Hilbert's 17th Problem

Anthony Rizzie

University of Connecticut

October 2, 2019

THE MOTIVATION

Given $a \in \mathbb{R}$ with $a \geqslant 0$, then $a = b^2$ for some $b \in \mathbb{R}$.

Does this work for polynomials, i.e., if f is a polynomial and $f(x) \geqslant 0$ for all $x \in \mathbb{R}$, do we have $f = g^2$ for some polynomial g?

Unfortunately, no. If $f(x) = x^2$, then this would be true for $g(x) = x$.

But $f(x) = x^2 + 1$ does not work.

So this begs the question: can f be written as a *sum of squares* of polynomials?

NOTATION

$\mathbb{R}[X]$ is the set of polynomials in one variable X with real coefficients

$\mathbb{R}[X_1, X_2, \ldots, X_n]$ is all polynomials in n variables

We typically shorten $\mathbb{R}[X_1, X_2, \ldots, X_n]$ as $\mathbb{R}[\underline{X}]$, $n > 1$. (And likewise $\mathbb{R}(\underline{X})$ is the field of fractions or set of rational functions)

For $x \in \mathbb{R}^n$, write x as a column vector with x^T its transpose. Then

$$x^T x = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = x_1^2 + \ldots + x_n^2 = ||x||^2.$$

THE BIG QUESTION

For $f \in \mathbb{R}[\underline{X}]$, we write $f \geqslant 0$ on $\mathbb{R}^n$ to mean $f(x) \geqslant 0$ for all $x \in \mathbb{R}^n$.

Let $f \in \mathbb{R}[\underline{X}]$. If f is a sum of squares $f = f_1^2 + \ldots + f_k^2$, then clearly $f \geqslant 0$ on $\mathbb{R}^n$.

So is the converse true, that is, if $f \geqslant 0$ on $\mathbb{R}^n$, can f be written as a sum of squares of elements of $\mathbb{R}[\underline{X}]$?

POLYNOMIALS IN ONE VARIABLE

It turns out that in one variable ($n = 1$) the answer is "yes;" in fact, such an f can always be expressed as a sum of *two* squares!

Let $f \neq 0$ with $f \in \mathbb{R}[X]$. We factor f into irreducibles in $\mathbb{R}[X]$ and write the factorization as

$$f = d \prod_i (X - a_i)^{k_i} \prod_j \left((X - b_j)^2 + c_j^2\right)^{l_j}.$$

Then the following are equivalent:

(1) $f \geqslant 0$ on $\mathbb{R}^n$

(2) $d > 0$ and each k_i is even

(3) $f = g^2 + h^2$ for some $g, h \in \mathbb{R}[X]$

PROOF

The most interesting part of the proof is (2) $\Rightarrow$ (3). The rest is clear if you think about what it means.

If we have two quadratic factors (i.e., complex roots), we need to show that their product can be written as a sum of squares.

This can be done via the "two squares identity:"

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$$

So any product of quadratics can be written as a sum of squares, which gives $f = g^2 + h^2$ by distributing any linear terms and the constant d.

WHAT IF $n \geqslant 2$?

Oddly enough, Hilbert knew this didn't work for $n \geqslant 2$ in 1888, but it took until Motzkin in 1967 to get a concrete counterexample!

The Motzkin example is

$$s(X, Y) = 1 - 3X^2Y^2 + X^2Y^4 + X^4Y^2.$$

As it turns out, $s \geqslant 0$ on $\mathbb{R}^2$ but s is <u>not</u> a sum of squares in $\mathbb{R}[X, Y]$!

Also, the Choi-Lam example for $n = 3$ from 1977:

$$q(X, Y, Z) = 1 + X^2Y^2 + Y^2Z^2 + Z^2X^2 - 4XYZ$$

PROOF OF MOTZKIN COUNTEREXAMPLE

There is an inequality relating the arithmetic and geometric means for $a, b, c \geqslant 0$ that says

$$\frac{a+b+c}{3} \geqslant \sqrt[3]{abc}.$$

So we have that

$$\frac{1+X^2Y^4+X^4Y^2}{3} \geqslant \sqrt[3]{1 \cdot X^2Y^4 \cdot X^4Y^2} = X^2Y^2,$$

which shows that $s(X,Y) \geqslant 0$ on $\mathbb{R}^2$.

Now, assume $s = \sum f_i^2$ for some $f_i \in \mathbb{R}[X,Y]$. Then every f_i has degree at most 3, and comparing the terms in $s(X,Y)$, we must have

$$f_i = a_i + b_iXY + c_iX^2Y + d_iXY^2.$$

But this implies that $\sum b_i^2 = -3$, which is impossible, so $s(X,Y)$ is <u>not</u> a sum of squares!

SOME NEW NOTATION

$V_{d,n}$ (polynomials degree $\leqslant d$, n variables) is isomorphic to $F_{d,n}$ (forms of degree d, n variables), so a sum of squares in one yields a sum of squares in the other.

A homogeneous polynomial, or form, has all of its terms with the same total degree. Examples are $X^2 - Y^2$, $X^2 + 3XY + 4Y^2$, $XYZ + Z^3$, and so on.

You can always make a polynomial $f \in \mathbb{R}[\underline{X}]$ of degree $\leqslant d$ homogeneous by

$$\overline{f}(X_0, \ldots, X_n) = X_0^d f\left(\frac{X_1}{X_0}, \cdots, \frac{X_n}{X_0}\right).$$

This is called the homogenization of f.

HILBERT'S PROGRESS

Denote by

- $P_{d,n}$ the subset of $F_{d,n}$ of all f with $f \geqslant 0$ on $\mathbb{R}^n$ (P for positive semidefinite)
- $\Sigma_{d,n}$ the subset of $F_{d,n}$ consisting of the sums of squares

In 1888, Hilbert proved the following:
For d even, $P_{d,n} = \Sigma_{d,n} \Leftrightarrow n \leqslant 2$ or $d = 2$ or ($n = 3$ and $d = 4$)

We have already shown that $P_{d,1} = \Sigma_{d,1}$. The Motzkin example and Choi-Lam example provide counterxamples in the cases ($d \geqslant 6$, $n \geqslant 3$) and ($d \geqslant 4$, $n \geqslant 4$), respectively, by homogenization.

THE OTHER CASES

$P_{d,2} = \Sigma_{d,2}$ can be deduced from our sum of two squares result for polynomials in one variable combined with homogenization.

If f is a quadratic form ($d = 2$), then we can write

$$f(X_1, \ldots, X_n) = \sum_{i,j=1}^{n} a_{ij} X_i X_j,$$

where $A = (a_{ij})$ is a symmetric matrix. If $f \geqslant 0$ on $\mathbb{R}^n$, it follows that

$$f(\underline{X}) = \underline{X}^T A \underline{X} = \underline{X}^T (U^T U) \underline{X} = (U\underline{X})^T (U\underline{X}) = ||U\underline{X}||^2,$$

which is a sum of squares of linear forms with $\underline{X}$ viewed as a column vector, so we have $P_{2,n} = \Sigma_{2,n}$.

See BCR (in references) for the proof that $P_{4,3} = \Sigma_{4,3}$.

Hilbert's 17th problem

For $f \in \mathbb{R}[\underline{X}]$, is it true that $f \geqslant 0$ on $\mathbb{R}^n \Rightarrow f$ is a sum of squares of *rational* functions, i.e., that

$$f = \sum f_i^2, \ f_i \in \mathbb{R}(\underline{X})?$$

- We already proved this for $n = 1$.
- Hilbert proved the $n = 2$ case in 1893.
- Artin proved the general case in 1927.

Pfister showed in 1967 that at most 2^n squares are needed.

What happens if we consider certain subsets of $\mathbb{R}^n$? Do the same results or something similar hold? The famous result here is often called the Positivstellensatz, the real counterpart of Hilbert's Nullstellensatz.

MOTZKIN EXAMPLE REVISITED

Recall that the Motzkin example is

$$s(X,Y) = 1 - 3X^2Y^2 + X^2Y^4 + X^4Y^2.$$

In light of Hilbert's 17th Problem and its proof, we know that it can be written of a sum of squares of at most $2^2 = 4$ rational functions:

$$s = \frac{X^2Y^2(X^2+Y^2+1)(X^2+Y^2-2)^2 + (X^2-Y^2)^2}{(X^2+Y^2)^2}$$

$$= \left[\frac{X^2Y(X^2+Y^2-2)}{X^2+Y^2}\right]^2 + \left[\frac{XY^2(X^2+Y^2-2)}{X^2+Y^2}\right]^2$$

$$+ \left[\frac{XY(X^2+Y^2-2)}{X^2+Y^2}\right]^2 + \left[\frac{X^2-Y^2}{X^2+Y^2}\right]^2$$

REFERENCES

1. Positive Polynomials and Sums of Squares by Murrary Marshall, Mathematical Surveys and Monographs, Vol 146, 2008

2. Real Algebraic Geometry by J. Bochnak, M. Coste, M.-F. Roy, Springer, 1998
(Note- commonly referred to as "BCR")