When Alice & Bob meet Banach

Asymptotic geometric analysis and Random matrix theory in Quantum information

Université Claude Bernard Lyon 1 & Universitat Autònoma de Barcelona

Cécilia Lancien

WYRM 2015 - Madrid
Outline

1 Introduction

2 Interlude: reminder about GUE and Wishart matrices

3 Mean-width of the set of states which are separable vs satisfying a separability criterion

4 Entanglement vs Violating a separability criterion for random states

5 Summary and broader perspectives
Why Asymptotic geometric analysis and Random matrix theory in Quantum information?

- **State of a quantum system**: Positive and trace 1 operator $\rho$ (*density operator*) on a Hilbert space $H$ (*state space*).
Why Asymptotic geometric analysis and Random matrix theory in Quantum information?

- State of a quantum system: Positive and trace 1 operator $\rho$ (density operator) on a Hilbert space $H$ (state space).

- Transformation on a quantum system: Completely Positive and Trace Preserving map $\phi : X \in \mathcal{B}(H) \mapsto \text{Tr}_{E} (VXV^*) \in \mathcal{B}(H')$ for some isometry $V : H \hookrightarrow E \otimes H'$ (quantum channel).
Why Asymptotic geometric analysis and Random matrix theory in Quantum information?

- **State of a quantum system**: Positive and trace 1 operator $\rho$ (*density operator*) on a Hilbert space $H$ (*state space*).

- **Transformation on a quantum system**: Completely Positive and Trace Preserving map $\phi : X \in B(H) \mapsto \text{Tr}_E (VXV^*) \in B(H')$ for some isometry $V : H \hookrightarrow E \otimes H'$ (*quantum channel*).

→ In finite dimension: Random states or transformations $\equiv$ Random matrices.

**Paradigm**: Constructing explicitly an operator having certain properties may be harder than asserting that a suitably chosen random one should work with large probability.

→ Usually, the curse of dimensionality then becomes an asset.
Why Asymptotic geometric analysis and Random matrix theory in Quantum information?

- **State of a quantum system**: Positive and trace 1 operator $\rho$ (*density operator*) on a Hilbert space $H$ (*state space*).

- **Transformation on a quantum system**: Completely Positive and Trace Preserving map $\phi : X \in \mathcal{B}(H) \mapsto \text{Tr}_E(VXV^*) \in \mathcal{B}(H')$ for some isometry $V : H \leftrightarrow E \otimes H'$ (*quantum channel*).

$\rightarrow$ In finite dimension: Random states or transformations $\equiv$ Random matrices.

**Paradigm**: Constructing explicitly an operator having certain properties may be harder than asserting that a suitably chosen random one should work with large probability. $\rightarrow$ Usually, the curse of dimensionality then becomes an asset.

**A few (partial) examples**:
- **Additivity conjectures in QI**: Both counterexamples (Aubrun/Szarek/Werner...) and "weak additivity" results (Montanaro, Collins/Fukuda/Nechita...) were provided by random matrix theory and local theory of Banach spaces.
- **Generic properties of states, measurements, evolutions etc. under certain constraints, such as noise, energy, locality etc.** (Hayden/Leung/Winter, Linden/Popescu/Short/Winter, Aubrun/Lancien...)
Separability vs Entanglement for bipartite quantum systems

Definition (Separable vs Entangled)

A bipartite quantum state $\rho_{AB}$ on $A \otimes B$ is separable if it may be written as a convex combination of product states, i.e. $\rho_{AB} = \sum_i p_i \sigma_A^{(i)} \otimes \tau_B^{(i)}$. Otherwise, it is entangled.
Separability vs Entanglement for bipartite quantum systems

Definition (Separable vs Entangled)

A bipartite quantum state $\rho_{AB}$ on $A \otimes B$ is separable if it may be written as a convex combination of product states, i.e. $\rho_{AB} = \sum_i p_i \sigma_A^{(i)} \otimes \tau_B^{(i)}$. Otherwise, it is entangled.

If a compound system is in a separable global state, there are no intrinsically quantum correlations between its local constituents.

→ Deciding whether a given bipartite state is entangled or (close to) separable is an important issue in quantum physics.
Separability vs Entanglement for bipartite quantum systems

Definition (Separable vs Entangled)

A bipartite quantum state $\rho_{AB}$ on $A \otimes B$ is *separable* if it may be written as a convex combination of product states, i.e. $\rho_{AB} = \sum_i p_i \sigma^{(i)}_A \otimes \tau^{(i)}_B$. Otherwise, it is *entangled*.

If a compound system is in a separable global state, there are no intrinsically quantum correlations between its local constituents.

→ Deciding whether a given bipartite state is entangled or (close to) separable is an important issue in quantum physics.

**Problem**: It is known to be a hard task, both from a mathematical and a computational point of view (Gurvits).

**Solution**: Find set of states which are easier to characterize and which contain the set of separable states.

→ Necessary conditions for separability that have a simple mathematical description and that may be checked efficiently on a computer (e.g. by a semi-definite programme).
The PPT criterion for separability

Definition (Partial Transpose)

The partial transpose of a state $\rho_{AB}$ on $A \otimes B$ is defined as

$$\Gamma_{AB}(\rho_{AB}) = Id_A \otimes T_B(\rho_{AB}),$$

where $Id$ denotes the identity map and $T$ denotes the transpose map.

Remarks:

- This is obvious since $\Gamma_{AB}(\sigma_A \otimes \tau_B) = \sigma_A \otimes T_B(\tau_B)$.
- NC for separability on $C_2 \otimes C_2$ or $C_2 \otimes C_3$ (Horodecki).
- In higher dimensions, there exist PPT entangled states.
- Special instance in the class of separability relaxations built on: $\rho_{AB}$ is separable iff for any positive but not completely positive map $\Lambda_B$, $Id_A \otimes \Lambda_B(\rho_{AB})$ is positive (Horodecki).

Cécilia Lancien
When Alice & Bob meet Banach
WYRM 2015 - Madrid
### Definition (Partial Transpose)

The partial transpose of a state $\rho_{AB}$ on $A \otimes B$ is defined as

$$\Gamma_{AB}(\rho_{AB}) = Id_A \otimes T_B(\rho_{AB}),$$

where $Id$ denotes the identity map and $T$ denotes the transpose map.

### NC for Separability (Peres)

On a bipartite Hilbert space $A \otimes B$, if a state is separable, then it is positive under partial transpose (PPT).
The PPT criterion for separability

**Definition (Partial Transpose)**

The partial transpose of a state $\rho_{AB}$ on $A \otimes B$ is defined as

$$\Gamma_{AB}(\rho_{AB}) = Id_A \otimes T_B(\rho_{AB}),$$

where $Id$ denotes the identity map and $T$ denotes the transpose map.

**NC for Separability (Peres)**

On a bipartite Hilbert space $A \otimes B$, if a state is separable, then it is positive under partial transpose (PPT).

**Remarks:**

- This is obvious since $\Gamma_{AB}(\sigma_A \otimes \tau_B) = \sigma_A \otimes T_B(\tau_B)$.
- NSC for separability on $C^2 \otimes C^2$ or $C^2 \otimes C^3$ (Horodecki). In higher dimensions, there exist PPT entangled states.
- Special instance in the class of separability relaxations built on: $\rho_{AB}$ is separable iff for any positive but not completely positive map $\Lambda_B$, $Id_A \otimes \Lambda_B(\rho_{AB})$ is positive (Horodecki).
The \( k \)-extendibility criterion for separability

**Definition (\( k \)-extendibility)**

Let \( k \geq 2 \). A state \( \rho_{AB} \) on \( A \otimes B \) is \( k \)-extendible with respect to \( B \) if there exists a state \( \rho_{AB}^k \) on \( A \otimes B \otimes^k \) which is invariant under any permutation of the \( B \) subsystems and such that

\[
\rho_{AB} = \text{Tr}_{B^{k-1}} \rho_{AB}^k.
\]
The $k$-extendibility criterion for separability

Definition ($k$-extendibility)

Let $k \geq 2$. A state $\rho_{AB}$ on $A \otimes B$ is $k$-extendible with respect to $B$ if there exists a state $\rho_{AB^k}$ on $A \otimes B^k$ which is invariant under any permutation of the $B$ subsystems and such that $\rho_{AB} = \text{Tr}_{B^{k-1}} \rho_{AB^k}$.

NSC for Separability (Doherty/Parrilo/Spedalieri)

On a bipartite Hilbert space $A \otimes B$, a state is separable if and only if it is $k$-extendible w.r.t. $B$ for all $k \geq 2$. 

Remarks:

• "$\rho_{AB}$ separable $\Rightarrow$ $\rho_{AB^k}$-extendible w.r.t. $B$ for all $k \geq 2"$ is obvious since $\sigma_A \otimes \tau_B = \text{Tr}_{B^{k-1}} (\sigma_A \otimes \tau_B^k)$.

• "$\rho_{AB^k}$-extendible w.r.t. $B$ for all $k \geq 2 \Rightarrow \rho_{AB}$ separable" relies on the quantum De Finetti theorem (Christandl/König/Mitchison/Renner).

• $\rho_{AB^k}$-extendible w.r.t. $B \Rightarrow \rho_{AB^k'}$-extendible w.r.t. $B$ for $k' \leq k$.

→ Hierarchy of NC for separability, which an entangled state is guaranteed to stop passing at some point (but one cannot tell when a priori).
The $k$-extendibility criterion for separability

**Definition ($k$-extendibility)**

Let $k \geq 2$. A state $\rho_{AB}$ on $A \otimes B$ is $k$-extendible with respect to $B$ if there exists a state $\rho_{AB}^k$ on $A \otimes B \otimes^k$ which is invariant under any permutation of the $B$ subsystems and such that $\rho_{AB} = \text{Tr}_{B}^{k-1} \rho_{AB}^k$.

**NSC for Separability** (Doherty/Parrilo/Spedalieri)

On a bipartite Hilbert space $A \otimes B$, a state is separable if and only if it is $k$-extendible w.r.t. $B$ for all $k \geq 2$.

**Remarks** :

- “$\rho_{AB}$ separable $\Rightarrow$ $\rho_{AB}$ $k$-extendible w.r.t. $B$ for all $k \geq 2$” is obvious since $\sigma_A \otimes \tau_B = \text{Tr}_{B}^{k-1} \left[ \sigma_A \otimes \tau_B \otimes^k \right]$.
- “$\rho_{AB}$ $k$-extendible w.r.t. $B$ for all $k \geq 2$ $\Rightarrow$ $\rho_{AB}$ separable” relies on the quantum De Finetti theorem (Christandl/König/Mitchison/Renner).
- $\rho_{AB}$ $k$-extendible w.r.t. $B$ $\Rightarrow$ $\rho_{AB}$ $k'$-extendible w.r.t. $B$ for $k' \leq k$.
- $\rightarrow$ Hierarchy of NC for separability, which an entangled state is guaranteed to stop passing at some point (but one cannot tell when $a priori$).
**Problem** : When relaxing the separability constraint to one which is easier to check, how “rough” is the approximation?

**Known** : There exist states which are PPT or $k$-extendible, and nevertheless “very” entangled (i.e. far away from the set of separable states in some standard or operational distance measure).

→ Instead of looking at worst case scenarios, can we say something stronger about average/typical behaviours?
Problem: When relaxing the separability constraint to one which is easier to check, how “rough” is the approximation?

Known: There exist states which are PPT or $k$-extendible, and nevertheless “very” entangled (i.e. far away from the set of separable states in some standard or operational distance measure).

→ Instead of looking at worst case scenarios, can we say something stronger about average/typical behaviours?

Two possible quantitative strategies

• Estimate the size of the set of states, either satisfying a given separability criterion or being indeed separable. → Information on how much bigger than the separable set the relaxed set is.

• Characterize when certain random states are with high probability, either violating a given separability criterion or indeed entangled. → Information on how powerful the separability test is to detect entanglement.
Outline

1. Introduction

2. Interlude: reminder about GUE and Wishart matrices

3. Mean-width of the set of states which are separable vs satisfying a separability criterion

4. Entanglement vs Violating a separability criterion for random states

5. Summary and broader perspectives
Asymptotic spectrum of GUE and Wishart matrices

**Definitions (Gaussian Unitary Ensemble and Wishart matrices)**

- **G** is a \( n \times n \) GUE matrix if \( G = (H + H^*)/\sqrt{2} \) with \( H \) a \( n \times n \) matrix having independent complex normal entries.
- **W** is a \((n, s)\)-Wishart matrix if \( W = HH^* \) with \( H \) a \( n \times s \) matrix having independent complex normal entries.

**Definitions (Semicircular and Marˇcenko-Pastur distributions)**

- \( d\mu_{SC}(m, \sigma^2)(x) = \frac{1}{2} \pi \sigma^2 \sqrt{4\sigma^2 - (x - m)^2} \text{1}_{[m-\sigma, m+\sigma]}(x) \text{d}x \)
- \( d\mu_{MP}(\lambda)(x) = \begin{cases} f_{\lambda}(x) \text{d}x & \text{if } \lambda > 1 \\ (1-\lambda)f_{\lambda}(x) \text{d}x & \text{if } \lambda \leq 1 \end{cases} \)

\( f_{\lambda}(x) = \frac{\sqrt{(\lambda+1-x)(x-\lambda-1)}}{2\pi x} \text{1}_{[\lambda-1, \lambda+1]}(x) \)
Asymptotic spectrum of GUE and Wishart matrices

**Definitions (Gaussian Unitary Ensemble and Wishart matrices)**

- $G$ is an $n \times n$ GUE matrix if $G = \frac{H + H^*}{\sqrt{2}}$ with $H$ a $n \times n$ matrix having independent complex normal entries.
- $W$ is a $(n, s)$-Wishart matrix if $W = HH^*$ with $H$ a $n \times s$ matrix having independent complex normal entries.

**Definitions (Semicircular and Marčenko-Pastur distributions)**

- $d\mu_{SC}(m, \sigma^2)(x) = \frac{1}{2\pi\sigma^2} \sqrt{4\sigma^2 - (x - m)^2} 1_{[m-2\sigma, m+2\sigma]}(x) dx$.
- $d\mu_{MP}(\lambda)(x) = \begin{cases} f_\lambda(x) dx & \text{if } \lambda > 1 \\ (1 - \lambda) \delta_0 + \lambda f_\lambda(x) dx & \text{if } \lambda \leq 1 \end{cases}$, where $f_\lambda$ is defined by
  
  $$f_\lambda(x) = \frac{\sqrt{(\lambda_+ - x)(x - \lambda_-)}}{2\pi\lambda x} 1_{[\lambda_- , \lambda_+]}(x), \text{ with } \lambda_\pm = (\sqrt{\lambda} \pm 1)^2.$$
Asymptotic spectrum of GUE and Wishart matrices

Definitions (Gaussian Unitary Ensemble and Wishart matrices)
- $G$ is a $n \times n$ GUE matrix if $G = (H + H^*) / \sqrt{2}$ with $H$ a $n \times n$ matrix having independent complex normal entries.
- $W$ is a $(n, s)$-Wishart matrix if $W = HH^*$ with $H$ a $n \times s$ matrix having independent complex normal entries.

Definitions (Semicircular and Marčenko-Pastur distributions)
- $d\mu_{SC}(m, \sigma^2)(x) = \frac{1}{2\pi\sigma^2} \sqrt{4\sigma^2 - (x - m)^2} \mathbf{1}_{[m-2\sigma, m+2\sigma]}(x)dx$.
- $d\mu_{MP}(\lambda)(x) = \begin{cases} f_\lambda(x)dx & \text{if } \lambda > 1 \\ (1 - \lambda)\delta_0 + \lambda f_\lambda(x)dx & \text{if } \lambda \leq 1 \end{cases}$, where $f_\lambda$ is defined by
  
  $f_\lambda(x) = \frac{\sqrt{(\lambda_+-x)(x-\lambda_-)}}{2\pi\lambda x} \mathbf{1}_{[\lambda_-, \lambda_+]}(x)$, with $\lambda_\pm = (\sqrt{\lambda} \pm 1)^2$.

→ For any Hermitian $M$ on $\mathbb{C}^n$, denote by $N_M = \frac{1}{n} \sum_{i=1}^{n} \delta_{\lambda_i(M)}$ its spectral distribution.
- $(G_n)_{n \in \mathbb{N}}$ sequence of $n \times n$ GUE matrices : $(N_{G_n/\sqrt{n}})_{n \in \mathbb{N}}$ converges to $\mu_{SC}(0,1)$.
- $(W_n)_{n \in \mathbb{N}}$ sequence of $(n, \lambda n)$-Wishart matrices : $(N_{W_n/\lambda n})_{n \in \mathbb{N}}$ converges to $\mu_{MP}(\lambda)$.

(convergence in distribution, but also in probability, and even almost surely).
Example: Density functions of a centered semicircular distribution of variance parameter 1 (on the left) and of a Marčenko-Pastur distribution of parameter 4 (on the right).
Outline

1. Introduction

2. Interlude: reminder about GUE and Wishart matrices

3. Mean-width of the set of states which are separable vs satisfying a separability criterion

4. Entanglement vs Violating a separability criterion for random states

5. Summary and broader perspectives
Mean-width of a set of states

Definitions

Let $K$ be a convex set of states on $\mathbb{C}^n$ containing $\text{Id}/n$ (maximally mixed state).

- For $\Delta$ a $n \times n$ Hermitian s.t. $\|\Delta\|_{HS} = 1$, the width of $K$ in the direction $\Delta$ is $w(K, \Delta) = \sup_{\sigma \in K} \text{Tr}(\Delta(\sigma - \text{Id}/n))$.

- The mean-width of $K$ is the average of $w(K, \cdot)$ over the Hilbert-Schmidt unit sphere of $n \times n$ Hermitians, equipped with the uniform probability measure.

It is equivalently defined as $w(K) = E w(K, G)/\gamma_n$, where $G$ is a $n \times n$ GUE matrix and $\gamma_n = E \|G\|_{HS} \sim n \rightarrow +\infty$ $n$. 
Mean-width of a set of states

Definitions

Let $K$ be a convex set of states on $\mathbb{C}^n$ containing $Id/n$ (maximally mixed state).

• For $\Delta$ a $n \times n$ Hermitian s.t. $\|\Delta\|_{HS} = 1$, the width of $K$ in the direction $\Delta$ is $w(K, \Delta) = \sup_{\sigma \in K} \text{Tr}(\Delta(\sigma - Id/n))$.

• The mean-width of $K$ is the average of $w(K, \cdot)$ over the Hilbert-Schmidt unit sphere of $n \times n$ Hermitians, equipped with the uniform probability measure. It is equivalently defined as $w(K) = \mathbb{E} w(K, G)/\gamma_n$, where $G$ is a $n \times n$ GUE matrix and $\gamma_n = \mathbb{E} \|G\|_{HS} \sim n \to +\infty \ n$.

The mean-width of a set of states is a certain measure of its size (for any “reasonable” $K$, $w(K) \approx vrad(K)$, where $vrad(K)$ is the volume-radius of $K$, i.e. the radius of the Euclidean ball with same volume as $K$).

Computing it amounts to estimating the supremum of some Gaussian process.
**Observation**: \( \mathbf{E} \sup_{\sigma \text{ state}} \text{Tr}(G(\sigma - I d/n)) = \mathbf{E} \|G\|_{\infty}. \) So by Wigner’s semicircle law, the mean-width of the set of all states on \( \mathbb{C}^n \) is asymptotically \( 2\sqrt{n}/\gamma_n \), i.e. \( 2/\sqrt{n} \).
Mean-width of the set of separable states

**Observation**: \( E \sup_{\sigma \text{ state}} \text{Tr}(G(\sigma - Id/n)) = E \|G\|_\infty \). So by Wigner’s semicircle law, the mean-width of the set of all states on \( \mathbb{C}^n \) is asymptotically \( 2\sqrt{n}/\gamma_n \), i.e. \( 2/\sqrt{n} \).

**Theorem** (Aubrun/Szarek)

Denote by \( S \) the set of separable states on \( \mathbb{C}^d \otimes \mathbb{C}^d \).

There exist universal constants \( c, C > 0 \) such that \( \frac{c}{d^{3/2}} \leq w(S) \leq \frac{C}{d^{3/2}} \).

**Remark**: The mean-width of the set of separable states is of order \( 1/d^{3/2} \), hence much smaller than the mean-width of the set of all states (of order \( 1/d \)).

\( \rightarrow \) On high dimensional bipartite systems, most states are entangled.
**Observation**: \( E \sup_{\sigma \text{ state}} \text{Tr}(G(\sigma - \text{Id}/n)) = E \| G \|_{\infty} \). So by Wigner’s semicircle law, the mean-width of the set of all states on \( \mathbb{C}^n \) is asymptotically \( 2\sqrt{n}/\gamma_n \), i.e. \( 2/\sqrt{n} \).

**Theorem** (Aubrun/Szarek)

Denote by \( S \) the set of separable states on \( \mathbb{C}^d \otimes \mathbb{C}^d \).

There exist universal constants \( c, C > 0 \) such that \( \frac{c}{d^{3/2}} \leq w(S) \leq \frac{C}{d^{3/2}} \).

**Remark**: The mean-width of the set of separable states is of order \( 1/d^{3/2} \), hence much smaller than the mean-width of the set of all states (of order \( 1/d \)).

\( \rightarrow \) On high dimensional bipartite systems, most states are entangled.

**Proof idea**:

- **Upper-bound**: Approximate \( S \) by a polytope with “few” vertices, and use that
  \( E \sup_{i \in I} Z_i \leq C \sqrt{\log |I|} \) for \((Z_i)_{i \in I}\) a finite bounded Gaussian process (Pisier).
- **Lower-bound**: Estimate the volume-radius of \( S \) by convex geometry considerations, and use that \( \text{vrad} \leq w \) (Urysohn).
Mean-width of the set of $k$-extendible states

**Theorem**

Fix $k \geq 2$ and denote by $\mathcal{E}_k$ the set of $k$-extendible states on $\mathbb{C}^d \otimes \mathbb{C}^d$.

Then, $w(\mathcal{E}_k) \sim \frac{2}{d \to +\infty} \frac{2}{\sqrt{kd}}$.

**Remark**: The mean-width of the set of $k$-extendible states is of order $1/d$, hence much bigger than the mean-width of the set of separable states.

→ On high dimensional bipartite systems, the set of $k$-extendible states is a very rough approximation of the set of separable states.
Mean-width of the set of $k$-extendible states

**Theorem**

Fix $k \geq 2$ and denote by $\mathcal{E}_k$ the set of $k$-extendible states on $\mathbb{C}^d \otimes \mathbb{C}^d$.

Then, $w(\mathcal{E}_k) \sim_{d \to +\infty} \frac{2}{\sqrt{kd}}$.

**Remark**: The mean-width of the set of $k$-extendible states is of order $1/d$, hence much bigger than the mean-width of the set of separable states.

→ On high dimensional bipartite systems, the set of $k$-extendible states is a very rough approximation of the set of separable states.

**Proof strategy**: $\sup_{\sigma} k_{\text{ext}} \text{Tr}(G(\sigma - \text{Id}/d^2))$ may be expressed as $\|\tilde{G}\|_\infty$ for some suitable $\tilde{G}$. So one has to estimate $\mathbb{E}\|\tilde{G}\|_\infty$ for the “modified” GUE matrix $\tilde{G}$. This is done by computing the $p$-order moments $\mathbb{E}\text{Tr}G^p$, and identifying the limiting spectral distribution (after rescaling by $d/k$): a centered semicircular distribution $\mu_{\text{SC}}(0,k)$. The latter has $2\sqrt{k}$ as upper-edge.
Outline

1. Introduction
2. Interlude: reminder about GUE and Wishart matrices
3. Mean-width of the set of states which are separable vs satisfying a separability criterion
4. Entanglement vs Violating a separability criterion for random states
5. Summary and broader perspectives
Definition (Pure vs mixed)

A quantum state $\rho$ on $H$ is *pure* if there exists a unit vector $|\psi\rangle$ in $H$ such that $\rho = |\psi\rangle\langle\psi|$. Otherwise, it is *mixed*. 
Random induced states

**Definition (Pure vs mixed)**

A quantum state $\rho$ on $H$ is *pure* if there exists a unit vector $|\psi\rangle$ in $H$ such that $\rho = |\psi\rangle\langle\psi|$. Otherwise, it is *mixed*.

System space $H \equiv \mathbb{C}^n$. Ancilla space $H' \equiv \mathbb{C}^s$.

**Random mixed state model on $H$** : $\rho = \text{Tr}_{H'} |\psi\rangle\langle\psi|$ with $|\psi\rangle$ a uniformly distributed pure state on $H \otimes H'$ (*quantum marginal*).

Equivalent description : $\rho = \frac{W}{\text{Tr} W}$ with $W$ a $(n, s)$-Wishart matrix.
Random induced states

**Definition (Pure vs mixed)**
A quantum state $\rho$ on $H$ is *pure* if there exists a unit vector $|\psi\rangle$ in $H$ such that $\rho = |\psi\rangle \langle \psi|$. Otherwise, it is *mixed*.

System space $H \equiv \mathbb{C}^n$. Ancilla space $H' \equiv \mathbb{C}^s$.

**Random mixed state model on $H$** : $\rho = \text{Tr}_{H'} |\psi\rangle \langle \psi|$ with $|\psi\rangle$ a uniformly distributed pure state on $H \otimes H'$ (*quantum marginal*).

Equivalent description : $\rho = \frac{W}{\text{Tr} W}$ with $W$ a $(n, s)$-Wishart matrix.

**Question** : Fix $d \in \mathbb{N}$ and consider $\rho$ a random state on $\mathbb{C}^d \otimes \mathbb{C}^d$ induced by some environment $\mathbb{C}^s$. For which values of $s$ is $\rho$ typically separable? PPT? $k$-extendible? “typically” = “with probability going to 1 as $d$ grows”. Hence 2 steps :

- Identify the range of $s$ where $\rho$ is, on average, separable/PPT/$k$-extendible.
- Show that the average behaviour is generic in high dimension (concentration of measure phenomenon : a sufficiently “well-behaved” function has an exponentially small probability of deviating from its average as the dimension grows).
Separability of random induced states

Theorem (Aubrun/Szarek/Ye)

Let \( \rho \) be a random state on \( \mathbb{C}^d \otimes \mathbb{C}^d \) induced by \( \mathbb{C}^s \). There exists a threshold \( s_0 \) satisfying \( cd^3 \leq s_0 \leq Cd^3 \log^2 d \) for some universal constants \( c, C > 0 \) such that, if \( s < s_0 \) then \( \rho \) is typically entangled, and if \( s > s_0 \) then \( \rho \) is typically separable.

Intuition: If \( s \leq d^2 \) then \( \rho \) is uniformly distributed on the set of states of rank at most \( s \), therefore generically entangled. If \( s \gg d^2 \) then \( \rho \) is expected to be close to \( \text{Id} / d^2 \), therefore separable.

\( \rightarrow \) Phase transition between these two regimes?
Theorem (Aubrun/Szarek/Ye)

Let $\rho$ be a random state on $\mathbb{C}^d \otimes \mathbb{C}^d$ induced by $\mathbb{C}^s$. There exists a threshold $s_0$ satisfying $cd^3 \leq s_0 \leq C d^3 \log^2 d$ for some universal constants $c, C > 0$ such that, if $s < s_0$ then $\rho$ is typically entangled, and if $s > s_0$ then $\rho$ is typically separable.

**Intuition**: If $s \leq d^2$ then $\rho$ is uniformly distributed on the set of states of rank at most $s$, therefore generically entangled. If $s \gg d^2$ then $\rho$ is expected to be close to $Id/d^2$, therefore separable.

→ Phase transition between these two regimes?

**Proof idea**: Convex geometry + Comparison of random matrix ensembles (majorization) + Concentration of measure in high dimension.
### Theorem (Aubrun)

Let $\rho$ be a random state on $\mathbb{C}^d \otimes \mathbb{C}^d$ induced by $\mathbb{C}^s$. If $s < 4d^2$ then $\rho$ is typically not PPT, and if $s > 4d^2$ then $\rho$ is typically PPT.

**Remark:** The threshold environment dimension at which random induced states are generically either PPT or NPT is of order $d^2$, hence much smaller than the one at which they are generically either separable or entangled (of order $d^3$).

→ In the range $d^2 \lesssim s \lesssim d^3$, typical entanglement of random induced states is typically not detected by the PPT test.
PPT of random induced states

**Theorem (Aubrun)**

Let $\rho$ be a random state on $\mathbb{C}^d \otimes \mathbb{C}^d$ induced by $\mathbb{C}^s$. If $s < 4d^2$ then $\rho$ is typically not PPT, and if $s > 4d^2$ then $\rho$ is typically PPT.

**Remark**: The threshold environment dimension at which random induced states are generically either PPT or NPT is of order $d^2$, hence much smaller than the one at which they are generically either separable or entangled (of order $d^3$).

$\rightarrow$ In the range $d^2 \lesssim s \lesssim d^3$, typical entanglement of random induced states is typically not detected by the PPT test.

**Proof strategy**: Everything boils down to characterizing when a partially transposed $(d^2, s)$-Wishart matrix $W$ is positive. This is done by computing the $p$-order moments $\mathbf{E} \text{Tr} \Gamma(W)^p$, and identifying the limiting spectral distribution (after rescaling by $s$) : a non-centered semicircular distribution $\mu_{\text{SC}}(1, d^2/s)$. The latter has positive support iff $1 - 2\sqrt{d^2/s} \geq 0$ i.e. iff $s \geq 4d^2$. 
Outline

1. Introduction
2. Interlude: reminder about GUE and Wishart matrices
3. Mean-width of the set of states which are separable vs satisfying a separability criterion
4. Entanglement vs Violating a separability criterion for random states
5. Summary and broader perspectives
Summary and broader perspectives

On high dimensional bipartite systems, the volume of PPT or $k$-extendible states is more like the one of all states than like the one of separable states. → Asymptotic weakness of these NC for separability: most PPT or $k$-extendible states are entangled in high dimension.

$\rho$ a random state on $C^d \otimes C^d$ induced by $C^s$. When $d \to +\infty$, $\rho$ is w.h.p. entangled if $s < cd^3$, and this entanglement is w.h.p. detected by the PPT or the $k$-extendibility test if $s < Cd^2$. But in the range $d^2 \ll s \ll d^3$, PPT or $k$-extendible entanglement is generic.

Similar features are exhibited by all other known separability criteria, e.g. realignment (Aubrun/Nechita) or reduction (Jivulescu/Lupa/Nechita).

Possible generalization to the unbalanced case $A \equiv C^{d_A}$, $B \equiv C^{d_B}$, $d_A \neq d_B$: often straightforward if $d_A, d_B \to +\infty$, but more subtle if $d_A$ or $d_B$ is fixed (free probability approach usually more relevant and powerful in this latter setting).

Generalizations to the multi-partite case? The problem becomes much richer because checking separability across every bi-partite cut is not even enough to assert full separability...

→ “Small” number of “big” subsystems can generally be dealt with by the same techniques, but the picture changes completely in the opposite high-dimensional setting, i.e. a “big” number of “small” subsystems.
Summary and broader perspectives

- On high dimensional bipartite systems, the volume of PPT or $k$-extendible states is more like the one of all states than like the one of separable states.
  → Asymptotic weakness of these NC for separability: most PPT or $k$-extendible states are entangled in high dimension.
Summary and broader perspectives

- On high dimensional bipartite systems, the volume of PPT or $k$-extendible states is more like the one of all states than like the one of separable states.
  $\rightarrow$ Asymptotic weakness of these NC for separability: most PPT or $k$-extendible states are entangled in high dimension.

- $\rho$ a random state on $\mathbb{C}^d \otimes \mathbb{C}^d$ induced by $\mathbb{C}^s$.
  When $d \rightarrow +\infty$, $\rho$ is w.h.p. entangled if $s < cd^3$, and this entanglement is w.h.p. detected by the PPT or the $k$-extendibility test if $s < Cd^2$. But in the range $d^2 \ll s \ll d^3$, PPT or $k$-extendible entanglement is generic.
Summary and broader perspectives

• On high dimensional bipartite systems, the volume of PPT or $k$-extendible states is more like the one of all states than like the one of separable states.
  → Asymptotic weakness of these NC for separability: most PPT or $k$-extendible states are entangled in high dimension.

• $\rho$ a random state on $\mathbb{C}^d \otimes \mathbb{C}^d$ induced by $\mathbb{C}^s$.
  When $d \to +\infty$, $\rho$ is w.h.p. entangled if $s < cd^3$, and this entanglement is w.h.p. detected by the PPT or the $k$-extendibility test if $s < Cd^2$. But in the range $d^2 \ll s \ll d^3$, PPT or $k$-extendible entanglement is generic.

• Similar features are exhibited by all other known separability criteria, e.g. realignment (Aubrun/Nechita) or reduction (Jivulescu/Lupa/Nechita).
Summary and broader perspectives

- On high dimensional bipartite systems, the volume of PPT or $k$-extendible states is more like the one of all states than like the one of separable states.
  → Asymptotic weakness of these NC for separability: most PPT or $k$-extendible states are entangled in high dimension.

- If $\rho$ a random state on $\mathbb{C}^d \otimes \mathbb{C}^d$ induced by $\mathbb{C}^s$.
  When $d \to +\infty$, $\rho$ is w.h.p. entangled if $s < cd^3$, and this entanglement is w.h.p. detected by the PPT or the $k$-extendibility test if $s < Cd^2$. But in the range $d^2 \ll s \ll d^3$, PPT or $k$-extendible entanglement is generic.

- Similar features are exhibited by all other known separability criteria, e.g. realignment (Aubrun/Nechita) or reduction (Jivulescu/Lupa/Nechita).

- Possible generalization to the unbalanced case $A \equiv \mathbb{C}^{d_A}$, $B \equiv \mathbb{C}^{d_B}$, $d_A \neq d_B$ : often straightforward if $d_A, d_B \to +\infty$, but more subtle if $d_A$ or $d_B$ is fixed (free probability approach usually more relevant and powerful in this latter setting).
Summary and broader perspectives

- On high dimensional bipartite systems, the volume of PPT or $k$-extendible states is more like the one of all states than like the one of separable states.
  → Asymptotic weakness of these NC for separability: most PPT or $k$-extendible states are entangled in high dimension.

- $\rho$ a random state on $\mathbb{C}^d \otimes \mathbb{C}^d$ induced by $\mathbb{C}^s$.
  When $d \to +\infty$, $\rho$ is w.h.p. entangled if $s < cd^3$, and this entanglement is w.h.p. detected by the PPT or the $k$-extendibility test if $s < Cd^2$. But in the range $d^2 \ll s \ll d^3$, PPT or $k$-extendible entanglement is generic.

- Similar features are exhibited by all other known separability criteria, e.g. realignment (Aubrun/Nechita) or reduction (Jivulescu/Lupa/Nechita).

- Possible generalization to the unbalanced case $A \equiv \mathbb{C}^{d_A}$, $B \equiv \mathbb{C}^{d_B}$, $d_A \neq d_B$: often straightforward if $d_A, d_B \to +\infty$, but more subtle if $d_A$ or $d_B$ is fixed (free probability approach usually more relevant and powerful in this latter setting).

- Generalizations to the multi-partite case? The problem becomes much richer because checking separability across every bi-partite cut is not even enough to assert full separability...
  → “Small” number of “big” subsystems can generally be dealt with by the same techniques, but the picture changes completely in the opposite high-dimensional setting, i.e. a “big” number of “small” subsystems.
A few references

- C. Lancien, “k-extendibility of high-dimensional bipartite quantum states”, arXiv :1504.06459