Random quantum states and channels

Ion Nechita (CNRS, LPT Toulouse)

Le Teich, June 21st 2019

Summary from yesterday

- Pure quantum states of one particle: unit norm vectors inside a Hilbert space
- More particles $\rightsquigarrow$ take the tensor product of the Hilbert spaces
- Separable states = rank-1 tensors; entangled states = rank ≥ 2 tensors
- Random pure states: uniform point on the unit sphere
- Mixed quantum states (or density matrices): positive semidefinite matrices of unit trace $\rho \geq 0$, $\operatorname{Tr} \rho = 1$
- Extreme points of the set of mixed states = P_x, with x pure
- Separable (i.e. non-entangled state)

$$\rho_{AB} = \sum_i t_i \sigma_i^{(A)} \otimes \sigma_i^{(B)}$$

- Random mixed states: normalized Wishart matrix
- Partial transposition $\rho_{AB}^\Gamma := [\mathrm{id} \otimes \Theta](\rho_{AB})$. If $\rho_{AB}^\Gamma \not\geq 0$, then ρ_{AB} is entangled.

Outline

Quantum channels

Random quantum channels

Entanglement of subspaces

Random subspaces

Quantum channels

Quantum channels

Channels	Deterministic	Random mixture
Classical	$f : \{1, \ldots, d\} \to \{1, \ldots, d\}$	Q Markov (stochastic)
Quantum	$U \in \mathcal{U}(d)$	Φ CPTP map

- Classical channels (acting on probability vectors):
  - Positivity: for all i, j, $Q_{ij} \geq 0$
  - Mass preservation: for all j, $\sum_i Q_{ij} = 1$.
- Quantum channels: CPTP maps $\Phi : \mathcal{M}_d(\mathbb{C}) \to \mathcal{M}_{d'}(\mathbb{C})$
  - CP - complete positivity: $\Phi \otimes \mathrm{id}_r$ is a positive map, $\forall r \geq 1$
  - TP - trace preservation: $\mathrm{Tr} \circ \Phi = \mathrm{Tr}$.

Structure of quantum channels

Theorem [Stinespring-Kraus-Choi]

Let $\Phi : \mathcal{M}_d(\mathbb{C}) \to \mathcal{M}_d(\mathbb{C})$ be a linear map. TFAE:

1. The map Φ is completely positive and trace preserving (CPTP).
2. [Stinespring] There exist an integer n ($n = d^2$ suffices) and an isometry $W : \mathbb{C}^d \to \mathbb{C}^d \otimes \mathbb{C}^n$ such that
$$\Phi(X) = [\mathrm{id}_d \otimes \mathrm{Tr}_n](WXW^*).$$
3. [Kraus] There exist operators $A_1, \ldots, A_n \in \mathcal{M}_d(\mathbb{C})$ satisfying $\sum_i A_i^* A_i = I_d$ such that
$$\Phi(X) = \sum_{i=1}^{n} A_i X A_i^*.$$
4. [Choi] The Choi matrix C_Φ is positive semidefinite, where
$$C_\Phi := \sum_{i,j=1}^{d} E_{ij} \otimes \Phi(E_{ij}) \in \mathcal{M}_d(\mathbb{C}) \otimes \mathcal{M}_d(\mathbb{C})$$
and $[\mathrm{id} \otimes \mathrm{Tr}](C_\Phi) = I_d$.

Examples and non-examples

- The identity channel $\mathrm{id} : \mathcal{M}_d \to \mathcal{M}_d$ has the (un-normalized) Bell state as its Choi matrix

$$C_{\mathrm{id}} = \sum_{i,j=1}^{d} |ii\rangle\langle jj| = \sum_{i,j=1}^{d} e_i \otimes e_i \cdot e_j^* \otimes e_j^*.$$

- The totally depolarizing channel (or the conditional expectation on scalars) $\Delta(X) = (\operatorname{Tr} X)I/d$ has Choi matrix I_{d^2}/d
- The totally dephasing channel (or the conditional expectation on diagonal matrices) D has Kraus decomposition

$$D(\rho) = \sum_{i=1}^{d} |i\rangle\langle i|\rho|i\rangle\langle i|.$$

- The transposition $\Theta(\rho) = \rho^\top$ is **not** a quantum channel, since it is not completely positive. Its Choi matrix is $C_\Theta = F$, where F is the flip operator $Fx \otimes y = y \otimes x$. F has eigenvalues $+1$ with multiplicity $d(d+1)/2$ and -1 with multiplicity $d(d-1)/2$.

Intermezzo: block modified random matrices

- Consider a sequence of unitarily invariant random matrices $X_d \in \mathbb{M}_n \otimes \mathbb{M}_d$. Fix n and assume that, as $d \to \infty$, the matrices X_d have have limiting spectral distribution μ: $\lim_{d\to\infty} \frac{1}{nd} \sum_{i=1}^{nd} \delta_{\lambda_i(X_d)} = \mu$.
- Define the modified version of X_d:

$$X_d^f = [f \otimes \mathrm{id}_d](X_d).$$

- Our goal: compute μ^f, the limiting spectral distribution of X_d^f, as a function of the initial distribution μ and the linear functional f.

Theorem (Arizmendi, Vargas, N. '16)

If the Choi matrix C_f satisfies the unitarity condition, then

$$\mu^f = \boxplus_{i=1}^{s} (D_{\rho_i/n}\mu)^{\boxplus nd_i},$$

where ρ_i are the distinct eigenvalues of C_f and nd_i are ranks of the corresponding eigenprojectors P_i.

Unitarity condition: $\forall i$, $[\mathrm{id} \otimes \mathrm{Tr}](P_i) = d_i I_n$.

Random quantum channels

Definition

There exist several natural candidates for probability distributions on the convex set of quantum channels:

- The Lebesgue measure
- Pick the isometry W in the Stinespring decomposition at random: W is a Haar-random isometry
- Pick the Kraus operators A_i at random: G_i are i.i.d. Ginibre matrices, define $A_i = G_i S^{-1/2}$, with $S = \sum_i G_i^* G_i$
- Pick the Choi matrix at random: $\tilde{C}$ is a Wishart matrix, define $C := [I \otimes T^{-1/2}]\tilde{C}[I \otimes T^{-1/2}]^*$, with $T = [\mathrm{Tr} \otimes \mathrm{id}]\tilde{C}$.

Theorem (Kukulski, N., Pawela, Puchala, Zyczkowski '19)

The above distributions are identical, when the respective parameters match.

Computationally, the random Kraus operators procedure is the cheapest; mathematically, the random isometry procedure is the more interesting and easier to deal with.

More on the distribution of random quantum channels

- For channels $\Phi : \mathcal{M}_{d_1} \to \mathcal{M}_{d_2}$, if s is an integer parameter, then:
  - One has to take a Haar-random isometry $W; \mathbb{C}^{d_1} \to \mathbb{C}^{d_2} \otimes \mathbb{C}^s$
  - One has to take G_i i.i.d. Ginibre matrices of size $d_2 \times d_1$, for $i = 1, 2, \ldots, s$
  - One has to take the un-normalized Choi matrix $\tilde{C}$ a Wishart matrix of parameters $d_1 d_2, s$
- The density of the normalized Choi matrix reads

$$f(C) = \delta([\mathrm{id} \otimes \mathrm{Tr}](C) - I_{d_1}) \det C^{s - d_1 d_2} \mathrm{dLeb}.$$

- The Lebesgue measure is obtained for $s = d_1 d_2$.
- For any fixed pure state $P_x = xx^*$, the output matrix $\rho = \Phi(P_x)$ follows the induced distribution of parameters (d_2, s), i.e. has the distribution of a trace-normalized Wishart.
- However, different inputs yield correlated outputs!

Some notions of entropy

- Let $\Delta_k = \{\lambda \in \mathbb{R}^k \, : \, \lambda_i \geq 0, \, \sum_i \lambda_i = 1, \}$ be the probability simplex. We write $\Delta_k^{\downarrow}$ for the set of ordered probability vectors, $\lambda_1 \geq \cdots \geq \lambda_k$.
- The Shannon entropy of a probability vector $\lambda \in \Delta_k$

$$H(\lambda) = -\sum_{i=1}^{k} \lambda_i \log \lambda_i \in [0, \log k].$$

- The von Neumann entropy of $\rho \in \mathcal{M}_k^{1,+}$

$$H(\rho) = -\mathrm{Tr}(\rho \log \rho) = -\sum_{i=1}^{k} \lambda_i(\rho) \log \lambda_i(\rho).$$

- For $p \geq 0$, define the p-Rényi entropy

$$H_p(\rho) = \frac{\log \mathrm{Tr}(\rho^p)}{1-p} = \frac{\log \sum_i \lambda_i(\rho)^p}{1-p}; \qquad H(\cdot) = \lim_{p \to 1} H_p(\cdot).$$

- The entropy is additive: $H_p(\rho_1 \otimes \rho_2) = H_p(\rho_1) + H_p(\rho_2)$.

Additivity of the minimum output entropy

The minimum output entropy of a quantum channel Φ is

$$\boxed{H_p^{\min}(\Phi) := \min_{\rho \in \mathcal{M}_d^{1,+}} H_p(\Phi(\rho)).}$$

Conjecture (Amosov, Holevo and Werner '00)

The quantity $H_p^{\min}$ is additive: for any quantum channels Φ_1, Φ_2

$$H_p^{min}(\Phi_1 \otimes \Phi_2) = H_p^{min}(\Phi_1) + H_p^{min}(\Phi_2).$$

- Additivity of $H_{p=1}^{\min}$ implies a simple formula for the capacity of channels to transmit classical information; in particular, it implies the additivity of the classical capacity C.
- $C(\Phi) = \lim_{r\to\infty} \frac{\chi(\Phi^{\otimes r})}{r}$, with the Holevo quantity

$$\chi(\Phi) := \max_{p_i, \rho_i} H\Big(\sum_i p_i \Phi(\rho_i)\Big) - \sum_i p_i H(\Phi(\rho_i))$$

- Compare with the capacity of a classical channel Q:

$$C(Q) = \min_X I(X : Y) \qquad \text{where } Y = Q(X).$$

Additivity of the minimum output entropy

Conjecture (Amosov, Holevo and Werner '00)

The quantity $H_p^{\min}(\Phi) = \min_{\rho \in \mathcal{M}_d^{1,+}} H_p(\Phi(\rho))$ *is additive: for any quantum channels* Φ_1, Φ_2

$$H_p^{min}(\Phi_1 \otimes \Phi_2) = H_p^{min}(\Phi_1) + H_p^{min}(\Phi_2).$$

- Given Φ_1, Φ_2, the $\leq$ direction of the equality is trivial, take $\rho_{12} = \rho_1 \otimes \rho_2$.
- Additivity has been shown to hold for a large class of channels: unitary, unital qubit, depolarizing, dephasing, entanglement breaking, ...
- But... the Additivity Conjecture is false ! [Hayden, Winter '08 for $p > 1$, Hastings '09 for $p = 1$]
- Counterexamples: mostly random channels. Deterministic counterexamples: '02 Werner & Holevo ($p > 4.79$), '07 Cubitt et al ($p < 0.11$) and '09 Grudka et al ($p > 2$).

Stinespring dilation

Theorem (Stinespring dilation)

For any channel $: \mathcal{M}_d \to \mathcal{M}_k$ *there exists an isometry* $W : \mathbb{C}^d \to \mathbb{C}^k \otimes \mathbb{C}^n$ *such that*

$$\Phi(\rho) = [\mathrm{id}_k \otimes \mathrm{Tr}_n](W \rho W^*).$$

- By convexity properties, the minimum output entropy of Φ is attained on pure states i.e. rank one projectors $P_x = xx^* = |x\rangle\langle x|$.
- Since $\Phi(P_x) = [\mathrm{id_k} \otimes \mathrm{Tr_n}](WP_xW^*) = [\mathrm{id}_k \otimes \mathrm{Tr}_n]P_{Wx}$, the minimum output entropy of the channel Φ is

$$H^{\min}(\Phi) = \min_{x \in \mathbb{C}^d,\, \|x\|=1} H(\Phi(P_x)) = \min_{y \in \mathrm{Im} W,\, \|y\|=1} H([\mathrm{id}_k \otimes \mathrm{Tr}_n] P_y),$$

  where $V = \mathrm{Im} W \subset \mathbb{C}^k \otimes \mathbb{C}^n$ is a subspace of dimension d.
- The MOE $H^{\min}(\Phi)$ depends only on the subspace V.

Entanglement of subspaces

Eigen- and singular values

Singular value decomposition of a matrix $X \in \mathcal{M}_{k\times n}(\mathbb{C})$ ($k \le n$)

$$X = U\Sigma V^* = \sum_{i=1}^{k} \sqrt{\lambda_i(XX^*)} e_i f_i^*,$$

where e_i, f_i are orthonormal families in $\mathbb{C}^k$, $\mathbb{C}^n$, and $\lambda_1 \ge \cdots \ge \lambda_k \ge 0$ are the (squares of the) singular values of X, or the eigenvalues of XX^*.

Using the isomorphism $\mathcal{M}_{k\times n} \simeq \mathbb{C}^k \otimes \mathbb{C}^n$, X can be seen as a vector in a tensor product $x \in \mathbb{C}^k \otimes \mathbb{C}^n$. The singular value decomposition of X corresponds to the Schmidt decomposition of x

$$x = \sum_{i=1}^{k} \sqrt{\lambda_i(x)} e_i \otimes f_i.$$

The numbers $\lambda_i(x)$ are also eigenvalues of the reduced density matrix

$$XX^* = [\mathrm{id}_k \otimes \mathrm{Tr}_n] P_x = \sum_{i=1}^{k} \lambda_i(x) e_i e_i^*.$$

Entanglement of a vector

For a vector

$$x = \sum_{i=1}^{k} \sqrt{\lambda_i(x)} e_i \otimes f_i,$$

define $H(x) = H(\lambda(x)) = H(\rho) = -\sum_i \lambda_i(x) \log \lambda_i(x)$, the entropy of entanglement of the bipartite pure state x.

Note that

1. The state x is separable, $x = e \otimes f$, iff. $H(x) = 0$.
2. The state x is maximally entangled, $x = k^{-1/2} \sum_i e_i \otimes f_i$, iff. $H(x) = \log k$.

Recall that we are interested in computing

$$\begin{aligned} H^{\min}(\Phi) &= \min_{x \in \mathbb{C}^d,\, \|x\|=1} H(\Phi(P_x)) = \min_{y \in \mathrm{Im}\, W,\, \|y\|=1} H([\mathrm{id}_k \otimes \mathrm{Tr}_n] P_y) \\ &= \min_{y \in \mathrm{Im}\, W,\, \|y\|=1} H(y). \end{aligned}$$

Entanglement of a subspace

For a subspace $V \subset \mathbb{C}^k \otimes \mathbb{C}^n$, define

$$\boxed{H^{\min}(V) := \min_{y \in V,\, \|y\|=1} H(y),}$$

the minimal entanglement of vectors in V.

A subspace V is called entangled if $H^{\min}(V) > 0$, i.e. if it does not contain separable vectors $x \otimes y$.

Proposition (Parthasarathy '03)

If V is entangled, then $\dim V \leq (k-1)(n-1)$.

Example: $V_{ent} = \{x : \forall r, \sum_{i+j=r} x_{ij} = 0\}$.

Singular values of vectors from a subspace

Entropy is just a statistic, look at the set of all singular values directly !

For a subspace $V \subset \mathbb{C}^k \otimes \mathbb{C}^n$ of dimension $\dim V = d$, define the set eigen-/singular values or Schmidt coefficients

$$K_V := \{\lambda(x) : x \in V, \|x\| = 1\}.$$

$\rightsquigarrow$ Our goal is to understand K_V.

- The set K_V is a compact subset of the ordered probability simplex $\Delta_k^{\downarrow}$.
- Local invariance: $K_{(U_1 \otimes U_2)V} = K_V$, for unitary matrices $U_1 \in \mathcal{U}(k)$ and $U_2 \in \mathcal{U}(n)$.
- Monotonicity: if $V_1 \subset V_2$, then $K_{V_1} \subset K_{V_2}$.
- Recovering minimum entropies:

$$H_p^{\min}(\Phi) = H_p^{\min}(V) = \min_{\lambda \in K_V} H_p(\lambda).$$

Examples

The anti-symmetric subspace provides the (explicit) counter-example for the additivity of the p-Rényi entropy.

- Let $k = n$ and put $V = \Lambda^2(\mathbb{C}^k)$
- The subspace V is almost half of the total space: $\dim V = k(k-1)/2$.
- Example of a vector in V:

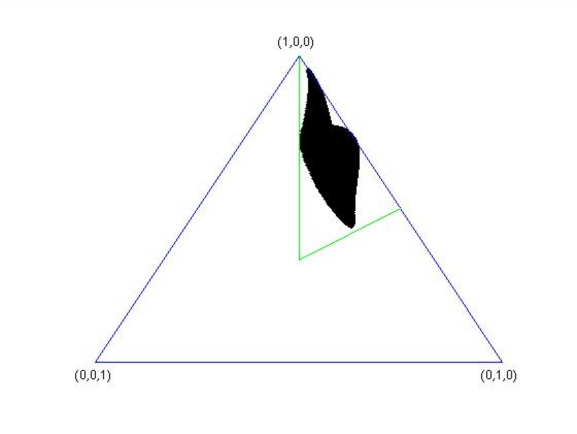
$$V \ni x = \frac{1}{\sqrt{2}}(e \otimes f - f \otimes e).$$

- Fact: singular values of vectors in V come in pairs.
- Hence, the least entropy vector in V is as above, with $e \perp f$ and $H(x) = \log 2$.
- Thus, $H^{\min}(V) = \log 2$ and one can show that

$$K_V = \{(\lambda_1, \lambda_1, \lambda_2, \lambda_2, \ldots) \in \Delta_k \,:\, \lambda_i \geq 0, \sum_i \lambda_i = 1/2\}.$$

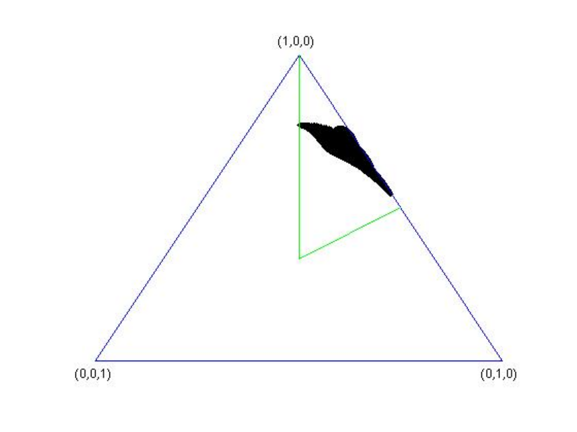
Examples

$V = \mathrm{span}\{G_1, G_2\}$, where $G_{1,2}$ are 3×3 independent Ginibre random matrices.



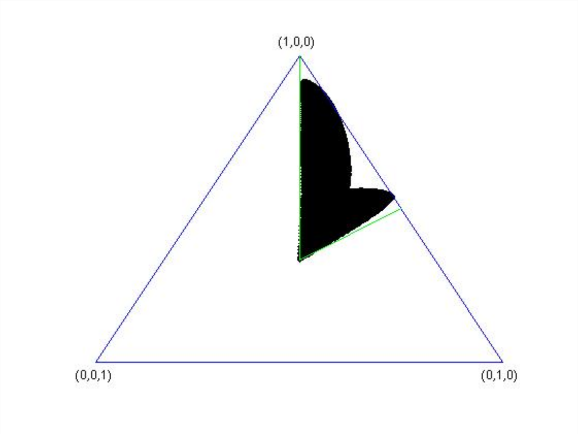
Examples

$V = \mathrm{span}\{G_1, G_2\}$, where $G_{1,2}$ are 3×3 independent Ginibre random matrices.



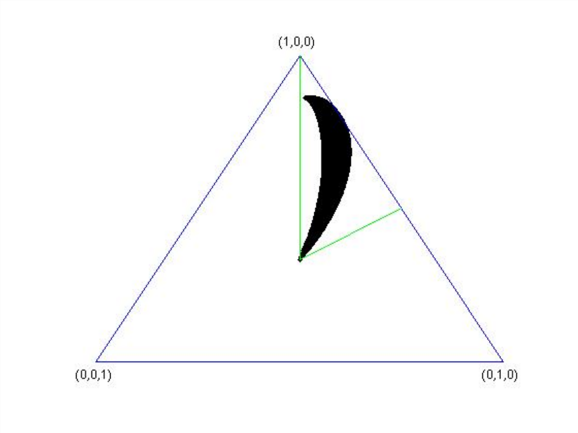
Examples

$V = \mathrm{span}\{\mathrm{I}_3, G\}$, where G is a 3×3 Ginibre random matrix.



Examples

$V = \mathrm{span}\{\mathrm{I}_3, G\}$, where G is a 3×3 Ginibre random matrix.



A big open problem

Find explicit examples of subspaces V with

1. large $\dim V$;
2. large $H^{\min}(V)$.

Random subspaces

Random subspaces

We are interested in random subspaces (or random channels).

- There is an uniform (or Haar) measure on the set of isometries $\{W : \mathbb{C}^d \to \mathbb{C}^k \otimes \mathbb{C}^n \, : \, WW^* = \mathrm{I}_d\}$: take a $kn \times kn$ Haar distributed random unitary matrix $U \in \mathcal{U}(kn)$ and take W to be the restriction of U to the first d coordinates.
- We call random quantum channels the probability distribution obtained as the push-forward of this measure through the Stinespring dilation.
- A random subspace is the image of a random isometry, $V = \mathrm{Im} W$.
- Equivalently, $V = \mathrm{span}\{U_1, \ldots, U_d\}$, where U_i are the columns of a Haar random unitary matrix $U \in \mathcal{U}(kn)$.

Main result

For the rest of the talk, we consider the following asymptotic regime: k fixed, $n \to \infty$, and $d \sim tkn$, for a fixed parameter $t \in (0,1)$.

Theorem (Belinschi, Collins, N. '10)

For a sequence of uniformly distributed random subspaces V_n, the set K_{V_n} of singular values of unit vectors from V_n converges (almost surely, in the Hausdorff distance) to a deterministic, convex subset $K_{k,t}$ of the probability simplex Δ_k

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

Corollary: exact limit of the minimum output entropy

By the previous theorem, in the specific asymptotic regime t, k fixed, $n \to \infty$, $d \sim tkn$, we have the following a.s. convergence result for random quantum channels Φ (defined via random isometries $W : \mathbb{C}^d \to \mathbb{C}^k \otimes \mathbb{C}^n$):

$$\lim_{n \to \infty} H^{\min}(\Phi) = \min_{\lambda \in K_{k,t}} H(\lambda).$$

It is not just a bound, the exact limit value is obtained.

Theorem (Belinschi, Collins, N. '13)

The minimum entropy element of $K_{k,t}$ is of the form $(a, b, b, \ldots, b)$. The lowest dimension for which a violation of the additivity for $H^{\min}$ can be observed is $k = 183$. For large k, violations of size $1 - \varepsilon$ bits can be obtained.

Free Probability Theory

Invented by Voiculescu in the 80s to solve problems in operator algebras.

- A non-commutative probability space $(\mathcal{A}, \tau)$ is an algebra $\mathcal{A}$ with a unital state $\tau : \mathcal{A} \to \mathbb{C}$. Elements $a \in \mathcal{A}$ are called random variables.
- Examples:
  - classical probability spaces $(L^\infty(\Omega, \mathcal{F}, \mathbb{P}), \mathbb{E})$;
  - group algebras $(\mathbb{C}G, \delta_e)$;
  - matrices $(\mathcal{M}_n, n^{-1}\mathrm{Tr})$;
  - random matrices $(\mathcal{M}_n(L^{\infty-}(\Omega, \mathcal{F}, \mathbb{P})), \mathbb{E} \circ n^{-1}\mathrm{Tr})$.
- Several notions of independence:
  - classical independence, implies commutativity of the random variables;
  - free independence.
- If a, b are freely independent random variables, the law of (a, b) can be computed in terms of the laws of a and b. Freeness provides an algorithm for computing joint moments in terms of marginals.
- Example: if $\{a_1, a_2\}$ and $\{b_1, b_2\}$ are free, then

$$\tau(a_1 b_1 a_2 b_2) = \tau(a_1 a_2)\tau(b_1)\tau(b_2) + \tau(a_1)\tau(a_2)\tau(b_1 b_2) - \tau(a_1)\tau(b_1)\tau(a_2)\tau(b_2).$$

Asymptotic freeness of random matrices

Theorem (Voiculescu '91)

Let (A_n) and (B_n) be sequences of $n \times n$ matrices such that A_n and B_n converge in distribution (with respect to $n^{-1}\mathrm{Tr}$) for $n \to \infty$. Furthermore, let (U_n) be a sequence of Haar unitary $n \times n$ random matrices. Then, A_n and $U_n B_n U_n^*$ are asymptotically free for $n \to \infty$.

If A_n, B_n are matrices of size n, whose spectra converge towards μ_a, μ_b, the spectrum of $A_n + U_n B_n U_n^*$ converges to $\mu_a \boxplus \mu_b$; here, $\mu_a \boxplus \mu_b$ is the distribution of $a + b$, where $a, b \in (\mathcal{A}, \tau)$ are free random variables having distributions resp. μ_a, μ_b.

If A_n, B_n are matrices of size n such that $A_n \geq 0$, whose spectra converge towards μ_a, μ_b, the spectrum of $A_n^{1/2} U_n B_n U_n^* A_n^{1/2}$ converges to $\mu_a \boxtimes \mu_b$.

Example: truncation of random matrices

Let $P_n \in \mathcal{M}_n$ a projection of rank $n/2$; its eigenvalues are 0 and 1, with multiplicity $n/2$. Hence, the distribution of P_n converges, when $n \to \infty$, to the Bernoulli probability measure $\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1$.

Let $C_n \in \mathcal{M}_{n/2}$ be the top $n/2 \times n/2$ corner of $U_n P_n U_n^*$, with U_n a Haar random unitary matrix. What is the distribution of C_n ? Up to zero blocks, $C_n = Q_n(U_n P_n U_n^*)Q_n$, where Q_n is the diagonal orthogonal projection on the first $n/2$ coordinates of $\mathbb{C}^n$. The distribution of Q_n converges to $\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1$.

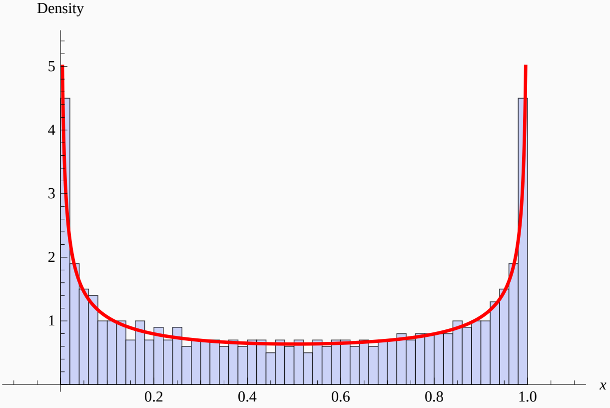
Free probability theory tells us that the distribution of C_n will converge to

$$(\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1) \boxtimes (\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1) = \frac{1}{\pi\sqrt{x(1-x)}}\mathbf{1}_{[0,1]}(x)dx,$$

which is the arcsine distribution.

Example: truncation of random matrices

Histogram of eigenvalues of a truncated randomly rotated projector of relative rank $1/2$ and size $n = 4000$; in red, the density of the arcsine distribution.



The t-norm

Definition

For a positive integer k, embed $\mathbb{R}^k$ as a self-adjoint real subalgebra $\mathcal{R}$ of a C^*-ncps $(\mathcal{A}, \tau)$, so that $\tau(x) = (x_1 + \cdots + x_k)/k$. Let p_t be a projection of rank $t \in (0, 1]$ in $\mathcal{A}$, free from $\mathcal{R}$. On the real vector space $\mathbb{R}^k$, we introduce the following norm, called the (t)-norm:

$$\|x\|_{(t)} := \|p_t x p_t\|_\infty,$$

where the vector $x \in \mathbb{R}^k$ is identified with its image in $\mathcal{R}$.

- One can show that $\| \cdot \|_{(t)}$ is indeed a norm, which is permutation invariant.
- When $t > 1 - 1/k$, $\| \cdot \|_{(t)} = \| \cdot \|_\infty$ on $\mathbb{R}^k$.
- $\lim_{t \to 0^+} \|x\|_{(t)} = k^{-1} |\sum_i x_i|$.

Corners of randomly rotated projections

Theorem (Collins '05)

In $\mathbb{C}^n$, choose at random according to the Haar measure two independent subspaces V_n and V_n' of respective dimensions $q_n \sim sn$ and $q_n' \sim tn$ where $s, t \in (0,1]$. Let P_n (resp. P_n') be the orthogonal projection onto V_n (resp. V_n'). Then,

$$\lim_n \|P_n P_n' P_n\|_\infty = \varphi(s,t) = \sup \operatorname{supp}((1-s)\delta_0 + s\delta_1) \boxtimes ((1-t)\delta_0 + t\delta_1),$$

with

$$\varphi(s,t) = \begin{cases} s + t - 2st + 2\sqrt{st(1-s)(1-t)} & \text{if } s + t < 1; \\ 1 & \text{if } s + t \geq 1. \end{cases}$$

Hence, we can compute

$$\|\underbrace{1, \cdots, 1}_{j \text{ times}}, \underbrace{0, \cdots, 0}_{k-j \text{ times}}\|_{(t)} = \varphi(\frac{j}{k}, t).$$

Idea of the proof

A simpler question: what is the largest maximal singular value $\max_{x \in V, \|x\|=1} \lambda_1(x)$ of vectors from the subspace V ?

$$\begin{aligned}
\max_{x \in V, \|x\|=1} \lambda_1(x) &= \max_{x \in V, \|x\|=1} \lambda_1([\mathrm{id}_k \otimes \mathrm{Tr}_n] P_x) \\
&= \max_{x \in V, \|x\|=1} \|[\mathrm{id}_k \otimes \mathrm{Tr}_n] P_x\| \\
&= \max_{x \in V, \|x\|=1} \max_{y \in \mathbb{C}^k, \|y\|=1} \mathrm{Tr}\left[([\mathrm{id}_k \otimes \mathrm{Tr}_n] P_x) \cdot P_y\right] \\
&= \max_{x \in V, \|x\|=1} \max_{y \in \mathbb{C}^k, \|y\|=1} \mathrm{Tr}\left[P_x \cdot P_y \otimes \mathrm{I}_n\right] \\
&= \max_{y \in \mathbb{C}^k, \|y\|=1} \max_{x \in V, \|x\|=1} \mathrm{Tr}\left[P_x \cdot P_y \otimes \mathrm{I}_n\right] \\
&= \max_{y \in \mathbb{C}^k, \|y\|=1} \|P_V \cdot P_y \otimes \mathrm{I}_n\|_\infty .
\end{aligned}$$

Limit of $\|P_V \cdot P_y \otimes \mathrm{I}_n\|_\infty$ for fixed y and random V ?

The set $K_{k,t}$ and t-norms

- $K_{k,t} := \{\lambda \in \Delta_k \mid \forall x \in \Delta_k, \langle \lambda, x \rangle \leq \|x\|_{(t)}\}$.
- Recall that

$$\max_{x \in V, \|x\|=1} \lambda_1(x) = \max_{y \in \mathbb{C}^k, \|y\|=1} \|P_V P_y \otimes \mathrm{I}_n\|_\infty .$$

- For fixed y, P_V and $P_y \otimes \mathrm{I}_n$ are independent projectors of relative ranks t and $1/k$ respectively.
- Thus, $\|P_V \cdot P_y \otimes \mathrm{I}_n\|_\infty \to \varphi(t, 1/k) = \|(1, 0, \ldots, 0)\|_{(t)}$.
- We can take the max over y at no cost, by considering a finite net of y's, since k is fixed.
- To get the full result $\limsup_{n\to\infty} K_{V_n} \subset K_{k,t}$, use $\langle \lambda, x \rangle$ (for all directions x) instead of λ_1.

The take-home slide

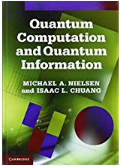
States	Deterministic	Random mixture
Classical	$x \in \{1, 2, \ldots, d\}$	$p \in \mathbb{R}^d$, $p_i \geq 0$, $\sum_i p_i = 1$
Quantum	$\psi \in \mathbb{C}^d$, $\|\psi\| = 1$	$\rho \in \mathcal{M}_d(\mathbb{C})$, $\rho \geq 0$, $\operatorname{Tr} \rho = 1$

- Random quantum states: $\rho = W / \operatorname{Tr} W$, with W a Wishart matrix.
- Used e.g. to test the power of entanglement criteria, such as the partial transposition $[\mathrm{id} \otimes \Theta](\rho_{AB})$.

Channels	Deterministic	Random mixture
Classical	$f \in \mathcal{S}_d$	Q Markov: $Q_{ij} \geq 0$ and $\forall i$, $\sum_j Q_{ij} = 1$
Quantum	$U \in \mathcal{U}(d)$	Φ CPTP map

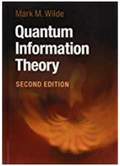
- Random quantum channels: Stinesrping dilation $\Phi(\rho) = [\mathrm{id} \otimes \operatorname{Tr}](V \rho V^*)$ for a Haar-random isometry $V : \mathbb{C}^d \to \mathbb{C}^k \otimes \mathbb{C}^n$.
- Used e.g. to disprove the additivity conjecture: $H^{\min}(\Phi \otimes \Psi) = H^{\min}(\Phi) + H^{\min}(\Psi)$.

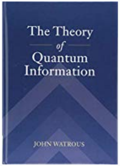
To go further - books



Nielsen, M., Chuang, I.
Quantum computation and quantum information
Cambridge University Press (2010)

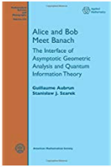
Wilde, M.
Quantum information theory
Cambridge University Press (2017)





Watrous, J.
The theory of quantum information
Cambridge University Press (2018)

Aubrun, G., Szarek, S. J.
Alice and Bob meet Banach
Mathematical Surveys and Monographs 105 (2018)



Merci!