Quantum information theory and Reznick's Positivstellensatz

Ion Nechita (CNRS, LPT Toulouse)
— joint work with Alexander Müller-Hermes and David Reeb

Besançon, November 29th, 2019

Talk outline

Sums of squares and Reznick's Positivstellensatz

Poylnomials vs. symmetric operators

The complex Positivstellensatz

Sums of squares and Reznick's Positivstellensatz

Hilbert's 17th problem

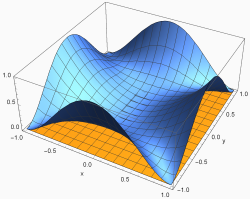
- $\mathbb{R}[x] \ni P(x) \geq 0 \iff P = Q_1(x)^2 + Q_2(x)^2$, for $Q_{1,2} \in \mathbb{R}[x]$
- $\mathrm{Pos}(d, n) := \{P \in \mathbb{R}[x_1, \ldots, x_d]$ hom. of deg. $2n$, $P(x) \geq 0, \forall x\}$
- $\mathrm{SOS}(d, n) := \{\sum_i Q_i^2$ with $Q_i \in \mathbb{R}[x_1, \ldots, x_d]$ hom. of deg. $n\}$
- Hilbert 1888:

$$\mathrm{SOS}(d, n) \subseteq \mathrm{Pos}(d, n), \text{ eq. iff } (d, n) \in \{(d, 1), (2, n), (3, 2)\}$$

- The Motzkin polynomial $x^4y^2 + y^4z^2 + z^4x^2 - 3x^2y^2z^2$ is positive but not SOS
- Membership in SOS can be efficiently decided with a semidefinite program (SDP) and provides an algebraic certificate for positivity

More on the Motzkin polynomial

The non-homogeneous Motzkin polynomial (set $z = 1$) $x^4y^2 + y^4 + x^2 - 3x^2y^2$ can be seen to be positive by the AMGM inequality



There exist computer algebra packages to check SOS and perform polynomial optimization using SOS ([NC]SOSTOOLS, Gloptipoly)

```
>> syms x y z; findsos(x^4*y^2 + y^4 + x^2 -
3*x^2*y^2)

Size:  49 19
...
No sum of squares decomposition is found.
```

Reznick's Positivstellensatz

- Hilbert 1900, Artin 1927:

$$P \geq 0 \iff P = \sum_i \frac{Q_i^2}{R_i^2}$$

In particular, if $P \geq 0$, there exists R such that $R^2 P$ is SOS

Theorem. [Reznick 1995]

Let $P \in \mathrm{Pos}(d, k)$ such that $m(P) := \min_{\|x\|=1} P(x) > 0$. Let also $M(P) := \max_{\|x\|=1} P(x)$. Then, for all

$$n \geq \frac{dk(2k-1)}{2 \ln 2} \frac{M(P)}{m(P)} - \frac{d}{2},$$

we have

$$(x_1^2 + \cdots + x_d^2)^{n-k} P(x) = \sum_{j=1}^{r} (a_1^{(j)} x_1 + \cdots a_d^{(j)} x_d)^{2n}.$$

In particular, $\|x\|^{2(n-k)} P$ is SOS.

Poylnomials vs. symmetric operators

From the symmetric subspace to polynomials — $\mathbb{R}$

- Homogeneous polynomials of degree n in d real variables $x_1, \ldots, x_d$ are in one-to-one correspondence with symmetric tensors:

$$\vee^n \mathbb{R}^d \ni v \rightsquigarrow P_v(x_1, \ldots, x_d) = \langle x^{\otimes n}, v \rangle$$

where $x = (x_1, \ldots, x_d)$ is the vector of variables

- $n = 1,\ P_v(x) = \sum_{i=1}^d v_i x_i$
- $|GHZ\rangle = |000\rangle + |111\rangle \rightsquigarrow P_{|GHZ\rangle}(x, y) = x^3 + y^3$
- $|W\rangle = |001\rangle + |010\rangle + |001\rangle \rightsquigarrow P_{|W\rangle}(x, y) = 3x^2 y$
- If $|\Omega\rangle = \sum_{i=1}^d |ii\rangle$, then $P_{|\Omega\rangle^{\otimes n}}(x_1, \ldots, x_d) = (\sum_{i=1}^d x_i^2)^n = \|x\|^{2n}$

- We denote $d[n] := \dim \vee^n \mathbb{R}^d = \binom{n+d-1}{n}$

From the symmetric subspace to polynomials — $\mathbb{C}$

- In the complex case, we are interested in bi-homogeneous polynomials of degree n in d complex variables: $P(z_1, \ldots, z_d)$ is hom. in the variables z_i and also in $\bar{z}_i$.
- Bi-hom. polynomials are in one-to-one correspondence with operators on $\vee^n \mathbb{C}^d$:

$$P(z_1, \ldots, z_d) = \langle z^{\otimes n} | W | z^{\otimes n} \rangle$$

- Self-adjoint W are associated to real, bi-hom. polynomials
- $\|z\|^{2n} = \langle z^{\otimes n} | P_{sym}^{(d,n)} | z^{\otimes n} \rangle$
- More generally, polynomials which are bi-hom. of degree n in complex variables $z_1, \ldots, z_d$ and, separately, bi-hom. of degree k in complex variables $u_1, \ldots, u_D$ are in one-to-one correspondence with operators on $\vee^n \mathbb{C}^d \otimes \vee^k \mathbb{C}^D$:

$$Q(z_1, \ldots, z_d, u_1, \ldots, u_D) = \langle z^{\otimes n} \otimes u^{\otimes k} | W | z^{\otimes n} \otimes u^{\otimes k} \rangle$$

The different notions of positivity

A self-adjoint matrix $W \in \mathcal{B}(\vee^n \mathbb{C}^d)$ is called

- block-positive if $\langle z^{\otimes n} | W | z^{\otimes n} \rangle \geq 0$, $\forall z \in \mathbb{C}^d$
- positive semidefinite (PSD) if $\langle u | W | u \rangle \geq 0$, $\forall u \in \vee^n \mathbb{C}^d$
- separable if $W \in \mathrm{conv}\{|z\rangle\langle z|^{\otimes n}\}_{z \in \mathbb{C}^d}$

We have: W separable $\implies$ W PSD $\implies$ W block-positive

- W is block-positive $\iff$ P_W is non-negative:

$$P_W(z) = \langle z^{\otimes n} | W | z^{\otimes n} \rangle \geq 0, \qquad \forall z \in \mathbb{C}^d$$

- W is PSD $\iff$ P_W is Sum Of hom. Squares:

$$W = \sum_j \lambda_j |w_j\rangle\langle w_j| \implies P_W(z) = \sum_j \lambda_j |\langle z^{\otimes n}, w_j \rangle|^2$$

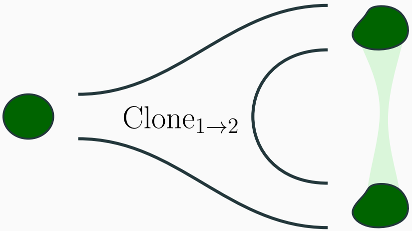
- W is separable $\iff$ P_W is Sum Of hom. Powers:

$$W = \sum_j t_j |a_j\rangle\langle a_j|^{\otimes n} \implies P_W(z) = \sum_j t_j |\langle z, a_j \rangle|^{2n}$$

Tensoring with the identity

- For $k \le n$, let $\mathrm{Tr}^*_{k\to n} : \mathcal{B}(\vee^k \mathbb{C}^d) \to \mathcal{B}(\vee^n \mathbb{C}^d)$ be the map
$$\mathrm{Tr}^*_{k\to n}(W) = P^{(d,n)}_{sym} \left[W \otimes I_d^{\otimes(n-k)} \right] P^{(d,n)}_{sym}$$
- We have: $P_{\mathrm{Tr}^*_{k\to n}(W)}(z) = \|z\|^{2(n-k)} P_W(z)$

$\mathrm{Clone}_{k\to n} := \frac{d[k]}{d[n]} \mathrm{Tr}^*_{k\to n}$ is the optimal Keyl-Werner cloning quantum channel: among all quantum channels sending states $\rho^{\otimes k}$ to symmetric n-partite states σ, it is the one which achieves the largest fidelity between ρ and $\mathrm{Tr}_{2\cdots n}\,\sigma$



The partial trace

For $k \le n$, let $\mathrm{Tr}_{n\to k} : \mathcal{B}(\vee^n \mathbb{C}^d) \to \mathcal{B}(\vee^k \mathbb{C}^d)$ be the partial trace

$$\mathrm{Tr}_{n\to k}(W) = \left[\mathrm{id}^{\otimes k} \otimes \mathrm{Tr}^{\otimes(n-k)}\right](W)$$

Lemma.

We have: $P_{\mathrm{Tr}_{n\to k}(W)} = ((n)_{n-k})^{-2} \Delta_{\mathbb{C}}^{n-k} P_W$, where $(x)_p = x(x-1)\cdots(x-p+1)$ and $\Delta_{\mathbb{C}}$ is the complex Laplacian

$$\Delta_{\mathbb{C}} = \sum_{i=1}^{d} \frac{\partial^2}{\partial \bar{z}_i \partial z_i}$$

Lemma (complex Bernstein inequality). ← we need analysis here

For any $W = W^* \in \mathcal{B}(\vee^n \mathbb{C}^d)$ we have

$$\forall \|z\| \le 1, \qquad \left|(\Delta_{\mathbb{C}}^s P_W)(z)\right| \le 4^{-s}(2d)^s (2n)_{2s} M(W)$$

The Dictionary	
Sym. operators $\in \mathcal{B}(\vee^n \mathbb{C}^d)$	Polynomials (d vars, bi-hom. deg. n)
W	$P_W(z) = \langle z^{\otimes n} \| W \| z^{\otimes n} \rangle$
Positivity notions	
block-positive	non-negative
positive semidefinite	Sum Of Squares
separable	Sum Of Powers
Operations	
Tensor with identity	mult. with the norm^2
Partial trace	complex Laplacian

The complex Positivstellensatz

A complex version of Reznick's PSS

Theorem.

Consider $W = W^* \in \mathcal{B}(\vee^k \mathbb{C}^d \otimes \mathbb{C}^D)$ with $m(W) > 0$ and $k \geq 1$. Then, for any

$$n \geq \frac{dk(2k-1)}{\ln\left(1 + \frac{m(W)}{M(W)}\right)} - k$$

with $n \geq k$, we have

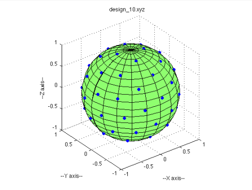
$$\|x\|^{2(n-k)} P_W(x,y) = \int P_{\tilde{W}}(\varphi, y) |\langle \varphi, x \rangle|^{2n} \mathrm{d}\varphi$$

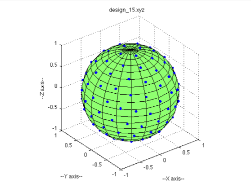
with $P_{\tilde{W}}(\varphi, y) \geq 0$ for all $\varphi \in \mathbb{C}^d$ and $y \in \mathbb{C}^D$, where $\tilde{W} \in \mathcal{B}(\vee^k \mathbb{C}^d \otimes \mathbb{C}^D)$ is explicitly computable in terms of W, and $\mathrm{d}\varphi$ is any $(n+k)$-spherical design. In the case $k = 1$, the bound on n can be improved to $n \geq dM(W)/m(W) - 1$.

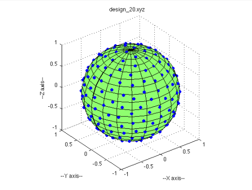
A similar result was obtained by To and Yeung with worse bounds and in a less general setting, by "complexifying" Reznick's proof

Spherical designs

- A complex n-spherical design in dimension d is a probability measure $\mathrm{d}\varphi$ on the unit sphere of $\mathbb{C}^d$ which approximates the uniform measure $\mathrm{d}z$ in the following sense: for any degree n bi-hom. polynomial $P(z)$ in d complex variables, $\int P(\varphi)\mathrm{d}\varphi = \int P(z)\mathrm{d}z$
- Equivalently, $\int |\varphi\rangle\langle\varphi|^{\otimes n}\mathrm{d}\varphi = P_{sym}^{(d,n)}/d[n]$
- For all d, n, there exist finite n-designs: the measure $\mathrm{d}\varphi$ has support of size $\leq (n+1)^{2d}$; in particular, the integral in the main theorem can be a finite sum
- Designs of orders 60, 120, 216 in $\mathbb{R}^3$ ©John Burkardt







Proof idea

$$\|x\|^{2(n-k)} P_W(x,y) = \int P_{\tilde{W}}(\varphi, y) |\langle \varphi, x \rangle|^{2n} \mathrm{d}\varphi$$

- We want to transform a non-negative polynomial into a sum of powers by multiplying with some power of the norm
- In terms of operators, this amounts to transforming a block-positive operator into a separable operator
- Ansatz: use the measure-and-prepare map

$$\mathrm{MP}_{n \to k} : \mathcal{B}(\vee^n \mathbb{C}^d) \to \mathcal{B}(\vee^k \mathbb{C}^d)$$
$$X \mapsto d[n] \int \langle \varphi^{\otimes n} | X | \varphi^{\otimes n} \rangle |\varphi\rangle\langle\varphi|^{\otimes k} \mathrm{d}\varphi,$$

  for some $(n+k)$-spherical design $\mathrm{d}\varphi$
- The linear map $\mathrm{MP}_{n \to k}$ is completely positive, and it is normalized to be trace preserving (i.e. it is a quantum channel)

Chiribella's identity

Theorem [Chiribella 2010].

For any $k \leq n$, we have

$$\mathrm{MP}_{n \to k} = \sum_{s=0}^{k} c(n,k,s)\, \mathrm{Clone}_{s \to k} \circ \mathrm{Tr}_{n \to s},$$

where $c(n,k,s) = \binom{n}{s}\binom{k+d-1}{k-s} / \binom{n+k+d-1}{k}$.

- $c(n,k,\cdot)$ is a probability distribution: $\sum_{s=0}^{k} c(n,k,s) = 1$
- The proof is a straightforward computation in the group algebra of $G = \mathcal{S}_{n+k}$:

$$\varepsilon_G = \sum_{s=0}^{\min(n,k)} \frac{\binom{n}{s}\binom{k}{s}}{\binom{n+k}{n}} \varepsilon_H \sigma_s \varepsilon_H$$

  where ε_X is the average of the elements in X, $H = \mathcal{S}_n \times \mathcal{S}_k \leq G$ is a Young subgroup and σ_s is some permutation swapping s elements from $[1,n]$ with s elements from $[n+1, n+k]$

The result is about the interplay between Clone and MP

- The equality $\|x\|^{2(n-k)} P_W(x,y) = \int P_{\tilde{W}}(\varphi, y) |\langle \varphi, x\rangle|^{2n} \mathrm{d}\varphi$ reads, in terms of linear maps over symmetric spaces

$$\mathsf{Clone}_{k\to n} \otimes \mathsf{id}_D = [\mathsf{MP}_{k\to n} \circ \Psi] \otimes \mathsf{id}_D$$

- The fact that the polynomial $P_{\tilde{W}}$ is non-negative reads

$$\tilde{W} := \Psi(W) \text{ is block-positive } \iff \langle z^{\otimes n} | \tilde{W} | z^{\otimes n} \rangle \geq 0$$

- Re-write the Chiribella identity as

$$\begin{aligned} \mathsf{MP}_{n\to k} &= \sum_{s=0}^{k} c(n,k,s)\, \mathsf{Clone}_{s\to k} \circ \mathsf{Tr}_{n\to s} \\ &= \sum_{s=0}^{k} c(n,k,s)\, \mathsf{Clone}_{s\to k} \circ \mathsf{Tr}_{k\to s} \circ \mathsf{Tr}_{n\to k} \\ &= \Phi^{(n)}_{k\to k} \circ \mathsf{Tr}_{n\to k} \end{aligned}$$

Invert the Chiribella formula

- $\mathrm{MP}_{n\to k} = \Phi^{(n)}_{k\to k} \circ \mathrm{Tr}_{n\to k}$

Key fact.

The linear map $\Phi^{(n)}_{k\to k} : \vee^k \mathbb{C}^d \to \vee^k \mathbb{C}^d$ is invertible, with inverse

$$\Psi^{(n)}_{k\to k} := \sum_{s=0}^{k} q(n,k,s)\,\mathrm{Clone}_{s\to k} \circ \mathrm{Tr}_{k\to s}$$

with

$$q(n,k,s) := (-1)^{s+k} \frac{\binom{n+s}{s}\binom{k}{s}}{\binom{n}{k}} \frac{d[k]}{d[s]}$$

- Hence, up to some constants, $\mathrm{Clone}_{k\to n} = \mathrm{MP}_{k\to n} \circ \Psi^{(n)}_{k\to k}$
- Final step: use hypotheses on $n, k, m(W), M(W)$ to ensure $\Psi^{(n)}_{k\to k}(W)$ is block-positive whenever W is (strictly) block-positive

Use the Bernstein inequality to prove $P_{\tilde{W}}$ non-negative

- Assume, wlog, $D = 1$, i.e. there is no y

$$\begin{aligned} P_{\tilde{W}}(\varphi) &= \sum_{s=0}^{k} q(n,k,s)\langle\varphi^{\otimes k}|\,\mathrm{Clone}_{s\to k}\circ \mathrm{Tr}_{k\to s}(W)|\varphi^{\otimes k}\rangle \\ &= \sum_{s=0}^{k} q(n,k,s)\|\varphi\|^{2(k-s)}\langle\varphi^{\otimes s}|\,\mathrm{Tr}_{k\to s}(W)|\varphi^{\otimes s}\rangle \\ &= \sum_{s=0}^{k} q(n,k,s)\|\varphi\|^{2(k-s)} P_{\mathrm{Tr}_{k\to s}(W)}(\varphi) \\ &= \sum_{s=0}^{k} \hat{q}(n,k,s)\|\varphi\|^{2(k-s)}(\Delta_{\mathbb{C}}^{k-s} p_W)(\varphi) \end{aligned}$$

- Use the complex version of the Bernstein inequality to ensure that

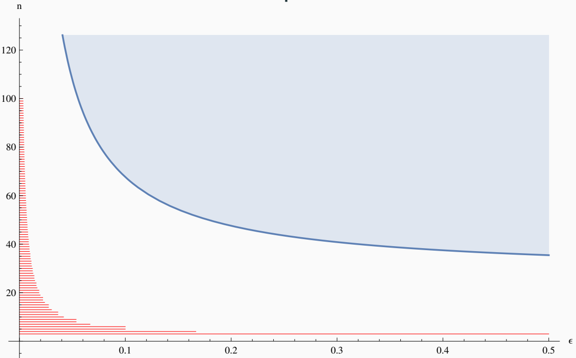
$$P_{\tilde{W}}(\varphi) \geq \left[m(W)\tilde{q}(n,k,k) - M(W)\sum_{s=0}^{k-1}|\tilde{q}(n,k,s)| \right] \geq 0$$

How good are the bounds?

- Consider the modified Motzkin polynomial

$$P_\varepsilon(x,y,z) = x^4y^2 + y^4z^2 + z^4x^2 - 3x^2y^2z^2 + \varepsilon(x^2+y^2+z^2)$$

- We have $m(P_\varepsilon) = \varepsilon$; $M(P_\varepsilon) = \varepsilon + 4/27$
- Let $P_{n,\varepsilon}(x,y,z) := (x^2+y^2+z^2)^{n-3}P_\varepsilon(x,y,z)$. If a PSS decomposition holds, then the $[2p,2q,2r]$ coefficient of $P_{n,\varepsilon}$ must be positive $\rightsquigarrow$ lower bound on optimal n



Thank you!

A. Müller-Hermes, I. Nechita, and D. Reeb - *A refinement of Reznick's Positivstellensatz with applications to quantum information theory* - **arXiv:1909.01705.**

B. Reznick - *Uniform denominators in Hilbert's seventeenth problem* - **Math. Z., 220(1):75–97 (1995).**

A. Harrow - *The Church of the Symmetric Subspace* - **arXiv:1308.6595**

W.-K. To and S.-K. Yeung - *Effective isometric embeddings for certain hermitian holomorphic line bundles* - **J. London Math. Soc. (2) 73, 607–624 (2006).**