Polynomial proofs and operator theory

Mihai Putinar
Mathematics Department
UC Santa Barbara
<mputinar@math.ucsb.edu>

Connections II- 2006

Contents

Proofs

cultural phenomena

depend on language; can produce new concepts, change the language

based on discovery; often including a transcendental element

not always constructive/algorithmic

short, complex, beautiful, wrong, illuminating, ingenious

Challenge

Quantify the fragility of a proof

A few examples

Theorem. *There are infinitely many prime numbers.*

Proof 1. Assume by contradiction that $p_1, ..., p_n$ are all the primes. And factor

$$p_1 ... p_n + 1.$$

Proof 2. (Euler)

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} (1 - \frac{1}{p^s})^{-1}.$$

Gives much more...

Every product of k successive positive integers is divisible by $k!$:

Proof.

$$\frac{(n+1)...(n+k)}{k!} =$$

$$\frac{(n+1)...(n+k)}{k!} = C_{n+k}^{k}$$

e is a transcendental number

Proof. (Hermite) Rewrite

$$e^x = 1 + x + \frac{x^2}{2!} + ... = P_n(x) + O(x^{n+1})$$

as

$$\frac{e^x - P_n(x)}{x^{n+1}} = \sum_{k=0}^{\infty} \frac{x^k}{(n+k+1)!}$$

and differentiate n times:

$$e^x Q(x) - R(x) = \frac{x^{2n+1}}{n!} \sum_{k=0}^{\infty} \frac{(k+n)!}{(n+1)...(2n+k+1)} \frac{x^k}{k!}$$

where Q, R are polynomials with integral coefficients.

Assume $e^N = p/q$ is rational, and take $x = N$ above: the right hand side is arbitrarily small, but not zero, the left hand side is greater than $1/q$.

The transcendence proof follows the same pattern.

Simple statements with complex proofs

The implicit function theorem: $F(x, y) = 0 \Rightarrow y = y(x)$.

$x' = f(t, x), x(0) = x_0$, *admits locally unique solutions if...*

Gauss: every polynomial equation has complex solutions

Stokes Theorem

$$\int_{\Omega} d\omega = \int_{\partial\Omega} \omega$$

Can we write the proof on a postcard?

Yes, if we accept "high" language

Positive polynomials: 1D

A long time favorite of logicians and algebraists and nowadays of everybody.

$p \in \mathbf{R}[x]$ satisfies $p \geq 0$ on $\mathbf{R}$ iff $p = q_1^2 + ... + q_n^2$, in short $p \in \Sigma^2\mathbf{R}[x]$

Reduction to two squares:

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

as follows from the multiplication of complex numbers

$$|a + ib|^2|c + id|^2 = |(ac - bd) + i(ad + bc)|^2.$$

Positive polynomials: nD

Structure far from being simple, requires Tarski's transfer principle and some transcendental elements (the real spectrum...)

Not all non-negative polynomials are sums of squares...

Open problem Given a polynomial $P(x) = \sum_{|\alpha| \leq d} c_\alpha x^\alpha$ find $effective$ criteria in terms of the coefficients (c_α), so that $P(a) \geq 0$ for all $a \in \mathbf{R}^n$.

Example, widely used today:

Stengle's Theorem

$p_1, ..., p_r \in \mathbf{R}[x_1, ..., x_d]$. Let $S = \{x \in \mathbf{R}^d; p_j(x) \geq 0\}$ and let $T = PO(p_1, ..., p_r)$ be the preorder generated by p_i. Let $f \in \mathbf{R}[x_1, ..., x_d]$. Then

(a). $f > 0$ on S if and only if there are $s, t \in T$ satisfying $sf = 1 + t$;

(b). $f \geq 0$ on S if and only if there are $s, t \in T$ and an integer $N \geq 0$, with the property $sf = f^{2N} + t$;

(c). $f = 0$ on S if and only if there exists an integer $N \geq 0$ with the property $-f^{2N} \in T$.

Linear algebra can help

two fold simplification:

pass to free variables

use matrix analysis instead of Tarski's principle

Some recent results

J.W.Helton, S. McCullough, M.P. ,

A non-commutative Positivstellensatz on isometries, J. reine angew. Math. **568**(2004), 71-80.

Non-negative hereditary polynomials in a free $*-$ algebra, Math. Zeitschrift **250**(2005), 515-522.

Strong majorization in a free $*$-algebra, Math. Zeitschrift, D.O. I. 10.1007/s00209-006-0032-0

Free $*$-algebra

$\mathbf{F} = \mathbf{R}\langle x, x^* \rangle$ is the free algebra in variables $x_1, ..., x_d, x_1^*, ..., x_d^*$.

with involution

$$(fg)^* = g^* f^*, \qquad (x_j)^* = x_j^*.$$

Every finite dim. representation $\rho : \mathbf{F} \longrightarrow M_n(\mathbf{R})$ is determined by an n-tuple of matrices

$$\rho(x_j) = X_j, \quad 1 \leq j \leq d.$$

No constraints on X_j.

Positivity sets and zero sets

Let $S \subset \mathbf{F}$. The associated zero set:

$$V(S) = \{(X, v) \in \bigcup_{d \geq 1} (M_d(\mathbb{R})^n \times \mathbb{R}^d); \quad v \neq 0, \ f(X)v = 0, \quad \text{all } f \in S\}.$$

Assume all elements of S are formally symmetric:

$$K_S = \{(X, v) \in \bigcup_{d \geq 1} (M_d(\mathbb{R})^n \times \mathbb{R}^d); \quad v \neq 0, \ \langle f(X)v, \ v\rangle \geq 0, \quad \text{all } f \in S\}.$$

Nichtnegativstellensatz

Assume $p_1(x), ..., p_m(x) \in \mathbf{F}$ do not depend on x^*

let $q = q^* \in \mathbf{F}$

If $\langle q(X)v, v\rangle \geq 0$ whenever $p_i(X)v = 0$, all i, then

$$q \in \Sigma^2 + \sum_i (f_i p_i + p_i^* f_i^*).$$

Nullstellensatz

Assume $p_1(x), ..., p_m(x) \in \mathbf{F}$ do not depend on x^*

let $q \in \mathbf{F}$

If $q(X)v = 0$ whenever $p_i(X)v = 0$, all i, then

$$q = \sum_i f_i p_i.$$

Commutative Nullstellensatz

Let I be an ideal in the commutative polynomial ring $\mathbb{C}[x_1, ..., x_d]$ and let $q \in \mathbb{C}[x_1, ..., x_d]$ be given. Then

$q \in I$ if and only if $q(X) = 0$

for all commuting tuples of matrices X annihilated by the ideal I.

In general, when only evaluating at points of $\mathbf{C}^d$, one needs

$$q^N \in I$$

.

Complex variables

Let $q \in \mathbf{C}[z, \overline{z}]$ be given. There exist polynomials $r_j \in \mathbf{C}[z],\ 1 \leq j \leq n$, with

$$q(z, \overline{z}) = \sum_{j=1}^{n} |r_j(z)|^2,$$

if and only if, for all commuting g-tuples of matrices X we have $q(X, X^*) \geq 0$.

General Nullstellensatz

Suppose $q, p_1, \ldots p_n \in \mathbf{F}$, and assume that the zero set $V(\{p_1, \ldots, p_n\})$ is non-empty. Then

$$V(\{p_1, \ldots, p_n\}) \subset V(q)$$

if and only if there exists $C_{min} > 0$ with the property that for each pair of real numbers $C > C_{min}$ and $\lambda > 0$, there exist sums of squares $\sigma_+, \sigma_-, \sigma_j \in \Sigma^2,\ j = 1, 2, \ldots, n$, such that

$$q^* q + \sigma_+ + \sigma_- \star (C^2 - \sum x_j^* x_j) = \lambda + \sum_{j=1}^{n} p_j^* \sigma_j p_j. \tag{1}$$

Nichtnegativstellensatz with spherical supports

Let

$$\mathbf{S} = \cup_n \{X = (X_1, ..., X_d) \in M_n(\mathbb{R}) : \ X_1^* X_1 + ... + X_d^* X_d = I\}$$

be the set of all spherical isometries.

Let $I_{\mathbf{S}} = \{f \in \mathbf{F};\ f(X, X^*) = 0,\ X \in \mathbf{S}\}$ the associated ideal in the free algebra.

If $p \in \mathbf{F}$ *satisfies* $p(X, X^*) \geq 0$ *whenever* $X \in \mathbf{S}$, *then*

$$p \in \Sigma^2 \mathbf{F} + I_{\mathbf{S}}.$$

Weyl algebra

Generated by the operators

$$\Phi(p_k)f = -i\frac{\partial f}{\partial x_k}, \quad \Phi(q_k)f = x_k f,$$

Schmüdgen: *Let $f \in W(g)$ be a self-adjoint element of even degree $2m$, and let $P(z,\overline{z})$ be its principal symbol. If*

a). There exists $\epsilon > 0$ such that $f - \epsilon \cdot 1 \in W(g)_+$,

b). $P(z,\overline{z}) > 0$ for $z \neq 0$,

then, if m is even there exists $b \in \mathcal{N}$ such that $bfb \in \Sigma^2 W(g)$; if m is odd, there exists $b \in \mathcal{N}$ such that $\sum_{j=1}^{g} ba_j f a_{-j} b \in \Sigma^2 W(g)$.

Matrix algebras

of a fixed dimension

S. A. AMITSUR, *A generalization of Hilbert's Nullstellensatz*, Proc. Amer. Math. Soc. **8**(1957), 649-656.

C. PROCESI, M. SCHACHER, *A non-commutative real Nullstellensatz and Hilbert's 17th problem*, Ann. of Math. **(2) 104** (1976), 395–406

Unifying factor: the proof

Consider the statement: $f(X) \geq 0$ *if* $X \in \mathbf{T} \Leftrightarrow f \in \Sigma^2\mathbf{F} + \mathrm{residual}(\mathbf{T})$.

In general $\Leftarrow$ is trivial.

The proof of the implication $\Rightarrow$ uses duality:

Assume that $f(X) \geq 0$ if $X \in \mathbf{T}$ and in the same time $f \notin \Sigma^2\mathbf{F} + \mathrm{residual}(\mathbf{T})$.

Construct a linear functional $L \in \mathbf{F}'$ such that

$$L|_{\Sigma^2\mathbf{F}+\mathrm{residual}(\mathbf{T})} \geq 0 \quad \text{but} \quad L(f) < 0.$$

Structure of non-negative functionals

Remember $L|_{\Sigma^2\mathbf{F}+\mathrm{residual}(\mathbf{T})} \geq 0$

This defines an inner product on $\mathbf{F}$:

$$\langle u, v \rangle = L(v^* u).$$

Left multiplication by the variables defines linear operators

$$M_j u = x_j u, \quad u \in \mathbf{F}.$$

Tautology

$M = (M_1, ..., M_d)$ left multipliers by the variables

$L|_{\text{residual}(\mathbf{T})} \geq 0$ implies $M \in \mathbf{T}$.

On the other hand

$$\langle f(M, M^*)1, 1\rangle = \langle f(x, x^*), 1\rangle = L(f) < 0,$$

a contradiction.

Old root: the spectral theorem

D. Hilbert, F. Riesz (about 100 years ago):

Let $X = X^* \in M_n(\mathbf{C}), \quad \|X\| \leq 1$

For every vector $\xi \in \mathbf{C}^n$ the functional

$$L_\xi(p) = \langle p(X)\xi, \xi \rangle$$

satisfies $(L_\xi)|_{\Sigma^2 + (1-x^2)\Sigma^2} \geq 0$. And vice-versa.

Thus $L_\xi(p) = \int_{-1}^{1} p d\mu_\xi, \quad p \in \mathbf{C}[x]$.