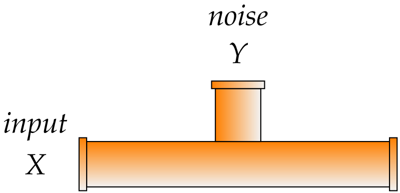
Entropy power inequalities for qudits

Māris Ozols
University of Cambridge

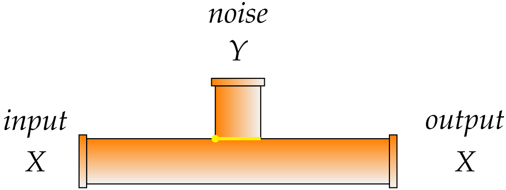
Nilanjana Datta
University of Cambridge

Koenraad Audenaert
Royal Holloway & Ghent

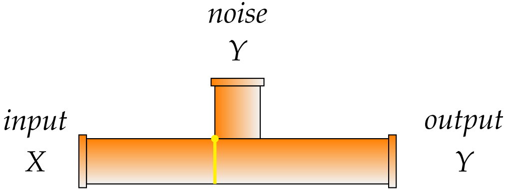
Additive noise channel



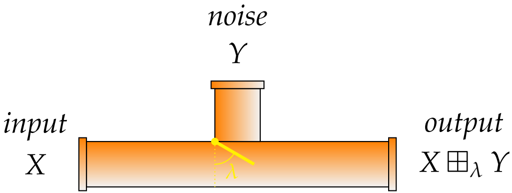
Additive noise channel



Additive noise channel

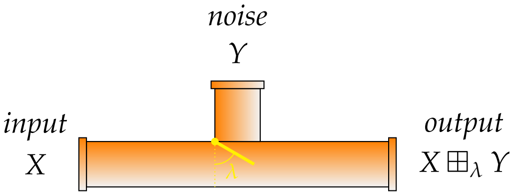


Additive noise channel



$\lambda \in [0, 1]$ – how much of the signal gets through

Additive noise channel



$\lambda \in [0,1]$ – how much of the signal gets through

How noisy is the output?

$$H(X \boxplus_\lambda Y) \overset{?}{\geq} \lambda H(X) + (1-\lambda) H(Y)$$

Prototypic entropy power inequality...

Entropy power inequalities

	Classical	Quantum
Continuous	Shannon [Sha48]	Koenig & Smith [KS14, DMG14]
Discrete	—	This work

Entropy power inequalities

	Classical	Quantum
Continuous	Shannon [Sha48]	Koenig & Smith [KS14, DMG14]
Discrete	—	This work

$$f(\rho \boxplus_\lambda \sigma) \geq \lambda f(\rho) + (1-\lambda) f(\sigma)$$

Entropy power inequalities

	Classical	Quantum
Continuous	Shannon [Sha48]	Koenig & Smith [KS14, DMG14]
Discrete	—	This work

$$f(\rho \boxplus_\lambda \sigma) \geq \lambda f(\rho) + (1-\lambda) f(\sigma)$$

- ρ, σ are distributions / states
- $f(\cdot)$ is an entropic function such as $H(\cdot)$ or $e^{cH(\cdot)}$
- $\rho \boxplus_\lambda \sigma$ interpolates between ρ and σ where $\lambda \in [0,1]$

Entropy power inequalities

	Classical	Quantum
Continuous	Shannon [Sha48] $\boxplus =$ *convolution*	Koenig & Smith [KS14, DMG14] $\boxplus =$ *beamsplitter*
Discrete	—	This work $\boxplus =$ *partial swap*

$$f(\rho \boxplus_\lambda \sigma) \geq \lambda f(\rho) + (1-\lambda) f(\sigma)$$

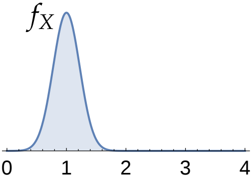
- ρ, σ are distributions / states
- $f(\cdot)$ is an entropic function such as $H(\cdot)$ or $e^{cH(\cdot)}$
- $\rho \boxplus_\lambda \sigma$ interpolates between ρ and σ where $\lambda \in [0,1]$

Classical EPI

Continuous random variables

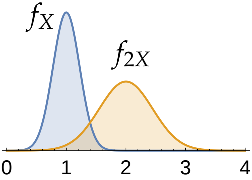
- X is a random variable over $\mathbb{R}^d$ with prob. density function

$$f_X : \mathbb{R}^d \to [0, \infty) \quad \text{s.t.} \quad \int_{\mathbb{R}^d} f_X(x)dx = 1$$



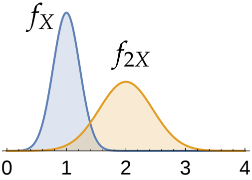
Continuous random variables

- X is a random variable over $\mathbb{R}^d$ with prob. density function
$$f_X : \mathbb{R}^d \to [0, \infty) \quad \text{s.t.} \quad \int_{\mathbb{R}^d} f_X(x)dx = 1$$
- αX is X scaled by α:

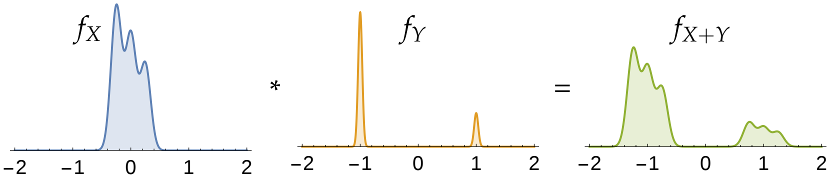


Continuous random variables

- X is a random variable over $\mathbb{R}^d$ with prob. density function
$$f_X : \mathbb{R}^d \to [0, \infty) \quad \text{s.t.} \quad \int_{\mathbb{R}^d} f_X(x)dx = 1$$
- αX is X scaled by α:



- prob. density of $X + Y$ is the convolution of f_X and f_Y:



Classical EPI for continuous variables

- Scaled addition:

$$X \boxplus_\lambda Y := \sqrt{\lambda}\, X + \sqrt{1-\lambda}\, Y$$

Classical EPI for continuous variables

- Scaled addition:

$$X \boxplus_\lambda Y := \sqrt{\lambda}\, X + \sqrt{1-\lambda}\, Y$$

- Shannon's EPI [Sha48]:

$$f(X \boxplus_\lambda Y) \geq \lambda f(X) + (1-\lambda) f(Y)$$

where $f(\cdot)$ is $H(\cdot)$ or $e^{2H(\cdot)/d}$ (equivalent)

Classical EPI for continuous variables

- Scaled addition:

$$X \boxplus_\lambda Y := \sqrt{\lambda}\, X + \sqrt{1-\lambda}\, Y$$

- Shannon's EPI [Sha48]:

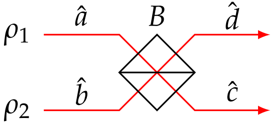
$$f(X \boxplus_\lambda Y) \geq \lambda f(X) + (1-\lambda) f(Y)$$

  where $f(\cdot)$ is $H(\cdot)$ or $e^{2H(\cdot)/d}$ (equivalent)
- Proof via Fisher info & de Bruijn's identity [Sta59, Bla65]
- Applications:
  - upper bounds on channel capacity [Ber74]
  - strengthening of the central limit theorem [Bar86]
  - …

Quantum EPI

Beamsplitter

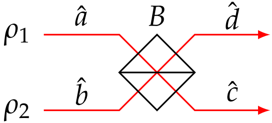
- Action on field operators:



$$B \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} = \begin{pmatrix} \hat{c} \\ \hat{d} \end{pmatrix} \qquad B \in \mathrm{U}(2)$$

Beamsplitter

- Action on field operators:



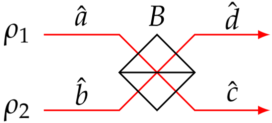
$$B \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} = \begin{pmatrix} \hat{c} \\ \hat{d} \end{pmatrix} \qquad B \in \mathrm{U}(2)$$

- Transmissivity λ:

$$B_\lambda := \sqrt{\lambda}\, I + i\sqrt{1-\lambda}\, X \qquad \Rightarrow \qquad U_\lambda \in \mathrm{U}(\mathcal{H} \otimes \mathcal{H})$$

Beamsplitter

- Action on field operators:



$$B \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} = \begin{pmatrix} \hat{c} \\ \hat{d} \end{pmatrix} \qquad B \in \mathrm{U}(2)$$

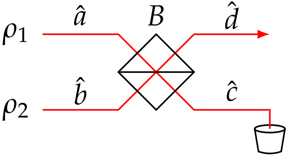
- Transmissivity λ:

$$B_\lambda := \sqrt{\lambda}\, I + i\sqrt{1-\lambda}\, X \qquad \Rightarrow \qquad U_\lambda \in \mathrm{U}(\mathcal{H} \otimes \mathcal{H})$$

- Output state:

$$U_\lambda(\rho_1 \otimes \rho_2)U_\lambda^\dagger$$

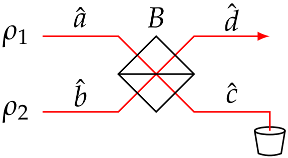
Continuous-variable quantum EPI



- Combining two states:

$$\rho_1 \boxplus_\lambda \rho_2 := \mathrm{Tr}_2\big(U_\lambda(\rho_1 \otimes \rho_2)U_\lambda^\dagger\big)$$

Continuous-variable quantum EPI



- Combining two states:

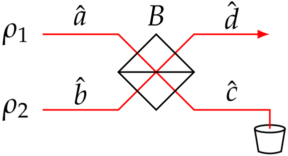
$$\rho_1 \boxplus_\lambda \rho_2 := \mathrm{Tr}_2\big(U_\lambda(\rho_1 \otimes \rho_2)U_\lambda^\dagger\big)$$

- Quantum EPI [KS14, DMG14]:

$$f(\rho_1 \boxplus_\lambda \rho_2) \geq \lambda f(\rho_1) + (1-\lambda) f(\rho_2)$$

where $f(\cdot)$ is $H(\cdot)$ or $e^{H(\cdot)/d}$ (*not* known to be equivalent)

Continuous-variable quantum EPI



- Combining two states:

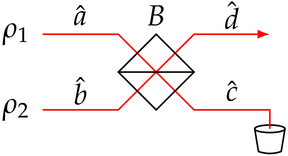
$$\rho_1 \boxplus_\lambda \rho_2 := \mathrm{Tr}_2\big(U_\lambda(\rho_1 \otimes \rho_2)U_\lambda^\dagger\big)$$

- Quantum EPI [KS14, DMG14]:

$$f(\rho_1 \boxplus_\lambda \rho_2) \geq \lambda f(\rho_1) + (1-\lambda) f(\rho_2)$$

  where $f(\cdot)$ is $H(\cdot)$ or $e^{H(\cdot)/d}$ (*not* known to be equivalent)
- Analogue, not a generalization

Continuous-variable quantum EPI



- Combining two states:

$$\rho_1 \boxplus_\lambda \rho_2 := \mathrm{Tr}_2\big(U_\lambda(\rho_1 \otimes \rho_2)U_\lambda^\dagger\big)$$

- Quantum EPI [KS14, DMG14]:

$$f(\rho_1 \boxplus_\lambda \rho_2) \geq \lambda f(\rho_1) + (1-\lambda) f(\rho_2)$$

  where $f(\cdot)$ is $H(\cdot)$ or $e^{H(\cdot)/d}$ (*not* known to be equivalent)
- Analogue, not a generalization
- Proof similar to the classical case (quantum generalizations of Fisher information & de Bruijn's identity)

Qudit EPI

Partial swap

- Swap: $S|i,j\rangle = |j,i\rangle$ for all $i,j \in \{1,\ldots,d\}$

Partial swap

- Swap: $S|i,j\rangle = |j,i\rangle$ for all $i,j \in \{1,\ldots,d\}$
- Use S as a Hamiltonian: $\exp(itS) = \cos t\, I + i \sin t\, S$

Partial swap

- Swap: $S|i,j\rangle = |j,i\rangle$ for all $i,j \in \{1,\ldots,d\}$
- Use S as a Hamiltonian: $\exp(itS) = \cos t\, I + i \sin t\, S$
- Partial swap:

$$U_\lambda := \sqrt{\lambda}\, I + i\sqrt{1-\lambda}\, S, \quad \lambda \in [0,1]$$

Partial swap

- Swap: $S|i,j\rangle = |j,i\rangle$ for all $i,j \in \{1,\dots,d\}$
- Use S as a Hamiltonian: $\exp(itS) = \cos t\, I + i \sin t\, S$
- Partial swap:

$$U_\lambda := \sqrt{\lambda}\, I + i\sqrt{1-\lambda}\, S, \quad \lambda \in [0,1]$$

- Combining two qudits:

$$\begin{aligned} \rho_1 \boxplus_\lambda \rho_2 :=\ & \mathrm{Tr}_2\big(U_\lambda(\rho_1 \otimes \rho_2)U_\lambda^\dagger\big) \\ &= \lambda\rho_1 + (1-\lambda)\rho_2 - \sqrt{\lambda(1-\lambda)}\, i[\rho_1,\rho_2] \end{aligned}$$

Partial swap

- Swap: $S|i,j\rangle = |j,i\rangle$ for all $i,j \in \{1,\ldots,d\}$
- Use S as a Hamiltonian: $\exp(itS) = \cos t\, I + i \sin t\, S$
- Partial swap:

$$U_\lambda := \sqrt{\lambda}\, I + i\sqrt{1-\lambda}\, S, \quad \lambda \in [0,1]$$

- Combining two qudits:

$$\begin{aligned} \rho_1 \boxplus_\lambda \rho_2 := \; & \mathrm{Tr}_2\big(U_\lambda(\rho_1 \otimes \rho_2)U_\lambda^\dagger\big) \\ & = \lambda\rho_1 + (1-\lambda)\rho_2 - \sqrt{\lambda(1-\lambda)}\, i[\rho_1, \rho_2] \end{aligned}$$

- This operation has applications for quantum algorithms! (Lloyd, Mohseni, Rebentrost [LMR14])

Main result

Theorem

For any concave and symmetric function $f : \mathcal{D}(\mathbb{C}^d) \to \mathbb{R}$,

$$f(\rho \boxplus_\lambda \sigma) \geq \lambda f(\rho) + (1-\lambda) f(\sigma)$$

for all $\lambda \in [0,1]$ and qudit states ρ and σ

Main result

Theorem

For any concave and symmetric function $f : \mathcal{D}(\mathbb{C}^d) \to \mathbb{R}$,

$$f(\rho \boxplus_\lambda \sigma) \geq \lambda f(\rho) + (1-\lambda) f(\sigma)$$

for all $\lambda \in [0,1]$ and qudit states ρ and σ

Relevant functions

- concave if $f\big(\lambda\rho + (1-\lambda)\sigma\big) \geq \lambda f(\rho) + (1-\lambda) f(\sigma)$
- symmetric if $f(\rho) = s(\mathrm{spec}(\rho))$ for some sym. function s

Typical example: von Neumann entorpy $H(\rho)$

Proof idea

Theorem $f(\rho \boxplus_\lambda \sigma) \geq \lambda f(\rho) + (1-\lambda) f(\sigma)$

Proof

Main tool: majorization. Assume we can show

$$\operatorname{spec}(\rho \boxplus_\lambda \sigma) \prec \lambda \operatorname{spec}(\rho) + (1-\lambda) \operatorname{spec}(\sigma)$$

Proof idea

Theorem $f(\rho \boxplus_\lambda \sigma) \geq \lambda f(\rho) + (1-\lambda) f(\sigma)$

Proof

Main tool: majorization. Assume we can show

$$\begin{aligned} \operatorname{spec}(\rho \boxplus_\lambda \sigma) &\prec \lambda \operatorname{spec}(\rho) + (1-\lambda)\operatorname{spec}(\sigma) \\ &= \operatorname{spec}\big(\lambda\tilde{\rho} + (1-\lambda)\tilde{\sigma}\big) \end{aligned}$$

where $\tilde{\rho} := \operatorname{diag}(\operatorname{spec}(\rho))$.

Proof idea

Theorem $f(\rho \boxplus_\lambda \sigma) \geq \lambda f(\rho) + (1-\lambda) f(\sigma)$

Proof

Main tool: majorization. Assume we can show

$$\begin{aligned} \operatorname{spec}(\rho \boxplus_\lambda \sigma) &\prec \lambda \operatorname{spec}(\rho) + (1-\lambda) \operatorname{spec}(\sigma) \\ &= \operatorname{spec}\big(\lambda\tilde{\rho} + (1-\lambda)\tilde{\sigma}\big) \end{aligned}$$

where $\tilde{\rho} := \operatorname{diag}(\operatorname{spec}(\rho))$. Then

$$f(\rho \boxplus_\lambda \sigma) \geq f\big(\lambda\tilde{\rho} + (1-\lambda)\tilde{\sigma}\big) \qquad \text{(Schur-concavity)}$$

Proof idea

Theorem $f(\rho \boxplus_\lambda \sigma) \geq \lambda f(\rho) + (1-\lambda) f(\sigma)$

Proof

Main tool: majorization. Assume we can show

$$\begin{aligned} \operatorname{spec}(\rho \boxplus_\lambda \sigma) &\prec \lambda \operatorname{spec}(\rho) + (1-\lambda) \operatorname{spec}(\sigma) \\ &= \operatorname{spec}\big(\lambda\tilde{\rho} + (1-\lambda)\tilde{\sigma}\big) \end{aligned}$$

where $\tilde{\rho} := \operatorname{diag}(\operatorname{spec}(\rho))$. Then

$$\begin{aligned} f(\rho \boxplus_\lambda \sigma) &\geq f\big(\lambda\tilde{\rho} + (1-\lambda)\tilde{\sigma}\big) && \text{(Schur-concavity)} \\ &\geq \lambda f(\tilde{\rho}) + (1-\lambda) f(\tilde{\sigma}) && \text{(concavity)} \end{aligned}$$

Proof idea

Theorem $f(\rho \boxplus_\lambda \sigma) \geq \lambda f(\rho) + (1-\lambda) f(\sigma)$

Proof

Main tool: majorization. Assume we can show

$$\begin{aligned}\operatorname{spec}(\rho \boxplus_\lambda \sigma) &\prec \lambda \operatorname{spec}(\rho) + (1-\lambda) \operatorname{spec}(\sigma) \\ &= \operatorname{spec}\big(\lambda\tilde{\rho} + (1-\lambda)\tilde{\sigma}\big)\end{aligned}$$

where $\tilde{\rho} := \operatorname{diag}(\operatorname{spec}(\rho))$. Then

$$\begin{aligned}f(\rho \boxplus_\lambda \sigma) &\geq f\big(\lambda\tilde{\rho} + (1-\lambda)\tilde{\sigma}\big) && \text{(Schur-concavity)} \\ &\geq \lambda f(\tilde{\rho}) + (1-\lambda) f(\tilde{\sigma}) && \text{(concavity)} \\ &= \lambda f(\rho) + (1-\lambda) f(\sigma) && \text{(symmetry)}\end{aligned}$$

Proof by Carlen, Lieb, Loss [CLL16] (from yesterday!)

Goal: $\operatorname{spec}(\rho \boxplus_\lambda \sigma) \prec \lambda \operatorname{spec}(\rho) + (1-\lambda) \operatorname{spec}(\sigma)$

Proof by Carlen, Lieb, Loss [CLL16] (from yesterday!)

Goal: $$\mathrm{spec}(\rho \boxplus_\lambda \sigma) \prec \lambda\, \mathrm{spec}(\rho) + (1-\lambda)\, \mathrm{spec}(\sigma)$$

Anti-symmetric extension of operator A:

$$A^{[k]}(v_1 \wedge \cdots \wedge v_k) := (Av_1 \wedge \cdots \wedge v_k) + \cdots + (v_1 \wedge \cdots \wedge Av_k)$$

Proof by Carlen, Lieb, Loss [CLL16] (from yesterday!)

Goal: $\mathrm{spec}(\rho \boxplus_\lambda \sigma) \prec \lambda\, \mathrm{spec}(\rho) + (1-\lambda)\, \mathrm{spec}(\sigma)$

Anti-symmetric extension of operator A:

$$A^{[k]}(v_1 \wedge \cdots \wedge v_k) := (Av_1 \wedge \cdots \wedge v_k) + \cdots + (v_1 \wedge \cdots \wedge Av_k)$$

Since $\|A^{[k]}\| = \sum_{j=1}^k \lambda_j(A)$, it only remains to show that $\forall k$

$$\|\rho^{[k]} \boxplus_\lambda \sigma^{[k]}\| \leq \lambda \|\rho^{[k]}\| + (1-\lambda)\|\sigma^{[k]}\|$$

Proof by Carlen, Lieb, Loss [CLL16] (from yesterday!)

Goal: $\operatorname{spec}(\rho \boxplus_\lambda \sigma) \prec \lambda \operatorname{spec}(\rho) + (1-\lambda) \operatorname{spec}(\sigma)$

Anti-symmetric extension of operator A:

$$A^{[k]}(v_1 \wedge \cdots \wedge v_k) := (Av_1 \wedge \cdots \wedge v_k) + \cdots + (v_1 \wedge \cdots \wedge Av_k)$$

Since $\|A^{[k]}\| = \sum_{j=1}^k \lambda_j(A)$, it only remains to show that $\forall k$

$$\|\rho^{[k]} \boxplus_\lambda \sigma^{[k]}\| \leq \lambda \|\rho^{[k]}\| + (1-\lambda)\|\sigma^{[k]}\|$$

We can forget about $[k]$'s and simply show that

$$0 \leq -\rho \boxplus_\lambda \sigma + \big(\lambda\|\rho\| + (1-\lambda)\|\sigma\|\big) I$$

Proof by Carlen, Lieb, Loss [CLL16] (from yesterday!)

Goal: $\operatorname{spec}(\rho \boxplus_\lambda \sigma) \prec \lambda \operatorname{spec}(\rho) + (1-\lambda) \operatorname{spec}(\sigma)$

Anti-symmetric extension of operator A:

$$A^{[k]}(v_1 \wedge \cdots \wedge v_k) := (Av_1 \wedge \cdots \wedge v_k) + \cdots + (v_1 \wedge \cdots \wedge Av_k)$$

Since $\|A^{[k]}\| = \sum_{j=1}^k \lambda_j(A)$, it only remains to show that $\forall k$

$$\|\rho^{[k]} \boxplus_\lambda \sigma^{[k]}\| \leq \lambda \|\rho^{[k]}\| + (1-\lambda)\|\sigma^{[k]}\|$$

We can forget about $[k]$'s and simply show that

$$\begin{aligned} 0 &\leq -\rho \boxplus_\lambda \sigma + \big(\lambda\|\rho\| + (1-\lambda)\|\sigma\|\big) I \\ &= \lambda\big(\|\rho\| I - \rho\big) + (1-\lambda)\big(\|\sigma\| I - \sigma\big) + \sqrt{\lambda(1-\lambda)}\, i[\rho, \sigma] \end{aligned}$$

Proof by Carlen, Lieb, Loss [CLL16] (from yesterday!)

Goal: $\operatorname{spec}(\rho \boxplus_\lambda \sigma) \prec \lambda \operatorname{spec}(\rho) + (1-\lambda) \operatorname{spec}(\sigma)$

Anti-symmetric extension of operator A:

$$A^{[k]}(v_1 \wedge \cdots \wedge v_k) := (Av_1 \wedge \cdots \wedge v_k) + \cdots + (v_1 \wedge \cdots \wedge Av_k)$$

Since $\|A^{[k]}\| = \sum_{j=1}^k \lambda_j(A)$, it only remains to show that $\forall k$

$$\|\rho^{[k]} \boxplus_\lambda \sigma^{[k]}\| \leq \lambda \|\rho^{[k]}\| + (1-\lambda)\|\sigma^{[k]}\|$$

We can forget about $[k]$'s and simply show that

$$\begin{aligned} 0 &\leq -\rho \boxplus_\lambda \sigma + \big(\lambda\|\rho\| + (1-\lambda)\|\sigma\|\big)I \\ &= \lambda\big(\|\rho\|I - \rho\big) + (1-\lambda)\big(\|\sigma\|I - \sigma\big) + \sqrt{\lambda(1-\lambda)}\, i[\rho,\sigma] \\ &= \lambda(X - X^2) + (1-\lambda)(Y - Y^2) + Z^\dagger Z \end{aligned}$$

where $X := \|\rho\|I - \rho,\ Y := \|\sigma\|I - \sigma,\ Z := \sqrt{\lambda}X + i\sqrt{1-\lambda}Y.$

Particular functions of interest

Functions of entropy

- entropy $H(\cdot)$
- entropy power $e^{cH(\cdot)}$
- entropy photon number $N_c(\cdot) := g^{-1}(cH(\cdot))$

Particular functions of interest

Functions of entropy

- entropy $H(\cdot)$
- entropy power $e^{cH(\cdot)}$
- entropy photon number $N_c(\cdot) := g^{-1}(cH(\cdot))$

Photon number

- Thermal state with N photons:

$$\rho_{\text{th}} = \sum_{i=0}^{\infty} \frac{N^i}{(N+1)^{i+1}} |i\rangle\langle i|$$

- It's entropy is $g(N) := (N+1)\log(N+1) - N\log N$
- $N_c(\rho) :=$ the average photon number of the thermal state that has the same entropy as ρ

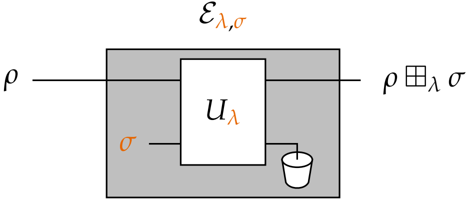
Summary of EPIs

	Continuous variable		Discrete
	Classical (d dims)	Quantum (d modes)	Quantum (d dims)
entropy $H(\cdot)$	✓	✓	✓
entropy power $e^{cH(\cdot)}$	$c = 2/d$	$c = 1/d$	$0 \leq c \leq 1/(\log d)^2$
entropy photon number $g^{-1}(cH(\cdot))$	—	$c = 1/d$ (conjectured)	$0 \leq c \leq 1/(d-1)$

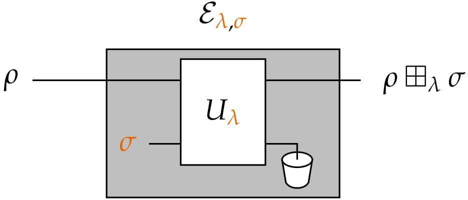
$$f(\rho \boxplus_\lambda \sigma) \geq \lambda f(\rho) + (1-\lambda) f(\sigma)$$

Applications

Product-state classical capacity



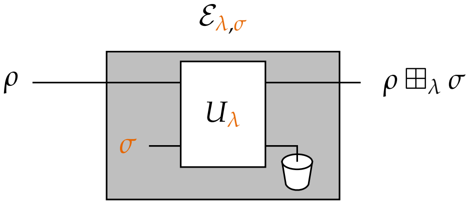
Product-state classical capacity



- Holevo quantity:

$$\chi(\mathcal{E}) := \max_{\{p_i,\rho_i\}} \left\{ H\Big(\sum_i p_i \mathcal{E}(\rho_i)\Big) - \sum_i p_i H\big(\mathcal{E}(\rho_i)\big) \right\}$$
$$\leq \log d - \min_\rho H(\mathcal{E}(\rho))$$

Product-state classical capacity



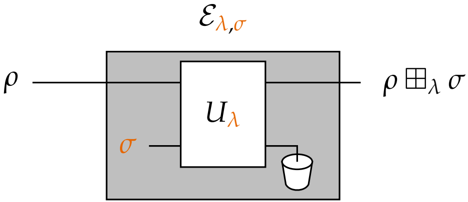
- Holevo quantity:

$$\chi(\mathcal{E}) := \max_{\{p_i,\rho_i\}} \left\{ H\left(\sum_i p_i \mathcal{E}(\rho_i)\right) - \sum_i p_i H(\mathcal{E}(\rho_i)) \right\}$$
$$\leq \log d - \min_\rho H(\mathcal{E}(\rho))$$

- Minimum output entropy:

$$H(\mathcal{E}_{\lambda,\sigma}(\rho)) = H(\rho \boxplus_\lambda \sigma) \geq \lambda H(\rho) + (1-\lambda) H(\sigma)$$

Product-state classical capacity



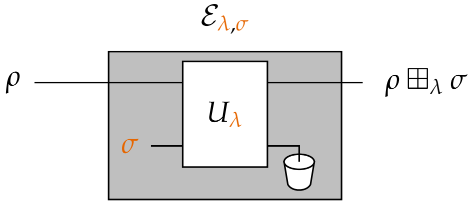
- Holevo quantity:

$$\chi(\mathcal{E}) := \max_{\{p_i,\rho_i\}} \Big\{ H\Big(\sum_i p_i \mathcal{E}(\rho_i)\Big) - \sum_i p_i H(\mathcal{E}(\rho_i)) \Big\}$$
$$\leq \log d - \min_\rho H(\mathcal{E}(\rho))$$

- Minimum output entropy:

$$H(\mathcal{E}_{\lambda,\sigma}(\rho)) = H(\rho \boxplus_\lambda \sigma) \geq \lambda H(\rho) + (1-\lambda) H(\sigma)$$
$$\geq (1-\lambda) H(\sigma)$$

Product-state classical capacity



- Holevo quantity:

$$\chi(\mathcal{E}) := \max_{\{p_i,\rho_i\}} \left\{ H\Big(\sum_i p_i \mathcal{E}(\rho_i)\Big) - \sum_i p_i H\big(\mathcal{E}(\rho_i)\big) \right\}$$
$$\leq \log d - \min_\rho H(\mathcal{E}(\rho))$$
$$\leq \log d - (1-\lambda) H(\sigma)$$

- Minimum output entropy:

$$H(\mathcal{E}_{\lambda,\sigma}(\rho)) = H(\rho \boxplus_\lambda \sigma) \geq \lambda H(\rho) + (1-\lambda) H(\sigma)$$
$$\geq (1-\lambda) H(\sigma)$$

Partial swap in quantum algorithms

Quantum principal component analysis [LMR14]

$$\sigma \otimes \rho^{\otimes n} \mapsto e^{-i\rho n t} \sigma e^{i\rho n t}$$

Partial swap in quantum algorithms

Quantum principal component analysis [LMR14]

$$\sigma \otimes \rho^{\otimes n} \mapsto e^{-i\rho n t} \sigma e^{i\rho n t}$$

- $e^X \sigma e^{-X} = \sigma + [X, \sigma] + \frac{1}{2!}[X, [X, \sigma]] + \cdots$

Partial swap in quantum algorithms

Quantum principal component analysis [LMR14]

$$\sigma \otimes \rho^{\otimes n} \mapsto e^{-i\rho n t} \sigma e^{i\rho n t}$$

- $e^X \sigma e^{-X} = \sigma + [X, \sigma] + \frac{1}{2!}[X, [X, \sigma]] + \cdots$
- $e^{-i\rho t} \sigma e^{i\rho t} = \sigma - it[\rho, \sigma] + O(t^2)$

Partial swap in quantum algorithms

Quantum principal component analysis [LMR14]

$$\sigma \otimes \rho^{\otimes n} \mapsto e^{-i\rho n t} \sigma e^{i\rho n t}$$

- $e^X \sigma e^{-X} = \sigma + [X, \sigma] + \frac{1}{2!}[X, [X, \sigma]] + \cdots$
- $e^{-i\rho t} \sigma e^{i\rho t} = \sigma - it[\rho, \sigma] + O(t^2)$
- Partial swap:

$$\begin{aligned} \mathrm{Tr}_2\left[e^{-iSt}(\sigma \otimes \rho)e^{iSt}\right] &= \cos^2 t\ \sigma + \sin^2 t\ \rho - i \sin t \cos t\ [\rho, \sigma] \\ &= \sigma - it[\rho, \sigma] + O(t^2) \end{aligned}$$

Partial swap in quantum algorithms

Quantum principal component analysis [LMR14]

$$\sigma \otimes \rho^{\otimes n} \mapsto e^{-i\rho n t}\sigma e^{i\rho n t}$$

- $e^{X}\sigma e^{-X} = \sigma + [X,\sigma] + \frac{1}{2!}[X,[X,\sigma]] + \cdots$
- $e^{-i\rho t}\sigma e^{i\rho t} = \sigma - it[\rho,\sigma] + O(t^2)$
- Partial swap:

$$\begin{aligned} \mathrm{Tr}_2\left[e^{-iSt}(\sigma \otimes \rho)e^{iSt}\right] &= \cos^2 t\ \sigma + \sin^2 t\ \rho - i \sin t \cos t\ [\rho,\sigma] \\ &= \sigma - it[\rho,\sigma] + O(t^2) \end{aligned}$$

- This approximates $e^{-i\rho t}\sigma e^{i\rho t}$ well when $t \ll 1$

Partial swap in quantum algorithms

Quantum principal component analysis [LMR14]

$$\sigma \otimes \rho^{\otimes n} \mapsto e^{-i\rho n t} \sigma e^{i\rho n t}$$

- $e^X \sigma e^{-X} = \sigma + [X, \sigma] + \frac{1}{2!}[X, [X, \sigma]] + \cdots$
- $e^{-i\rho t} \sigma e^{i\rho t} = \sigma - it[\rho, \sigma] + O(t^2)$
- Partial swap:

$$\begin{aligned} \operatorname{Tr}_2\left[e^{-iSt}(\sigma \otimes \rho)e^{iSt}\right] &= \cos^2 t\ \sigma + \sin^2 t\ \rho - i \sin t \cos t\ [\rho, \sigma] \\ &= \sigma - it[\rho, \sigma] + O(t^2) \end{aligned}$$

- This approximates $e^{-i\rho t} \sigma e^{i\rho t}$ well when $t \ll 1$
- Using n copies of ρ can boost t to nt:

$$\Big(\big((\sigma \boxplus_\lambda \rho) \boxplus_\lambda \rho\big) \boxplus_\lambda \cdots\Big) \boxplus_\lambda \rho$$

Extensions of $\boxplus_\lambda$

How to combine n states?

$$(\rho_1, \ldots, \rho_n) \mapsto \mathrm{Tr}_{2,\ldots,n}\big(U(\rho_1 \otimes \cdots \otimes \rho_n)U^\dagger\big)$$

- For $n = 2$, U is a linear combination of I and S:

$$U = \sqrt{\lambda}\, I + i\sqrt{1-\lambda}\, S$$

How to combine n states?

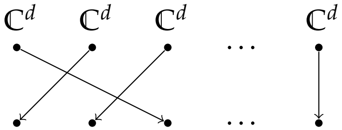
$$(\rho_1, \dots, \rho_n) \mapsto \mathrm{Tr}_{2,\dots,n}\big(U(\rho_1 \otimes \cdots \otimes \rho_n)U^\dagger\big)$$

- For $n = 2$, U is a linear combination of I and S:

$$U = \sqrt{\lambda}\, I + i\sqrt{1-\lambda}\, S$$

- Permutations of n qudits:

$\pi \in \mathrm{S}_n$



$Q_\pi \in \mathrm{U}(d^n)$

How to combine n states?

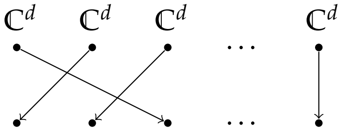
$$(\rho_1, \dots, \rho_n) \mapsto \mathrm{Tr}_{2,\dots,n}\big(U(\rho_1 \otimes \cdots \otimes \rho_n)U^\dagger\big)$$

- For $n = 2$, U is a linear combination of I and S:

$$U = \sqrt{\lambda}\, I + i\sqrt{1-\lambda}\, S$$

- Permutations of n qudits:

$\pi \in \mathrm{S}_n$



$Q_\pi \in \mathrm{U}(d^n)$

- Question:

$$\text{When is } U := \sum_{\pi \in \mathrm{S}_n} z_\pi Q_\pi \text{ unitary } (z_\pi \in \mathbb{C})?$$

Unitary Cayley's Theorem

Cayley's Theorem

Every finite group G is isomorphic to a subgroup of $S_{|G|}$.

Unitary Cayley's Theorem

Cayley's Theorem

Every finite group G is isomorphic to a subgroup of $\mathrm{S}_{|G|}$.

Proof: Represent g by L_g defined as $L_g|h\rangle := |gh\rangle$.
This is known as *left regular representation*.

Unitary Cayley's Theorem

Cayley's Theorem

Every finite group G is isomorphic to a subgroup of $\mathrm{S}_{|G|}$.

Proof: Represent g by L_g defined as $L_g|h\rangle := |gh\rangle$.
This is known as *left regular representation*.

$$G \hookrightarrow \mathrm{S}_{|G|} \overset{?}{\hookrightarrow} \mathrm{U}(|G|)$$

Unitary Cayley's Theorem

Cayley's Theorem

Every finite group G is isomorphic to a subgroup of $S_{|G|}$.

Proof: Represent g by L_g defined as $L_g|h\rangle := |gh\rangle$.
This is known as *left regular representation*.

$$G \hookrightarrow S_{|G|} \overset{?}{\hookrightarrow} U(|G|)$$

Q: When is $L := \sum_{g \in G} z_g L_g$ unitary $(z_g \in \mathbb{C})$?

Fourier transform to the rescue!

Q: When is $L := \sum_{g \in G} z_g L_g$ unitary ($z_g \in \mathbb{C}$)?

Fourier transform to the rescue!

Q: When is $L := \sum_{g \in G} z_g L_g$ unitary ($z_g \in \mathbb{C}$)?

Fact: $\hat{L}_g := F L_g F^\dagger = \bigoplus_{\tau \in \hat{G}} \left[\tau(g) \otimes I_{d_\tau} \right]$

Fourier transform to the rescue!

Q: When is $L := \sum_{g \in G} z_g L_g$ unitary ($z_g \in \mathbb{C}$)?

Fact: $\hat{L}_g := F L_g F^\dagger = \bigoplus_{\tau \in \hat{G}} \left[\tau(g) \otimes I_{d_\tau} \right]$

$$\hat{L} = \sum_{g \in G} z_g \hat{L}_g = \bigoplus_{\tau \in \hat{G}} \left[\underbrace{\left(\sum_{g \in G} z_g \tau(g) \right)}_{U_\tau} \otimes I_{d_\tau} \right] \stackrel{?}{\in} \mathrm{U}(|G|)$$

Fourier transform to the rescue!

Q: When is $L := \sum_{g \in G} z_g L_g$ unitary ($z_g \in \mathbb{C}$)?

Fact: $\hat{L}_g := F L_g F^\dagger = \bigoplus_{\tau \in \hat{G}} \left[\tau(g) \otimes I_{d_\tau} \right]$

$$\hat{L} = \sum_{g \in G} z_g \hat{L}_g = \bigoplus_{\tau \in \hat{G}} \left[\underbrace{\left(\sum_{g \in G} z_g \tau(g) \right)}_{U_\tau} \otimes I_{d_\tau} \right] \overset{?}{\in} \mathrm{U}(|G|)$$

Theorem: $L = \sum_{g \in G} z_g L_g$ is unitary iff for some $U_\tau \in \mathrm{U}(d_\tau)$,

$$z_g = \sum_{\tau \in \hat{G}} \frac{d_\tau}{|G|} \operatorname{Tr}\left(\tau(g)^\dagger U_\tau \right)$$

Fourier transform to the rescue!

Q: When is $L := \sum_{g \in G} z_g L_g$ unitary ($z_g \in \mathbb{C}$)?

Fact: $\hat{L}_g := F L_g F^\dagger = \bigoplus_{\tau \in \hat{G}} \left[\tau(g) \otimes I_{d_\tau} \right]$

$$\hat{L} = \sum_{g \in G} z_g \hat{L}_g = \bigoplus_{\tau \in \hat{G}} \left[\underbrace{\left(\sum_{g \in G} z_g \tau(g) \right)}_{U_\tau} \otimes I_{d_\tau} \right] \overset{?}{\in} \mathrm{U}(|G|)$$

Theorem: $L = \sum_{g \in G} z_g L_g$ is unitary iff for some $U_\tau \in \mathrm{U}(d_\tau)$,

$$z_g = \sum_{\tau \in \hat{G}} \frac{d_\tau}{|G|} \operatorname{Tr}\left(\tau(g)^\dagger U_\tau \right)$$

Note: If $L = \sum_{\pi \in S_n} z_\pi L_\pi$ is unitary then so is $U = \sum_{\pi \in S_n} z_\pi Q_\pi$

EPI conjecture for 3 states

If f is concave and symmetric then

$$f(\rho) \geq p_1 f(\rho_1) + p_2 f(\rho_2) + p_3 f(\rho_3)$$

where $\rho = \mathrm{Tr}_{2,3}\big(U(\rho_1 \otimes \rho_2 \otimes \rho_3)U^\dagger\big)$ is explicitly given by

$$\begin{aligned}
\rho = {} & p_1\,\rho_1 + p_2\,\rho_2 + p_3\,\rho_3 \\
& + \sqrt{p_1 p_2}\ \sin\delta_{12}\, i[\rho_1, \rho_2] \\
& + \sqrt{p_2 p_3}\ \sin\delta_{23}\, i[\rho_2, \rho_3] \\
& + \sqrt{p_3 p_1}\ \sin\delta_{31}\, i[\rho_3, \rho_1] \\
& + \sqrt{p_1 p_2}\ \cos\delta_{12}\, i[\rho_1, i[\rho_2, \rho_3]] \\
& + \sqrt{p_2 p_3}\ \cos\delta_{23}\, i[i[\rho_1, \rho_2], \rho_3]
\end{aligned}$$

where δ_{ij} are subject to $\delta_{12} + \delta_{23} + \delta_{31} = 0$ and $\sqrt{p_1 p_2}\ \cos\delta_{12} + \sqrt{p_2 p_3}\ \cos\delta_{23} + \sqrt{p_3 p_1}\ \cos\delta_{31} = 0$

Open problems

- Entropy photon number inequality for c.v. states
  - useful for bounding classical capacities of various bosonic channels [GGL+04, GSE07, GSE08]
  - proved only for Gaussian states [Guh08]
  - does not seem to follow from qudit EPI by taking $d \to \infty$

Open problems

- Entropy photon number inequality for c.v. states
  - useful for bounding classical capacities of various bosonic channels [GGL+04, GSE07, GSE08]
  - proved only for Gaussian states [Guh08]
  - does not seem to follow from qudit EPI by taking $d \to \infty$
- Conditional version of qudit EPI
  - trivial for c.v. distributions
  - proved for Gaussian c.v. states [Koe15]
  - qudit analogue...?

Open problems

- Entropy photon number inequality for c.v. states
  - useful for bounding classical capacities of various bosonic channels [GGL+04, GSE07, GSE08]
  - proved only for Gaussian states [Guh08]
  - does not seem to follow from qudit EPI by taking $d \to \infty$
- Conditional version of qudit EPI
  - trivial for c.v. distributions
  - proved for Gaussian c.v. states [Koe15]
  - qudit analogue…?
- Generalization to 3 or more systems
  - trivial for c.v. distributions
  - proved for c.v. states [DMLG15]
  - extension of $\boxplus_\lambda$ for combining ≥ 3 states [Ozo15]
  - proving the EPI…?

Open problems

- Entropy photon number inequality for c.v. states
  - useful for bounding classical capacities of various bosonic channels [GGL+04, GSE07, GSE08]
  - proved only for Gaussian states [Guh08]
  - does not seem to follow from qudit EPI by taking $d \to \infty$
- Conditional version of qudit EPI
  - trivial for c.v. distributions
  - proved for Gaussian c.v. states [Koe15]
  - qudit analogue…?
- Generalization to 3 or more systems
  - trivial for c.v. distributions
  - proved for c.v. states [DMLG15]
  - extension of $\boxplus_\lambda$ for combining ≥ 3 states [Ozo15]
  - proving the EPI…?
- Applications
  - lower bounds for min output entropy & upper bounds for product-state classical capacity
  - more…? for quantum algorithms…?

Thank you!

`arXiv:1503.04213` – Qudit EPIs

`arXiv:1508.00860` – Unitary Cayley’s theorem

Bibliography I

[Bar86] Andrew R. Barron.
Entropy and the central limit theorem.
The Annals of Probability, 14(1):336–342, 1986.
URL: `http://projecteuclid.org/euclid.aop/1176992632`.

[Ber74] Patrick P. Bergmans.
A simple converse for broadcast channels with additive white Gaussian noise.
Information Theory, IEEE Transactions on, 20(2):279–280, Mar 1974.
`doi:10.1109/TIT.1974.1055184`.

[Bla65] Nelson M. Blachman.
The convolution inequality for entropy powers.
Information Theory, IEEE Transactions on, 11(2):267–271, Apr 1965.
`doi:10.1109/TIT.1965.1053768`.

[CLL16] Eric A. Carlen, Elliott H. Lieb, and Michael Loss.
On a quantum entropy power inequality of Audenaert, Datta and Ozols.
2016.
`arXiv:1603.07043`.

[DMG14] Giacomo De Palma, Andrea Mari, and Vittorio Giovannetti.
A generalization of the entropy power inequality to bosonic quantum systems.
Nature Photonics, 8(12):958–964, 2014.
`arXiv:1402.0404`, `doi:10.1038/nphoton.2014.252`.

Bibliography II

[DMLG15] Giacomo De Palma, Andrea Mari, Seth Lloyd, and Vittorio Giovannetti.
Multimode quantum entropy power inequality.
Phys. Rev. A, 91(3):032320, Mar 2015.
arXiv:1408.6410, doi:10.1103/PhysRevA.91.032320.

[GGL+04] Vittorio Giovannetti, Saikat Guha, Seth Lloyd, Lorenzo Maccone, Jeffrey H. Shapiro, and Horace P. Yuen.
Classical capacity of the lossy bosonic channel: the exact solution.
Phys. Rev. Lett., 92(2):027902, Jan 2004.
arXiv:quant-ph/0308012, doi:10.1103/PhysRevLett.92.027902.

[GSE07] Saikat Guha, Jeffrey H. Shapiro, and Baris I. Erkmen.
Classical capacity of bosonic broadcast communication and a minimum output entropy conjecture.
Phys. Rev. A, 76(3):032303, Sep 2007.
arXiv:0706.3416, doi:10.1103/PhysRevA.76.032303.

[GSE08] Saikat Guha, Jeffrey H. Shapiro, and Baris I. Erkmen.
Capacity of the bosonic wiretap channel and the entropy photon-number inequality.
In *IEEE International Symposium on Information Theory, 2008 (ISIT 2008)*, pages 91–95, Jul 2008.
arXiv:0801.0841, doi:10.1109/ISIT.2008.4594954.

Bibliography III

[Guh08] Saikat Guha.
Multiple-user quantum information theory for optical communication channels.
PhD thesis, Dept. Electr. Eng. Comput. Sci., MIT, Cambridge, MA, USA, 2008.
URL: `http://hdl.handle.net/1721.1/44413`.

[Koe15] Robert Koenig.
The conditional entropy power inequality for Gaussian quantum states.
Journal of Mathematical Physics, 56(2):022201, 2015.
`arXiv:1304.7031`, `doi:10.1063/1.4906925`.

[KS14] Robert König and Graeme Smith.
The entropy power inequality for quantum systems.
Information Theory, IEEE Transactions on, 60(3):1536–1548, Mar 2014.
`arXiv:1205.3409`, `doi:10.1109/TIT.2014.2298436`.

[LMR14] Seth Lloyd, Masoud Mohseni, and Patrick Rebentrost.
Quantum principal component analysis.
Nature Physics, 10(9):631–633, 2014.
`arXiv:1307.0401`, `doi:10.1038/nphys3029`.

[Ozo15] Maris Ozols.
How to combine three quantum states.
2015.
`arXiv:1508.00860`.

Bibliography IV

[Sha48] Claude E. Shannon.
A mathematical theory of communication.
The Bell System Technical Journal, 27:623–656, Oct 1948.
URL: http://cm.bell-labs.com/cm/ms/what/shannonday/shannon1948.pdf.

[Sta59] A. J. Stam.
Some inequalities satisfied by the quantities of information of Fisher and Shannon.
Information and Control, 2(2):101–112, Jun 1959.
doi:10.1016/S0019-9958(59)90348-1.