Entanglement of random subspaces

Ion Nechita

CNRS, Université de Toulouse

joint work with
Serban Belinschi (Queen's) and Benoit Collins (uOttawa)

Autrans, July 16th 2013

Outline of the talk

1. Additivity problems in QIT
   - Quantum states and channels
   - The additivity problem
   - From channels to subspaces
2. Entanglement of subspaces
   - Singular values of matrices / bipartite vectors
   - Minimal entanglement vs. MOE
   - The set K_V
3. Random subspaces
   - Statement of the main result and applications
   - Free probability - a review
   - Sketch of the proof

States and channels in quantum information theory

- Quantum states with n degrees of freedom are described by density matrices

$$\rho \in \mathbb{M}_n^{1,+} = \mathrm{End}^{1,+}(\mathbb{C}^n); \qquad \mathrm{Tr}\rho = 1 \text{ and } \rho \geq 0.$$

States and channels in quantum information theory

- Quantum states with n degrees of freedom are described by density matrices

$$\rho \in \mathbb{M}_n^{1,+} = \mathrm{End}^{1,+}(\mathbb{C}^n); \qquad \mathrm{Tr}\rho = 1 \text{ and } \rho \geq 0.$$

- Pure states are rank-one projectors $\rho = xx^* = P_x$, with $x \in \mathbb{C}^n$, $\|x\| = 1$.

States and channels in quantum information theory

- Quantum states with n degrees of freedom are described by density matrices

$$\rho \in \mathbb{M}_n^{1,+} = \mathrm{End}^{1,+}(\mathbb{C}^n); \qquad \mathrm{Tr}\rho = 1 \text{ and } \rho \geq 0.$$

- Pure states are rank-one projectors $\rho = xx^* = P_x$, with $x \in \mathbb{C}^n$, $\|x\| = 1$.
- Two quantum systems: $\rho_{12} \in \mathrm{End}^{1,+}(\mathbb{C}^m \otimes \mathbb{C}^n) = \mathbb{M}_{mn}^{1,+}$.

States and channels in quantum information theory

- Quantum states with n degrees of freedom are described by density matrices

$$\rho \in \mathbb{M}_n^{1,+} = \mathrm{End}^{1,+}(\mathbb{C}^n); \qquad \mathrm{Tr}\rho = 1 \text{ and } \rho \geq 0.$$

- Pure states are rank-one projectors $\rho = xx^* = P_x$, with $x \in \mathbb{C}^n$, $\|x\| = 1$.
- Two quantum systems: $\rho_{12} \in \mathrm{End}^{1,+}(\mathbb{C}^m \otimes \mathbb{C}^n) = \mathbb{M}_{mn}^{1,+}$.
- Quantum channels $F : \mathbb{M}_d^{1,+} \to \mathbb{M}_k^{1,+}$ are completely positive, trace-preserving maps. In particular, they send quantum states to quantum states.

States and channels in quantum information theory

- Quantum states with n degrees of freedom are described by density matrices

$$\rho \in \mathbb{M}_n^{1,+} = \mathrm{End}^{1,+}(\mathbb{C}^n); \qquad \mathrm{Tr}\rho = 1 \text{ and } \rho \geq 0.$$

- Pure states are rank-one projectors $\rho = xx^* = P_x$, with $x \in \mathbb{C}^n$, $\|x\| = 1$.
- Two quantum systems: $\rho_{12} \in \mathrm{End}^{1,+}(\mathbb{C}^m \otimes \mathbb{C}^n) = \mathbb{M}_{mn}^{1,+}$.
- Quantum channels $F : \mathbb{M}_d^{1,+} \to \mathbb{M}_k^{1,+}$ are completely positive, trace-preserving maps. In particular, they send quantum states to quantum states.
    - Complete positivity CP: $F \otimes \mathrm{id}_s$ preserves positivity, for all s.

States and channels in quantum information theory

- Quantum states with n degrees of freedom are described by density matrices

$$\rho \in \mathbb{M}_n^{1,+} = \mathrm{End}^{1,+}(\mathbb{C}^n); \qquad \mathrm{Tr}\rho = 1 \text{ and } \rho \geq 0.$$

- Pure states are rank-one projectors $\rho = xx^* = P_x$, with $x \in \mathbb{C}^n$, $\|x\| = 1$.
- Two quantum systems: $\rho_{12} \in \mathrm{End}^{1,+}(\mathbb{C}^m \otimes \mathbb{C}^n) = \mathbb{M}_{mn}^{1,+}$.
- Quantum channels $F : \mathbb{M}_d^{1,+} \to \mathbb{M}_k^{1,+}$ are completely positive, trace-preserving maps. In particular, they send quantum states to quantum states.
  - Complete positivity CP: $F \otimes \mathrm{id}_s$ preserves positivity, for all s.
  - Trace preservation TP: $\mathrm{Tr}[F(X)] = \mathrm{Tr}(X)$ for all X.

States and channels in quantum information theory

- Quantum states with n degrees of freedom are described by density matrices

$$\rho \in \mathbb{M}_n^{1,+} = \mathrm{End}^{1,+}(\mathbb{C}^n); \qquad \mathrm{Tr}\rho = 1 \text{ and } \rho \geq 0.$$

- Pure states are rank-one projectors $\rho = xx^* = P_x$, with $x \in \mathbb{C}^n$, $\|x\| = 1$.
- Two quantum systems: $\rho_{12} \in \mathrm{End}^{1,+}(\mathbb{C}^m \otimes \mathbb{C}^n) = \mathbb{M}_{mn}^{1,+}$.
- Quantum channels $F : \mathbb{M}_d^{1,+} \to \mathbb{M}_k^{1,+}$ are completely positive, trace-preserving maps. In particular, they send quantum states to quantum states.
  - Complete positivity CP: $F \otimes \mathrm{id}_s$ preserves positivity, for all s.
  - Trace preservation TP: $\mathrm{Tr}[F(X)] = \mathrm{Tr}(X)$ for all X.
- Examples: $F_U(X) = UXU^*$, $F_{dep}(X) = \mathrm{Tr}(X)I_k/k$.

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 $\lambda \in \Delta_k$

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

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 $X \in \mathbb{M}_k^{1,+}$

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

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 $X \in \mathbb{M}_k^{1,+}$

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

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

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

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 $X \in \mathbb{M}_k^{1,+}$

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

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

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

- The entropy is additive: $H_p(X_1 \otimes X_2) = H_p(X_1) + H_p(X_2)$.

Additivity of the minimum output entropy

The minimum output entropy of a quantum channel F is

$$\boxed{H_p^{\min}(F) = \min_{X \in \mathbb{M}_d^{1,+}} H_p(F(X)).}$$

Additivity of the minimum output entropy

The minimum output entropy of a quantum channel F is

$$\boxed{H_p^{\min}(F) = \min_{X \in \mathbb{M}_d^{1,+}} H_p(F(X)).}$$

Conjecture (Amosov, Holevo and Werner '00)

The quantity $H_p^{\min}$ is additive: for any quantum channels F_1, F_2

$$H_p^{min}(F_1 \otimes F_2) = H_p^{min}(F_1) + H_p^{min}(F_2).$$

Additivity of the minimum output entropy

The minimum output entropy of a quantum channel F is

$$\boxed{H_p^{\min}(F) = \min_{X \in \mathbb{M}_d^{1,+}} H_p(F(X)).}$$

Conjecture (Amosov, Holevo and Werner '00)

The quantity $H_p^{\min}$ is additive: for any quantum channels F_1, F_2

$$H_p^{min}(F_1 \otimes F_2) = H_p^{min}(F_1) + H_p^{min}(F_2).$$

- 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. Moreover, it is equivalent to the additivity of the Holevo capacity and the additivity of the entanglement of formation

Additivity of the minimum output entropy

Conjecture (Amosov, Holevo and Werner '00)

The quantity $H_p^{\min}(F) = \min_{X \in \mathbb{M}_d^{1,+}} H_p(F(X))$ *is additive: for any quantum channels* F_1, F_2

$$H_p^{min}(F_1 \otimes F_2) = H_p^{min}(F_1) + H_p^{min}(F_2).$$

Additivity of the minimum output entropy

Conjecture (Amosov, Holevo and Werner '00)

The quantity $H_p^{\min}(F) = \min_{X \in \mathbb{M}_d^{1,+}} H_p(F(X))$ *is additive: for any quantum channels* F_1, F_2

$$H_p^{min}(F_1 \otimes F_2) = H_p^{min}(F_1) + H_p^{min}(F_2).$$

- Given F_1, F_2, the $\leq$ direction of the equality is trivial, take $X_{12} = X_1 \otimes X_2$.

Additivity of the minimum output entropy

Conjecture (Amosov, Holevo and Werner '00)

The quantity $H_p^{\min}(F) = \min_{X \in \mathbb{M}_d^{1,+}} H_p(F(X))$ *is additive: for any quantum channels* F_1, F_2

$$H_p^{min}(F_1 \otimes F_2) = H_p^{min}(F_1) + H_p^{min}(F_2).$$

- Given F_1, F_2, the $\leq$ direction of the equality is trivial, take $X_{12} = X_1 \otimes X_2$.
- Additivity has been shown to hold for a large class of channels: unitary, unital qubit, depolarizing, dephasing, entanglement breaking, ...

Additivity of the minimum output entropy

Conjecture (Amosov, Holevo and Werner '00)

The quantity $H_p^{\min}(F) = \min_{X \in \mathbb{M}_d^{1,+}} H_p(F(X))$ is additive: for any quantum channels F_1, F_2

$$H_p^{min}(F_1 \otimes F_2) = H_p^{min}(F_1) + H_p^{min}(F_2).$$

- Given F_1, F_2, the $\leq$ direction of the equality is trivial, take $X_{12} = X_1 \otimes X_2$.
- 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 $p = 1$]

Additivity of the minimum output entropy

Conjecture (Amosov, Holevo and Werner '00)

The quantity $H_p^{\min}(F) = \min_{X \in \mathbb{M}_d^{1,+}} H_p(F(X))$ *is additive: for any quantum channels* F_1, F_2

$$H_p^{min}(F_1 \otimes F_2) = H_p^{min}(F_1) + H_p^{min}(F_2).$$

- Given F_1, F_2, the $\leq$ direction of the equality is trivial, take $X_{12} = X_1 \otimes X_2$.
- 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 $F : \mathbb{M}_d \to \mathbb{M}_k$ *there exists an isometry* $W : \mathbb{C}^d \to \mathbb{C}^k \otimes \mathbb{C}^n$ *such that*

$$F(X) = [\mathrm{id}_k \otimes \mathrm{Tr}_n](WXW^*).$$

Stinespring dilation

Theorem (Stinespring dilation)

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

$$F(X) = [\mathrm{id}_k \otimes \mathrm{Tr}_n](WXW^*).$$

- By convexity properties, the minimum output entropy of F is attained on pure states i.e. rank one projectors.

Stinespring dilation

Theorem (Stinespring dilation)

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

$$F(X) = [\mathrm{id}_k \otimes \mathrm{Tr}_n](WXW^*).$$

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

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

where $V = \mathrm{Im} W \subset \mathbb{C}^k \otimes \mathbb{C}^n$ is a subspace of dimension d.

Stinespring dilation

Theorem (Stinespring dilation)

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

$$F(X) = [\mathrm{id}_k \otimes \mathrm{Tr}_n](WXW^*).$$

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

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

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

Eigen- and singular values

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

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

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

Eigen- and singular values

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

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

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

Using the isomorphism $\mathbb{M}_{k \times n} \simeq \mathbb{C}^k \otimes \mathbb{C}^n$, X can be seen as a vector in a tensor product $x \in \mathbb{C}^k \otimes \mathbb{C}^n$.

Eigen- and singular values

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

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

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

Using the isomorphism $\mathbb{M}_{k \times n} \simeq \mathbb{C}^k \otimes \mathbb{C}^n$, 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

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

Eigen- and singular values

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

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

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

Using the isomorphism $\mathbb{M}_{k\times n} \simeq \mathbb{C}^k \otimes \mathbb{C}^n$, 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.

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. $H(x) = \log k$.

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.

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. $H(x) = \log k$.

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

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

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.

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 $x \otimes y$.

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 $\dim V \leq (k-1)(n-1)$.

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

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

Singular values of vectors from a subspace

Our idea: 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

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

Singular values of vectors from a subspace

Our idea: 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

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

$\rightsquigarrow$ Our goal is to understand K_V.

Singular values of vectors from a subspace

Our idea: 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

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

$\rightsquigarrow$ Our goal is to understand K_V.

- The set K_V is a compact subset of the ordered probability simplex $\Delta_k^{\downarrow}$.

Singular values of vectors from a subspace

Our idea: 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

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

$\rightsquigarrow$ 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 $U_2 \in \mathcal{U}(n)$.

Singular values of vectors from a subspace

Our idea: 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

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

$\rightsquigarrow$ 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 $K_{V_1} \subset K_{V_2}$.

Singular values of vectors from a subspace

Our idea: 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

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

$\rightsquigarrow$ 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:

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

Examples

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

Examples

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

- Let $k = n$ and put $V = \Lambda^2(\mathbb{C}^k)$

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: $\dim V = k(k-1)/2$.

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:

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

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.

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 $H(x) = \log 2$.

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:

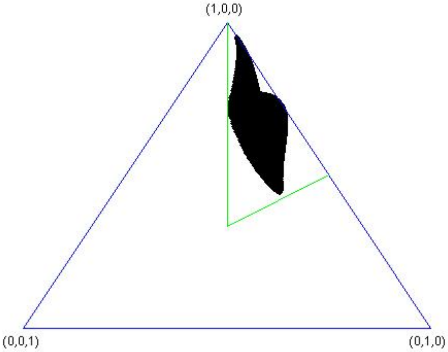
$$V \ni x = \frac{1}{\sqrt{2}}(e \otimes f - f \otimes e).$$

- 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

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

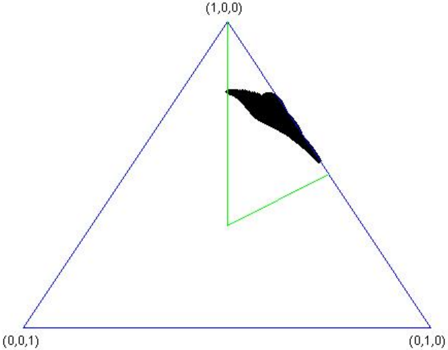
Examples

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



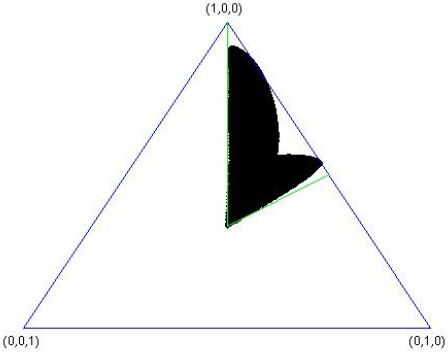
Examples

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



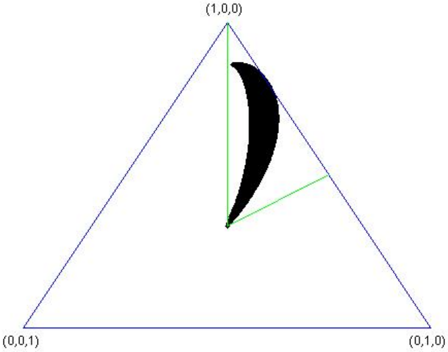
Examples

$V = \mathrm{span}\{\mathrm{I}_3, G\}$, 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

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

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.

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.

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, $V = \mathrm{Im} W$.

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 $t \in (0, 1)$.

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

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

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 F (defined via random isometries $W : \mathbb{C}^d \to \mathbb{C}^k \otimes \mathbb{C}^n$):

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

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

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 F (defined via random isometries $W : \mathbb{C}^d \to \mathbb{C}^k \otimes \mathbb{C}^n$):

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

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.

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.

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 $(\mathbb{M}_n, n^{-1}\mathrm{Tr})$;
  - random matrices $(\mathbb{M}_n(L^\infty(\Omega, \mathcal{F}, \mathbb{P})), \mathbb{E} \circ n^{-1}\mathrm{Tr})$.

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 $(\mathbb{M}_n, n^{-1}\mathrm{Tr})$;
  - random matrices $(\mathbb{M}_n(L^\infty(\Omega, \mathcal{F}, \mathbb{P})), \mathbb{E} \circ n^{-1}\mathrm{Tr})$.
- Several notions of independence:
  - classical independence, implies commutativity of the radom variables;
  - free independence.

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 $(\mathbb{M}_n, n^{-1}\mathrm{Tr})$;
  - random matrices $(\mathbb{M}_n(L^\infty(\Omega, \mathcal{F}, \mathbb{P})), \mathbb{E} \circ n^{-1}\mathrm{Tr})$.
- Several notions of independence:
  - classical independence, implies commutativity of the radom 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.

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 $(\mathbb{M}_n, n^{-1}\mathrm{Tr})$;
  - random matrices $(\mathbb{M}_n(L^\infty(\Omega, \mathcal{F}, \mathbb{P})), \mathbb{E} \circ n^{-1}\mathrm{Tr})$.
- Several notions of independence:
  - classical independence, implies commutativity of the radom 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 $n \to \infty$.

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.

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 $P_n \in \mathbb{M}_n$ 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 $\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1$.

Example: truncation of random matrices

Let $P_n \in \mathbb{M}_n$ 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 $C_n \in \mathbb{M}_{n/2}$ 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 ?

Example: truncation of random matrices

Let $P_n \in \mathbb{M}_n$ 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 $C_n \in \mathbb{M}_{n/2}$ 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 $\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1$.

Example: truncation of random matrices

Let $P_n \in \mathbb{M}_n$ 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 $C_n \in \mathbb{M}_{n/2}$ 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 $\frac{1}{2}\delta_0 + \frac{1}{2}\delta_1$.

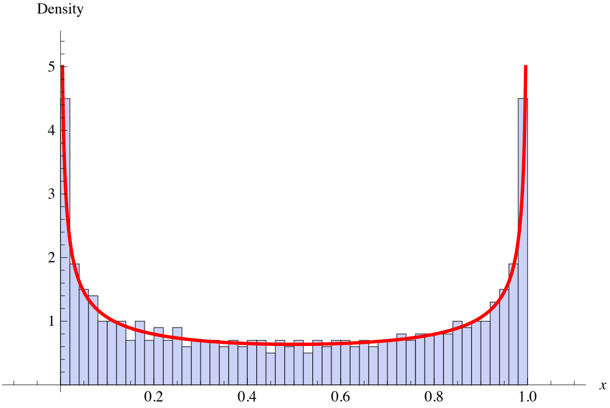
Free probability theory tells us that the distribution of C_n will converge to

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

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 $\mathcal{R}$.

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.

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 $\mathbb{R}^k$.

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 ?

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 ?

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

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

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

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

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

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.

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, $\|P_V \cdot P_y \otimes \mathrm{I}_n\|_\infty \to \varphi(t, 1/k) = \|(1, 0, \ldots, 0)\|_{(t)}$.

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.

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.

Thank you!

Collins, N. - *Random quantum channels II: Entanglement of random subspaces, Rényi entropy estimates and additivity problems*.

Belinschi, Collins, N. - *Laws of large numbers for eigenvectors and eigenvalues associated to random subspaces in a tensor product*.

Belinschi, Collins, N. - *Almost one bit violation for the additivity of the minimum output entropy*.