

Quantum de Finetti theorems and Reznick's Positivstellensatz

Ion Nechita (CNRS, LPT Toulouse)

— joint work with Alexander Müller-Hermes and David Reeb

ICMAT Madrid, May 13th, 2019



(Quantum) de Finetti theorems

The classical de Finetti theorem

- Let V be a finite alphabet, $|V| = d$. A probability \mathbb{P} on V^n is called **exchangeable** if it is **symmetric under permutations**:

$$\forall \sigma \in \mathcal{S}_n, \quad \mathbb{P}[x_1, x_2, \dots, x_n] = \mathbb{P}[x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}].$$

- In particular, i.i.d. distributions are exchangeable

$$\mathbb{P} = \pi^{\otimes n} \quad \text{i.e.} \quad \mathbb{P}[x_1, x_2, \dots, x_n] = \prod_{i=1}^n \pi(x_i) = \prod_{a \in V} \pi(a)^{|x^{-1}(a)|}.$$

Theorem

Let \mathbb{P} be an exchangeable probability distribution on V^n . Then, for $k \ll n$, its k -marginal \mathbb{P}_k is close to a convex mixture of i.i.d. distributions. More precisely, for any $k \leq n$, there exists a probability measure μ on $\mathcal{P}(V)$ such that

$$\left\| \mathbb{P}_k - \int \pi^{\otimes k} d\mu(\pi) \right\|_{\text{TV}} \leq \frac{2kd}{n}.$$

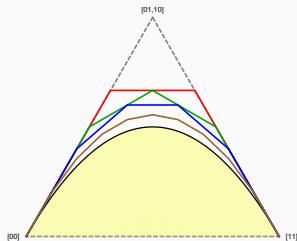


Figure 1: $k = 2$; $n = 3, 4, 5, 10$.

Quantum de Finetti theorems - the setup

- Finite alphabet $[d] \rightsquigarrow$ vector space \mathbb{C}^d
- Probability distribution on $[d] \rightsquigarrow$ quantum state (density matrix)
 $\rho \in \mathcal{M}_d(\mathbb{C})$, $\rho \geq 0$, $\text{Tr } \rho = 1$
- i.i.d. probability distribution $\pi^{\otimes n}$ on $[d]^{\times n} \rightsquigarrow$ multipartite product quantum state $\rho^{\otimes n} \in \mathcal{M}_d(\mathbb{C})^{\otimes n}$
- **Exchangeable distribution** $\mathbb{P}[x_1, \dots, x_n] = \mathbb{P}[x_{\sigma(1)}, \dots, x_{\sigma(n)}] \rightsquigarrow$ two different notions of **symmetry for quantum states**:
 1. Permutation symmetry: $\pi \rho_n \pi^* = \rho_n$, for all $\pi \in \mathcal{S}_n$
 2. Bose symmetry: ρ_n supported on $\vee^n \mathbb{C}^d$, i.e. $P_{\text{sym}}^{(d,n)} \rho_n P_{\text{sym}}^{(d,n)} = \rho_n$
- Any permutationally symmetric state can be purified to a Bose symmetric pure state in $\vee^n (\mathbb{C}^d \otimes \mathbb{C}^d)$

The finite quantum de Finetti theorem

Theorem.

Let $\rho \in \mathcal{B}(\vee^n \mathbb{C}^d)$ be a (Bose symmetric) quantum state. Then, for all $k \leq n$, there exists a probability measure μ_ρ on the unit sphere of \mathbb{C}^d such that

$$\| \text{Tr}_{n \rightarrow k} \rho - \int |\varphi\rangle\langle\varphi|^{\otimes k} d\mu_\rho(\varphi) \|_1 \leq \frac{2k(d+k)}{n+d}.$$

Among the many applications of the quantum de Finetti theorem:

- The convex body of separable quantum states

$$\text{SEP} = \text{conv}\{ |x\rangle\langle x| \otimes |y\rangle\langle y| : x \in \mathbb{C}^{d_A}, y \in \mathbb{C}^{d_B} \}$$

is hard to approximate

- A quantum state ρ_{AB} is said to be **k -extendible** if $\exists \sigma_{AB_1 \dots B_k}$ such that $\sigma_{B_1 \dots B_k} \in \mathcal{B}(\vee^k \mathbb{C}^{d_B})$ and $\sigma_{AB_1} = \rho_{AB}$

Theorem.

A state ρ_{AB} is separable iff it is k -extendible for all $k \geq 1$.

The measure-and-prepare map

- Let $d[n] := \dim P_{sym}^{(d,n)} = \binom{n+d-1}{d-1}$ the dimension of the symmetric subspace
- Define $\text{MP}_{n \rightarrow k} : \mathcal{B}(\mathbb{V}^n \mathbb{C}^d) \rightarrow \mathcal{B}(\mathbb{V}^k \mathbb{C}^d)$ by

$$\text{MP}_{n \rightarrow k}(X) = d[n] \int \langle \varphi^{\otimes n} | X | \varphi^{\otimes n} \rangle | \varphi \rangle \langle \varphi |^{\otimes k} d\varphi,$$

where $d\varphi$ is the Lebesgue measure on the unit sphere of \mathbb{C}^d , or even a $n+k$ spherical design

- The linear map $\text{MP}_{n \rightarrow k}$ is completely positive, and it is normalized to be trace preserving (i.e. it is a **quantum channel**):

$$\int | \varphi \rangle \langle \varphi |^{\otimes n} d\varphi = \frac{P_{sym}^{(d,n)}}{d[n]}$$

Spherical designs

Definition.

For $N, d, n \in \mathbb{N}$ a complex spherical n -design of order N on \mathbb{C}^d is a set of vectors $\{\gamma_i\}_{i=1}^N \subset \mathbb{C}^d$ and a set of probability weights $\{p_i\}_{i=1}^N \subset \mathbb{R}_+$ such that

$$P_{sym}^{(d,n)} = \sum_{i=1}^N p_i |\gamma_i\rangle \langle \gamma_i|^{\otimes n}.$$

Equivalently, the following polynomial identity holds

$$(|z_1|^2 + \dots + |z_d|^2)^n = \sum_{i=1}^N p_i |\langle z, \gamma_i \rangle|^{2n}$$

Theorem.

There exists a complex spherical n -design in \mathbb{C}^d of order $N = (n+1)^{2d}$

Chiribella's formula

- Assuming $k \leq n$, let $\text{Tr}_{n \rightarrow k} : \mathcal{B}(\mathbb{V}^n \mathbb{C}^d) \rightarrow \mathcal{B}(\mathbb{V}^k \mathbb{C}^d)$ be the partial trace map and $\text{Tr}_{k \rightarrow n}^* : \mathcal{B}(\mathbb{V}^k \mathbb{C}^d) \rightarrow \mathcal{B}(\mathbb{V}^n \mathbb{C}^d)$ be its dual w.r.t. the Hilbert-Schmidt scalar product

$$\text{Tr}_{k \rightarrow n}^*(X) = P_{\text{sym}}^{(d,n)} \left[X \otimes I_d^{\otimes (n-k)} \right] P_{\text{sym}}^{(d,n)}$$

- $\text{Clone}_{k \rightarrow n} := \frac{d \binom{k}{d}}{d \binom{n}{d}} \text{Tr}_{k \rightarrow n}^*$ is the optimal Keyl-Werner cloning quantum channel

Theorem.

For any $k \leq n$, we have

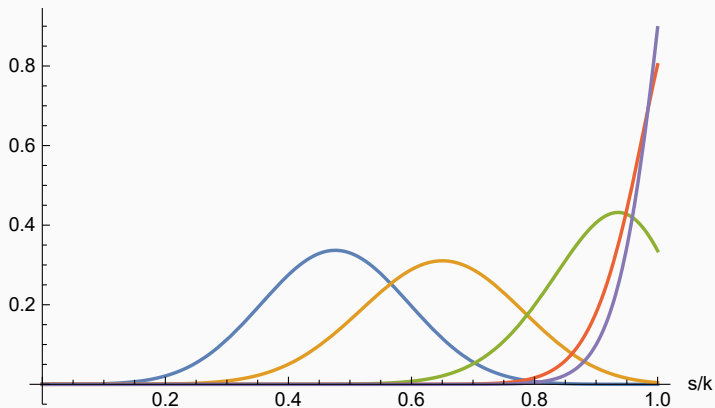
$$\text{MP}_{n \rightarrow k} = \sum_{s=0}^k c(n, k, s) \text{Clone}_{s \rightarrow k} \circ \text{Tr}_{n \rightarrow s},$$

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

Fact: $c(n, k, \cdot)$ is a probability distribution, $\sum_{s=0}^k c(n, k, s) = 1$

Proof of the quantum de Finetti theorem

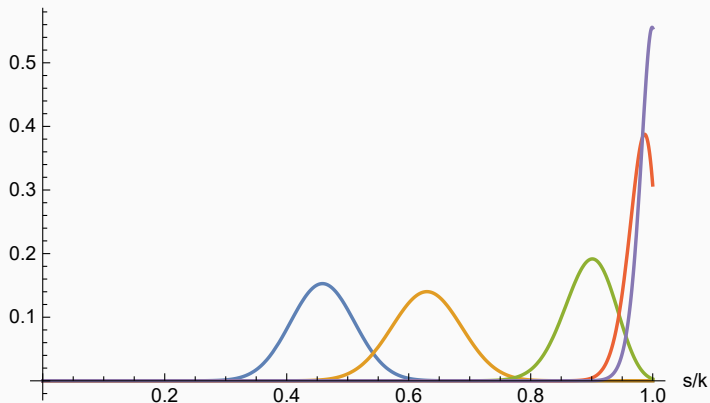
$c(n,k,s)$ for $d=2$ and $k=10$



— $n/k=1$ — $n/k=2$ — $n/k=10$ — $n/k=50$ — $n/k=100$

Proof of the quantum de Finetti theorem

$c(n,k,s)$ for $d=10$ and $k=50$



— $n/k=1$ — $n/k=2$ — $n/k=10$ — $n/k=50$ — $n/k=100$

Proof of the quantum de Finetti theorem

- Let $\|\cdot\|_\diamond$ be the $\mathcal{S}_1 \rightarrow \mathcal{S}_1$ CB norm, aka the **diamond norm**

$$\|\Phi\|_\diamond = \sup_k \sup_{\|X\|_1 \leq 1} \|[\text{id}_k \otimes \Phi](X)\|_1$$

- We have

$$\begin{aligned} & \|\text{Tr}_{n \rightarrow k} - \text{MP}_{n \rightarrow k}\|_\diamond \\ &= \|(1 - c(n, k, k)) \text{Tr}_{n \rightarrow k} - \sum_{s=0}^{k-1} c(n, k, s) \text{Clone}_{s \rightarrow k} \circ \text{Tr}_{n \rightarrow s}\|_\diamond \\ &\leq 2(1 - c(n, k, k)) \\ &\leq \frac{2k(d+k)}{n+d} \end{aligned}$$

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 $Q_{1,2} \in \mathbb{R}[x]$
- $\text{Pos}(d, n) := \{P \in \mathbb{R}[x_1, \dots, x_d] \text{ hom. of deg. } 2n, P(x) \geq 0, \forall x\}$
- $\text{SOS}(d, n) := \{\sum_i Q_i^2 \text{ with } Q_i \in \mathbb{R}[x_1, \dots, x_d] \text{ hom. of deg. } n\}$
- Hilbert 1888:

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

- The Motzkin polynomial

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

is positive but not SOS

- Membership in SOS can be decided with a SDP: $P \in \text{SOS}(d, n)$ iff $\exists A \geq 0$ such that $P = \langle v_{d,n} | A | v_{d,n} \rangle$, where $v_{d,n}$ is the vector containing all the hom. monomials in d variables of degree n

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^2P is SOS

- Polya 1928: P even, $P \geq 0 \implies \exists r$ such that $(\sum_i x_i^2)^r P$ has non-negative coefficients (and thus is SOS)

Theorem. [Reznick 1995]

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

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

we have

$$\|x\|^{2(n-k)} P(x) = \sum_{j=1}^r t_j \langle x, a_j \rangle^{2n},$$

where $t_j > 0$ and $a_j \in \mathbb{R}^d$

A complex version of Reznick's PSS

- In the complex case, we are interested in **bi-homogeneous polynomials** of degree n in d complex variables: $P(z_1, \dots, z_d)$ 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 $\vee^n \mathbb{C}^d$:

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

- Self-adjoint W are associated to real, bi-hom. polynomials
- Non-negative polynomials P are associated to **block-positive** matrices W :

$$\langle z^{\otimes n} | W | z^{\otimes n} \rangle \geq 0, \quad \forall z \in \mathbb{C}^d$$

- W PSD $\implies P$ SOS: if $W = \sum_j t_j |a_j\rangle\langle a_j|$, then

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

- $\|z\|^{2n} = \langle z^{\otimes n} | P_{sym}^{(d,n)} | z^{\otimes n} \rangle$

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

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

with $n \geq k$, we have

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

with $p_{\tilde{W}}(\varphi, y) \geq 0$ for all $\varphi \in \mathbb{C}^d$ and $y \in \mathbb{C}^D$, where $p_{\tilde{W}}(\varphi, y)$ is a bihermitian form of degree k in φ and $\bar{\varphi}$ and degree 1 in y and \bar{y} , explicitly computable in terms of W , and $d\varphi$ is any $(n+k)$ spherical design. In the case $k=1$, the bound (1) can be improved

$$n \geq d \frac{M(W)}{m(W)} - 1.$$

Similar result obtained by [To and Yeung] with worse bounds and in a less general setting, by “complexifying” Reznick’s proof

The proof: inverting the Chiribella formula

Proof strategy

- The equality

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

reads, in terms of linear maps over symmetric spaces

$$\text{Clone}_{k \rightarrow n} \otimes \text{id}_D = \left[\text{MP}_{k \rightarrow n} \circ \tilde{\Psi} \right] \otimes \text{id}_D$$

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

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

- Re-write the **Chiribella identity** as

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

Proof strategy

- $MP_{n \rightarrow k} = \Phi_{k \rightarrow k}^{(n)} \circ \text{Tr}_{n \rightarrow k}$

Key fact.

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

$$\Psi_{k \rightarrow k}^{(n)} := \sum_{s=0}^k q(n, k, s) \text{Clone}_{s \rightarrow k} \circ \text{Tr}_{k \rightarrow s}$$

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, $\text{Clone}_{k \rightarrow n} = MP_{k \rightarrow n} \circ \Psi_{k \rightarrow k}^{(n)}$
- Final step: use hypotheses on $n, k, m(W), M(W)$ to ensure $\Psi_{k \rightarrow k}^{(n)}(W)$ is block-positive

Proof strategy

Note: $p_{\text{Tr}_{k \rightarrow n}^*(W)}(x) = \|x\|^{2(n-k)} p_W(x)$

Lemma.

For any $W \in \mathcal{B}(\vee^k \mathbb{C}^d)$, we have

$$p_{\text{Tr}_{k \rightarrow k-s}(W)} = ((k)_s)^{-2} \Delta_{\mathbb{C}}^s p_W,$$

where $\Delta_{\mathbb{C}}$ is the Laplacian

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

Lemma.

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

$$\forall \|z\| = 1, \quad \left| (\Delta_{\mathbb{C}}^s p_W)(z) \right| \leq 4^{-s} (2d)^s (2k)_{2s} M(W)$$

Proof strategy

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

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

- Use the complex version of the Bernstein inequality

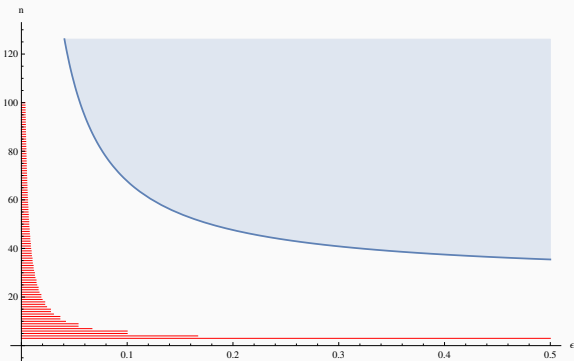
$$p_{\tilde{W}}(\varphi) \geq \left[m(W) \tilde{q}(n, k, k) - M(W) \sum_{s=0}^{k-1} |\tilde{q}(n, k, s)| \right]$$

How good are the bounds?

- Consider the modified Motzkin polynomial

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

- 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!

P. Diaconis and D. Freedman - *Finite exchangeable sequences* - **The Annals of Probability**, 745-764 (1980).

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

B. Reznick - *Uniform denominators in Hilberts seventeenth problem* - **Math. Z.**, 220(1):7597 (1995).

W.-K. To and S.-K. Yeung - *Effective isometric embeddings for certain hermitian holomorphic line bundles* - **J. London Math. Soc. (2)** 73, 607624 (2006).