Def: To a quadratic module M we associate

$$H(M) := \{ a \in \mathbb{R}\langle x \rangle \mid \exists N \in \mathbb{N} \quad N - a^* a \in M \}$$

Lemma: $H(M)$ is a subring.

Proof: $a, b \in H(M)$, say $p_1 := \alpha^2 - a^* a \in M$

$p_2 := \beta^2 - b^* b \in M$ for $\alpha, \beta > 0$.

Then $(\lambda a + \mu b)^* (\lambda a + \mu b) =: p_{\lambda,\mu} \in M$

$$\lambda\mu (a^* b + b^* a) = p_{\lambda,\mu} - \lambda^2 a^* a - \mu^2 b^* b$$

Apply to $\lambda = \beta, \ \mu = \pm \alpha$

$$\pm (a^* b + b^* a) + 2\alpha\beta = \frac{1}{\alpha\beta}\left(p_- + \beta^2 p_1 + \alpha^2 p_2\right) \in M$$

Hence

$$(\alpha+\beta)^2 - (a+b)^*(a+b) = \underbrace{\alpha^2 - a^* a}_{\in M} + \underbrace{\beta^2 - b^* b}_{\in M} + \underbrace{(2\alpha\beta - a^* b - b^* a)}_{\in M} \in M$$

- $b^* \backslash \ \alpha^2 - a^* a = p_1 \in M \ / b$

$$b^* a^* a b = \alpha^2 b^* b - b^* p_1 b$$

$$= \alpha^2 (\beta^2 - p_2) - b^* p_1 b \Rightarrow \alpha^2 \beta^2 - (ab)^*(ab) - \alpha^2 p_2 + b^* p_1 b \in M.$$

Lemma: A q. module M is archimedean $\iff H(M) = \mathbb{R}\langle X\rangle$

Proof: Suppose $\overbrace{N - \sum X_j^2}^{P} \in M$

Then $N - x_j^2 = P + \sum_{k \neq j} x_k^2 \in M$

$\Rightarrow \forall j \quad x_j \in H(M) \Rightarrow H(M) = \mathbb{R}\langle x\rangle$.

Conversely, if $H(M) = \mathbb{R}\langle x\rangle$ then

$\forall j \ \exists N_j .\ N_j - x_j^2 \in M$.

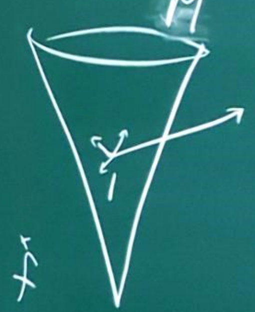
Then $\underbrace{\left(\sum N_j\right)}_{N} - \sum x_j^2 \in M$ ■

Puzzle Of The Day #2

Suppose $QM(S) \subseteq \mathbb{R}[t_1, t_d]$ is archimedean.
$\varphi : \mathbb{R}[t] \to \mathbb{R}$ is a <u>state</u> if $\varphi(1) = 1$ & $\varphi(QM(S)) \subseteq [0,\infty)$
("states form a convex set")
What are pure states
(:= extreme points)

For $s \in \mathbb{R}\langle X\rangle_{sa}$ we have $s = \left(\frac{s+1}{2}\right)^2 - \left(\frac{s-1}{2}\right)^2$

Hence $1 \in \mathbb{R}\langle X\rangle_{sa}$ is an <u>algebraic interior point</u> for arch. $M \subseteq \mathbb{R}\langle X\rangle_{sa}$.



$\forall p \ \exists \varepsilon > 0$

$1 + \varepsilon \cdot p \in M$

Proof (HM04 Positivstellensatz): $f \succ 0$ on $\mathcal{D}_S^\infty$

Assume $f \notin QM(S)$.

By "a" Hahn–Banach separation theorem
(Eidelheit–Kakutani 30s) $\quad \exists L : \mathbb{R}\langle X\rangle_{sa} \to \mathbb{R}$ st.

$L(QM(S)) \subseteq [0,\infty)$

$L(f) \leq 0$

Extend L to $\mathbb{R}\langle x\rangle$ by $p \mapsto \frac{1}{2}L(p+p^*)$.

$\langle p, q\rangle := L(q^*p)$ is a semi-scalar product

$\mathcal{N} := \{p \mid L(p^*p) = 0\}$ is a subspace of $\mathbb{R}\langle x\rangle$

(Cauchy–Schwarz ineq.)

Letting $\overline{} : \mathbb{R}\langle x\rangle \longrightarrow \mathbb{R}\langle x\rangle/\mathcal{N}$, $\langle \bar{p}, \bar{q}\rangle := L(q^*p)$

defines a scalar product on $\mathbb{R}\langle x\rangle/\mathcal{N}$.

Let E be its completion.

- Construct $X_j \in \mathcal{B}(E)_{sa}$.

$\mathcal{N}$ is a left ideal. To show $x_j\mathcal{N} \subseteq \mathcal{N}$.

Let $m \in \mathbb{N}$ satisfy $m - x_i^2 \in QM(S)$

Then for $p \in \mathbb{R}\langle x\rangle$,

$$(*) \quad 0 \leq L\left(p^*(m - x_i^2)p\right) \leq m \cdot L(p^*p)$$

So for $p \in \mathcal{N}$, we set $L(p^*x_i^2p) = 0$, i.e., $x_ip \in \mathcal{N}$

The map $X_j : \mathbb{R}\langle x\rangle/\mathcal{N} \longrightarrow \mathbb{R}\langle x\rangle/\mathcal{N}$, $\bar{p} \longmapsto \overline{x_jp}$ is a (well-defined) linear map.

By $(*)$, X_j is bounded.

As yesterday, X_j is s.a.

So extends to $X_j \in \mathcal{B}(E)_{sa}$

We claim $X=(X_1\dots X_d)\in \mathcal{D}_S^\infty$.

Let $p\in S$, $v\in E$. Wlog $v=\overline{h}\in \mathbb{R}\langle x\rangle/\mathcal{N}$

Then $\langle p(X)v,v\rangle = \langle p(X)\overline{h},\overline{h}\rangle$

$= \langle \overline{ph}, \overline{h}\rangle = L(\underbrace{h^* \underset{\underset{S}{\in}}{p} h}_{\in QM(S)}) \geq 0$

Then

$0\geq L(f) = \langle \overline{f},\overline{T}\rangle = \langle f(x)\overline{T},\overline{T}\rangle \overset{f\succ 0 \text{ on } \mathcal{D}_S^\infty}{>} 0$

$\lightning$

Puzzle Of The Day #2

Suppose $QM(S)\subseteq \mathbb{R}[t_1 \dots t_d]$ is archimedean.

$\varphi: \mathbb{R}[t]\to\mathbb{R}$ is a state if $\varphi(1)=1$ & $\varphi(QM(S))\subseteq[0,\infty)$

(states form a convex set)

What are pure states (:= extreme points)

Commutative Detour

$t=(t_1\dots t_d)$ commuting variables

$\mathbb{R}[t]$ commutative polynomials

$K_S=\{a\in\mathbb{R}^d \mid \forall s\in S \ \ s(a)\geq 0\}$

$S\subseteq\mathbb{R}[t]$, $\underbrace{QM(S)}_{\text{q. module}}=\left\{\sum_{i=1}^r a_i^2\cdot s_i \,\middle|\, r\in\mathbb{N},\ a_i\in\mathbb{R}[t],\ s_i\in S\cup\{1\}\right\}$

$S\cup\{1\}\subseteq QM(S)$, $QM(S)+QM(S)$, $\forall a\in\mathbb{R}[t]\ \ a^2\cdot QM(S)\subseteq QM(S)$

Corollary (Putinar 1993): Suppose $QM(S)$ is archim.

If $p|_{K_S}>0$, then $p\in QM(S)$.

Proof: As in HM04, $\exists$ Hilbert space E,

$\exists$ s.a. $T_j\in\mathcal{B}(E)$, T_j's commute.

We claim $X = (X_1 \ldots X_d) \in \mathcal{D}_S^{\infty}$.

Let $p \in S$, $v \in E$. Wlog $v = \overline{h} \in \mathbb{R}\langle x \rangle / \mathcal{N}$

Then $\langle p(X) v, v \rangle = \langle p(X) \overline{h}, \overline{h} \rangle$

$= \langle \overline{ph}, \overline{h} \rangle = L(\underbrace{h^* \underset{\underset{S}{\in}}{p} h}_{\in QM(S)}) \geq 0$

Then

$$0 \geq L(f) = \langle \overline{f}, \overline{1} \rangle = \langle f(x) \overline{1}, \overline{1} \rangle \overset{\substack{f \succ 0 \\ \text{on } \mathcal{D}_S^{\infty}}}{>} 0$$

$\Downarrow$

$\blacksquare$

Puzzle Of The Day #2

Suppose $QM(S) \subseteq \mathbb{R}[t_1 \ldots t_d]$ is archimedean.

$\varphi : \mathbb{R}[t] \to \mathbb{R}$ is a state if $\varphi(1) = 1$ & $\varphi(QM(S)) \subseteq [0, \infty)$

(states form a convex set)

What are pure states (:= extreme points)

Commutative Detour

$t = (t_1 \ldots t_d)$ commuting variables

$\mathbb{R}[t]$ commutative polynomials

$\boxed{K_S = \{ a \in \mathbb{R}^d \mid \forall s \in S \ \ s(a) \geq 0 \}}$

$S \subseteq \mathbb{R}[t]$, $\underbrace{QM(S) = \left\{ \sum_{i=1}^{r} a_i^2 \cdot s_i \,\middle|\, r \in \mathbb{N}, a_i \in \mathbb{R}[t], s_i \in S \cup \{1\} \right\}}_{q.\text{ module}}$

$S \cup \{1\} \subseteq QM(S)$, $QM(S) + QM(S)$, $\forall a \in \mathbb{R}[t]$ $a^2 \cdot QM(S) \subseteq QM(S)$

Corollary (Putinar 1993): Suppose $QM(S)$ is archim.

If $p|_{K_S} > 0$, then $p \in QM(S)$.

Proof: As in HM04, $\exists$ Hilbert space E,

$\exists$ s.a. $T_j \in \mathcal{B}(E)$, T_j's commute.

$\exists \eta \in E$ s.t. $L(f) = \langle f(T) \eta, \eta \rangle$.

Apply Spectral Theorem to T_j's.

E = spectral measure

Then $\mu(B) := \langle E(B)\eta, \eta \rangle$

is a Borel measure on $\mathbb{R}^d$

w/ moments $\mu_\alpha = L(t^\alpha)$; $t^\alpha = t_1^{\alpha_1} \cdots t_d^{\alpha_d}$, $\alpha = (\alpha_1, \dots, \alpha_d)$

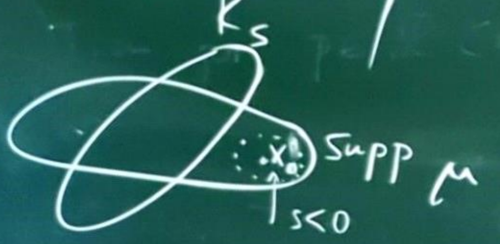
By archimedeanity, $\|T_j\| \le N$ for some $N \in \mathbb{N}$

and thus $\operatorname{supp}\mu \subseteq [-N, N]^d$

Claim: $\operatorname{supp}\mu \subseteq K_S$.

Note $L(f^2 s) \ge 0 \quad \forall s \in S \quad \forall f \in \mathbb{R}[t]$

Suppose $s \not\geq 0$ on $\operatorname{supp}\mu$.



$s(x_0) < 0$

Pick c cts function s.t. $c|_{K_S} = 0$ & $c > 0$ on

& $c| = 0$

Then $\int c \cdot s \, d\mu < 0$

By Stone–Weierstraß $\exists$ seq of polys $(p_n)_n$ s.t. $p_n \xrightarrow{\mu} \sqrt{c}$

Thus

$$0 \le \int p_n^2 s \, d\mu \xrightarrow{n \to \infty} \int c \cdot s \, d\mu < 0 \quad \lightning$$

Putinar[93] = comm. version of HM04.

What is the comm. version of Helton's SOS thm?

Example (Motzkin 1965) $m = t_1^4 t_2^2 + t_1^2 t_2^4 + 1 - 3t_1^2 t_2^2$

Then $m|_{\mathbb{R}^2} \geq 0$ and m is not sos.

AM-GM inequality

$$\frac{t_1^4 t_2^2 + t_1^2 t_2^4 + 1}{3} \geq \sqrt[3]{t_1^4 t_2^2 t_1^2 t_2^4 \cdot 1} = t_1^2 \cdot t_2^2$$

OR

$(t_1^2+t_2^2)\cdot m = t_1^2 t_2^2 (t_1^2+t_2^2+1)(t_1^2+t_2^2-2)^2 + (t_1^2-t_2^2)^2$ is sos

Puzzle Of The Day #2

Suppose $QM(S) \subseteq \mathbb{R}[t_1, t_2]$ is archimedean.

$\varphi : \mathbb{R}[t] \to \mathbb{R}$ is a state if $\varphi(1)=1$ & $\varphi(QM(S)) \subseteq [0,\infty)$

(states form a convex set)

What are pure states (:= extreme points)

Commutative Detour

Why is m not sos?

m is sos $\Leftrightarrow \exists G \succeq 0 \quad m = \overrightarrow{[t]_3}^T \cdot G \cdot \overrightarrow{[t]_3}$

If m is sos, only monomials in

$1, \cancel{t_1}, \cancel{t_2}, \cancel{t_1^2}, t_1t_2, \cancel{t_2^2}, \cancel{t_1^3}, t_1^2t_2, t_1t_2^2, \cancel{t_2^3}$

can appear in sos decomposition. Proof w/ colors ($t_1^2t_2^2$ coeff must be ≥ 0)

Ex (Choi-Lam 76)

$$r = t_1^2t_2^2 + t_2^2t_3^2 + t_1^2t_3^2 + 1 - 4t_1t_2t_3$$

is ≥ 0 on $\mathbb{R}^3$, not sos.

pos vs sos

deg \ #vars	1	2	3	4
2	✓	✓	✓	✓
4	✓	✓	X	X
6	✓	X	X	X
8	✓	X	X	X

Hilbert

Hilbert's 17th Problem (1900)

If $f \in \mathbb{R}[t]$ satisfies $f|_{\mathbb{R}^d} \geq 0$, must $f \in \underbrace{\sum \mathbb{R}(t)^2}_{\overset{\shortparallel}{P}}$?

Theorem (Artin 1926): Yes.

Proof: Assume $f \notin P$.

P satisfies $\underbrace{P+P \subseteq P,\ P\cdot P \subseteq P,\ \forall a \in \mathbb{R}(t):\ a^2 \in P}_{\text{preordering}},\ \underbrace{-1 \notin P}_{\text{proper}}$

Consider $Q \leftarrow$ max. proper preordering w/ $f \notin Q$.

$Q \cap -Q = \{0\}$: if $0 \neq a \in Q \cap -Q$ then

$$-a^{-1} = \underset{\overset{\cap}{Q}}{(-a)} \cdot \underset{\overset{\cap}{Q}}{(a^{-1})^2} \in Q$$

$\Rightarrow -1 \in Q$ ↯

$Q \cup -Q = \mathbb{R}(t)$: $a \notin Q$

$Q - a\cdot Q$ is a preordering

if $-1 \in Q - aQ$, say $-1 = x - ay$

then $a = (x+1)\cdot y \cdot (y^{-1})^2 \in Q$ ↯

$\Rightarrow$ $a \geq_Q 0 :\Leftrightarrow a \in Q$ is a total (linear) ordering on $\mathbb{R}(t)$.

Tarski's transfer principle

if a system of real polynomial equations and inequalities has a solution in an **ordered** field extension of $\mathbb{R}$, then it must have real solutions!

Consider System $\{f<0\}$

This system has a solution in $(\mathbb{R}(t), \leq_Q)$, namely $(t_1 \dots t_d)$ since $f(t_1 \dots t_d) = f <_Q 0$.

So $\exists (a_1 \dots a_d) \in \mathbb{R}^d$ s.t. $f(a_1 \dots a_d) < 0$ by Tarski. $\lightning$ ∎

Puzzle Of The Day #2

Suppose $QM(S) \subseteq \mathbb{R}[t_1 \dots t_d]$ is archimedean.

$\varphi : \mathbb{R}[t] \to \mathbb{R}$ is a **state** if $\varphi(1) = 1$ & $\varphi(QM(S)) \subseteq \mathbb{R}_{\geq 0}$

(states form a convex set)

What are pure states ($:=$ extreme points)

Semialgebraic sets: Boolean algebra generated by $U(f) := \{a \in \mathbb{R}^d \mid f(a) > 0\}$

(Boolean algebra: finite $\cup$, finite $\cap$, complements)

Tarski (reformulated): Projection of a semialgebraic set is semialgebraic

Ex: $B := \{(p, q, X) \in \mathbb{R}^3 \mid X^2 + pX + q = 0\}$ is semialgebraic

$$pr_X B = \{(p,q) \in \mathbb{R}^2 \mid \exists X \in \mathbb{R} \; X^2 + pX + q = 0\}$$

$$= \{(p,q) \in \mathbb{R}^2 \mid p^2 - 4q \geq 0\}$$ is indeed semialg.

Applications

Putnar[93] has been "implemented" by Lassorre[2001].

This computes optima of polys / cpt. semialg sets

$\longrightarrow$ Polynomial Optimazation

HM04 has been "implemented" by PNA

P – Pironio, N – Navascues, A – Acin
2007, 2008, 2010

Wanted to solve Bell inequalities

CHSH (Clauser, Horne, Shimony, Holt 1969)

$x_1, x_2, \quad y_1, y_2$ nc variables

$$\max \operatorname{spec}\big(\overbrace{x_1 y_1 + x_1 y_2 + x_2 y_1 - x_2 y_2}^{b}\big)$$

s.t. $X_j, Y_j \in B(H)_{sa}$

$X_j^2 = 1, \; Y_j^2 = 1$

$[X_j, Y_k] = 0$

$QM := SOS + \operatorname{ideal}(x_j^2 - 1, y_k^2 - 1, [x_p, y_q])$

is an archimedean QM.

$b \le \lambda \iff \lambda - b \ge 0$

$\overset{}{\underset{HM04}{\iff}} \lambda - b + \varepsilon \in QM \;\; \forall \varepsilon > 0$ (PNA "computes" this)

Answ: $2\sqrt{2}$

Tarski's transfer principle

if a system of real polynomial equations and inequalities has a solution in an ordered field extension of $\mathbb{R}$, then it must have real solutions!

Consider System $\{f<0\}$

This system has a solution in $(\mathbb{R}(t), \leq_Q)$, namely $(t_1, \dots, t_d)$ since $f(t_1, \dots, t_d) = f <_Q 0$.

So $\exists (a_1, \dots, a_d) \in \mathbb{R}^d$ s.t. $f(a_1, \dots, a_d) < 0$ by Tarski. $\lightning$ $\blacksquare$

Puzzle Of The Day #2

Suppose $QM(S) \subseteq \mathbb{R}[t_1, \dots, t_d]$ is archimedean.

$\varphi : \mathbb{R}[t] \to \mathbb{R}$ is a state if $\varphi(1) = 1$ & $\varphi(QM(S)) \subseteq [0, \infty)$

(states form a convex set)

What are pure states (:= extreme points)

Tsirelson conjecture[93]: Solving a Bell ineq. over finite dim $\mathcal{H}$ gives the same value as solving the Bell ineq. over general Hilb. spaces

Fritz[2012] & Junge – Navascues – Palazuelos – Perez-Garcia – Scholz – Werner[2011]

Tsirelson $\Leftrightarrow$ Connes' embedding Conjecture $\Leftrightarrow$ Kirchberg conjecture

Prof. Ozawa[2013] survey

$C^*(\mathbb{F}_d) \otimes_{max} C^*(\mathbb{F}_d) = C^*(\mathbb{F}_d) \otimes_{min} C^*(\mathbb{F}_d)$

Ji – Natarajan – Vidick – Wright – Yuen[2020].

CEC is false.