Positive and completely positive maps via free additive powers of probability measures

Ion Nechita

TU München and CNRS

joint work with Benoit Collins (Kyoto) and Patrick Hayden (Stanford)

arXiv:1505.08042

München, July 23rd 2015

Outline of the talk

1. Entanglement detection with positive maps
2. Some elements of free probability
3. Positive maps from random Choi matrices

Entanglement detection with positive maps

Entanglement in Quantum Information Theory

- Quantum states with n degrees of freedom are described by density matrices

$$\rho \in \mathcal{M}_n^{1,+} = \mathrm{End}^{1,+}(\mathbb{C}^n); \qquad \mathrm{Tr}\rho = 1 \text{ and } \rho \geq 0$$

- Two quantum systems: $\rho_{12} \in \mathrm{End}^{1,+}(\mathbb{C}^m \otimes \mathbb{C}^n) = \mathcal{M}_{mn}^{1,+}$
- A state ρ_{12} is called separable if it can be written as a convex combination of product states

$$\rho_{12} \in \mathcal{SEP} \iff \rho_{12} = \sum_i t_i \rho_1(i) \otimes \rho_2(i),$$

where $t_i \geq 0$, $\sum_i t_i = 1$, $\rho_1(i) \in \mathcal{M}_m^{1,+}$, $\rho_2(i) \in \mathcal{M}_n^{1,+}$

- Equivalently, $\mathcal{SEP} = \mathrm{conv}\left[\mathcal{M}_m^{1,+} \otimes \mathcal{M}_n^{1,+}\right]$
- Non-separable states are called entangled

Separability criteria

- Let $\mathcal{A}$ be a C^* algebra. A map $f : \mathcal{M}_n \to \mathcal{A}$ is called
  - positive if $A \geq 0 \implies f(A) \geq 0$;
  - completely positive (CP) if $\mathrm{id}_k \otimes f$ is positive for all $k \geq 1$ ($k = n$ is enough).
- Let $f : \mathcal{M}_n \to \mathcal{A}$ be a completely positive map. Then, for every state $\rho_{12} \in \mathcal{M}_{mn}^{1,+}$, one has $[\mathrm{id}_m \otimes f](\rho_{12}) \geq 0$.
- Let $f : \mathcal{M}_n \to \mathcal{A}$ be a positive map. Then, for every separable state $\rho_{12} \in \mathcal{M}_{mn}^{1,+}$, one has $[\mathrm{id}_m \otimes f](\rho_{12}) \geq 0$.
  - ρ_{12} separable $\implies \rho_{12} = \sum_i t_i \rho_1(i) \otimes \rho_2(i)$.
  - $[\mathrm{id}_m \otimes f](\rho_{12}) = \sum_i t_i \rho_1(i) \otimes f(\rho_2(i))$.
  - For all i, $f(\rho_2(i)) \geq 0$, so $[\mathrm{id}_m \otimes f](\rho_{12}) \geq 0$.
- Hence, positive, but not CP maps f provide sufficient entanglement criteria: if $[\mathrm{id}_m \otimes f](\rho_{12}) \ngeq 0$, then ρ_{12} is entangled.
- Moreover, if $[\mathrm{id}_m \otimes f](\rho_{12}) \geq 0$ for all positive (but not CP maps) $f : \mathcal{M}_n \to \mathcal{M}_m$, then ρ_{12} is separable.

The Choi-Jamiołkowski isomorphism

- For any n, recall that the maximally entangled state is the orthogonal projection $\Omega_n = \omega_n \omega_n^*$ onto

$$\mathbb{C}^n \otimes \mathbb{C}^n \ni \omega_n = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} e_i \otimes e_i.$$

- To any map $f : \mathcal{M}_n \to \mathcal{M}_d$, associate its Choi matrix

$$C_f = [\mathrm{id}_n \otimes f](\Omega_n) = \sum_{i,j=1}^{n} E_{ij} \otimes f(E_{ij}) \in \mathcal{M}_n \otimes \mathcal{M}_d.$$

- The map $f \mapsto C_f$ is called the Choi-Jamiołkowski isomorphism. It sends:
  1. All linear maps to all operators;
  2. Hermicity preserving maps to hermitian operators;
  3. Entanglement breaking maps to separable quantum states;
  4. Unital maps to operators with unit left partial trace ($[\mathrm{Tr} \otimes \mathrm{id}]C_f = \mathrm{I}_d$);
  5. Trace preserving maps to operators with unit left partial trace ($[\mathrm{id} \otimes \mathrm{Tr}]C_f = \mathrm{I}_n$).

Structure of CP maps

Theorem (Stinespring-Kraus-Choi)

Let $f : \mathcal{M}_n \to \mathcal{M}_n$ be a linear map. The following assertions are equivalent:

1. *The map f is completely positive and trace preserving.*
2. *There exist an integer k ($k = n^2$ suffices), a unit vector $e \in \mathbb{C}^k$, and a unitary operator $U \in \mathcal{U}_{nk}$ such that*

$$f(X) = [\mathrm{id}_n \otimes \mathrm{Tr}_k](U(X \otimes ee^*)U^*).$$

3. *There exist operators $A_1, \ldots, A_k \in \mathcal{M}_n$ satisfying $\sum_i A_i^* A_i = I_n$ such that*

$$f(X) = \sum_{i=1}^{k} A_i X A_i^*.$$

4. *The Choi matrix C_f is positive semidefinite.*

Positive Partial Transpose matrices

- The transposition map $\mathrm{t} : A \mapsto A^t$ is positive, but not CP. Define the convex set
$$\mathcal{PPT} = \{\rho_{12} \in \mathcal{M}_{mn}^{1,+} \mid [\mathrm{id}_m \otimes \mathrm{t}_n](\rho_{12}) \geq 0\}.$$
- For $(m, n) \in \{(2, 2), (2, 3)\}$ we have $\mathcal{SEP} = \mathcal{PPT}$. In other dimensions, the inclusion $\mathcal{SEP} \subset \mathcal{PPT}$ is strict.
- Low dimensions are special because every positive map $f : \mathcal{M}_2 \to \mathcal{M}_{2/3}$ is decomposable:
$$f = g_1 + g_2 \circ \mathrm{t},$$
with $g_{1,2}$ completely positive. Among all decomposable maps, the transposition criterion is the strongest.
- The result above is the only "structural" result for positive maps.

Intermediate positivity notions

- A map $f : \mathcal{M}_n \to \mathcal{M}_d$ is called k-positive if $\mathrm{id}_k \otimes f$ is positive.
- A matrix $C \in \mathcal{M}_{nd}$ is called k-positive if $\langle x, Cx \rangle \geq 0$ for all vectors $x \in \mathbb{C}^n \otimes \mathbb{C}^d$ of rank at most k.
- In particular, C is 1-positive (or block-positive) if

$$\forall x \in \mathbb{C}^n, \forall y \in \mathbb{C}^d \qquad \langle x \otimes y, C \cdot x \otimes y \rangle \geq 0.$$

Theorem

Consider a map $f : \mathcal{M}_n \to \mathcal{M}_d$. The following assertions are equivalent

1. *The map f is k-positive*
2. *The Choi matrix C_f is k-positive*
3. *For any self-adjoint projection $P \in \mathcal{M}_n$ of rank k, the operator $(P \otimes I_d) C_f (P \otimes I_d)$ is positive semidefinite*

In particular, f is positive iff C_f is block-positive.

Some elements of free probability

Non-commutative probability

Classical (or commutative) probability space

- A triple $(\Omega, \mathcal{F}, \mathbb{P})$
- Random variables (here, bounded): elements $x \in L^\infty(\Omega, \mathbb{P})$
- Expectation / integration: $\mathbb{E}(x) = \int_\Omega x(\omega) d\mathbb{P}(\omega)$
- Tensor independence: random variables x, y are independent if (they commute and) for all m, n

$$\mathbb{E}(x^m y^n) = \mathbb{E}(x^m)\mathbb{E}(y^n)$$

Non-commutative probability space

- A pair $(\mathcal{A}, \varphi)$, where $\mathcal{A}$ is a unital ($*$-, C^*-,von Neumann) algebra, and $\varphi : \mathcal{A} \to \mathbb{C}$ is a unital linear form $\varphi(1) = 1$.
- Random variables: elements $x \in \mathcal{A}$
- Expectation / integration given by φ

Free independence

$\rightsquigarrow$ A non-commutative analog of $\mathbb{E}(x^m y^n) = \mathbb{E}(x^m)\mathbb{E}(y^n)$

Definition (Voiculescu '85)

Consider a non-commutative probability space $(\mathcal{A}, \varphi)$. Unital subalgebras $(\mathcal{A}_i)_{i \in I}$ are called free of freely independent if $\varphi(a_1 a_2 \cdots a_n) = 0$ whenever

- $a_i \in \mathcal{A}_{j(i)}$, $\forall i$
- $j(1) \neq j(2) \neq \cdots \neq j(n)$
- $\varphi(a_i) = 0$, $\forall i$

Random variables $x_1, x_2, \ldots, x_n$ are called free if the unital subalgebras they generate are free.

Free independence is a rule (different than the one in classical probability) for calculating mixed moments in freely independent random variables in terms of the marginals. The structure of this rule is intimately related to the combinatorial theory of non-crossing partitions [Speicher '93].

Free independence

Assume x, y are free, non-commutative random variables. Denote by x_0, y_0 their centered versions, i.e. $x = x_0 + \varphi(x)1$, $y = y_0 + \varphi(y)1$

Example

$$\begin{aligned} \varphi(xy) &= \varphi\left((x_0 + \varphi(x)1)(y_0 + \varphi(y)1)\right) \\ &= \varphi(x_0 y_0) + \varphi(x_0)\varphi(y) + \varphi(x)\varphi(y_0) + \varphi(x)\varphi(y) \\ &= 0 + 0 + 0 + \varphi(x)\varphi(y) \\ &= \varphi(x)\varphi(y) \end{aligned}$$

Example

$$\varphi(x^{m_1} y^n x^{m_2}) = \varphi(x^{m_1+m_2})\varphi(y^n)$$

... but ...

Example

$$\varphi(xyxy) = \varphi(x^2)\varphi(y)^2 + \varphi(x)^2\varphi(y^2) - \varphi(x)^2\varphi(y)^2$$

Free independence - random matrices

Free independence appears in very different contexts, such as free groups, creation and annihilation operators in the full Fock space, and large random matrices.

Theorem (Voiculescu '91,'98)

Independent random matrices (with some invariance property) become asymptotically free, as their size $n \to \infty$.

- Random matrices (say with entries having moments of all orders) are elements of $(\mathcal{A}_n, \varphi_n)$, where

$$\mathcal{A}_n = \mathcal{M}_n(L^{\infty-}(\Omega, \mathbb{P})), \qquad \varphi_n = \mathbb{E}\frac{1}{n}\mathrm{Tr}$$

- The distribution of $S_n \in \mathcal{A}_n$ is the collection of moments

$$\left[\varphi_n(S_n^p) = \mathbb{E}n^{-1}\mathrm{Tr}(X_n^p)\right]_{k=1}^{\infty}$$

Free independence - random matrices

Example

A GUE element is a random matrix $S_n \in \mathcal{A}_n$ having i.i.d. entries (up to symmetry) with complex Gaussian distribution of variance n^{-1}.

Theorem (Wigner '55)

A sequence of GUE elements $(S_n)_n$ converges in moments to the standard semicircle distribution

$$\forall p \geq 1, \quad \lim_{n\to\infty} \varphi_n(S_n^p) = \int x^p ds_{0,1}(x) = \begin{cases} \mathrm{Cat}_{p/2} & \text{if } p \text{ is even} \\ 0 & \text{if } p \text{ is odd} \end{cases},$$

where $ds_{0,1} = (2\pi)^{-1}\sqrt{4-x^2}\mathbf{1}_{[-2,2]}(x)dx$.

Consider two (classically) independent sequences of GUE random matrices $(S_n)_n$ and $(T_n)_n$. By Voiculescu's theorem, they are asymptotically free $\implies$

$$\lim_{n\to\infty} \mathbb{E}n^{-1}\mathrm{Tr}(S_nT_nT_nS_n) = 1 \qquad \lim_{n\to\infty} \mathbb{E}n^{-1}\mathrm{Tr}(S_nT_nS_nT_n) = 0$$

Sums of free random variables

The distribution of a random variable $x = x^* \in \mathcal{A}$ is the probability measure μ_x satisfying

$$\forall p \geq 1, \quad \varphi(x^p) = \int t^p d\mu_x(t)$$

Definition

Let x, y be two free random variables, having distributions μ_x, resp. μ_y. Using freeness, the distribution of $x + y$ depends only on the individual (marginal) distributions of x and y. It is denoted by

$$\mu_{x+y} = \mu_x \boxplus \mu_y$$

There is an analytical machinery (the R-transform), developed by Voiculescu, which allows to compute $\mu_x \boxplus \mu_y$ in terms of μ_x, μ_y.

Example

$$(\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1) \boxplus (\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1) = \frac{1}{\pi\sqrt{t(2-t)}}\mathbf{1}_{(0,2)}(t)dt$$

Sums of free random variables

In terms of random matrices, consider two sequences of orthogonal projections $P_n, Q_n \in \mathcal{M}_n^{sa}$ having ranks $\lfloor n/2 \rfloor$.

- The distribution of P_n (resp. Q_n) converges, as $n \to \infty$, to $b := 1/2\delta_0 + 1/2\delta_1$:

$$\forall k \geq 1, \quad \lim_{n \to \infty} \mathbb{E} n^{-1} \mathrm{Tr}(P_n^k) = 1/2 = \int t^k db$$

- Let U_n be a Haar-distributed random unitary matrix. Put $\tilde{Q}_n = U_n Q_n U_n^*$. The matrices Q_n and $\tilde{Q}_n$ have the same eigenvalues, hence the same limit distribution.
- By Voiculescu's theorem, the sequences $(P_n)_n$ and $(\tilde{Q}_n)_n$ are asymptotically free.
- Hence, the limiting distribution of $P_n + U_n Q_n U_n^*$ is the arcsine distribution

$$\frac{1}{\pi\sqrt{t(2-t)}} \mathbf{1}_{(0,2)}(t) dt$$

Products of free random variables

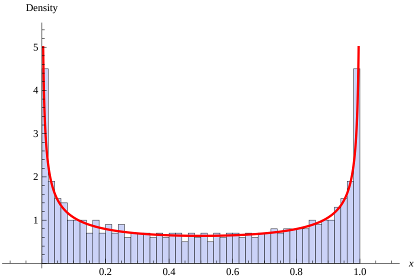
Definition

Let x, y be two free random variables, having distributions μ_x, resp. μ_y, and assume $x \geq 0$. We denoted by

$$\mu_{x^{-1/2}yx^{-1/2}} = \mu_x \boxtimes \mu_y$$

There is an analytical machinery (the S-transform), developed by Voiculescu, which allows to compute $\mu_x \boxtimes \mu_y$ in terms of μ_x, μ_y.

$$\left(\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1\right) \boxtimes \left(\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1\right) = \frac{1}{\pi\sqrt{t(1-t)}}\mathbf{1}_{(0,1)}(t)dt$$



Positive maps from random Choi matrices

Random Choi matrices

- Let μ be a compactly supported probability measure on $\mathbb{R}$. For each d we introduce a real valued diagonal matrix X_d of $\mathcal{M}_n \otimes \mathcal{M}_d$ whose eigenvalue counting distribution converges to μ and whose extremal eigenvalues converge to the respective extrema of the support of μ.
- Let U_d be a random Haar unitary matrix in the unitary group $\mathcal{U}_{nd}$, and $f_\mu^{(d)} : \mathcal{M}_n \to \mathcal{M}_d$ be the map whose Choi matrix is $C_\mu^{(d)} := U_d X_d U_d^*$.
- Note that $f_\mu^{(d)}$ is CP as $d \to \infty$ iff. μ is supported on $[0, \infty)$.
- For a compactly supported probability measure μ, define

$$\mu^{\boxplus n} := \underbrace{\mu \boxplus \mu \boxplus \cdots \boxplus \mu}_{n \text{ times}}$$

- This definition can be extended to non-integer $n \geq 1$.

Theorem

Under the above assumptions, if $\operatorname{supp}(\mu^{\boxplus n/k}) \subset (0, \infty)$ then, almost surely as $d \to \infty$, the map $f_\mu^{(d)}$ is k-positive. On the other hand, if $\operatorname{supp}(\mu^{\boxplus n/k}) \cap (-\infty, 0) \neq \emptyset$ then, almost surely as $d \to \infty$, $f_\mu^{(d)}$ is not k-positive.

Proof ingredients

- We fix $k = 1$, i.e. we want to know when the map $f_\mu^{(d)}$ is positive.
- We need to check that for all rank 1 projections $P \in \mathcal{M}_n$, the matrix $(P \otimes I_d) C_\mu^{(d)} (P \otimes I_d)$ is positive semidefinite. Fix such a projector P.
- Recall that $C_\mu^{(d)}$ is unitarily invariant, so $C_\mu^{(d)}$ and $P \otimes I_d$ are asymptotically free.
- The distribution of $C_\mu^{(d)}$ converges to μ as $d \to \infty$, while the distribution of $P \otimes I_d$ is $(1 - 1/n)\delta_0 + 1/n\delta_1$ (for all d).
- Hence, by Voicuelscu's result, the asymptotic distribution of $(P \otimes I_d) C_\mu^{(d)} (P \otimes I_d)$ is

$$((1 - 1/n)\delta_0 + 1/n\delta_1) \boxtimes \mu.$$

- Note that the above measure does not depend on P; the unitarily invariance of $C_\mu^{(d)}$ takes care of that.
- Choose an ε net of P's. For each element, the above convergence result holds.

Conclusion: the asymptotic positivity of $f_\mu^{(d)}$ depends on the support of the measure

$$(1 - 1/n)\delta_0 + 1/n\delta_1) \boxtimes \mu$$

Proof ingredients

Let $f_\mu^{(d)} : \mathcal{M}_n \to \mathcal{M}_d$ be the map whose Choi matrix is $U_d X_d U_d^*$

Theorem

If $\operatorname{supp}(\mu^{\boxplus n/k}) \subset (0, \infty)$ then, almost surely as $d \to \infty$, the map $f_\mu^{(d)}$ is k-positive. If $\operatorname{supp}(\mu^{\boxplus n/k}) \cap (-\infty, 0) \neq \emptyset$ then, almost surely as $d \to \infty$, $f_\mu^{(d)}$ is not k-positive.

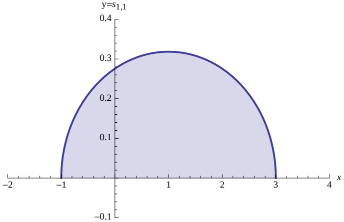
Proposition (Nica and Speicher)

Let x, p be free elements in a ncps $(\mathcal{M}, \tau)$ and assume that p is a selfadjoint projection of rank $\tau(p) = 1/t$ $(t \geq 1)$ and that x has distribution μ. Then, the distribution of $t^{-1}pxp$ inside the contracted ncps $(p\mathcal{M}p, \tau(p \cdot p))$ is $\mu^{\boxplus t}$.

$\rightsquigarrow$ The result above replaces the computation of a $\boxtimes$ operation with that of a $\boxplus$-power, which is easier to deal with.

Example: semicircular measures

- Let $s_{a,\sigma}$ be the semi-circle distribution of mean a and variance σ^2, having support $[a - 2\sigma, a + 2\sigma]$



- We have $s_{a,\sigma}^{\boxplus n/k} = s_{an/k,\sigma\sqrt{n/k}}$, with support $\mathrm{supp}(s_{a,\sigma}^{\boxplus n/k}) = [an/k - 2\sigma\sqrt{n/k}, an/k + 2\sigma\sqrt{n/k}]$

Theorem

Let n be an integer and a, σ positive parameters. The map $f_{a,\sigma} : \mathcal{M}_n \to \mathcal{M}$ associated to a semi-circular distribution $s_{a,\sigma}$ is k-positive iff $k \leq 4n\sigma^2/a^2$. In particular, for any n and any $k < n$, there exist parameters $a, \sigma > 0$ such that the above map is k-positive but not $(k+1)$-positive.

Semicircular measures vs. PPT

- We show next that the maps $f_{a,\sigma}$ detect some PPT and entangled states. Importantly, the states detected are correlated to the Choi matrix defining $f_{a,\sigma}$
- A random matrix $S \in \mathcal{M}_d^{sa}$ is called a GUE element if its elements are i.i.d. complex Gaussian random variables with variance d^{-1} (up to the $S = S^*$ condition)
- Wigner's theorem: a sequence (S_d) of GUE random matrices converges in distribution to a standard semicircular variable $s_{0,1}$
- Consider (normalized) i.i.d. GUE matrices $S_{ij}, S'_{ij} \in \mathcal{M}_d^{sa}$ and define, for $\alpha \in (-1, 1)$, the selfadjoint test matrix $X_d \in \mathcal{M}_n \otimes \mathcal{M}_d$, with the following blocks:
  - diagonal blocks $X_d(i,i) = 2\sqrt{2}\sqrt{n}\mathrm{I}_d - \alpha\sqrt{2}S_{ii}$ for $1 \leq i \leq n$
  - off-diagonal blocks $X_d(i,j) = \alpha(-\bar{S}_{ij} + \sqrt{-1}\bar{S}'_{ij})$, for $1 \leq i < j \leq n$
- We have $X_d = \sqrt{2n}(2\mathrm{I}_{dn} + \alpha Y_d)$, where $Y_d \in \mathcal{M}_{dn}^{sa}$ is a GUE
- Almost surely, as $d \to \infty$, X_d is positive semidefinite and PPT (since the GUE ensemble is invariant under partial transposition)

Semicircular measures vs. PPT

- Fix a small $\varepsilon > 0$ and let $f_d : \mathcal{M}_n \to \mathcal{M}_d$ be the linear map whose Choi matrix C_d has blocks
  - diagonal blocks $C_d(i,i) = (2\sqrt{2} + \varepsilon)\mathrm{I}_d + \sqrt{2}S_{ii}$ for $1 \leq i \leq n$;
  - off-diagonal blocks $C_d(i,j) = S_{ij} + \sqrt{-1}S'_{ij}$, for $1 \leq i < j \leq n$
- Using our main result, we check easily that, almost surely as $d \to \infty$, the maps f_d are positive (1-positive)
- A direct computation shows that, almost surely as $d \to \infty$,

$$\langle \omega_d, [f_d \otimes \mathrm{id}_d](X_d) \cdot \omega_d \rangle \sim n(2\sqrt{2n}(2\sqrt{2} + \varepsilon) - 2\alpha) - 2n(n-1)\alpha$$

Theorem

Given $\alpha \in (-1, 1)$, there exists $\varepsilon > 0$ small enough, such that, as soon as $n\alpha^2 > 16$, the matrix $[f_d \otimes \mathrm{id}_d](X_d)$ is almost surely not positive semidefinite, as $d \to \infty$, and thus X_d is entangled and PPT. In particular, the maps f_d are indecomposable.

The End

arXiv:1505.08042