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

Ion Nechita

CNRS, Laboratoire de Physique Théorique, Université de Toulouse

*joint work with Benoit Collins (uOttawa) and Patrick Hayden (McGill)*

St John's, January 25th, 2013

# Quantum Information Theory, Quantum Computing

- New branches of {Physics, Computer Science, Mathematics} dealing with quantum information.

# Quantum Information Theory, Quantum Computing

- New branches of {Physics, Computer Science, Mathematics} dealing with quantum information.
- Quantum information = information held in a quantum physical system.

# Quantum Information Theory, Quantum Computing

- New branches of $\{\text{Physics}, \text{Computer Science}, \text{Mathematics}\}$ dealing with quantum information.
- Quantum information $=$ information held in a quantum physical system.
- Basic idea: replace $\{0, 1\}$ with $\operatorname{span}\{|0\rangle, |1\rangle\}$, the state space of a two-level quantum system.

# Quantum Information Theory, Quantum Computing

- New branches of $\{$Physics, Computer Science, Mathematics$\}$ dealing with quantum information.
- Quantum information $=$ information held in a quantum physical system.
- Basic idea: replace $\{0, 1\}$ with $\mathrm{span}\{|0\rangle, |1\rangle\}$, the state space of a two-level quantum system.
- Shows great promise:

# Quantum Information Theory, Quantum Computing

- New branches of $\{\text{Physics}, \text{Computer Science}, \text{Mathematics}\}$ dealing with quantum information.
- Quantum information $=$ information held in a quantum physical system.
- Basic idea: replace $\{0, 1\}$ with $\mathrm{span}\{|0\rangle, |1\rangle\}$, the state space of a two-level quantum system.
- Shows great promise:
    1. Secure transmission of data, protocol security guaranteed by the laws of nature

# Quantum Information Theory, Quantum Computing

- New branches of $\{\text{Physics}, \text{Computer Science}, \text{Mathematics}\}$ dealing with quantum information.
- Quantum information = information held in a quantum physical system.
- Basic idea: replace $\{0, 1\}$ with $\operatorname{span}\{|0\rangle, |1\rangle\}$, the state space of a two-level quantum system.
- Shows great promise:
  1. Secure transmission of data, protocol security guaranteed by the laws of nature
  2. Fast integer factorization $\rightsquigarrow$ current algorithms (RSA, etc) obsolete

# Quantum Information Theory, Quantum Computing

- New branches of $\{$Physics, Computer Science, Mathematics$\}$ dealing with quantum information.
- Quantum information $=$ information held in a quantum physical system.
- Basic idea: replace $\{0, 1\}$ with $\mathrm{span}\{|0\rangle, |1\rangle\}$, the state space of a two-level quantum system.
- Shows great promise:
  1. Secure transmission of data, protocol security guaranteed by the laws of nature
  2. Fast integer factorization $\rightsquigarrow$ current algorithms (RSA, etc) obsolete
  3. Fast database search

# Quantum Information Theory, Quantum Computing

- New branches of $\{$Physics, Computer Science, Mathematics$\}$ dealing with quantum information.
- Quantum information $=$ information held in a quantum physical system.
- Basic idea: replace $\{0, 1\}$ with $\mathrm{span}\{|0\rangle, |1\rangle\}$, the state space of a two-level quantum system.
- Shows great promise:
    1. Secure transmission of data, protocol security guaranteed by the laws of nature
    2. Fast integer factorization $\rightsquigarrow$ current algorithms (RSA, etc) obsolete
    3. Fast database search
    4. Fast simulation of quantum systems

# Quantum Information Theory, Quantum Computing

- New branches of $\{$Physics, Computer Science, Mathematics$\}$ dealing with quantum information.
- Quantum information = information held in a quantum physical system.
- Basic idea: replace $\{0, 1\}$ with $\mathrm{span}\{|0\rangle, |1\rangle\}$, the state space of a two-level quantum system.
- Shows great promise:
  1. Secure transmission of data, protocol security guaranteed by the laws of nature
  2. Fast integer factorization $\rightsquigarrow$ current algorithms (RSA, etc) obsolete
  3. Fast database search
  4. Fast simulation of quantum systems
  5. etc...

# Entanglement in Quantum Information Theory

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

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

# Entanglement in Quantum Information Theory

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

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

- Two quantum systems: $\rho_{12} \in \mathrm{End}^{1,+}(\mathbb{C}^m \otimes \mathbb{C}^n) = \mathbb{M}_{mn}^{1,+}$.

# Entanglement in Quantum Information Theory

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

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

- Two quantum systems: $\rho_{12} \in \mathrm{End}^{1,+}(\mathbb{C}^m \otimes \mathbb{C}^n) = \mathbb{M}_{mn}^{1,+}$.
- A state $\rho_{12}$ 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 $t_i \geqslant 0$, $\sum_i t_i = 1$, $\rho_1(i) \in \mathbb{M}_m^{1,+}$, $\rho_2(i) \in \mathbb{M}_n^{1,+}$.

# Entanglement in Quantum Information Theory

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

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

- Two quantum systems: $\rho_{12} \in \mathrm{End}^{1,+}(\mathbb{C}^m \otimes \mathbb{C}^n) = \mathbb{M}_{mn}^{1,+}$.
- A state $\rho_{12}$ 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 $t_i \geqslant 0$, $\sum_i t_i = 1$, $\rho_1(i) \in \mathbb{M}_m^{1,+}$, $\rho_2(i) \in \mathbb{M}_n^{1,+}$.
- Equivalently, $\mathcal{SEP} = \mathrm{conv}\left[\mathbb{M}_m^{1,+} \otimes \mathbb{M}_n^{1,+}\right]$.

# Entanglement in Quantum Information Theory

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

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

- Two quantum systems: $\rho_{12} \in \mathrm{End}^{1,+}(\mathbb{C}^m \otimes \mathbb{C}^n) = \mathbb{M}_{mn}^{1,+}$.
- A state $\rho_{12}$ 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 $t_i \geqslant 0$, $\sum_i t_i = 1$, $\rho_1(i) \in \mathbb{M}_m^{1,+}$, $\rho_2(i) \in \mathbb{M}_n^{1,+}$.
- Equivalently, $\mathcal{SEP} = \mathrm{conv}\left[\mathbb{M}_m^{1,+} \otimes \mathbb{M}_n^{1,+}\right]$.
- Non-separable states are called entangled.

# More on entanglement - pure states

- Separable rank one (pure) states $\rho_{12} = P_{e \otimes f} = P_e \otimes P_f$.

# More on entanglement - pure states

- Separable rank one (pure) states $\rho_{12} = P_{e \otimes f} = P_e \otimes P_f$.
- Bell state or maximally entangled state $\rho_{12} = P_{\mathrm{Bell}}$, where

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \ni \mathrm{Bell} = \frac{1}{\sqrt{2}}(e_1 \otimes f_1 + e_2 \otimes f_2) \neq x \otimes y.$$

# More on entanglement - pure states

- Separable rank one (pure) states $\rho_{12} = P_{e \otimes f} = P_e \otimes P_f$.
- Bell state or maximally entangled state $\rho_{12} = P_{\mathrm{Bell}}$, where

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \ni \mathrm{Bell} = \frac{1}{\sqrt{2}}(e_1 \otimes f_1 + e_2 \otimes f_2) \neq x \otimes y.$$

- For rank one quantum states, entanglement can be detected and quantified by the entropy of entanglement

$$E_{\mathrm{ent}}(P_x) = H(s(x)) = -\sum_{i=1}^{\min(m,n)} s_i(x) \log s_i(x),$$

where $x \in \mathbb{C}^m \otimes \mathbb{C}^n \cong \mathbb{M}_{m \times n}(\mathbb{C})$ is seen as a $m \times n$ matrix and $s_i(x)$ are its singular values.

# More on entanglement - pure states

- Separable rank one (pure) states $\rho_{12} = P_{e \otimes f} = P_e \otimes P_f$.
- Bell state or maximally entangled state $\rho_{12} = P_{\mathrm{Bell}}$, where

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \ni \mathrm{Bell} = \frac{1}{\sqrt{2}}(e_1 \otimes f_1 + e_2 \otimes f_2) \neq x \otimes y.$$

- For rank one quantum states, entanglement can be detected and quantified by the entropy of entanglement

$$E_{\mathrm{ent}}(P_x) = H(s(x)) = -\sum_{i=1}^{\min(m,n)} s_i(x) \log s_i(x),$$

where $x \in \mathbb{C}^m \otimes \mathbb{C}^n \cong \mathbb{M}_{m \times n}(\mathbb{C})$ is seen as a $m \times n$ matrix and $s_i(x)$ are its singular values.

- A pure state $x \in \mathbb{C}^m \otimes \mathbb{C}^n$ is separable $\iff$ $E_{\mathrm{ent}}(P_x) = 0$.

# An image of entanglement

# Deciding separability vs. entanglement

- "I would not call entanglement one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought." [Schrödinger]

# Deciding separability vs. entanglement

- "I would not call entanglement one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought." [Schrödinger]
- Entanglement is essential to the exponential speed-up of some quantum algorithms.

# Deciding separability vs. entanglement

- "I wou... t of quant... classical lines ...
- Entar... tum algori...

## Shor's quantum factoring algorithm

- Runs on a quantum computer with polynomial time $O(\log^3 N)$.
- Classical sieve algorithms run in sub-exponential time $O(\exp(\log^{1/3} N))$.
- Entanglement is necessary for the exponential speed-up.
- State of the art factorization in labs: $21 = 3 \times 7$ [2011], 143 (?) [2012].

# Deciding separability vs. entanglement

- "I would not call entanglement one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought." [Schrödinger]
- Entanglement is essential to the exponential speed-up of some quantum algorithms.
- Deciding if a given $\rho_{12}$ is separable is NP-hard [Gurvitz].

# Deciding separability vs. entanglement

- "I would not call entanglement one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought." [Schrödinger]
- Entanglement is essential to the exponential speed-up of some quantum algorithms.
- Deciding if a given $\rho_{12}$ is separable is NP-hard [Gurvitz].
- Detecting entanglement for general states in low dimension $\mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathbb{C}^2 \otimes \mathbb{C}^3$ is possible via the PPT criterion [Horodecki].

# Deciding separability vs. entanglement

- "I would not call entanglement one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought." [Schrödinger]
- Entanglement is essential to the exponential speed-up of some quantum algorithms.
- Deciding if a given $\rho_{12}$ is separable is NP-hard [Gurvitz].
- Detecting entanglement for general states in low dimension $\mathbb{C}^2 \otimes \mathbb{C}^2$ and $\mathbb{C}^2 \otimes \mathbb{C}^3$ is possible via the PPT criterion [Horodecki].
- In general, there exists a countable hierarchy of conditions characterizing separability [Doherty et al] that can be checked by semidefinite programming.

# Separability via positive, but not completely positive maps

- Let $\mathcal{A}$ be a $C^*$ algebra. A map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ is called

# Separability via positive, but not completely positive maps

- Let $\mathcal{A}$ be a $C^*$ algebra. A map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ is called
  - positive if $A \geqslant 0 \implies \mathcal{N}(A) \geqslant 0$;

# Separability via positive, but not completely positive maps

- Let $\mathcal{A}$ be a $C^*$ algebra. A map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ is called
  - positive if $A \geqslant 0 \implies \mathcal{N}(A) \geqslant 0$;
  - completely positive (CP) if $\mathrm{id}_k \otimes \mathcal{N}$ is positive for all $k \geqslant 1$.

# Separability via positive, but not completely positive maps

- Let $\mathcal{A}$ be a $C^*$ algebra. A map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ is called
  - positive if $A \geqslant 0 \implies \mathcal{N}(A) \geqslant 0$;
  - completely positive (CP) if $\mathrm{id}_k \otimes \mathcal{N}$ is positive for all $k \geqslant 1$.
- Let $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ be a completely positive map. Then, for every state $\rho_{12} \in \mathbb{M}_{mn}^{1,+}$, one has $[\mathrm{id}_m \otimes \mathcal{N}](\rho_{12}) \geqslant 0$.

# Separability via positive, but not completely positive maps

- Let $\mathcal{A}$ be a $C^*$ algebra. A map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ is called
  - positive if $A \geqslant 0 \implies \mathcal{N}(A) \geqslant 0$;
  - completely positive (CP) if $\mathrm{id}_k \otimes \mathcal{N}$ is positive for all $k \geqslant 1$.
- Let $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ be a completely positive map. Then, for every state $\rho_{12} \in \mathbb{M}_{mn}^{1,+}$, one has $[\mathrm{id}_m \otimes \mathcal{N}](\rho_{12}) \geqslant 0$.
- Let $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ be a positive map. Then, for every separable state $\rho_{12} \in \mathbb{M}_{mn}^{1,+}$, one has $[\mathrm{id}_m \otimes \mathcal{N}](\rho_{12}) \geqslant 0$.
  1. $\rho_{12}$ separable $\implies \rho_{12} = \sum_i t_i \rho_1(i) \otimes \rho_2(i)$.
  2. $[\mathrm{id}_m \otimes \mathcal{N}](\rho_{12}) = \sum_i t_i \rho_1(i) \otimes \mathcal{N}[\rho_2(i)]$.
  3. For all $i$, $\mathcal{N}[\rho_2(i)] \geqslant 0$, so $[\mathrm{id}_m \otimes \mathcal{N}](\rho_{12}) \geqslant 0$.

# Separability via positive, but not completely positive maps

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

# Separability via positive, but not completely positive maps

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

# Positive Partial Transpose matrices

- The transposition map $\mathrm{t}$ is positive, but not CP. Define the convex set

$$\mathcal{PPT} = \{\rho_{12} \in \mathbb{M}_{mn}^{1,+} \mid [\mathrm{id}_m \otimes \mathrm{t}_n](\rho_{12}) \geqslant 0\}.$$

# Positive Partial Transpose matrices

- The transposition map $\mathrm{t}$ is positive, but not CP. Define the convex set

$$\mathcal{PPT} = \{\rho_{12} \in \mathbb{M}_{mn}^{1,+} \mid [\mathrm{id}_m \otimes \mathrm{t}_n](\rho_{12}) \geqslant 0\}.$$

- 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.

# The PPT criterion at work

- Recall the Bell state $\rho_{12} = P_{\mathrm{Bell}}$, where

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \ni \mathrm{Bell} = \frac{1}{\sqrt{2}}(e_1 \otimes f_1 + e_2 \otimes f_2).$$

# The PPT criterion at work

- Recall the Bell state $\rho_{12} = P_{\mathrm{Bell}}$, where

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \ni \mathrm{Bell} = \frac{1}{\sqrt{2}}(e_1 \otimes f_1 + e_2 \otimes f_2).$$

- Written as a matrix in $\mathbb{M}_{2\cdot 2}^{1,+}$

$$\rho_{12} = \frac{1}{2}\left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right) = \frac{1}{2}\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}.$$

# The PPT criterion at work

- Recall the Bell state $\rho_{12} = P_{\mathrm{Bell}}$, where

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \ni \mathrm{Bell} = \frac{1}{\sqrt{2}}(e_1 \otimes f_1 + e_2 \otimes f_2).$$

- Written as a matrix in $\mathbb{M}_{2 \cdot 2}^{1,+}$

$$\rho_{12} = \frac{1}{2}\left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right) = \frac{1}{2}\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}.$$

- Partial transposition: transpose each block $B_{ij}$:

$$\rho_{12}^{\Gamma} = [\mathrm{id}_2 \otimes \mathrm{t}_2](\rho_{12}) = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

# The PPT criterion at work

- Recall the Bell state $\rho_{12} = P_{\mathrm{Bell}}$, where

$$\mathbb{C}^2 \otimes \mathbb{C}^2 \ni \mathrm{Bell} = \frac{1}{\sqrt{2}}(e_1 \otimes f_1 + e_2 \otimes f_2).$$

- Written as a matrix in $\mathbb{M}^{1,+}_{2\cdot 2}$

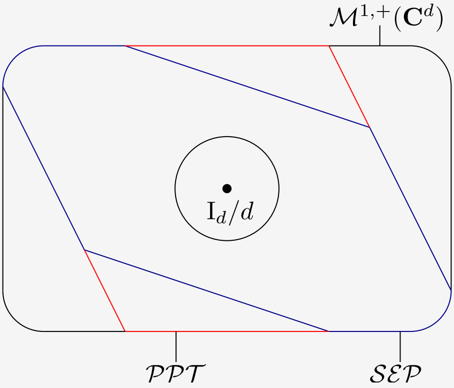
$$\rho_{12} = \frac{1}{2}\left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{array}\right) = \frac{1}{2}\begin{pmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{pmatrix}.$$

- Partial transposition: transpose each block $B_{ij}$:

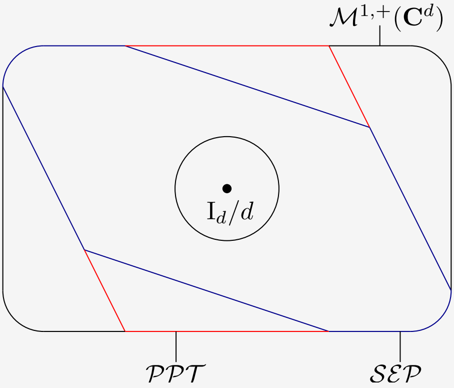
$$\rho_{12}^{\Gamma} = [\mathrm{id}_2 \otimes \mathrm{t}_2](\rho_{12}) = \frac{1}{2}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

- This matrix is no longer positive $\implies$ the state is entangled.

# Three convex sets

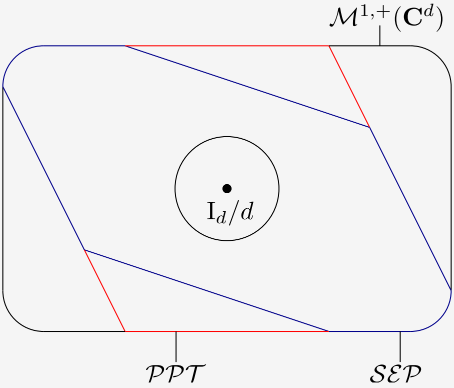


# Three convex sets




- States in $\mathcal{PPT} \setminus \mathcal{SEP}$ are called bound entangled: no "maximal" entangled can be distilled from them.

# Three convex sets




- States in $\mathcal{PPT} \setminus \mathcal{SEP}$ are called bound entangled: no "maximal" entangled can be distilled from them.
- All these sets contain an open ball around the identity.

# The Choi matrix of a map

- For any $n$, recall that the maximally entangled state is the orthogonal projection onto

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

# The Choi matrix of a map

- For any $n$, recall that the maximally entangled state is the orthogonal projection onto

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

- To any map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$, associate its Choi matrix

$$C_{\mathcal{N}} = [\mathrm{id}_n \otimes \mathcal{N}](P_{\mathrm{Bell}}) \in \mathbb{M}_n \otimes \mathcal{A}.$$

# The Choi matrix of a map

- For any $n$, recall that the maximally entangled state is the orthogonal projection onto

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

- To any map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$, associate its Choi matrix

$$C_{\mathcal{N}} = [\mathrm{id}_n \otimes \mathcal{N}](P_{\mathrm{Bell}}) \in \mathbb{M}_n \otimes \mathcal{A}.$$

- Equivalently, if $E_{ij}$ are the matrix units in $\mathbb{M}_n$, then

$$C_{\mathcal{N}} = \sum_{i,j=1}^{n} E_{ij} \otimes \mathcal{N}(E_{ij}).$$

# The Choi matrix of a map

- For any $n$, recall that the maximally entangled state is the orthogonal projection onto

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

- To any map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$, associate its Choi matrix

$$C_{\mathcal{N}} = [\mathrm{id}_n \otimes \mathcal{N}](P_{\mathrm{Bell}}) \in \mathbb{M}_n \otimes \mathcal{A}.$$

- Equivalently, if $E_{ij}$ are the matrix units in $\mathbb{M}_n$, then

$$C_{\mathcal{N}} = \sum_{i,j=1}^{n} E_{ij} \otimes \mathcal{N}(E_{ij}).$$

**Theorem (Choi '72)**

*A map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ is CP iff its Choi matrix $C_{\mathcal{N}}$ is positive.*

# The Choi-Jamiolkowski isomorphism

- Recall (here $\mathcal{A} = \mathbb{M}_d$)

$$C_{\mathcal{N}} = [\mathrm{id}_n \otimes \mathcal{N}](P_{\mathrm{Bell}}) = \sum_{i,j=1}^{n} E_{ij} \otimes \mathcal{N}(E_{ij}) \in \mathbb{M}_n \otimes \mathbb{M}_d.$$

# The Choi-Jamiolkowski isomorphism

- Recall (here $\mathcal{A} = \mathbb{M}_d$)

$$C_{\mathcal{N}} = [\mathrm{id}_n \otimes \mathcal{N}](P_{\mathrm{Bell}}) = \sum_{i,j=1}^{n} E_{ij} \otimes \mathcal{N}(E_{ij}) \in \mathbb{M}_n \otimes \mathbb{M}_d.$$

- The map $\mathcal{N} \mapsto C_{\mathcal{N}}$ is called the Choi-Jamiolkowski isomorphism.

# The Choi-Jamiolkowski isomorphism

- Recall (here $\mathcal{A} = \mathbb{M}_d$)

$$C_{\mathcal{N}} = [\mathrm{id}_n \otimes \mathcal{N}](P_{\mathrm{Bell}}) = \sum_{i,j=1}^{n} E_{ij} \otimes \mathcal{N}(E_{ij}) \in \mathbb{M}_n \otimes \mathbb{M}_d.$$

- The map $\mathcal{N} \mapsto C_{\mathcal{N}}$ is called the Choi-Jamiolkowski 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 ($[\mathrm{Tr} \otimes \mathrm{id}]C_{\mathcal{N}} = \mathrm{I}_d$);
  5. Trace preserving maps to operators with unit left partial trace ($[\mathrm{id} \otimes \mathrm{Tr}]C_{\mathcal{N}} = \mathrm{I}_n$).

# Intermediate positivity notions

- A map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ is called *k-positive* if $\mathrm{id}_k \otimes \mathcal{N}$ is positive.

# Intermediate positivity notions

- A map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ is called *k-positive* if $\mathrm{id}_k \otimes \mathcal{N}$ is positive.
- A matrix $C \in \mathbb{M}_{nd}$ is called *k-positive* if $\langle x, Cx \rangle \geqslant 0$ for all vectors $x \in \mathbb{C}^n \otimes \mathbb{C}^d$ of rank at most $k$.

# Intermediate positivity notions

- A map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ is called $k$-positive if $\mathrm{id}_k \otimes \mathcal{N}$ is positive.
- A matrix $C \in \mathbb{M}_{nd}$ is called $k$-positive if $\langle x, Cx \rangle \geqslant 0$ 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

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

# Intermediate positivity notions

- A map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ is called $k$-positive if $\mathrm{id}_k \otimes \mathcal{N}$ is positive.
- A matrix $C \in \mathbb{M}_{nd}$ is called $k$-positive if $\langle x, Cx \rangle \geqslant 0$ 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

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

**Theorem**

*A map $\mathcal{N} : \mathbb{M}_n \to \mathcal{A}$ is $k$-positive iff its Choi matrix $C_{\mathcal{N}}$ is $k$-positive. In particular, $\mathcal{N}$ is positive iff $C_{\mathcal{N}}$ is block-positive.*

# Random Choi matrices

- Let $\mu$ be a compactly supported probability measure on $\mathbb{R}$.

# Random Choi matrices

- Let $\mu$ be a compactly supported probability measure on $\mathbb{R}$.
- For each $d$ we introduce a real valued diagonal matrix $X_d$ of $\mathbb{M}_n \otimes \mathbb{M}_d$ whose eigenvalue counting distribution converges to $\mu$ and whose extremal eigenvalues converge to the respective extrema of the support of $\mu$.

# Random Choi matrices

- Let $\mu$ be a compactly supported probability measure on $\mathbb{R}$.
- For each $d$ we introduce a real valued diagonal matrix $X_d$ of $\mathbb{M}_n \otimes \mathbb{M}_d$ whose eigenvalue counting distribution converges to $\mu$ and whose extremal eigenvalues converge to the respective extrema of the support of $\mu$.
- Let $U_d$ be a random Haar unitary matrix in the unitary group $\mathcal{U}_{nd}$.

# Random Choi matrices

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

# Random Choi matrices

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

**Theorem**

*Under the above assumptions, if* $\operatorname{supp}(\mu^{\boxplus n/k}) \subset (0, \infty)$ *then, almost surely as* $d \to \infty$, *the map* $\mathcal{N}_\mu^{(d)}$ *is k-positive.*

# Random Choi matrices

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

## Theorem

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

# Free Probability Theory

- Invented by Voiculescu in the 80s to solve problems in operator algebras.

# Free Probability Theory

- Invented by Voiculescu in the 80s to solve problems in operator algebras.
- A non-commutative probability space $(\mathcal{A}, \tau)$ is an algebra $\mathcal{A}$ with a unital state $\tau : \mathcal{A} \to \mathbb{C}$. Elements $a \in \mathcal{A}$ are called random variables.

# Free Probability Theory

- Invented by Voiculescu in the 80s to solve problems in operator algebras.
- A non-commutative probability space $(\mathcal{A}, \tau)$ is an algebra $\mathcal{A}$ with a unital state $\tau : \mathcal{A} \to \mathbb{C}$. Elements $a \in \mathcal{A}$ are called random variables.
- Examples: $(L^\infty(\Omega, \mathcal{F}, \mathbb{P}), \mathbb{E})$, $\mathbb{M}_d(\mathbb{C}), d^{-1}\mathrm{Tr})$, $(\mathbb{C}G, \delta_e)$.

# Free Probability Theory

- Invented by Voiculescu in the 80s to solve problems in operator algebras.
- A non-commutative probability space $(\mathcal{A}, \tau)$ is an algebra $\mathcal{A}$ with a unital state $\tau : \mathcal{A} \to \mathbb{C}$. Elements $a \in \mathcal{A}$ are called random variables.
- Examples: $(L^\infty(\Omega, \mathcal{F}, \mathbb{P}), \mathbb{E})$, $\mathbb{M}_d(\mathbb{C}), d^{-1}\mathrm{Tr})$, $(\mathbb{C}G, \delta_e)$.
- Several notions of independence: classical independence, free independence.

# Free Probability Theory

- Invented by Voiculescu in the 80s to solve problems in operator algebras.
- A non-commutative probability space $(\mathcal{A}, \tau)$ is an algebra $\mathcal{A}$ with a unital state $\tau : \mathcal{A} \to \mathbb{C}$. Elements $a \in \mathcal{A}$ are called random variables.
- Examples: $(L^\infty(\Omega, \mathcal{F}, \mathbb{P}), \mathbb{E})$, $\mathbb{M}_d(\mathbb{C}), d^{-1}\mathrm{Tr})$, $(\mathbb{C}G, \delta_e)$.
- Several notions of independence: classical independence, free independence.
- If $a, b$ are freely independent random variables, the law of $(a, b)$ can be computed in terms of the laws of $a$ and $b$.

# Free Probability Theory

- Invented by Voiculescu in the 80s to solve problems in operator algebras.
- A non-commutative probability space $(\mathcal{A}, \tau)$ is an algebra $\mathcal{A}$ with a unital state $\tau : \mathcal{A} \to \mathbb{C}$. Elements $a \in \mathcal{A}$ are called random variables.
- Examples: $(L^\infty(\Omega, \mathcal{F}, \mathbb{P}), \mathbb{E})$, $\mathbb{M}_d(\mathbb{C}), d^{-1}\mathrm{Tr})$, $(\mathbb{C}G, \delta_e)$.
- Several notions of independence: classical independence, free independence.
- If $a, b$ are freely independent random variables, the law of $(a, b)$ can be computed in terms of the laws of $a$ and $b$.
- Random matrices are asymptotically free.

# Free Probability Theory

- Invented by Voiculescu in the 80s to solve problems in operator algebras.
- A non-commutative probability space $(\mathcal{A}, \tau)$ is an algebra $\mathcal{A}$ with a unital state $\tau : \mathcal{A} \to \mathbb{C}$. Elements $a \in \mathcal{A}$ are called random variables.
- Examples: $(L^\infty(\Omega, \mathcal{F}, \mathbb{P}), \mathbb{E})$, $\mathbb{M}_d(\mathbb{C}), d^{-1}\mathrm{Tr})$, $(\mathbb{C}G, \delta_e)$.
- Several notions of independence: classical independence, free independence.
- If $a, b$ are freely independent random variables, the law of $(a, b)$ can be computed in terms of the laws of $a$ and $b$.
- Random matrices are asymptotically free.
- If $A_d, B_d$ are matrices of size $d$, whose spectra converge towards $a, b$, what is the spectrum of $A_d + B_d$ ?

# Free Probability Theory

- Invented by Voiculescu in the 80s to solve problems in operator algebras.
- A non-commutative probability space $(\mathcal{A}, \tau)$ is an algebra $\mathcal{A}$ with a unital state $\tau : \mathcal{A} \to \mathbb{C}$. Elements $a \in \mathcal{A}$ are called random variables.
- Examples: $(L^\infty(\Omega, \mathcal{F}, \mathbb{P}), \mathbb{E})$, $\mathbb{M}_d(\mathbb{C}), d^{-1}\mathrm{Tr})$, $(\mathbb{C}G, \delta_e)$.
- Several notions of independence: classical independence, free independence.
- If $a, b$ are freely independent random variables, the law of $(a, b)$ can be computed in terms of the laws of $a$ and $b$.
- Random matrices are asymptotically free.
- If $A_d, B_d$ are matrices of size $d$, whose spectra converge towards $a, b$, what is the spectrum of $A_d + B_d$ ?
- When $d \to \infty$, the spectrum of $A_d + B_d$ converges to $a \boxplus b$.

# Proof ingredients

Let $\mathcal{N}_\mu^{(d)} : \mathbb{M}_n \to \mathbb{M}_d$ 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 $\mathcal{N}_\mu^{(d)}$ is $k$-positive. If $\operatorname{supp}(\mu^{\boxplus n/k}) \cap (-\infty, 0) \neq \emptyset$ then, almost surely as $d \to \infty$, $\mathcal{N}_\mu^{(d)}$ is not $k$-positive.*

# Proof ingredients

Let $\mathcal{N}_\mu^{(d)} : \mathbb{M}_n \to \mathbb{M}_d$ 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 $\mathcal{N}_\mu^{(d)}$ is $k$-positive. If $\operatorname{supp}(\mu^{\boxplus n/k}) \cap (-\infty, 0) \neq \emptyset$ then, almost surely as $d \to \infty$, $\mathcal{N}_\mu^{(d)}$ is not $k$-positive.*

## Proposition

*A map $\mathcal{N}$ is $k$-positive iff for any self-adjoint projection $P \in \mathbb{M}_n$ of rank $k$, the operator $P \otimes \mathrm{I}_\mathcal{A} \cdot C_\mathcal{N} \cdot P \otimes 1_\mathcal{A}$ is positive.*

# Proof ingredients

Let $\mathcal{N}_\mu^{(d)} : \mathbb{M}_n \to \mathbb{M}_d$ 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* $\mathcal{N}_\mu^{(d)}$ *is* $k$*-positive. If* $\operatorname{supp}(\mu^{\boxplus n/k}) \cap (-\infty, 0) \neq \emptyset$ *then, almost surely as* $d \to \infty$, $\mathcal{N}_\mu^{(d)}$ *is not* $k$*-positive.*

## Proposition

*A map* $\mathcal{N}$ *is* $k$*-positive iff for any self-adjoint projection* $P \in \mathbb{M}_n$ *of rank* $k$*, the operator* $P \otimes \mathrm{I}_\mathcal{A} \cdot C_\mathcal{N} \cdot P \otimes 1_\mathcal{A}$ *is positive.*

## Proposition (Nica and Speicher)

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

# Maps associated to probability measures

- Let $\mu$ be a compactly supported probability measure on $\mathbb{R}$.

# Maps associated to probability measures

- Let $\mu$ be a compactly supported probability measure on $\mathbb{R}$.
- The vN algebra $L^\infty(\mathbb{R}, \mu)$, endowed with the expectation trace $\mathbb{E}$ is a non-commutative probability space. Let $X \in L^\infty(\mathbb{R}, \mu)$ be the identity map $x \mapsto x$.

# Maps associated to probability measures

- Let $\mu$ be a compactly supported probability measure on $\mathbb{R}$.
- The vN algebra $L^\infty(\mathbb{R}, \mu)$, endowed with the expectation trace $\mathbb{E}$ is a non-commutative probability space. Let $X \in L^\infty(\mathbb{R}, \mu)$ be the identity map $x \mapsto x$.
- Consider the vN ncps free product $(\tilde{M}, \mathrm{tr} * \mathbb{E}) = (\mathbb{M}_n, \mathrm{tr}) * (L^\infty(\mathbb{R}, \mu), \mathbb{E})$.

# Maps associated to probability measures

- Let $\mu$ be a compactly supported probability measure on $\mathbb{R}$.
- The vN algebra $L^\infty(\mathbb{R}, \mu)$, endowed with the expectation trace $\mathbb{E}$ is a non-commutative probability space. Let $X \in L^\infty(\mathbb{R}, \mu)$ be the identity map $x \mapsto x$.
- Consider the vN ncps free product $(\tilde{M}, \mathrm{tr} * \mathbb{E}) = (\mathbb{M}_n, \mathrm{tr}) * (L^\infty(\mathbb{R}, \mu), \mathbb{E})$.
- Finally, let $(M, \tau)$ be the contracted vN ncps $M = E_{11} \tilde{M} E_{11}$.

# Maps associated to probability measures

- Let $\mu$ be a compactly supported probability measure on $\mathbb{R}$.
- The vN algebra $L^\infty(\mathbb{R}, \mu)$, endowed with the expectation trace $\mathbb{E}$ is a non-commutative probability space. Let $X \in L^\infty(\mathbb{R}, \mu)$ be the identity map $x \mapsto x$.
- Consider the vN ncps free product $(\tilde{M}, \mathrm{tr} * \mathbb{E}) = (\mathbb{M}_n, \mathrm{tr}) * (L^\infty(\mathbb{R}, \mu), \mathbb{E})$.
- Finally, let $(M, \tau)$ be the contracted vN ncps $M = E_{11} \tilde{M} E_{11}$.
- Define

$$\begin{aligned} \mathcal{N}_\mu : \mathbb{M}_n &\to M \\ E_{ij} &\mapsto E_{1i} X E_{j1} \end{aligned}$$

# Maps associated to probability measures

- Define

$$\begin{aligned} \mathcal{N}_\mu : \mathbb{M}_n &\to M \\ E_{ij} &\mapsto E_{1i} X E_{j1} \end{aligned}$$

**Theorem**

*The map $\mathcal{N}_\mu$ is k-positive iff* $\operatorname{supp}(\mu^{\boxplus n/k}) \subseteq \mathbb{R}_+$.

# Example: semicircular measures

- Let $s_{a,\sigma}$ be the semi-circle distribution of mean $a$ and variance $\sigma^2$.

# Example: semicircular measures

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

# Example: semicircular measures

- Let $s_{a,\sigma}$ be the semi-circle distribution of mean $a$ and variance $\sigma^2$.
- Its support is $[a - 2\sigma, a + 2\sigma]$.
- In free probability theory, $s_{0,1}$ plays the role of the standard Gaussian in classical probability, cf Free Central Limit Theorem.

# Example: semicircular measures

- Let $s_{a,\sigma}$ be the semi-circle distribution of mean $a$ and variance $\sigma^2$.
- Its support is $[a-2\sigma, a+2\sigma]$.
- In free probability theory, $s_{0,1}$ plays the role of the standard Gaussian in classical probability, cf Free Central Limit Theorem.
- 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 $a, \sigma$ some positive parameters. The map $\mathcal{N}_{a,\sigma} : \mathbb{M}_n \to M$ associated to a semi-circular distribution $s_{a,\sigma}$ is $k$-positive iff $k \leqslant 4n\sigma/a^2$. 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.*

Merci !