Random Matrices from the Classical Compact Groups: a Panorama

Part VIII: Random unitary matrices in quantum information theory

Mark Meckes

Case Western Reserve University

Oxford, 12 March 2021

References

- Benoît Collins and Ion Nechita, "Random matrix techniques in quantum information theory", *J. Math. Physics* 57, 015215, 2016.

- Guillaume Aubrun and Stanisław Szarek, , *Alice and Bob Meet Banach: The Interface of Asymptotic Geometric Analysis and Quantum Information Theory*, Cambridge, 2019.

- Ingemar Bengtsson and Karol Życzkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement*, Cambridge, 2006.

Quantum mechanics in a hurry

The state of a system is represented by a unit vector ψ in a (finite- or infinite-dimensional) complex Hilbert space $\mathcal{H}$.

Measurements correspond to an ONB $\{u_j\}$ of $\mathcal{H}$:

- j indexes the possible outcomes.
- $|\langle \psi, u_j \rangle|^2$ is the probability of the j^{th} outcome.

Measurements can't distinguish ψ from $e^{i\theta}\psi$, so really a state is an element of projective space.

Equivalently, use $\rho = \psi\psi^* \in B(\mathcal{H})$, so that

$$|\langle \psi, u_j \rangle|^2 = \langle \rho u_j, u_j \rangle.$$

Time evolution corresponds to a unitary map $U \in B(\mathcal{H})$:

$$\psi \mapsto U(\psi), \qquad \rho \mapsto U\rho U^*.$$

Quantum mechanics in a hurry

A compound system is modeled via a tensor product $\mathcal{H} = \mathcal{S} \otimes \mathcal{E}$.

What if we only measure what's happening in $\mathcal{S}$?

Say $\{u_j\}$ and $\{v_k\}$ are ONBs of $\mathcal{S}$ and $\mathcal{E}$.

The total probability of the j^{th} outcome of the $\mathcal{S}$ measurement is

$$\sum_k \left|\langle \psi, u_j \otimes v_k \rangle\right|^2 = \sum_k \langle \rho(u_j \otimes v_k), u_j \otimes v_k \rangle = \langle (\mathrm{Tr}_{\mathcal{E}}\, \rho) u_j, u_j \rangle,$$

where $\mathrm{Tr}_{\mathcal{E}} = I \otimes \mathrm{Tr} : B(\mathcal{S}) \otimes B(\mathcal{E}) \to B(\mathcal{S})$ is the partial trace.

$\mathrm{Tr}_{\mathcal{E}}\, \rho$ is a positive semidefinite operator with trace 1 (mixed state or density matrix), called a quantum marginal of ρ.

Evolution of mixed states

Suppose $\rho \in B(\mathcal{S} \otimes \mathcal{E})$ evolves according to $U \in B(\mathcal{S} \otimes \mathcal{E})$.

The quantum marginal $\sigma = \mathrm{Tr}_{\mathcal{E}}\, \rho$ evolves as

$$\sigma \mapsto \mathrm{Tr}_{\mathcal{E}}(U \rho U^*).$$

Every mixed state $\sigma \in B(\mathcal{S})$ can be written as $\sigma = \mathrm{Tr}_{\mathcal{E}}(\sigma \otimes \epsilon)$ for some $\mathcal{E}$ and density matrix $\varepsilon \in B(\mathcal{E})$, so

$$\sigma \mapsto \mathrm{Tr}_{\mathcal{E}}(U(\sigma \otimes \varepsilon)U^*)$$

for U acting on $\mathcal{S} \otimes \mathcal{E}$ is the most general type of evolution for mixed states.

Quantum channels

Proposition

The following are equivalent for a linear map $\Phi : M_n(\mathbb{C}) \to M_n(\mathbb{C})$:

1. (*Stinespring representation*) $\Phi(\rho) = \mathrm{Tr}_{\mathbb{C}^k}[U(\rho \otimes \epsilon)U^*]$ *for some* k, *density matrix* $\varepsilon \in M_k(\mathbb{C})$, *and* $U \in \mathbb{U}(nk)$.
2. (*Kraus decomposition*) $\Phi(\rho) = \sum_{i=1}^{k} V_i \rho V_i^*$ *for some* $V_i \in M_n(\mathbb{C})$ *with* $\sum_i V_i^* V_i = I_n$.
3. Φ *is completely positive and trace-preserving.*

Such a map Φ is called a quantum channel.

We can always take $k \leq n^2$ and $\varepsilon = E_{11}$.

Random matrices in QIT

Quantum information theory deals with various properties of (the sets of) density matrices and quantum channels.

Random matrices arise in QIT as

- random density matrices,
- random quantum channels (or building blocks of them),
- outputs of random quantum channels.

The sets of density matrices or of quantum channels do not possess canonical probability measures.

But there are many natural probability measures we can choose from.

I'll discuss a few results about random quantum channels built from Haar-distributed unitary matrices.

Almost randomizing channels

$\rho_* = \frac{1}{n} I_n$ is the maximally mixed state on $\mathbb{C}^n$.

A channel Φ is ε-randomizing if

$$\|\Phi(\rho) - \rho_*\|_{op} \leq \frac{\varepsilon}{n}.$$

The completely randomizing channel $R(\rho) = \rho_*$ requires n^2 terms in its Kraus decomposition.

Almost randomizing channels via random Kraus decomposition

Theorem (Hayden–Leung–Shor–Winter, Aubrun)

Let

$$\Phi(\rho) = \frac{1}{k} \sum_{i=1}^{k} U_i \rho U_i^*,$$

where $U_1, \ldots, U_k \in \mathbb{U}(n)$ are independent and Haar-distributed. If $0 < \varepsilon < 1$ and $k \geq C\varepsilon^{-2} n$ then Φ is ε-randomizing with high probability.

Idea of proof:

- $\|A\|_{op} = \sup_{\sigma} |\mathrm{Tr}(A\sigma)|$, where the sup is over density matrices.
- For each $\rho, \sigma \in M_n(\mathbb{C})$, $\mathrm{Tr}(\Phi(\rho)\sigma)$ is tightly concentrated.
- Discretization of the set of density matrices.

Random Stinespring decomposition

Fix n and k. For $U \in \mathbb{U}(nk)$ define the channel

$$\Phi^U(\rho) = \mathrm{Tr}_{\mathbb{C}^k}[U(\rho \otimes E_{11})U^*]$$

for $E_{11} \in M_k(\mathbb{C})$.

Given $U, V \in \mathbb{U}(nk)$, $\Phi^U \otimes \Phi^V$ is a quantum channel on $\mathbb{C}^n \otimes \mathbb{C}^n \cong \mathbb{C}^{n^2}$.

If U and V are random and $\rho \in M_{n^2}(\mathbb{C})$ is fixed, then

$$\Phi^U \otimes \Phi^V(\rho)$$

is an $n^2 \times n^2$ random matrix.

We consider a Bell state $\beta = \psi\psi^*$, where $\psi = \dfrac{1}{\sqrt{n}} \sum_{i=1}^{n} e_i \otimes e_i$ is maximally entangled, and let $\sigma = \Phi^U \otimes \Phi^V(\beta)$.

Outputs from Bell states

Theorem (Collins–Nechita)

Suppose $U, V \in \mathbb{U}(nk)$ are independent. Then

1. *For fixed n, $\sigma \xrightarrow{k\to\infty} \rho_* = \frac{1}{n^2} I_{n^2}$.*
2. *For fixed k, essentially $\mu_\sigma \xrightarrow{n\to\infty} \frac{k^2}{n^2}\delta_{1/k^2} + \left(1 - \frac{k^2}{n^2}\right)\delta_0$.*

Suppose $U \in \mathbb{U}(nk)$ is random and $V = \overline{U}$. Then

1. *For fixed n, $\sigma \xrightarrow{k\to\infty} \rho_* = \frac{1}{n^2} I_{n^2}$.*
2. *For fixed k, essentially*

$$\mu_\sigma \xrightarrow{n\to\infty} \frac{1}{n^2}\delta_{\frac{1}{k}+\frac{1}{k^2}-\frac{1}{k^3}} + \frac{k^2-1}{n^2}\delta_{\frac{1}{k^2}-\frac{1}{k^3}} + \left(1 - \frac{k^2}{n^2}\right)\delta_0.$$

Idea of proof: Method of moments, using Weingarten calculus.

Entropy in QIT

The von Neumann entropy of a density matrix ρ is

$$S(\rho) = -\operatorname{Tr}(\rho \log \rho) = -\sum_i \lambda_i(\rho) \log \lambda_i(\rho).$$

The entropy of entanglement of $\psi \in \mathbb{C}^n \otimes \mathbb{C}^m$ is

$$E(\psi) = S\left(\operatorname{Tr}_{\mathbb{C}^m}(\psi\psi^*)\right) = S\left(\operatorname{Tr}_{\mathbb{C}^n}(\psi\psi^*)\right).$$

We can generalize a quantum channel as a completely positive trace-preserving linear map $\Phi : M_n(\mathbb{C}) \to M_m(\mathbb{C})$.

The minimum output entropy of a channel Φ is

$$S^{\min}(\Phi) = \min_\rho S(\Phi(\rho)),$$

where the $\min$ is over density matrices ρ.

Additivity problem

If Φ and Ψ are quantum channels then $\Phi \otimes \Psi$ is a channel and

$$S^{\min}(\Phi \otimes \Psi) \leq S^{\min}(\Phi) + S^{\min}(\Psi).$$

A major open problem in QIT for some time was whether

$$S^{\min}(\Phi \otimes \Psi) = S^{\min}(\Phi) + S^{\min}(\Psi).$$

Theorem (Hastings)

For sufficiently large m and n, there exist quantum channels $\Phi, \Psi : M_n(\mathbb{C}) \to M_m(\mathbb{C})$ such that

$$S^{\min}(\Phi \otimes \Psi) < S^{\min}(\Phi) + S^{\min}(\Psi).$$

The counterexample

For $U \in \mathbb{U}(mk)$ random, let

$$V : \mathbb{C}^n \to \mathbb{C}^m \otimes \mathbb{C}^k \cong \mathbb{C}^{mk}$$

be given by the first n columns of U. Then

$$\Phi^U(\rho) = \mathrm{Tr}_{\mathbb{C}^k}(V \rho V^*)$$

is a random quantum channel $\Phi^U : M_n(\mathbb{C}) \to M_m(\mathbb{C})$.

Proposition

If $k = m^2$ and $n = cm^2$, then for sufficiently large m,

$$S^{\min}\left(\Phi^U \otimes \Phi^{\overline{U}}\right) < S^{\min}\left(\Phi^U\right) + S^{\min}\left(\Phi^{\overline{U}}\right)$$

with high probability.

The counterexample

Ideas in the proof:

$S^{\min}\left(\Phi^{U} \otimes \Phi^{\overline{U}}\right)$ is fairly small because $\Phi^{U} \otimes \Phi^{\overline{U}}(\beta)$ has a large eigenvalue.

$S^{\min}\left(\Phi^{U}\right) = S^{\min}\left(\Phi^{\overline{U}}\right) = \min_{\psi \subseteq \mathrm{range}\, V} E(\psi)$ is fairly large with high probability by measure concentration.

The latter can be seen as a manifestation of (a generalization of) Dvoretzky's theorem (Aubrun–Szarek–Werner).

Sharper results can be obtained using other RMT techniques, including free probability (Belinschi–Collins–Nechita).

Thank you!