Random matrices in quantum information

Motohisa Fukuda

Quantum states and channels

- A quantum state ρ (in finite dimension) is a positive semi-definite Hermitian operator with trace one on a Hilbert space $\mathbb{C}^n$.
- A channel can be written as

$$\Phi(\rho) = \mathrm{Tr}_{\mathbb{C}^k}\left[V \rho V^*\right]$$

Here, $V : \mathbb{C}^\ell \to \mathbb{C}^k \otimes \mathbb{C}^n$ is a partial isometry. This means that a channel is completely positive and trace preserving.

Remark: Taking $\mathrm{Tr}_{\mathbb{C}^k}$ or $\mathrm{Tr}_{\mathbb{C}^n}$ does not matter for our problems and in this talk we can think that $l = n \gg 1$ and k is fixed.

Minimum output entropy (MOE)

The minimal output entropy of channel Φ is defined by

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

where ρ are input states. [King, Ruskai '01]

Here, the von Neumann entropy $S(\cdot)$ of quantum state ρ is:

$$S(\rho) = -\operatorname{Tr}[\rho \log \rho] = -\sum_{i=1}^{d} \lambda_i \log \lambda_i$$

where λ_i are eigenvalues of ρ.

Additivity question is stated as

$$S_{\min}(\Phi \otimes \Omega) \stackrel{?}{=} S_{\min}(\Phi) + S_{\min}(\Omega)$$

for quantum channels Φ and Ω.

Note that

$$\min_{\rho \otimes \sigma} S((\Phi \otimes \Omega)(\rho \otimes \sigma)) = \min_{\rho} S(\Phi(\rho)) + \min_{\sigma} S(\Omega(\sigma))$$

because

$$S(\rho \otimes \sigma) = S(\rho) + S(\sigma)$$

Additivity violation of von Neumann entropy

Write quantum channels:

$$\Phi(\rho) = \mathrm{Tr}_{\mathbb{C}^k}\left[V\rho V^*\right]$$

and their complex conjugate channels:

$$\bar{\Phi}(\rho) = \mathrm{Tr}_{\mathbb{C}^k}\left[\bar{V}\rho V^T\right]$$

Then, with high probability we have additivity violation [1] :

$$S_{\min}(\Phi \otimes \bar{\Phi}) < S_{\min}(\Phi) + S_{\min}(\bar{\Phi})$$

where V is chosen randomly in the push-forward measure of $\mathcal{U}(kn)$.

[1] [Hastings '09]: more precisely, a slightly different model was used.

Violation of additivity and multiplicativity for $p > 1$
[Hayden, Winter '08]

- Additivity violation of minimum output Rényi entropy:

$$S_{\min,p}(\Phi \otimes \bar{\Phi}) < S_{\min,p}(\Phi) + S_{\min,p}(\bar{\Phi})$$

where Rényi entropy is defined as

$$S_p(\sigma) = \frac{1}{1-p} \log \operatorname{Tr}[\sigma^p] = \frac{p}{1-p} \log \|\sigma\|_p$$

- Multiplicativity violation of maximum output p-norm:

$$\|\Phi \otimes \bar{\Phi}\|_{1\to p} > \|\Phi\|_{1\to p} \|\bar{\Phi}\|_{1\to p}$$

I.e., $\|\Phi \otimes \bar{\Phi}\|_{1\to p}$ is "large" and $\|\Phi\|_{1\to p}$ is "small".

How Weingarten calculus came into play

To show violation of additivity one can use the following trick:

$$\|\Phi \otimes \bar{\Phi}\|_{1\to p} \geq \|\Phi \otimes \bar{\Phi}(|b\rangle\langle b|)\|_p \geq \|\Phi \otimes \bar{\Phi}(|b\rangle\langle b|)\|_\infty \geq \frac{\ell}{kn}$$

where $|b\rangle$ is a Bell state in the bra-ket notaion.

This trick was introduced by Hayden and Winter and they predicted that there is only one big eigenvalue and the other ones are rather flat, based on numerics.

However, [Collins, Nechita '10] made an explicit calculation by using Weingarten functions and showed a.e. convergence of eigenvalues to

$$\left\{\frac{1}{k} - \frac{1}{k^2} + \frac{1}{k^3}, \quad \frac{1}{k^2} - \frac{1}{k^3}, \ldots, \frac{1}{k^2} - \frac{1}{k^3}\right\}$$

when $\ell = n$.

Hastings' idea to show that $\|\Phi\|_{1\to p}$ is "small"

- Fix an input to be $|x\rangle\langle x|$ with a unit vector $|x\rangle \in \mathbb{C}^\ell$.
- Then, $|w\rangle = V|x\rangle$ is a random unite vector in $\mathbb{C}^k \otimes \mathbb{C}^n$.
- WW^* is a normalized Wishart matrix.

Here is the picture:

$$|x\rangle\langle x| \mapsto V|x\rangle\langle x|V^* = |w\rangle\langle w| \mapsto \mathrm{Tr}_{\mathbb{C}^n}\left[|w\rangle\langle w|\right] = WW^*$$

The eigenvalue distribution of WW^* is proportional to:

$$\delta\left(1 - \sum_{1\le i\le k} p_i\right) \prod_{1\le i<j\le k} (p_i - p_j)^2 \prod_{1\le i\le k} p_i^{n-k}$$

The last factor shows that $n \gg k$ implies concentration of eigenvalues, and typical eigenvalues of outputs are rather flat for randomly chosen quantum channels.

[Aubrun, Szarek, Werner '10] applied Dvoretzky theorem

A random quantum channel is defined for random isometry V:

$$\Phi(|x\rangle\langle x|) = \mathrm{Tr}_{\mathbb{C}^n}\left[V|x\rangle\langle x|V^*\right]$$

This is equivalent to choose random subspaces $S \leq \mathbb{C}^k \otimes \mathbb{C}^n$ w.l.o.g. so that

$$\begin{aligned} \Phi : \mathcal{B}(S) &\to M_k(\mathbb{C}) \\ |x\rangle\langle x| &\mapsto \mathrm{Tr}_{\mathbb{C}^n}\left[|x\rangle\langle x|\right] = XX^* \end{aligned}$$

On the other hand, for a (unit) vector $|x\rangle \in \mathbb{C}^k \otimes \mathbb{C}^n$

$$|x\rangle \mapsto \sqrt{\left\|\Phi(|x\rangle\langle x|)\right\|_p} = \sqrt{\left\|XX^*\right\|_p} = \|X\|_{2p}$$

is a norm and one can use Dvoretzky's theorem.

[Belinschi, Collins, Nechita, '16] applied free probability

To identify the set of output states one can calculate

$$f(A) = \max_{|x\rangle \text{ is a unit vector}} \operatorname{Tr}\left[\Phi(|x\rangle\langle x|)\, A\right]$$

for $A \in \mathcal{M}_k(\mathbb{C})$.
Then, we calculate

$$\begin{aligned} f(A) &= \max_{|x\rangle \text{ is a unit vector}} \operatorname{Tr}\left[\operatorname{Tr}_{\mathbb{C}^n}\left[V|x\rangle\langle x|V^*\right]\, A\right] \\ &= \max_{|x\rangle \text{ is a unit vector}} \operatorname{Tr}\left[(V|x\rangle\langle x|V^*)\,(A\otimes I_n)\right] \\ &= \|V^*(A\otimes I_n)V\|_\infty = \|P(A\otimes I_n)P\|_\infty \end{aligned}$$

where $P = V\,V^*$ is a random projection.
Therefore,

$$f(A) \to \|a\|$$

for some norm $\|\cdot\|$ in an algebraic probability space by the property of strong convergence for Haar-distributed unitary matrices.

What I am interested in: is to find best inputs for maximum output entropy of tensor powers of quantum channels. Because

- minimum output entropy is closely related to capacity.
- multiple channel uses is represented by tensor powers if we assume independence of noise.

So far we know (see Appendix):

- for fixed inputs and random quantum channels $(\Phi \otimes \bar{\Phi})^{\otimes n}$, products of Bell states are best. [F, Nechita '14]
- for fixed inputs and random quantum channels $(\Phi)^{\otimes 2n}$, where Φ is generated by $\mathcal{O}(kn)$, products of Bell states are best. [F, Nechita '18]
- there are bounds for random quantum channels $(\Phi)^{\otimes 2n}$. [Montanaro '13][F, Nechita '15]
- there are tight bounds for unital quantum channels. [F, Gour '17]

Motivation: In quantum information, entanglement plays an important role. To detect entanglement mathematically we can use partial transpose.

What is entanglement?: A quantum state $\rho \in \mathcal{M}_m(\mathbb{C}) \otimes \mathcal{M}_n(\mathbb{C})$ is entangled if one cannot write it as

$$\rho = \sum_i \sigma_i \otimes \theta_i \tag{1}$$

for some quantum states σ_i, θ_i.

What is Peres-Horodecki criteria (1996)?: For a quantum state ρ in (1) we have

$$\rho^\Gamma = \sum_i \sigma_i \otimes \theta_i^T \geq 0$$

In general partial transpose does not preserve positivity.

Random quantum states and their partial transpose

Take a random unit vector $|x\rangle \in \mathbb{C}^\ell \otimes \mathbb{C}^m \otimes \mathbb{C}^n$ and take partial trace over $\mathbb{C}^\ell$ to generate random quantum states and investigate eigenvalue distributions of their partial transpose:

$$|x\rangle \mapsto |x\rangle\langle x| \mapsto \mathrm{Tr}_{\mathbb{C}^\ell}\left[|x\rangle\langle x|\right] = XX^* \mapsto (XX^*)^\Gamma$$

Then, we have three interesting regimes (simplified):

- Aubrun '12

  $\ell \propto d,\ m, n \propto d^2,\ d \to \infty \quad \Rightarrow \quad$ Shifted semi-circular law

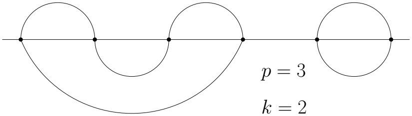
- Banica and Nechita '12

  m is fixed, $\ell/n \to b \Rightarrow$ free difference of free Poisson laws

- F and Sniady '13

  ℓ is fixed $m/n \to 1 \Rightarrow$ Moments give meander polynomials

Meander problems:
Even number of bridges over an infinitely long river. How many non-intersecting closed paths to pass each bridge only once?



Meander polynomials: If the number of bridges is 2p,

$$M_p(\ell) = \sum_{k=1}^{p} \ell^k M_p^{(k)}$$

where $M_p^{(k)}$ is the number of patterns with k paths.

Generating the polynomial: ℓ is fixed and $m/n \to 1$, then

$$\lim_{m,n\to\infty} \frac{1}{mn} \mathbb{E}\left[\left((\ell m XX^*)^\Gamma\right)^{2p}\right] = M_p(\ell)$$

Appendix

How about tensor powers $(\Phi \otimes \bar{\Phi})^{\otimes r}$?[2]

Our calculation shows that tensor-products of Bell states are best.
Suppose we have a random quantum channel:

$$\overset{1}{\Phi} \otimes \overset{2}{\Phi} \otimes \cdots \otimes \overset{r}{\Phi} \otimes \overline{\overset{\hat{1}}{\Phi}} \otimes \overline{\overset{\hat{2}}{\Phi}} \otimes \cdots \otimes \overline{\overset{\hat{r}}{\Phi}}$$

where best inputs are

$$|b_{\pi(1),\hat{1}}\rangle \otimes |b_{\pi(2),\hat{2}}\rangle \otimes \cdots \otimes |b_{\pi(r),\hat{r}}\rangle$$

where $\pi \in S_r$. Here, $|b_{i,j}\rangle$ is a Bell state over the i-th space for Φ and j-th space for $\bar{\Phi}$.

Remark. Hastings conjectured that violation of additivity happens only within each conjugate pair.

[2] [F, Nechita '14]

How about tensor powers $\Phi^{\otimes 2r}$, where Φ is orthogonal ? [3]

This time, we generate random channels by orthogonal matrices instead of unitary ones. So, $\bar{\Phi} = \Phi$.

$$\overset{1}{\Phi} \otimes \overset{2}{\Phi} \otimes \cdots \otimes \overset{r}{\Phi} \otimes \overset{r+1}{\Phi} \otimes \overset{r+2}{\Phi} \otimes \cdots \otimes \overset{2r}{\Phi}$$

where best inputs are

$$\bigotimes_{c \in \pi} |b_c\rangle$$

where π is a paring of $2r$ elements. Here, $|b_c\rangle$ is a Bell state over the i-th and j-th spaces when $c = (i, j)$.

We conjecture that typically for orthogonal case

$$S_{\min}(\Phi^{\otimes 2r}) = r\, S_{\min}(\Phi^{\otimes 2})$$

or, we can make it weaker:

$$\lim_{r \to \infty} \frac{1}{r} S_{\min}(\Phi^{\otimes r}) = \frac{1}{2} S_{\min}(\Phi^{\otimes 2})$$

[3] [F, Nechita '18]

Montanaro's multiplicative bound (2013)

$$\|\Phi^{\otimes r}\|_{1\to\infty} \leq \left(\|(V V^*)^\Gamma\|_\infty\right)^r$$

where V is the isometry defining Φ.

F-Nechita's multiplicative bound (2015)

$$\|\Phi^{\otimes r}\|_{1\to 2} \leq \left(\|C_\Phi^\Gamma\|_\infty\right)^r$$

where C_Φ^Γ is the partially transposed Choi matrix of Φ.

Then the bounds lead to the following weak additivity respectively for $p = \infty, 2$: typically under random choice of channels

$$S_{p,\min}(\Phi^{\otimes r}) \geq \frac{r}{2} S_{p,\min}(\Phi)$$

Montanaro first described it as “weakly multiplicative”, in terms of maximum output p-norms.

F-Gour's multiplicative bound; no random here (2017)

For a unital quantum channel: $M_n(\mathbb{C}) \to M_k(\mathbb{C})$,

$$\|\Phi^{\otimes r}\|_{1\to 2} \leq (\gamma_\Phi)^{r/2}.$$

Here,

$$\gamma_\Phi = \frac{1}{k} + \left(1 - \frac{1}{n}\right) \|D_\Phi D_\Phi^*\|_\infty$$

where D_Φ is the dynamical matrix of Φ restricted on trace-less Hermitian matrices.

We also got an upper bound for the classical capacity:

$$C(\Phi) \leq \log k + \log \gamma_\Phi.$$

This bound is saturated by the Werner-Holevo channel.

Perspective:

- (of course) we should look for more interactions of random matrix and free probability with quantum information.

Thank you very much.

Acknowledgement: JSPS KAKENHI Grant Number JP16K00005