar{\beta}}^{(1)}, \dots, u_{\bar{\beta}}^{(t)})$. Then comparing coefficients

$$\bar{\alpha} = \sum_{\bar{\beta}+\bar{\beta}'=\bar{\alpha}} u_{\bar{\beta}} \cdot u_{\bar{\beta}'}$$

Conversely, if such vectors $u_{\bar{\beta}}$ exist satisfying the above equations for all α, $f(\bar{x})$ may be expressed as a sum of squares.

Defn: A matrix with the dot product form $(u_{\bar{\beta}} \cdot u_{\bar{\beta}'})$ is a Gram Matrix associated to $f(\bar{x}) = \sum_k h_k(\bar{x})^2$

Prop: A symmetric matrix M is a Gram Matrix for vectors in $\mathbb{R}^t \Leftrightarrow$ it's corresponding quadratic form is PSD and M has rank at most t.

Thm [Choi, Lam, Reznick 1995]: Let $f(\bar{x}) = \sum_{\bar{\alpha}} c_{\bar{\alpha}} \bar{x}^{\bar{\alpha}}$, $V = (u_{\bar{\beta}\bar{\beta}'})$ a symmetric matrix
TFAE

(A) $f(\bar{x})$ is SOS and V is a Gram Matrix associated to $f(\bar{x})$

(B) V is PSD and $\sum_{\bar{\beta}+\bar{\beta}'} u_{\bar{\beta}\bar{\beta}'} = c_{\bar{\alpha}}$ $\forall \bar{\alpha}$