Is a random state entangled ?

Guillaume AUBRUN

(joint work with Stanisław Szarek and Deping Ye)

Université Lyon 1, France

The probabilistic method in quantum information theory

The probabilistic method: use random techniques to show existence of objects for which explicit constructions are not known (Erdős–Rényi ; Shannon). Major revolution in combinatorics since 1950s !

A priori, Quantum Information Theory is a good candidate for applying the probabilistic method, because the objects have very very large dimensions. While the "curse of dimensionality" makes numerical method impractical, high dimensions usually boost random techniques ("blessom of dimensionality").

In QIT, the probabilistic method has been applied successfully by Hastings (counterexample to the additivity conjecture). An important pioneering work by Hayden–Leung–Winter: "Aspects of generic entanglement".

This motivates the study the properties of random states or random channels, which might become a basic tool in future years.

The probabilistic method in quantum information theory

The probabilistic method: use random techniques to show existence of objects for which explicit constructions are not known (Erdős–Rényi ; Shannon). Major revolution in combinatorics since 1950s !

A priori, Quantum Information Theory is a good candidate for applying the probabilistic method, because the objects have very very large dimensions. While the "curse of dimensionality" makes numerical method impractical, high dimensions usually boost random techniques ("blessom of dimensionality").

In QIT, the probabilistic method has been applied successfully by Hastings (counterexample to the additivity conjecture). An important pioneering work by Hayden–Leung–Winter: "Aspects of generic entanglement".

This motivates the study the properties of random states or random channels, which might become a basic tool in future years.

The probabilistic method in quantum information theory

The probabilistic method: use random techniques to show existence of objects for which explicit constructions are not known (Erdős–Rényi ; Shannon). Major revolution in combinatorics since 1950s !

A priori, Quantum Information Theory is a good candidate for applying the probabilistic method, because the objects have very very large dimensions. While the "curse of dimensionality" makes numerical method impractical, high dimensions usually boost random techniques ("blessom of dimensionality").

In QIT, the probabilistic method has been applied successfully by Hastings (counterexample to the additivity conjecture). An important pioneering work by Hayden–Leung–Winter: "Aspects of generic entanglement".

This motivates the study the properties of random states or random channels, which might become a basic tool in future years.

The probabilistic method in quantum information theory

The probabilistic method: use random techniques to show existence of objects for which explicit constructions are not known (Erdős–Rényi ; Shannon). Major revolution in combinatorics since 1950s !

A priori, Quantum Information Theory is a good candidate for applying the probabilistic method, because the objects have very very large dimensions. While the "curse of dimensionality" makes numerical method impractical, high dimensions usually boost random techniques ("blessom of dimensionality").

In QIT, the probabilistic method has been applied successfully by Hastings (counterexample to the additivity conjecture). An important pioneering work by Hayden–Leung–Winter: "Aspects of generic entanglement".

This motivates the study the properties of random states or random channels, which might become a basic tool in future years.

States in quantum information theory

Definition

A (mixed) **state** *on* $\mathbf{C}^n$ *is a positive, self-adjoint, trace* 1 *operator on* $\mathbf{C}^n$.

A **pure state** *is a state with rank* 1, *i.e. a one-dimensional projector. A pure state is denoted* $|\psi\rangle\langle\psi|$, *where* ψ *is a unit vector in the range.*

Pure states are the extreme points of the set $\mathcal{D} = \mathcal{D}(\mathbf{C}^n)$ of all states.

$\mathcal{D}(\mathbf{C}^n)$ is a convex body in the (affine) space of trace 1 self-adjoint operators on $\mathbf{C}^n$. The Euclidean structure is given by the Hilbert–Schmidt inner product $\langle A, B\rangle = \operatorname{Tr} AB$, and $\dim \mathcal{D}(\mathbf{C}^n) = n^2 - 1$.

The role of the origin is played by Id/n, the maximally mixed state. We write for example

$$\|\mathrm{Id}/n\|_{\mathcal{D}} = 0,$$

where $\|\cdot\|_{\mathcal{D}}$ stands for the gauge of convex body $\mathcal{D}$ (which is not centrally symmetric).

States in quantum information theory

Definition

A (mixed) **state** *on* $\mathbf{C}^n$ *is a positive, self-adjoint, trace* 1 *operator on* $\mathbf{C}^n$.

A **pure state** *is a state with rank* 1, *i.e. a one-dimensional projector. A pure state is denoted* $|\psi\rangle\langle\psi|$, *where* ψ *is a unit vector in the range.*

Pure states are the extreme points of the set $\mathcal{D} = \mathcal{D}(\mathbf{C}^n)$ of all states.

$\mathcal{D}(\mathbf{C}^n)$ is a convex body in the (affine) space of trace 1 self-adjoint operators on $\mathbf{C}^n$. The Euclidean structure is given by the Hilbert–Schmidt inner product $\langle A, B\rangle = \operatorname{Tr} AB$, and $\dim \mathcal{D}(\mathbf{C}^n) = n^2 - 1$.

The role of the origin is played by Id/n, the maximally mixed state. We write for example

$$\|\mathrm{Id}/n\|_{\mathcal{D}} = 0,$$

where $\|\cdot\|_{\mathcal{D}}$ stands for the gauge of convex body $\mathcal{D}$ (which is not centrally symmetric).

States in quantum information theory

Definition

A (mixed) **state** *on* $\mathbf{C}^n$ *is a positive, self-adjoint, trace* 1 *operator on* $\mathbf{C}^n$.

A **pure state** *is a state with rank* 1, *i.e. a one-dimensional projector. A pure state is denoted* $|\psi\rangle\langle\psi|$, *where* ψ *is a unit vector in the range.*

Pure states are the extreme points of the set $\mathcal{D} = \mathcal{D}(\mathbf{C}^n)$ of all states.

$\mathcal{D}(\mathbf{C}^n)$ is a convex body in the (affine) space of trace 1 self-adjoint operators on $\mathbf{C}^n$. The Euclidean structure is given by the Hilbert–Schmidt inner product $\langle A, B\rangle = \operatorname{Tr} AB$, and $\dim \mathcal{D}(\mathbf{C}^n) = n^2 - 1$.

The role of the origin is played by Id/n, the maximally mixed state. We write for example

$$\|\mathrm{Id}/n\|_{\mathcal{D}} = 0,$$

where $\|\cdot\|_{\mathcal{D}}$ stands for the gauge of convex body $\mathcal{D}$ (which is not centrally symmetric).

Random induced states

Mixed states on $\mathcal{D}(\mathbf{C}^n)$ can be obtained as partial traces of pure states on a larger system.

Definition (random "induced" states)

Let n, s be integers, $|\psi\rangle\langle\psi|$ be a random Haar-distributed pure state on $\mathbf{C}^n \otimes \mathbf{C}^s$, and $\rho = \mathrm{Tr}_{\mathbf{C}^s} |\psi\rangle\langle\psi|$ (partial trace over the environment). Then ρ is a random state on $\mathbf{C}^n$. We denote by $\mu_{n,s}$ be its distribution.

Miracle: $\mu_{n,n}$ is the normalized Lebesgue measure on $\mathcal{D}(\mathbf{C}^n)$ (Życzkowski–Sommers).

More generally, for $s \geqslant n$, the measure $\mu_{n,s}$ has a log-concave density, proportionnal to $(\det \rho)^{s-n}$.

Random induced states

Mixed states on $\mathcal{D}(\mathbf{C}^n)$ can be obtained as partial traces of pure states on a larger system.

Definition (random "induced" states)

Let n, s be integers, $|\psi\rangle\langle\psi|$ be a random Haar-distributed pure state on $\mathbf{C}^n \otimes \mathbf{C}^s$, and $\rho = \mathrm{Tr}_{\mathbf{C}^s} |\psi\rangle\langle\psi|$ (partial trace over the environment). Then ρ is a random state on $\mathbf{C}^n$. We denote by $\mu_{n,s}$ be its distribution.

Miracle: $\mu_{n,n}$ is the normalized Lebesgue measure on $\mathcal{D}(\mathbf{C}^n)$ (Życzkowski–Sommers).

More generally, for $s \geqslant n$, the measure $\mu_{n,s}$ has a log-concave density, proportionnal to $(\det \rho)^{s-n}$.

Random induced states

Mixed states on $\mathcal{D}(\mathbf{C}^n)$ can be obtained as partial traces of pure states on a larger system.

Definition (random "induced" states)

Let n, s be integers, $|\psi\rangle\langle\psi|$ be a random Haar-distributed pure state on $\mathbf{C}^n \otimes \mathbf{C}^s$, and $\rho = \mathrm{Tr}_{\mathbf{C}^s} |\psi\rangle\langle\psi|$ (partial trace over the environment). Then ρ is a random state on $\mathbf{C}^n$. We denote by $\mu_{n,s}$ be its distribution.

Miracle: $\mu_{n,n}$ is the normalized Lebesgue measure on $\mathcal{D}(\mathbf{C}^n)$ (Życzkowski–Sommers).

More generally, for $s \geqslant n$, the measure $\mu_{n,s}$ has a log-concave density, proportionnal to $(\det \rho)^{s-n}$.

Wishart random matrices

Uniform measure on the sphere = normalized Gaussian vector

Fact (Induced states = normalized Wishart matrices)

If W is a $n \times s$ random matrix with independent $N_{\mathbf{C}}(0,1)$ entries, then

$$\frac{WW^*}{\mathrm{Tr}(WW^*)}$$

has distribution $\mu_{n,s}$.

What happens when n if fixed and $s \to \infty$?

Law of large numbers : the measure $\mu_{n,s}$ converge to the state Id/n.

Central limit approximation : the measure $\mu_{n,s}$ can be approximated by

$$\frac{Id}{n} + \frac{1}{n\sqrt{s}} G$$

where G is a GUE_0 matrix (GUE conditionned to have trace 0).

Wishart random matrices

Uniform measure on the sphere = normalized Gaussian vector

Fact (Induced states = normalized Wishart matrices)

If W is a $n \times s$ random matrix with independent $N_{\mathbf{C}}(0,1)$ entries, then

$$\frac{WW^*}{\mathrm{Tr}(WW^*)}$$

has distribution $\mu_{n,s}$.

What happens when n if fixed and $s \to \infty$?

Law of large numbers : the measure $\mu_{n,s}$ converge to the state Id/n.

Central limit approximation : the measure $\mu_{n,s}$ can be approximated by

$$\frac{Id}{n} + \frac{1}{n\sqrt{s}} G$$

where G is a GUE_0 matrix (GUE conditionned to have trace 0).

Wishart random matrices

Uniform measure on the sphere = normalized Gaussian vector

Fact (Induced states = normalized Wishart matrices)

If W is a $n \times s$ random matrix with independent $N_{\mathbf{C}}(0,1)$ entries, then

$$\frac{WW^*}{\mathrm{Tr}(WW^*)}$$

has distribution $\mu_{n,s}$.

What happens when n if fixed and $s \to \infty$?

Law of large numbers : the measure $\mu_{n,s}$ converge to the state Id/n.

Central limit approximation : the measure $\mu_{n,s}$ can be approximated by

$$\frac{Id}{n} + \frac{1}{n\sqrt{s}} G$$

where G is a GUE_0 matrix (GUE conditionned to have trace 0).

Wishart random matrices

Uniform measure on the sphere = normalized Gaussian vector

Fact (Induced states = normalized Wishart matrices)

If W is a $n \times s$ random matrix with independent $N_{\mathbf{C}}(0,1)$ entries, then

$$\frac{WW^*}{\mathrm{Tr}(WW^*)}$$

has distribution $\mu_{n,s}$.

What happens when n if fixed and $s \to \infty$?
Law of large numbers : the measure $\mu_{n,s}$ converge to the state Id/n.
Central limit approximation : the measure $\mu_{n,s}$ can be approximated by

$$\frac{Id}{n} + \frac{1}{n\sqrt{s}} G$$

where G is a GUE_0 matrix (GUE conditionned to have trace 0).

Central limit approximation made rigorous

Proposition

Let $K \subset \mathcal{D}(\mathbf{C}^n)$ be a convex body. Let ρ be a state with distribution $\mu_{n,s}$ and G a $n \times n$ GUE_0 matrix. Then, when n and s/n tend to infinity,

$$\mathbf{E}\,\|\rho\|_K \sim \frac{1}{n\sqrt{s}}\mathbf{E}\,\|\mathrm{Id}/n + G\|_K\,.$$

Two ingredients in the proof:

1. Both sides converge to the semicircle distribution (Marčenko–Pastur distributions degenerate to semicircles when s/n become large), and extreme eigenvalues are under control (Bai–Yin).
2. Majorization theory: $A \prec B$ if $A \in \mathrm{conv}\{UBU^* \ : \ U \text{ unitary}\}$.

$$A \prec B \iff \forall t \in \mathbf{R}, \quad \mathrm{Tr}\,|A - t\mathrm{Id}| \leqslant \mathrm{Tr}\,|B - t\mathrm{Id}|.$$

Can be checked from an approximate knowledge of spectra.

Central limit approximation made rigorous

Proposition

Let $K \subset \mathcal{D}(\mathbf{C}^n)$ be a convex body. Let ρ be a state with distribution $\mu_{n,s}$ and G a $n \times n$ GUE_0 matrix. Then, when n and s/n tend to infinity,

$$\mathbf{E}\,\|\rho\|_K \sim \frac{1}{n\sqrt{s}}\mathbf{E}\,\|\mathrm{Id}/n + G\|_K\,.$$

Two ingredients in the proof:

1. Both sides converge to the semicircle distribution (Marčenko–Pastur distributions degenerate to semicircles when s/n become large), and extreme eigenvalues are under control (Bai–Yin).
2. Majorization theory: $A \prec B$ if $A \in \mathrm{conv}\{UBU^* \ : \ U \text{ unitary}\}$.

$$A \prec B \iff \forall t \in \mathbf{R}, \quad \mathrm{Tr}\,|A - t\mathrm{Id}| \leqslant \mathrm{Tr}\,|B - t\mathrm{Id}|.$$

Can be checked from an approximate knowledge of spectra.

Central limit approximation made rigorous

Proposition

Let $K \subset \mathcal{D}(\mathbf{C}^n)$ be a convex body. Let ρ be a state with distribution $\mu_{n,s}$ and G a $n \times n$ GUE_0 matrix. Then, when n and s/n tend to infinity,

$$\mathbf{E}\,\|\rho\|_K \sim \frac{1}{n\sqrt{s}}\mathbf{E}\,\|\mathrm{Id}/n + G\|_K\,.$$

Two ingredients in the proof:

1. Both sides converge to the semicircle distribution (Marčenko–Pastur distributions degenerate to semicircles when s/n become large), and extreme eigenvalues are under control (Bai–Yin).
2. Majorization theory: $A \prec B$ if $A \in \mathrm{conv}\{UBU^* \ : \ U \text{ unitary}\}$.

$$A \prec B \iff \forall t \in \mathbf{R}, \quad \mathrm{Tr}\,|A - t\mathrm{Id}| \leqslant \mathrm{Tr}\,|B - t\mathrm{Id}|.$$

Can be checked from an approximate knowledge of spectra.

Central limit approximation made rigorous

Proposition

Let $K \subset \mathcal{D}(\mathbf{C}^n)$ be a convex body. Let ρ be a state with distribution $\mu_{n,s}$ and G a $n \times n$ GUE_0 matrix. Then, when n and s/n tend to infinity,

$$\mathbf{E}\,\|\rho\|_K \sim \frac{1}{n\sqrt{s}}\mathbf{E}\,\|\mathrm{Id}/n + G\|_K\,.$$

Two ingredients in the proof:

1. Both sides converge to the semicircle distribution (Marčenko–Pastur distributions degenerate to semicircles when s/n become large), and extreme eigenvalues are under control (Bai–Yin).
2. Majorization theory: $A \prec B$ if $A \in \mathrm{conv}\{UBU^* \ : \ U \text{ unitary}\}$.

$$A \prec B \iff \forall t \in \mathbf{R},\quad \mathrm{Tr}\,|A - t\mathrm{Id}| \leqslant \mathrm{Tr}\,|B - t\mathrm{Id}|.$$

Can be checked from an approximate knowledge of spectra.

Separable states

We now replace $\mathbf{C}^n$ by $\mathbf{C}^d \otimes \mathbf{C}^d$ ($n = d^2$) and introduce the entanglement vs separability dichotomy.

Definition (entanglement vs. separability)

A **product state** *on* $\mathbf{C}^d \otimes \mathbf{C}^d$ *is a state of the form* $\rho_1 \otimes \rho_2$, *where* ρ_1, ρ_2 *are states on* $\mathbf{C}^d$.
A state on $\mathbf{C}^d \otimes \mathbf{C}^d$ *is* **separable** *if it can be written as a convex combination of product states — otherwise it is* **entangled**.

Let $\mathcal{S}$ be the set of separable states on $\mathbf{C}^d \otimes \mathbf{C}^d$.

$$\mathcal{S} = \mathrm{conv}\{|\psi_1 \otimes \psi_2\rangle\langle\psi_1 \otimes \psi_2| \ : \ \psi_1, \psi_2 \in \mathbf{C}^d, |\psi_1| = |\psi_2| = 1\}.$$

Fact

The dimension of $\mathcal{S}$ *is* $d^4 - 1$, *and equals the dimension of* $\mathcal{D}$.

Even more: $\mathcal{D}$ and $\mathcal{S}$ have the same inradius (Barnum–Gurvits).

Separable states

We now replace $\mathbf{C}^n$ by $\mathbf{C}^d \otimes \mathbf{C}^d$ ($n = d^2$) and introduce the entanglement vs separability dichotomy.

Definition (entanglement vs. separability)

A **product state** *on* $\mathbf{C}^d \otimes \mathbf{C}^d$ *is a state of the form* $\rho_1 \otimes \rho_2$, *where* ρ_1, ρ_2 *are states on* $\mathbf{C}^d$.
A state on $\mathbf{C}^d \otimes \mathbf{C}^d$ *is* **separable** *if it can be written as a convex combination of product states — otherwise it is* **entangled**.

Let $\mathcal{S}$ be the set of separable states on $\mathbf{C}^d \otimes \mathbf{C}^d$.

$$\mathcal{S} = \mathrm{conv}\{|\psi_1 \otimes \psi_2\rangle\langle\psi_1 \otimes \psi_2| \ : \ \psi_1, \psi_2 \in \mathbf{C}^d, |\psi_1| = |\psi_2| = 1\}.$$

Fact

The dimension of $\mathcal{S}$ *is* $d^4 - 1$, *and equals the dimension of* $\mathcal{D}$.

Even more: $\mathcal{D}$ and $\mathcal{S}$ have the same inradius (Barnum–Gurvits).

Separable states

We now replace $\mathbf{C}^n$ by $\mathbf{C}^d \otimes \mathbf{C}^d$ ($n = d^2$) and introduce the entanglement vs separability dichotomy.

Definition (entanglement vs. separability)

A **product state** *on* $\mathbf{C}^d \otimes \mathbf{C}^d$ *is a state of the form* $\rho_1 \otimes \rho_2$, *where* ρ_1, ρ_2 *are states on* $\mathbf{C}^d$.
A state on $\mathbf{C}^d \otimes \mathbf{C}^d$ *is* **separable** *if it can be written as a convex combination of product states — otherwise it is* **entangled**.

Let $\mathcal{S}$ be the set of separable states on $\mathbf{C}^d \otimes \mathbf{C}^d$.

$$\mathcal{S} = \mathrm{conv}\{|\psi_1 \otimes \psi_2\rangle\langle\psi_1 \otimes \psi_2| \ : \ \psi_1, \psi_2 \in \mathbf{C}^d, |\psi_1| = |\psi_2| = 1\}.$$

Fact

The dimension of $\mathcal{S}$ *is* $d^4 - 1$, *and equals the dimension of* $\mathcal{D}$.

Even more: $\mathcal{D}$ and $\mathcal{S}$ have the same inradius (Barnum–Gurvits).

The problem: (when) is a random state entangled ?

The dichotomy entangled vs separable is fundamental in QIT (useful vs useless). This motivates the following question.

Question

Let ρ be a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$ with distribution $\mu_{d^2,s}$. For which values of d, s is ρ typically separable ?

1. If $s = 1$, ρ is entangled with probability 1.
2. If $s \ggg d$, ρ is separable with large probability (law of large numbers).

So we expect a threshold between typical entanglement and typical separability.

The problem: (when) is a random state entangled ?

The dichotomy entangled vs separable is fundamental in QIT (useful vs useless). This motivates the following question.

Question

Let ρ be a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$ with distribution $\mu_{d^2,s}$. For which values of d, s is ρ typically separable ?

1. If $s = 1$, ρ is entangled with probability 1.
2. If $s \ggg d$, ρ is separable with large probability (law of large numbers).

So we expect a threshold between typical entanglement and typical separability.

The problem: (when) is a random state entangled ?

The dichotomy entangled vs separable is fundamental in QIT (useful vs useless). This motivates the following question.

Question

Let ρ be a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$ with distribution $\mu_{d^2,s}$. For which values of d, s is ρ typically separable ?

1. If $s = 1$, ρ is entangled with probability 1.
2. If $s \ggg d$, ρ is separable with large probability (law of large numbers).

So we expect a threshold between typical entanglement and typical separability.

The problem: (when) is a random state entangled ?

The dichotomy entangled vs separable is fundamental in QIT (useful vs useless). This motivates the following question.

Question

Let ρ be a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$ with distribution $\mu_{d^2,s}$. For which values of d, s is ρ typically separable ?

1. If $s = 1$, ρ is entangled with probability 1.
2. If $s \ggg d$, ρ is separable with large probability (law of large numbers).

So we expect a threshold between typical entanglement and typical separability.

Our main theorem

We prove that the threshold is **sharp** and holds somewhere between d^3 and $d^3 \log^2 d$.

Theorem (A+Szarek+Ye)

There is a function $s_0(d)$, satisfying $d^3 \lesssim s_0(d) \lesssim d^3 \log^2 d$, such that if ρ is a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$ with distribution $\mu_{d^2,s}$, and $\varepsilon > 0$,

1. *If $s \leqslant (1-\varepsilon)s_0(d)$, then ρ is entangled w.h.p.*
2. *If $s \geqslant (1+\varepsilon)s_0(d)$, then ρ is separable w.h.p.*

w.h.p. = with high probability, i.e. $\mathbf{P}(\cdot) \geqslant 1 - C(\varepsilon)\exp(-c(\varepsilon)s)$.

Known before: ρ entangled for $s \leqslant d^2$ and ρ separable for $s \geqslant Cd^4$ (Hayden–Leung–Winter).

Our main theorem

We prove that the threshold is **sharp** and holds somewhere between d^3 and $d^3 \log^2 d$.

Theorem (A+Szarek+Ye)

There is a function $s_0(d)$, satisfying $d^3 \lesssim s_0(d) \lesssim d^3 \log^2 d$, such that if ρ is a random state on $\mathbf{C}^d \otimes \mathbf{C}^d$ with distribution $\mu_{d^2,s}$, and $\varepsilon > 0$,

1. *If $s \leqslant (1-\varepsilon)s_0(d)$, then ρ is entangled w.h.p.*
2. *If $s \geqslant (1+\varepsilon)s_0(d)$, then ρ is separable w.h.p.*

w.h.p. = with high probability, i.e. $\mathbf{P}(\cdot) \geqslant 1 - C(\varepsilon)\exp(-c(\varepsilon)s)$.

Known before: ρ entangled for $s \leqslant d^2$ and ρ separable for $s \geqslant Cd^4$ (Hayden–Leung–Winter).

Convex geometry

Let $\|\cdot\|_{\mathcal{S}}$ be the gauge of the convex body $\mathcal{S}$. Then

$$\rho \text{ is separable} \iff \|\rho\|_{\mathcal{S}} \leqslant 1$$

$$\rho \text{ is entangled} \iff \|\rho\|_{\mathcal{S}} > 1$$

If ρ is a random state with distribution $\mu_{d^2,s}$, we have to decide whether the random variable $\|\rho\|_{\mathcal{S}}$ is typically larger or smaller than 1.

Convex geometry

Let $\|\cdot\|_{\mathcal{S}}$ be the gauge of the convex body $\mathcal{S}$. Then

$$\rho \text{ is separable} \iff \|\rho\|_{\mathcal{S}} \leqslant 1$$

$$\rho \text{ is entangled} \iff \|\rho\|_{\mathcal{S}} > 1$$

If ρ is a random state with distribution $\mu_{d^2,s}$, we have to decide whether the random variable $\|\rho\|_{\mathcal{S}}$ is typically larger or smaller than 1.

The strategy of proof

We proceed via two independent steps.

1. Decide for which values of d, s, one has

$$\mathbf{E}\|\rho\|_{\mathcal{S}} < 1 - \varepsilon \text{ or } \mathbf{E}\|\rho\|_{\mathcal{S}} > 1 + \varepsilon.$$

2. Show that the function $\rho \mapsto \|\rho\|_{\mathcal{S}}$ concentrate arounds its mean.

Step 2 is relatively routine, except for the following simple idea.

Idea

If $f : S^{N-1} \to \mathbf{R}$ is a 1-Lipschitz function, and $\Omega \subset S^{N-1}$ a subset of large measure such that $f_{|\Omega}$ is ε-Lipschitz, one may consider

$$\tilde{f} = \text{ any } \varepsilon\text{-Lipschitz extension of } f_{|\Omega} \text{ to } S^{N-1}.$$

and apply standard concentration inequalities to $\tilde{f}$.

The strategy of proof

We proceed via two independent steps.

1. Decide for which values of d, s, one has

$$\mathbf{E}\|\rho\|_{\mathcal{S}} < 1 - \varepsilon \text{ or } \mathbf{E}\|\rho\|_{\mathcal{S}} > 1 + \varepsilon.$$

2. Show that the function $\rho \mapsto \|\rho\|_{\mathcal{S}}$ concentrate arounds its mean.

Step 2 is relatively routine, except for the following simple idea.

Idea

If $f : S^{N-1} \to \mathbf{R}$ is a 1-Lipschitz function, and $\Omega \subset S^{N-1}$ a subset of large measure such that $f_{|\Omega}$ is ε-Lipschitz, one may consider

$$\tilde{f} = \text{ any } \varepsilon\text{-Lipschitz extension of } f_{|\Omega} \text{ to } S^{N-1}.$$

and apply standard concentration inequalities to $\tilde{f}$.

Mean width

Definition

If $K \subset \mathbf{R}^N$ is a convex body containing the origin, its *mean width* is

$$w(K) = \int_{S^{N-1}} \max_{x \in K} \langle x, \theta \rangle d\theta = \int_{S^{N-1}} \|\theta\|_{K^\circ} d\theta.$$

We have to compute $\mathbf{E}\|\rho\|_{\mathcal{S}}$. By our proposition about Gaussian approximation, if $s \gg d^2$, and G a $d^2 \times d^2$ GUE_0 random matrix.

$$\mathbf{E}\|\rho\|_{\mathcal{S}} \sim \frac{1}{d^2\sqrt{s}} \mathbf{E}\|\mathrm{Id}/d^2 + G\|_{\mathcal{S}}.$$

The right-hand side is the Gaussian mean width of the dual (polar) convex body $\mathcal{S}^\circ$, which equals $\sqrt{\dim} \approx d^2$ times the usual mean width. Therefore

$$\mathbf{E}\|\rho\|_{\mathcal{S}} \sim \frac{1}{\sqrt{s}} w(\mathcal{S}^\circ).$$

This shows that a sharp threshold occurs at the value $s_0 = w(\mathcal{S}^\circ)^2$.

Mean width

Definition

If $K \subset \mathbf{R}^N$ is a convex body containing the origin, its *mean width* is

$$w(K) = \int_{S^{N-1}} \max_{x \in K} \langle x, \theta \rangle d\theta = \int_{S^{N-1}} \|\theta\|_{K^\circ} d\theta.$$

We have to compute $\mathbf{E}\|\rho\|_{\mathcal{S}}$. By our proposition about Gaussian approximation, if $s \gg d^2$, and G a $d^2 \times d^2$ GUE_0 random matrix.

$$\mathbf{E}\|\rho\|_{\mathcal{S}} \sim \frac{1}{d^2\sqrt{s}} \mathbf{E}\|\mathrm{Id}/d^2 + G\|_{\mathcal{S}}.$$

The right-hand side is the Gaussian mean width of the dual (polar) convex body $\mathcal{S}^\circ$, which equals $\sqrt{\dim} \approx d^2$ times the usual mean width. Therefore

$$\mathbf{E}\|\rho\|_{\mathcal{S}} \sim \frac{1}{\sqrt{s}} w(\mathcal{S}^\circ).$$

This shows that a sharp threshold occurs at the value $s_0 = w(\mathcal{S}^\circ)^2$.

Mean width

Definition

If $K \subset \mathbf{R}^N$ is a convex body containing the origin, its *mean width* is

$$w(K) = \int_{S^{N-1}} \max_{x \in K} \langle x, \theta \rangle d\theta = \int_{S^{N-1}} \|\theta\|_{K^\circ} d\theta.$$

We have to compute $\mathbf{E}\|\rho\|_{\mathcal{S}}$. By our proposition about Gaussian approximation, if $s \gg d^2$, and G a $d^2 \times d^2$ GUE_0 random matrix.

$$\mathbf{E}\|\rho\|_{\mathcal{S}} \sim \frac{1}{d^2\sqrt{s}} \mathbf{E}\|\mathrm{Id}/d^2 + G\|_{\mathcal{S}}.$$

The right-hand side is the Gaussian mean width of the dual (polar) convex body $\mathcal{S}^\circ$, which equals $\sqrt{\dim} \approx d^2$ times the usual mean width. Therefore

$$\mathbf{E}\|\rho\|_{\mathcal{S}} \sim \frac{1}{\sqrt{s}} w(\mathcal{S}^\circ).$$

This shows that a sharp threshold occurs at the value $s_0 = w(\mathcal{S}^\circ)^2$.

Computing the mean width of $\mathcal{S}^\circ$

To complete the proof it remains to compute the mean width of $\mathcal{S}^\circ$.

Proposition

For absolute constants c, C, we have

$$cd^{3/2} \leqslant w(\mathcal{S}^\circ) \leqslant Cd^{3/2} \log d$$

Challenge: remove the $\log(d)$ factor.

It turns out that $w(\mathcal{S})$ is simple to estimate, instead of $w(\mathcal{S}^\circ)$.

Lemma

For absolute constants c, C, we have

$$cd^{-3/2} \leqslant w(\mathcal{S}) \leqslant Cd^{-3/2}.$$

Computing the mean width of $\mathcal{S}^\circ$

To complete the proof it remains to compute the mean width of $\mathcal{S}^\circ$.

Proposition

For absolute constants c, C, we have

$$cd^{3/2} \leqslant w(\mathcal{S}^\circ) \leqslant Cd^{3/2} \log d$$

Challenge: remove the $\log(d)$ factor.

It turns out that $w(\mathcal{S})$ is simple to estimate, instead of $w(\mathcal{S}^\circ)$.

Lemma

For absolute constants c, C, we have

$$cd^{-3/2} \leqslant w(\mathcal{S}) \leqslant Cd^{-3/2}.$$

Estimating $w(\mathcal{S})$

Fact (union bound)

If $P \subset B_2^N$ is a polytope with v vertices, then

$$w(P) \leqslant C\sqrt{\frac{\log v}{N}}.$$

Here $N = d^4 - 1$, and the convex body $\mathcal{S}$ can be approximated by a polytope with 100^d vertices. Hence

$$w(\mathcal{S}) \leqslant Cd^{-3/2}.$$

For the lower bound, we use the Urysohn inequality $w(\mathcal{S}) \geqslant \mathrm{vrad}(\mathcal{S})$. The volume of $\mathcal{S}$ is large because the symmetrized body (with one extra dimension) $\Sigma = \mathrm{conv}(-\mathcal{S} \bigcup \mathcal{S})$ has a large inradius. By the Rogers–Shephard inequality, the volumes of $\mathcal{S}$ and Σ are comparable.

Estimating $w(\mathcal{S})$

Fact (union bound)

If $P \subset B_2^N$ is a polytope with v vertices, then

$$w(P) \leqslant C\sqrt{\frac{\log v}{N}}.$$

Here $N = d^4 - 1$, and the convex body $\mathcal{S}$ can be approximated by a polytope with 100^d vertices. Hence

$$w(\mathcal{S}) \leqslant Cd^{-3/2}.$$

For the lower bound, we use the Urysohn inequality $w(\mathcal{S}) \geqslant \mathrm{vrad}(\mathcal{S})$. The volume of $\mathcal{S}$ is large because the symmetrized body (with one extra dimension) $\Sigma = \mathrm{conv}(-\mathcal{S} \bigcup \mathcal{S})$ has a large inradius. By the Rogers–Shephard inequality, the volumes of $\mathcal{S}$ and Σ are comparable.

Duality argument: the MM^*-estimate

One trivially has $w(K)w(K^\circ) \geqslant 1$. Conversely, one has

Theorem (The MM^*-estimate; Pisier, Figiel–Tomczak-Jaegermann)

If $K \subset \mathbf{R}^N$ is a **symmetric** *convex body in the ℓ-position, then*

$$1 \leqslant w(K)w(K^\circ) \leqslant C \log N.$$

Every symmetric convex body has an linear image which is in the ℓ-position. A guarantee for K being in the ℓ-position is that the group of isometries of K acts irreducibly.

Applying the MM^*-estimate

We cannot apply the MM^*-estimate to $\mathcal{S}$ directly because

1. $\mathcal{S}$ is not symmetric,
2. Its group of isometries does not act irreducibly.

We introduce another symmetrization, $\mathcal{S}_{\text{sym}} = \mathcal{S} \cap -\mathcal{S}$. It is checked that $\mathcal{S}$ and $\mathcal{S}_{\text{sym}}$ have comparable volumes, mean widths and dual mean widths.

For the second point, the isometry group contains "local unitaries"

$$\rho \mapsto (U \otimes V)\rho(U^* \otimes V^*)$$

and has an irreducible subspace of small codimension: the space

$$\text{span}\{\sigma_1 \otimes \sigma_2 \ : \ \text{Tr}\,\sigma_1 = \text{Tr}\,\sigma_2 = 0\}.$$

We can apply the MM^*-estimate into this subspace, and this is enough.

Applying the MM^*-estimate

We cannot apply the MM^*-estimate to $\mathcal{S}$ directly because

1. $\mathcal{S}$ is not symmetric,
2. Its group of isometries does not act irreducibly.

We introduce another symmetrization, $\mathcal{S}_{\text{sym}} = \mathcal{S} \cap -\mathcal{S}$. It is checked that $\mathcal{S}$ and $\mathcal{S}_{\text{sym}}$ have comparable volumes, mean widths and dual mean widths.

For the second point, the isometry group contains "local unitaries"

$$\rho \mapsto (U \otimes V)\rho(U^* \otimes V^*)$$

and has an irreducible subspace of small codimension: the space

$$\text{span}\{\sigma_1 \otimes \sigma_2 \ : \ \text{Tr}\,\sigma_1 = \text{Tr}\,\sigma_2 = 0\}.$$

We can apply the MM^*-estimate into this subspace, and this is enough.

Applying the MM^*-estimate

We cannot apply the MM^*-estimate to $\mathcal{S}$ directly because

1. $\mathcal{S}$ is not symmetric,
2. Its group of isometries does not act irreducibly.

We introduce another symmetrization, $\mathcal{S}_{\text{sym}} = \mathcal{S} \cap -\mathcal{S}$. It is checked that $\mathcal{S}$ and $\mathcal{S}_{\text{sym}}$ have comparable volumes, mean widths and dual mean widths.

For the second point, the isometry group contains "local unitaries"

$$\rho \mapsto (U \otimes V)\rho(U^* \otimes V^*)$$

and has an irreducible subspace of small codimension: the space

$$\text{span}\{\sigma_1 \otimes \sigma_2 \ : \ \text{Tr}\,\sigma_1 = \text{Tr}\,\sigma_2 = 0\}.$$

We can apply the MM^*-estimate into this subspace, and this is enough.

The case of N qubits

A harder problem: $(\mathbf{C}^2)^{\otimes N}$ instead of $(\mathbf{C}^d)^{\otimes 2}$.

Definition

A state ρ on $(\mathbf{C}^2)^{\otimes N}$ is a **product state** *if it is of the form $\rho_1 \otimes \cdots \otimes \rho_N$, where (ρ_i) are states on $\mathbf{C}^2$. A state is* **separable** *if it is a convex combination of product states, otherwise it is* **entangled**.

Question

Consider a random state on $(\mathbf{C}^2)^{\otimes N}$ with distribution $\mu_{2^N,s}$. It is typically separable or entangled ? What is the threshold ?

The volume and mean width of $\mathcal{S}$ can be estimated (not so directly, one has to put our convex body in the Löwner position). However, the same approach fails at the very last step, because the set of separable states on N qubits has "few" symmetries, and one cannot apply efficiently the MM^*-estimate.

The case of N qubits

A harder problem: $(\mathbf{C}^2)^{\otimes N}$ instead of $(\mathbf{C}^d)^{\otimes 2}$.

Definition

A state ρ on $(\mathbf{C}^2)^{\otimes N}$ is a **product state** *if it is of the form $\rho_1 \otimes \cdots \otimes \rho_N$, where (ρ_i) are states on $\mathbf{C}^2$. A state is* **separable** *if it is a convex combination of product states, otherwise it is* **entangled**.

Question

Consider a random state on $(\mathbf{C}^2)^{\otimes N}$ with distribution $\mu_{2^N,s}$. It is typically separable or entangled ? What is the threshold ?

The volume and mean width of $\mathcal{S}$ can be estimated (not so directly, one has to put our convex body in the Löwner position). However, the same approach fails at the very last step, because the set of separable states on N qubits has "few" symmetries, and one cannot apply efficiently the MM^*-estimate.

The case of N qubits

A harder problem: $(\mathbf{C}^2)^{\otimes N}$ instead of $(\mathbf{C}^d)^{\otimes 2}$.

Definition

A state ρ on $(\mathbf{C}^2)^{\otimes N}$ is a **product state** *if it is of the form $\rho_1 \otimes \cdots \otimes \rho_N$, where (ρ_i) are states on $\mathbf{C}^2$. A state is* **separable** *if it is a convex combination of product states, otherwise it is* **entangled**.

Question

Consider a random state on $(\mathbf{C}^2)^{\otimes N}$ with distribution $\mu_{2^N,s}$. It is typically separable or entangled ? What is the threshold ?

The volume and mean width of $\mathcal{S}$ can be estimated (not so directly, one has to put our convex body in the Löwner position). However, the same approach fails at the very last step, because the set of separable states on N qubits has "few" symmetries, and one cannot apply efficiently the MM^*-estimate.

The end

THANK YOU !