# RANDOM QUANTUM STATES AND CHANNELS

## ① Introduction

→ Quantum Information Theory ↳ "quantum Shannon theory"

- data compression
- noisy channels
- capacity

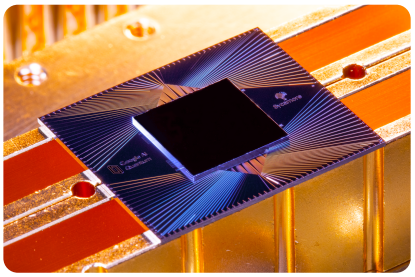
f.d. Hilbertspaces

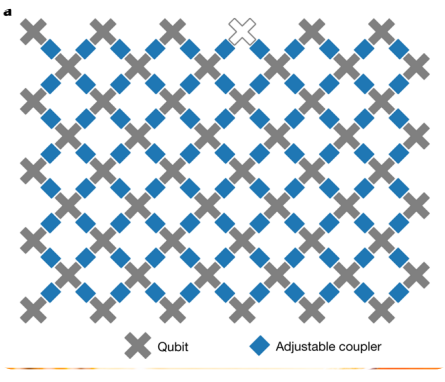
$\{0,1\} \to \mathbb{C}|0\rangle \oplus \mathbb{C}|1\rangle \simeq \mathbb{C}^2$

bits → qubits

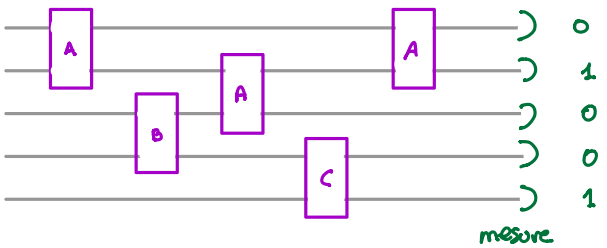
→ what do random matrices have to do with all this?

- where it all started: Wigner
- quantum theory has randomness built-in (measurement results, Born's rule)
- mathematical description of q. th.: matrices / tensors / tensor product structure
- properties of typical / generic states/operations:
  - ↳ what is the probability that a random q. state is entangled?
  - ↳ what is the prob. that 2 indep. q. measurements are compatible?
  - ↳ what is the capacity of a random quantum channel?
- important source of (counter-) examples in QIT (e.g. additivity of the minimum output entropy)
- Google's Quantum Supremacy experiment






- Sycamore chip samples the output probabilities of a random quantum circuit




- arguably, this is hard to do classically

## ② Random quantum states

→ **pure** quantum states : vectors $\psi \in \mathcal{H}$, $\|\psi\| = 1$ (f.d complex Hilbert space $\mathcal{H} \simeq \mathbb{C}^d$)
↳ isolated from the environment

→ natural probability distribution : **uniform measure on the unit sphere of $\mathbb{C}^d$**

→ **mixed states** (density matrices) : $\rho \in M_d(\mathbb{C})$, $\rho \geq 0$ ($\Leftrightarrow p_i \geq 0$) $\quad \mathrm{Tr}\,\rho = 1$ ($\Leftrightarrow \sum p_i = 1$)

↳ can be understood as n.c. prob. distributions : $p_i \geq 0$, $\sum p_i = 1$

↳ QIT restricted to diagonal ($\Leftrightarrow$ commutative) matrices $\equiv$ classical theory

→ the set of density matrices $DM_d = \{\rho \in M_d(\mathbb{C}) : \rho \geq 0 \text{ and } \mathrm{Tr}\,\rho = 1\}$ is a **convex body**

↳ can consider the (normalized) **Lebesgue measure**

→ **open quantum** systems point of view : System $\otimes$ Environment
total system is in a pure state

→ total Hilbert space $\mathcal{H}_{tot} = \mathbb{C}^d \otimes \mathbb{C}^s$ ($s$ : size of the environment)

→ system + environment is in a state $|\varphi\rangle \in \mathbb{C}^d \otimes \mathbb{C}^s \simeq \mathbb{C}^{ds}$

→ $|\varphi\rangle$ is random, uniform over the unit sphere

→ state of the system is mixed : $\rho = [\mathrm{id}_d \otimes \mathrm{Tr}_s]\,|\varphi\rangle\langle\varphi| \in M_d$ ($|\varphi\rangle\langle\varphi|$ in math notation)
($[\mathrm{id}_d \otimes \mathrm{Tr}_s]$ : partial trace ; $|\varphi\rangle\langle\varphi|$ : projection on $\mathbb{C}\varphi$)

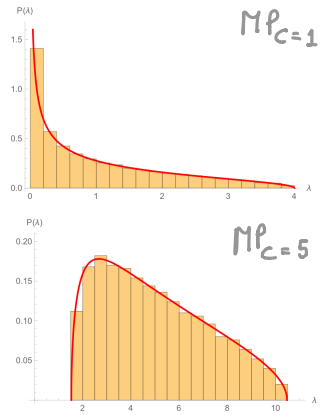
**Proposition** Let $\mu_{d,s}$ be the measure **induced** by the Lebesgue measure on the unit sphere of $\mathbb{C}^{ds}$ by the map $\varphi \mapsto \mathrm{Tr}_s\,|\varphi\rangle\langle\varphi|$.

If $W$ is a **Wishart** matrix of parameters $(d,s)$ (i.e. $W = GG^*$ with $G \in M_{d\times s}(\mathbb{C})$ having iid complex Gaussian entries), then $\rho = \frac{W}{\mathrm{Tr}\,W} \sim \mu_{d,s}$. The choice **$s=d$** yields **Lebesgue**.

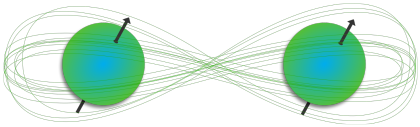
**Proof idea** If $W$ is a Wishart R.M., $\mathrm{Tr}\,W$ ($\chi^2$) and $\frac{W}{\mathrm{Tr}\,W}$ ($\rho$) are **indep.**

→ moment computations : $\mathbb{E}\,\mathrm{Tr}\,\rho = 1$ ; $\mathbb{E}\,\mathrm{Tr}\,\rho^2 = \frac{d+s}{1+ds}$

→ $d,s \to \infty$, $\frac{s}{d} \to c \in (0,\infty)$, then $\mathrm{spec}(s\cdot\rho) \to MP_c$
(Marchenko-Pastur distribution)



## ③ Entanglement vs. Separability



→ quantum entanglement is a central notion in quantum theory

↳ at the heart of many q. protocols, such as teleportation, Bell inequalities

↳ no quantum speed up without entanglement

**Definition** Separable states are convex mixtures of product states

$$SEP_{d_A,d_B} := \left\{ \sum p_i \rho_i^{(A)} \otimes \rho_i^{(B)} : p_i \geq 0, \sum p_i = 1, \rho_i^{(A/B)} \in DM_{d_{A/B}} \right\}$$

Non-separable states are called entangled.

→ $SEP_{d_A,d_B} \subseteq DM_{d_A d_B}$ is an open, convex subset. $Ext(SEP) = \left\{ |\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta| \right\}_{\substack{\alpha \in \mathbb{C}^{d_A} \\ \beta \in \mathbb{C}^{d_B}}}$

**Examples**

- $|0\rangle\langle 0| \otimes |1\rangle\langle 1| = |01\rangle\langle 01| \in SEP_{2,2}$
- $\frac{I}{d_A} \otimes \frac{I}{d_B} \in SEP_{d_A,d_B}$
- $\frac{1}{\sqrt{2}}(|00\rangle\langle 00| + |11\rangle\langle 11|) \in SEP_{2,2}$
- $\omega := |\Omega\rangle\langle\Omega| \notin SEP_{2,2}$ with $|\Omega\rangle := \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$
  ↳ maximally entangled state
- In general, $|\Omega_d\rangle := \frac{1}{\sqrt{d}} \sum_{i=1}^{d} e_i \otimes e_i \in \mathbb{C}^d \otimes \mathbb{C}^d$

→ It is NP-hard to decide whether a given $\rho_{AB} \in SEP_{d_A,d_B}$

→ necessary criterion for separability: if $\rho \in SEP$, then

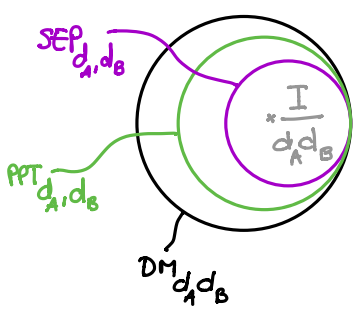
$$\rho^\Gamma := [id_A \otimes transp_B](\rho) \geq 0 : \left(\sum_i p_i \sigma_i \otimes \tau_i\right)^\Gamma = \sum_i p_i \sigma_i \otimes \overline{\tau_i}^T \geq 0$$

**Example** $\omega_2 = |\Omega\rangle\langle\Omega|$ with $|\Omega\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$

$$\omega^\Gamma = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}^\Gamma = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$ with spectrum $\frac{1}{2}(1,1,1,-1) \not\geq 0 \Rightarrow \omega^\Gamma \not\geq 0 \Rightarrow \omega$ ent.

**Definition** The set of positive partial transpose states

$$PPT_{d_A,d_B} := \left\{ \rho : \rho^\Gamma \geq 0 \right\} \supseteq SEP_{d_A,d_B}$$

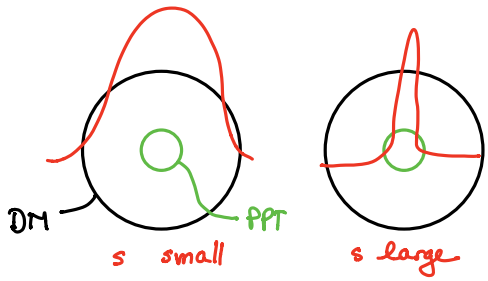



**Theorem** [Woronowicz] If $(d_A, d_B) = (2,2)$ or $(2,3)$, then $PPT = SEP$

## ④ When is a random quantum state PPT ?

→ induced measures $\mu_{d,s}$ : $d$ fixed, $\mu_{d,s} \xrightarrow[s\to\infty]{} \delta_{I/d}$

($d$: Hilbert space dimension, $s$: env. dim param.)




→ we are interested in $\mathbb{P}(\underbrace{\rho \in PPT}_{\rho^\Gamma \geq 0})$ for $\rho \sim \mu_{\underbrace{d_A d_B}_{d=d_A\cdot d_B},s}$

→ two asymptotic regimes:

- balanced → $d_A = d_B = d \to \infty$ ; $s \sim cd^2$
- unbalanced → $d_A = n$ fixed, $d_B = d \to \infty$ ; $s \sim cnd$

↳ in both cases, $s\rho \to MP_c$ (no partial transpose)

**Theorem** [Aubrun '12] In the balanced regime, $\rho \sim \mu_{d^2, cd^2}$, $spec(d\cdot\rho^\Gamma) \to SC(1, \frac{1}{c})$

In particular, if (threshold occurs at $c=4$)

- $c > 4$, $\lim_{d\to\infty} \mathbb{P}(\rho^\Gamma \geq 0) = 0$
- $c < 4$, $\lim_{d\to\infty} \mathbb{P}(\rho^\Gamma \geq 0) = 1$ (need extra result on the conv of $\lambda_{min}(\rho^\Gamma)$)

**Theorem** [Banica, N. '13] In the unbalanced case, $\rho \sim \mu_{nd, cnd}$ with $n \in \mathbb{N}$, $c > 0$

$$spec(d\rho^\Gamma) \to MP_{c\frac{n(n+1)}{2}} \boxminus MP_{c\frac{n(n-1)}{2}}$$

The limit measure has positive support iff $c > \underbrace{2 + 2\sqrt{1-\frac{1}{n^2}}}_{\text{threshold}}$

→ above, $\mu_1 \boxminus \mu_2 = \mu_1 \boxplus (\underbrace{D_{-1}\mu_2}_{\text{law of } -X, \text{ when } X\sim\mu_2})$ is the free difference operation

→ how about the threshold for SEP instead of PPT ? More complicated, exact result still open

**Theorem** [Aubrun, Szarek, Ye '14] In the balanced case, the threshold for SEP satisfies $c_1 d^3 < s(d) < c_2 d^3 \log^2 d$

→ threshold for SEP $\sim d^3$ vs threshold for PPT $\sim d^2$ $\Rightarrow$ for $\rho \sim \mu_{d^2, d^\kappa}$ with $\kappa \in (2,3)$, $\mathbb{P}(\rho \in PPT \text{ and } \rho \text{ entangled}) \xrightarrow[d\to\infty]{} 1$ i.e. PPT criterion is useless

## ⑤ Random quantum channels

→ quantum channels model the physically admissible transformations of quantum states

→ they generalize Markov matrices ($p' = Mp$ for $p, p'$ prob. vectors)

→ $\Phi : M_d(\mathbb{C}) \to M_D(\mathbb{C})$ must be linear, positivity preserving, trace preserving
($d$: input dim, $D$: output dim)

→ positivity-preserving is not enough because of entanglement:

$[id_2 \otimes transp_2](\omega_2) \not\geq 0$ although $transp_2 : M_2 \to M_2$ is positivity-pres.

**Definition** A linear map $\Phi : M_d \to M_D$ is called completely positive if

$$\forall\, n \geq 1 \quad \forall\, M_n \otimes M_d \ni X \geq 0 \quad [id_n \otimes \Phi](X) \geq 0$$

A quantum channel is a linear, completely positive, trace preserving map.

**Theorem 4.2.1.** *Let $\Phi : \mathcal{M}_d \to \mathcal{M}_D$ a linear transformation. The following assertions are equivalent:*

*(1) The map $\Phi$ is a quantum channel.*

*(2) The map $\Phi \otimes \mathrm{id}_d$ is positive and trace preserving.*

*(3) The Choi map $J(\Phi)$ is positive semidefinite and $\mathrm{Tr}_D J(\Phi) = I_d$.*

$$J(\Phi) := \sum_{i,j=1}^{d} E_{ij} \otimes \Phi(E_{ij}) \in M_d \otimes M_D$$

*(4) The exist $R$ matrices $A_1, \ldots, A_R \in \mathcal{M}_{D \times d}$ such that*

$$\Phi(X) = \sum_{i=1}^{R} A_i X A_i^* \qquad \text{and} \qquad \sum_{i=1}^{R} A_i^* A_i = I_d. \tag{4.14}$$

*(5) There exist some positive integer $R$ and an isometry $V : \mathbb{C}^d \to \mathbb{C}^D \otimes \mathbb{C}^R$ such that*

$$\Phi(X) = \mathrm{Tr}_R(VXV^*). \tag{4.15}$$

*The decomposition (4) above is known as the* Kraus decomposition, *while (5) is know as the* Stinespring dilation *of the channel $\Phi$. The integer $R$ above can be taken to be $R = \mathrm{rank}\, J(\Phi)$, value which is called the* Choi rank *of $\Phi$.*

**Examples**

- the identity channel $id : M_d \to M_d$
- unitary conjugations $ad_U : M_d \to M_d \quad \rho \mapsto U \rho U^*$
- depolarizing channel $\Delta(X) = (\mathrm{Tr}\, X) \frac{I_D}{D}$
- diagonal conditional expectation $diag : M_d \to M_d \quad X \to (X_{ii})_{i=1}^{d}$

→ what are **natural** probability distributions on the set of quantum channels $\Gamma_d \to \Gamma_D$ ?

→ each item in the characterization theorem comes with a candidate :

→ (1,2) : use the (normalized) **Lebesgue measure** on the convex body of q. channels

→ (3) : pick $\widetilde{J} \sim \text{Wishart}_{dD,M}$ and **normalize** it $J := (I_d \otimes Z^{-1/2})\widetilde{J}(I_d \otimes Z^{-1/2})$,

where $Z := (\mathrm{Tr}_d \otimes \mathrm{id}_D)(\widetilde{J})$. Define $\Phi := \widetilde{J}^{-1}(J)$

→ (4) Pick **iid Ginibres** $\widetilde{A}_1, \dots, \widetilde{A}_M \in \Gamma_{D\times d}(\mathbb{C})$ and **normalize** them : $A_i := \widetilde{A}_i Y^{-1/2}$

where $Y := \sum_{i=1}^{M} \widetilde{A}_i^* \widetilde{A}_i$

→ (5) Pick **Haar-random isometry** $V : \mathbb{C}^d \to \mathbb{C}^D \otimes \mathbb{C}^M \simeq \mathbb{C}^{DM}$ (by truncating a random unitary $U \in \mathcal{U}_{DM}$ to its first d columns)

**Theorem** [Kukulski, N., Pawela, Puchała, Życzkowski '20] These families of measures are identical

$$\mu^{\text{Lebesgue}} \in \left\{ \mu^{\text{Stinespring}}_{d,D;M} \right\}_{\substack{M \in \mathbb{N} \\ M \geq \frac{d}{D}}} = \left\{ \mu^{\text{Kraus}}_{d,D;M} \right\}_{\substack{M \in \mathbb{N} \\ M \geq \frac{d}{D}}} \subseteq \left\{ \mu^{\text{Choi}}_{d,D;M} \right\}_{M \in \mathcal{M}_{d,D}}$$

(Lebesgue: for $M = dD$)

where $\mathcal{M}_{d,D} := \{\lceil \frac{d}{D} \rceil, \dots, dD-1\} \sqcup [dD, +\infty)$

---

## ⑥ Output sets of random quantum channels

→ the **classical capacity** of a quantum channel $\Phi$ (how much classical information can be reliably sent trough multiple uses of the channel) is expressed as an entropic quantity depending on the output set of $\Phi^{\otimes n}$ $(n \to \infty)$

→ a mathematically simple relevant quantity is the **minimum output entropy**

$$H^{\min}(\Phi) = \min_{\rho \in D M_d} H(\Phi(\rho))$$

($H$: **von Neumann entropy** $H(\sigma) = -\mathrm{Tr}\,\sigma \log \sigma$)

→ additivity conjecture : $H^{\min}(\Phi \otimes \Psi) = H^{\min}(\Phi) + H^{\min}(\Psi)$ **false** [Hastings '10]

→ using the concavity of the entropy, we can restrict the min to pure states $\rho = |x\rangle\langle x|$

→ if $\Phi : M_d \to M_k$ is defined via an isometry $V : \mathbb{C}^d \to \mathbb{C}^k \otimes \mathbb{C}^n$, then

$$H^{\min}(\Phi) = \min \{ H(\mathrm{Tr}_n |y\rangle\langle y|) : y \in \mathrm{Ran}\, V,\ \|y\| = 1 \}$$

→ for a subspace ($\mathrm{Ran}\, V =$) $W \subseteq \mathbb{C}^k \otimes \mathbb{C}^n$, define the set

$$K_W := \{ \lambda(y) : y \in W, \|y\| = 1 \}, \text{ where}$$

$\lambda(y)$ is the vector of singular values (Schmidt coefficients) of $y$

$$y = \sum_{i=1}^{k \wedge n} \sqrt{\lambda_i(y)}\, e_i \otimes f_i \quad \text{for } \perp_n \text{ families } \{e_i\} \subseteq \mathbb{C}^k, \{f_i\} \subseteq \mathbb{C}^n$$

$\hookrightarrow y \in \mathbb{C}^k \otimes \mathbb{C}^n \simeq M_{k \times n}(\mathbb{C})$

→ computing $H^{\min}(\Phi) \equiv$ minimizing the usual entropy over $K_{\mathrm{Ran}\, V}$, where $V : \mathbb{C}^d \to \mathbb{C}^k \otimes \mathbb{C}^n$ is the isometry defining $\Phi$: $\Phi(X) = \mathrm{Tr}_n(VXV^*)$

**Theorem** [Belinschi, Collins, N. '12, '16] Consider a sequence of Haar-distributed random subspaces $W_n \subseteq \mathbb{C}^k \otimes \mathbb{C}^n$, where $k$ is fixed, $n \to \infty$ and $\dim W_n \sim t k n$ for a fixed $t \in (0,1)$. The (random) sets $K_{W_n} \subseteq \Delta_k$ (prob. simplex) converge almost surely as $n \to \infty$, in Hausdorff distance to a deterministic convex set

$$K_{k,t} := \{ \lambda \in \Delta_k : \forall x \in \Delta_k,\ \langle \lambda, x \rangle \leq \|x\|_{(t)} \}.$$ ($\|x\|_{(t)}$: polar dual)

The element of $K_{k,t}$ having min entropy is of the form $\lambda_* = (a, b, b, \dots, b)$ and it can be computed explicitely.

→ this result gives the SOTA violation of additivity for $H^{\min}$, as well as the smallest value of $k$ for which a violation occurs

**Definition** The $(t)$-norm on $\mathbb{R}^k$ is defined by $\|x\|_{(t)} = \|P_t\, x\, P_t\|$, where we identify $\mathbb{R}^k$ with a diagonal subalgebra of a $C^*$-ncps $(\mathcal{A}, \tau)$ and $P_t$ is a projection of rank $t \in (0,1)$, free from $\mathbb{R}^n$ in $\mathcal{A}$.

→ $\|x\|_{(t)}$ is the largest (in absolute value) element of the support of

$$\left(\tfrac{1}{k}\delta_{x_1} + \cdots + \tfrac{1}{k}\delta_{x_k}\right) \boxtimes \left(t\delta_1 + (1-t)\delta_0\right)$$

**Proof idea**

$$\max_{y \in W,\, \|y\|=1} \lambda_1(y) = \max_{\substack{y \in W,\, \|y\|=1 \\ z \in \mathbb{C}^k,\, \|z\|=1}} \mathrm{Tr}\left(P_y \cdot P_z \otimes I_n\right) = \max_z \max_y \mathrm{Tr}\left(P_y \cdot P_z \otimes I_n\right)$$

$$= \max_z \|P_W \cdot P_z \otimes I_n\|_\infty \xrightarrow{n \to \infty} \|(1, 0, \dots, 0)\|_{(t)}$$

(eigenvalues of $P_z$)