Uncertainty Relations in the Presence of Quantum Memory for Mutually Unbiased Measurements

Kun Wang

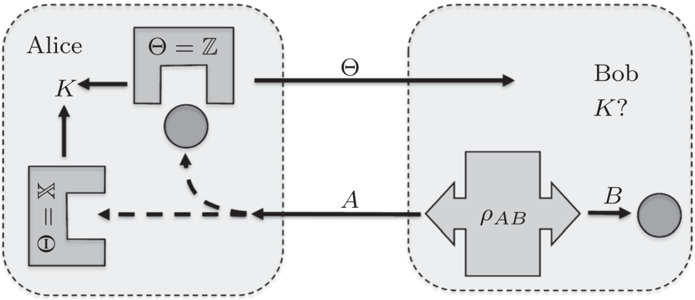
Department of Computer Science and Technology, Nanjing University

Joint work with Nan Wu and Fangmin Song (arXiv:1807.01047)

July 12, 2018

Outline

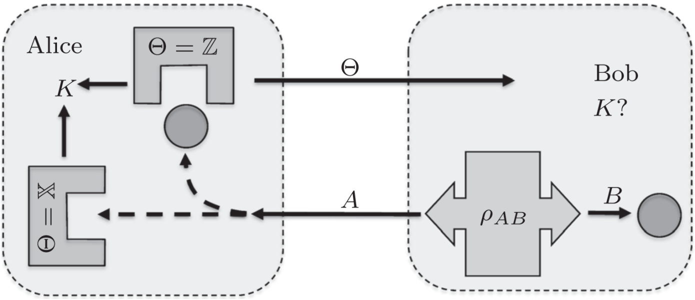
Guessing game



- A guessing game[1] played by Alice and Bob
  1. Bob prepares state ρ_{AB} and sends ρ_A to Alice
  2. Alice measures either $\mathbb{X}$ or $\mathbb{Z}$ (uniformly) and stores outcome K
  3. Alice tells Bob which measurement Θ has been conducted
  4. Bob guesses the value of K
- $\mathbb{X}$ and $\mathbb{Z}$ are known to both Alice and Bob
- How well can Bob guess K on average?

[1] Patrick J Coles et al. "Entropic uncertainty relations and their applications". In: *Reviews of Modern Physics* 89.1 (2017), p. 015002.

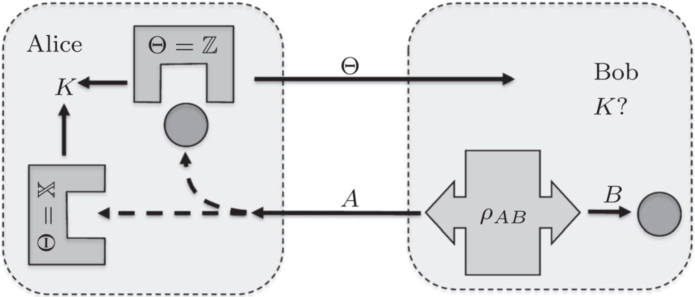
Guessing game



- A guessing game[1] played by Alice and Bob
  1. Bob prepares state ρ_{AB} and sends ρ_A to Alice
  2. Alice measures either $\mathbb{X}$ or $\mathbb{Z}$ (uniformly) and stores outcome K
  3. Alice tells Bob which measurement Θ has been conducted
  4. Bob guesses the value of K
- $\mathbb{X}$ and $\mathbb{Z}$ are known to both Alice and Bob
- How well can Bob guess K on average?

[1] Patrick J Coles et al. "Entropic uncertainty relations and their applications". In: *Reviews of Modern Physics* 89.1 (2017), p. 015002.

Guessing game



- A guessing game[1] played by Alice and Bob
  1. Bob prepares state ρ_{AB} and sends ρ_A to Alice
  2. Alice measures either $\mathbb{X}$ or $\mathbb{Z}$ (uniformly) and stores outcome K
  3. Alice tells Bob which measurement Θ has been conducted
  4. Bob guesses the value of K
- $\mathbb{X}$ and $\mathbb{Z}$ are known to both Alice and Bob
- How well can Bob guess K on average?

[1] Patrick J Coles et al. "Entropic uncertainty relations and their applications". In: *Reviews of Modern Physics* 89.1 (2017), p. 015002.

Entanglement helps!

- Assume $\mathbb{X} = \{|x_i\rangle\}$ and $\mathbb{Z} = \{|z_j\rangle\}$ be complementary on A: $|\langle x_i|z_j\rangle| = 1/\sqrt{d}$ for arbitrary i, j
- Suppose Bob prepares a maximally entangled state

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_i |x_i\rangle_A |x_i\rangle_B = \frac{1}{\sqrt{d}} \sum_j |z_j\rangle_A |z_j\rangle_B$$

  and sends ρ_A to Alice
- Measuring ρ_A with $\mathbb{X}/\mathbb{Z}$, Alice gets classical-quantum (cq.) states

$$\omega_{XB} = \frac{1}{d} \sum_i |x_i\rangle\langle x_i|_A \otimes |x_i\rangle\langle x_i|_B$$

$$\tau_{ZB} = \frac{1}{d} \sum_j |z_j\rangle\langle z_j|_A \otimes |z_j\rangle\langle z_j|_B$$

- If Alice obtains x_i, Bob processes state x_i. Similar for $\mathbb{Z}$
- Bob can guess K with certainty by measuring his state
- **Entanglement** reduces the Bob's **uncertainty** about K

Entanglement helps!

- Assume $\mathbb{X} = \{|x_i\rangle\}$ and $\mathbb{Z} = \{|z_j\rangle\}$ be complementary on A: $|\langle x_i|z_j\rangle| = 1/\sqrt{d}$ for arbitrary i, j
- Suppose Bob prepares a maximally entangled state

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{d}}\sum_i |x_i\rangle_A|x_i\rangle_B = \frac{1}{\sqrt{d}}\sum_j |z_j\rangle_A|z_j\rangle_B$$

  and sends ρ_A to Alice
- Measuring ρ_A with $\mathbb{X}/\mathbb{Z}$, Alice gets classical-quantum (cq.) states

$$\omega_{XB} = \frac{1}{d}\sum_i |x_i\rangle\langle x_i|_A \otimes |x_i\rangle\langle x_i|_B$$

$$\tau_{ZB} = \frac{1}{d}\sum_j |z_j\rangle\langle z_j|_A \otimes |z_j\rangle\langle z_j|_B$$

- If Alice obtains x_i, Bob processes state x_i. Similar for $\mathbb{Z}$
- Bob can guess K with certainty by measuring his state
- **Entanglement** reduces the Bob's **uncertainty** about K

Entanglement helps!

- Assume $\mathbb{X} = \{|x_i\rangle\}$ and $\mathbb{Z} = \{|z_j\rangle\}$ be complementary on A: $|\langle x_i|z_j\rangle| = 1/\sqrt{d}$ for arbitrary i, j
- Suppose Bob prepares a maximally entangled state

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_i |x_i\rangle_A |x_i\rangle_B = \frac{1}{\sqrt{d}} \sum_j |z_j\rangle_A |z_j\rangle_B$$

  and sends ρ_A to Alice
- Measuring ρ_A with $\mathbb{X}/\mathbb{Z}$, Alice gets classical-quantum (cq.) states

$$\omega_{XB} = \frac{1}{d} \sum_i |x_i\rangle\langle x_i|_A \otimes |x_i\rangle\langle x_i|_B$$
$$\tau_{ZB} = \frac{1}{d} \sum_j |z_j\rangle\langle z_j|_A \otimes |z_j\rangle\langle z_j|_B$$

- If Alice obtains x_i, Bob processes state x_i. Similar for $\mathbb{Z}$
- Bob can guess K with certainty by measuring his state
- **Entanglement** reduces the Bob's **uncertainty** about K

Entanglement helps!

- Assume $\mathbb{X} = \{|x_i\rangle\}$ and $\mathbb{Z} = \{|z_j\rangle\}$ be complementary on A: $|\langle x_i|z_j\rangle| = 1/\sqrt{d}$ for arbitrary i, j
- Suppose Bob prepares a maximally entangled state

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_i |x_i\rangle_A |x_i\rangle_B = \frac{1}{\sqrt{d}} \sum_j |z_j\rangle_A |z_j\rangle_B$$

  and sends ρ_A to Alice
- Measuring ρ_A with $\mathbb{X}/\mathbb{Z}$, Alice gets classical-quantum (cq.) states

$$\omega_{XB} = \frac{1}{d} \sum_i |x_i\rangle\langle x_i|_A \otimes |x_i\rangle\langle x_i|_B$$

$$\tau_{ZB} = \frac{1}{d} \sum_j |z_j\rangle\langle z_j|_A \otimes |z_j\rangle\langle z_j|_B$$

- If Alice obtains x_i, Bob processes state x_i. Similar for $\mathbb{Z}$
- Bob can guess K with certainty by measuring his state
- **Entanglement** reduces the Bob's **uncertainty** about K

Entanglement helps!

- Assume $\mathbb{X} = \{|x_i\rangle\}$ and $\mathbb{Z} = \{|z_j\rangle\}$ be complementary on A: $|\langle x_i|z_j\rangle| = 1/\sqrt{d}$ for arbitrary i, j
- Suppose Bob prepares a maximally entangled state

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_i |x_i\rangle_A |x_i\rangle_B = \frac{1}{\sqrt{d}} \sum_j |z_j\rangle_A |z_j\rangle_B$$

  and sends ρ_A to Alice
- Measuring ρ_A with $\mathbb{X}/\mathbb{Z}$, Alice gets classical-quantum (cq.) states

$$\begin{aligned} \omega_{XB} &= \frac{1}{d} \sum_i |x_i\rangle\langle x_i|_A \otimes |x_i\rangle\langle x_i|_B \\ \tau_{ZB} &= \frac{1}{d} \sum_j |z_j\rangle\langle z_j|_A \otimes |z_j\rangle\langle z_j|_B \end{aligned}$$

- If Alice obtains x_i, Bob processes state x_i. Similar for $\mathbb{Z}$
- Bob can guess K with certainty by measuring his state
- **Entanglement** reduces the Bob's **uncertainty** about K

Uncertainty relation (in the presence of memory)

- How much can the entanglement reduce uncertainty?
- That is, what if Bob prepares an arbitrary state ρ_{AB}?
- Measuring ρ_A with $\mathbb{X}/\mathbb{Z}$, Alice gets two cq. states

$$\omega_{XB} = \sum_i p_i |x_i\rangle\langle x_i| \otimes \omega_i^B, \quad p_i = \mathrm{Tr}\langle x_i|\rho_{AB}|x_i\rangle,$$

$$\tau_{ZB} = \sum_j q_j |z_j\rangle\langle z_j| \otimes \tau_j^B, \quad q_j = \mathrm{Tr}\langle z_j|\rho_{AB}|z_j\rangle,$$

- To answer this question, we must know
  1. How to quantify the entanglement of ρ_{AB}?
  2. How to quantify the uncertainty of ω_{XB} and τ_{ZB}?
- Uncertainty relation in the presence of memory (UR)[2]

$$\mathrm{H}(X|B)_\omega + \mathrm{H}(Z|B)_\tau \geqslant \log d + \mathrm{H}(A|B)_\rho$$

- $\mathrm{H}(A|B)_{\omega,\tau,\rho}$ is the conditional entropy of state ω, τ, and ρ
- $\mathrm{H}(A|B)$ quantifies the uncertainty about A given knowledge of B

[2] Mario Berta et al. "The uncertainty principle in the presence of quantum memory". In: *Nature Physics* 6.9 (2010), pp. 659–662.

Uncertainty relation (in the presence of memory)

- How much can the entanglement reduce uncertainty?
- That is, what if Bob prepares an arbitrary state ρ_{AB}?
- Measuring ρ_A with $\mathbb{X}/\mathbb{Z}$, Alice gets two cq. states

$$\omega_{XB} = \sum_i p_i |x_i\rangle\langle x_i| \otimes \omega_i^B, \quad p_i = \mathrm{Tr}\langle x_i|\rho_{AB}|x_i\rangle,$$
$$\tau_{ZB} = \sum_j q_j |z_j\rangle\langle z_j| \otimes \tau_j^B, \quad q_j = \mathrm{Tr}\langle z_j|\rho_{AB}|z_j\rangle,$$

- To answer this question, we must know
  1. How to quantify the entanglement of ρ_{AB}?
  2. How to quantify the uncertainty of ω_{XB} and τ_{ZB}?
- Uncertainty relation in the presence of memory (UR)[2]

$$\mathrm{H}(X|B)_\omega + \mathrm{H}(Z|B)_\tau \geqslant \log d + \mathrm{H}(A|B)_\rho$$

- $\mathrm{H}(A|B)_{\omega,\tau,\rho}$ is the conditional entropy of state ω, τ, and ρ
- $\mathrm{H}(A|B)$ quantifies the uncertainty about A given knowledge of B

[2] Mario Berta et al. "The uncertainty principle in the presence of quantum memory". In: *Nature Physics* 6.9 (2010), pp. 659–662.

Uncertainty relation (in the presence of memory)

- How much can the entanglement reduce uncertainty?
- That is, what if Bob prepares an arbitrary state ρ_{AB}?
- Measuring ρ_A with $\mathbb{X}/\mathbb{Z}$, Alice gets two cq. states

$$\omega_{XB} = \sum_i p_i |x_i\rangle\langle x_i| \otimes \omega_i^B, \quad p_i = \mathrm{Tr}\langle x_i|\rho_{AB}|x_i\rangle,$$

$$\tau_{ZB} = \sum_j q_j |z_j\rangle\langle z_j| \otimes \tau_j^B, \quad q_j = \mathrm{Tr}\langle z_j|\rho_{AB}|z_j\rangle,$$

- To answer this question, we must know
  1. How to quantify the entanglement of ρ_{AB}?
  2. How to quantify the uncertainty of ω_{XB} and τ_{ZB}?
- Uncertainty relation in the presence of memory (UR)[2]

$$\mathrm{H}(X|B)_\omega + \mathrm{H}(Z|B)_\tau \geqslant \log d + \mathrm{H}(A|B)_\rho$$

- $\mathrm{H}(A|B)_{\omega,\tau,\rho}$ is the conditional entropy of state ω, τ, and ρ
- $\mathrm{H}(A|B)$ quantifies the uncertainty about A given knowledge of B

[2] Mario Berta et al. "The uncertainty principle in the presence of quantum memory". In: *Nature Physics* 6.9 (2010), pp. 659–662.

Uncertainty relation (in the presence of memory)

- How much can the entanglement reduce uncertainty?
- That is, what if Bob prepares an arbitrary state ρ_{AB}?
- Measuring ρ_A with $\mathbb{X}/\mathbb{Z}$, Alice gets two cq. states

$$\omega_{XB} = \sum_i p_i |x_i\rangle\langle x_i| \otimes \omega_i^B, \quad p_i = \mathrm{Tr}\langle x_i|\rho_{AB}|x_i\rangle,$$

$$\tau_{ZB} = \sum_j q_j |z_j\rangle\langle z_j| \otimes \tau_j^B, \quad q_j = \mathrm{Tr}\langle z_j|\rho_{AB}|z_j\rangle,$$

- To answer this question, we must know
  1. How to quantify the entanglement of ρ_{AB}?
  2. How to quantify the uncertainty of ω_{XB} and τ_{ZB}?
- Uncertainty relation in the presence of memory (UR)[2]

$$\mathrm{H}(X|B)_\omega + \mathrm{H}(Z|B)_\tau \geqslant \log d + \mathrm{H}(A|B)_\rho$$

- $\mathrm{H}(A|B)_{\omega,\tau,\rho}$ is the conditional entropy of state ω, τ, and ρ
- $\mathrm{H}(A|B)$ quantifies the uncertainty about A given knowledge of B

[2] Mario Berta et al. "The uncertainty principle in the presence of quantum memory". In: *Nature Physics* 6.9 (2010), pp. 659–662.

Uncertainty relation (in the presence of memory)

- How much can the entanglement reduce uncertainty?
- That is, what if Bob prepares an arbitrary state ρ_{AB}?
- Measuring ρ_A with $\mathbb{X}/\mathbb{Z}$, Alice gets two cq. states

$$\omega_{XB} = \sum_i p_i |x_i\rangle\langle x_i| \otimes \omega_i^B, \quad p_i = \mathrm{Tr}\langle x_i|\rho_{AB}|x_i\rangle,$$

$$\tau_{ZB} = \sum_j q_j |z_j\rangle\langle z_j| \otimes \tau_j^B, \quad q_j = \mathrm{Tr}\langle z_j|\rho_{AB}|z_j\rangle,$$

- To answer this question, we must know
  1. How to quantify the entanglement of ρ_{AB}?
  2. How to quantify the uncertainty of ω_{XB} and τ_{ZB}?
- Uncertainty relation in the presence of memory (UR)[2]

$$\mathrm{H}(X|B)_\omega + \mathrm{H}(Z|B)_\tau \geqslant \log d + \mathrm{H}(A|B)_\rho$$

- $\mathrm{H}(A|B)_{\omega,\tau,\rho}$ is the conditional entropy of state ω, τ, and ρ
- $\mathrm{H}(A|B)$ quantifies the uncertainty about A given knowledge of B

[2] Mario Berta et al. "The uncertainty principle in the presence of quantum memory". In: *Nature Physics* 6.9 (2010), pp. 659–662.

Uncertainty relation (in the presence of memory)

- How much can the entanglement reduce uncertainty?
- That is, what if Bob prepares an arbitrary state ρ_{AB}?
- Measuring ρ_A with $\mathbb{X}/\mathbb{Z}$, Alice gets two cq. states

$$\omega_{XB} = \sum_i p_i |x_i\rangle\langle x_i| \otimes \omega_i^B, \quad p_i = \mathrm{Tr}\langle x_i|\rho_{AB}|x_i\rangle,$$
$$\tau_{ZB} = \sum_j q_j |z_j\rangle\langle z_j| \otimes \tau_j^B, \quad q_j = \mathrm{Tr}\langle z_j|\rho_{AB}|z_j\rangle,$$

- To answer this question, we must know
  1. How to quantify the entanglement of ρ_{AB}?
  2. How to quantify the uncertainty of ω_{XB} and τ_{ZB}?
- Uncertainty relation in the presence of memory (UR)[2]

$$\mathrm{H}(X|B)_\omega + \mathrm{H}(Z|B)_\tau \ \geqslant\ \log d + \mathrm{H}(A|B)_\rho$$

- $\mathrm{H}(A|B)_{\omega,\tau,\rho}$ is the conditional entropy of state ω, τ, and ρ
- $\mathrm{H}(A|B)$ quantifies the uncertainty about A given knowledge of B

[2] Mario Berta et al. "The uncertainty principle in the presence of quantum memory". In: *Nature Physics* 6.9 (2010), pp. 659–662.

Ingredients of a uncertainty relation

$$\mathrm{H}(X|B)_\omega + \mathrm{H}(Z|B)_\tau \geqslant \log d + \mathrm{H}(A|B)_\rho$$

- Five ingredients of a general uncertainty relation

  Incompatible measurements: $\mathbb{X}$ and $\mathbb{Z}$
  State being measured: bipartite state ρ_{AB}
  Uncertainty measure: conditional entropy $\mathrm{H}(A|B)_{\omega,\tau}$
  Uncertainty relation form: lower bound on sum of uncertainties
  Entanglement measure: conditional entropy $\mathrm{H}(A|B)_\rho$

- Our relation

  Incompatible measurements: complete set of mutually unbiased measurements
  State being measured: bipartite state ρ_{AB}
  Uncertainty measure: conditional collision entropy $\mathrm{H}_2(A|B)_{\omega,\tau}$
  Uncertainty relation form: an equality
  Entanglement measure: conditional collision entropy $\mathrm{H}_2(A|B)_\rho$

Ingredients of a uncertainty relation

$$\mathrm{H}(X|B)_\omega + \mathrm{H}(Z|B)_\tau \;\geqslant\; \log d + \mathrm{H}(A|B)_\rho$$

- Five ingredients of a general uncertainty relation

  Incompatible measurements: $\mathbb{X}$ and $\mathbb{Z}$
  State being measured: bipartite state ρ_{AB}
  Uncertainty measure: conditional entropy $\mathrm{H}(A|B)_{\omega,\tau}$
  Uncertainty relation form: lower bound on sum of uncertainties
  Entanglement measure: conditional entropy $\mathrm{H}(A|B)_\rho$

- Our relation

  Incompatible measurements: complete set of mutually unbiased measurements
  State being measured: bipartite state ρ_{AB}
  Uncertainty measure: conditional collision entropy $\mathrm{H}_2(A|B)_{\omega,\tau}$
  Uncertainty relation form: an equality
  Entanglement measure: conditional collision entropy $\mathrm{H}_2(A|B)_\rho$

Mutually unbiased measurements

- Let $\mathcal{P}^{(1)} = \{P_x^{(1)}\}_{x\in[d]}$ and $\mathcal{P}^{(2)} = \{P_x^{(2)}\}_{x\in[d]}$ be two POVMs:

$$\forall\theta = 1,2, \quad P_x^{(\theta)} \geqslant 0, \quad \sum_x P_x^{(\theta)} = \mathbb{1}$$

- They are mutually unbiased[3] if for all $x, x' \in [d], \theta = 1, 2$

$$\mathrm{Tr}\left[P_x^{(\theta)}\right] = 1, \quad \textit{each operator is normalized}$$

$$\mathrm{Tr}\left[P_x^{(1)} P_x^{(2)}\right] = \frac{1}{d}, \quad \textit{two measurements are unbiased}$$

$$\mathrm{Tr}\left[P_x^{(\theta)} P_{x'}^{(\theta)}\right] = \delta_{x,x'}\kappa + (1-\delta_{x,x'})\frac{1-\kappa}{d-1}.$$

- The *efficiency parameter* κ satisfies $1/d < \kappa \leqslant 1$
- $\{\mathcal{P}^{(\theta)}\}_{\theta\in\Theta}$ forms a set of MUMs if they are pairwise unbiased
- A complete set of MUMs is a set of MUMs of size $d+1$
- A complete set of MUMs can be explicitly constructed[3]

[3] Amir Kalev and Gilad Gour. "Mutually unbiased measurements in finite dimensions". In: *New Journal of Physics* 16.5 (2014), p. 053038.

Mutually unbiased measurements

- Let $\mathcal{P}^{(1)} = \{P_x^{(1)}\}_{x\in[d]}$ and $\mathcal{P}^{(2)} = \{P_x^{(2)}\}_{x\in[d]}$ be two POVMs:

$$\forall\theta = 1, 2, \quad P_x^{(\theta)} \geqslant 0, \quad \sum_x P_x^{(\theta)} = \mathbb{1}$$

- They are mutually unbiased[3] if for all $x, x' \in [d], \theta = 1, 2$

$$\begin{aligned} \mathrm{Tr}\left[P_x^{(\theta)}\right] &= 1, \quad \textit{each operator is normalized} \\ \mathrm{Tr}\left[P_x^{(1)} P_x^{(2)}\right] &= \frac{1}{d}, \quad \textit{two measurements are unbiased} \\ \mathrm{Tr}\left[P_x^{(\theta)} P_{x'}^{(\theta)}\right] &= \delta_{x,x'}\kappa + (1-\delta_{x,x'})\frac{1-\kappa}{d-1}. \end{aligned}$$

- The *efficiency parameter* κ satisfies $1/d < \kappa \leqslant 1$
- $\{\mathcal{P}^{(\theta)}\}_{\theta\in\Theta}$ forms a set of MUMs if they are pairwise unbiased
- A complete set of MUMs is a set of MUMs of size $d+1$
- A complete set of MUMs can be explicitly constructed[3]

[3] Amir Kalev and Gilad Gour. “Mutually unbiased measurements in finite dimensions”. In: *New Journal of Physics* 16.5 (2014), p. 053038.

Mutually unbiased measurements

- Let $\mathcal{P}^{(1)} = \{P_x^{(1)}\}_{x\in[d]}$ and $\mathcal{P}^{(2)} = \{P_x^{(2)}\}_{x\in[d]}$ be two POVMs:

$$\forall\theta = 1,2, \quad P_x^{(\theta)} \geqslant 0, \quad \sum_x P_x^{(\theta)} = \mathbb{1}$$

- They are mutually unbiased[3] if for all $x, x' \in [d], \theta = 1,2$

$$\mathrm{Tr}\left[P_x^{(\theta)}\right] = 1, \quad \textit{each operator is normalized}$$

$$\mathrm{Tr}\left[P_x^{(1)} P_x^{(2)}\right] = \frac{1}{d}, \quad \textit{two measurements are unbiased}$$

$$\mathrm{Tr}\left[P_x^{(\theta)} P_{x'}^{(\theta)}\right] = \delta_{x,x'}\kappa + (1-\delta_{x,x'})\frac{1-\kappa}{d-1}.$$

- The *efficiency parameter* κ satisfies $1/d < \kappa \leqslant 1$
- $\{\mathcal{P}^{(\theta)}\}_{\theta\in\Theta}$ forms a set of MUMs if they are pairwise unbiased
- A complete set of MUMs is a set of MUMs of size $d+1$
- A complete set of MUMs can be explicitly constructed[3]

[3] Amir Kalev and Gilad Gour. "Mutually unbiased measurements in finite dimensions". In: *New Journal of Physics* 16.5 (2014), p. 053038.

Mutually unbiased measurements

- Let $\mathcal{P}^{(1)} = \{P_x^{(1)}\}_{x\in[d]}$ and $\mathcal{P}^{(2)} = \{P_x^{(2)}\}_{x\in[d]}$ be two POVMs:

$$\forall\theta = 1,2, \quad P_x^{(\theta)} \geqslant 0, \quad \sum_x P_x^{(\theta)} = \mathbb{1}$$

- They are mutually unbiased[3] if for all $x, x' \in [d], \theta = 1,2$

$$\begin{aligned} \mathrm{Tr}\left[P_x^{(\theta)}\right] &= 1, && \textit{each operator is normalized} \\ \mathrm{Tr}\left[P_x^{(1)}P_x^{(2)}\right] &= \frac{1}{d}, && \textit{two measurements are unbiased} \\ \mathrm{Tr}\left[P_x^{(\theta)}P_{x'}^{(\theta)}\right] &= \delta_{x,x'}\kappa + (1-\delta_{x,x'})\frac{1-\kappa}{d-1}. \end{aligned}$$

- The *efficiency parameter* κ satisfies $1/d < \kappa \leqslant 1$
- $\{\mathcal{P}^{(\theta)}\}_{\theta\in\Theta}$ forms a set of MUMs if they are pairwise unbiased
- A complete set of MUMs is a set of MUMs of size $d+1$
- A complete set of MUMs can be explicitly constructed[3]

[3] Amir Kalev and Gilad Gour. "Mutually unbiased measurements in finite dimensions". In: *New Journal of Physics* 16.5 (2014), p. 053038.

Mutually unbiased measurements

- Let $\mathcal{P}^{(1)} = \{P_x^{(1)}\}_{x\in[d]}$ and $\mathcal{P}^{(2)} = \{P_x^{(2)}\}_{x\in[d]}$ be two POVMs:

$$\forall\theta = 1,2, \quad P_x^{(\theta)} \geqslant 0, \quad \sum_x P_x^{(\theta)} = \mathbb{1}$$

- They are mutually unbiased[3] if for all $x, x' \in [d], \theta = 1, 2$

$$\mathrm{Tr}\left[P_x^{(\theta)}\right] = 1, \quad \textit{each operator is normalized}$$
$$\mathrm{Tr}\left[P_x^{(1)} P_x^{(2)}\right] = \frac{1}{d}, \quad \textit{two measurements are unbiased}$$
$$\mathrm{Tr}\left[P_x^{(\theta)} P_{x'}^{(\theta)}\right] = \delta_{x,x'}\kappa + (1-\delta_{x,x'})\frac{1-\kappa}{d-1}.$$

- The *efficiency parameter* κ satisfies $1/d < \kappa \leqslant 1$
- $\{\mathcal{P}^{(\theta)}\}_{\theta\in\Theta}$ forms a set of MUMs if they are pairwise unbiased
- A complete set of MUMs is a set of MUMs of size $d+1$
- A complete set of MUMs can be explicitly constructed[3]

[3] Amir Kalev and Gilad Gour. "Mutually unbiased measurements in finite dimensions". In: *New Journal of Physics* 16.5 (2014), p. 053038.

Mutually unbiased measurements

- Let $\mathcal{P}^{(1)} = \{P_x^{(1)}\}_{x\in[d]}$ and $\mathcal{P}^{(2)} = \{P_x^{(2)}\}_{x\in[d]}$ be two POVMs:

$$\forall\theta = 1,2, \quad P_x^{(\theta)} \geqslant 0, \quad \sum_x P_x^{(\theta)} = \mathbb{1}$$

- They are mutually unbiased[3] if for all $x, x' \in [d], \theta = 1, 2$

$$\begin{aligned} \mathrm{Tr}\left[P_x^{(\theta)}\right] &= 1, && \textit{each operator is normalized} \\ \mathrm{Tr}\left[P_x^{(1)} P_x^{(2)}\right] &= \frac{1}{d}, && \textit{two measurements are unbiased} \\ \mathrm{Tr}\left[P_x^{(\theta)} P_{x'}^{(\theta)}\right] &= \delta_{x,x'}\kappa + (1-\delta_{x,x'})\frac{1-\kappa}{d-1}. \end{aligned}$$

- The *efficiency parameter* κ satisfies $1/d < \kappa \leqslant 1$
- $\{\mathcal{P}^{(\theta)}\}_{\theta\in\Theta}$ forms a set of MUMs if they are pairwise unbiased
- A complete set of MUMs is a set of MUMs of size $d + 1$
- A complete set of MUMs can be explicitly constructed[3]

[3] Amir Kalev and Gilad Gour. "Mutually unbiased measurements in finite dimensions". In: *New Journal of Physics* 16.5 (2014), p. 053038.

Conditional collision entropy

- Let ρ_{AB} be a quantum state on system AB
- The conditional collision entropy is defined as[4]

$$\mathrm{H}_2(A|B)_\rho = -\log \mathrm{Tr}\left[\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}\right]$$

- $\mathbb{1}_A$ is the identity operator
- $-\log d \leqslant \mathrm{H}_2(A|B)_\rho \leqslant \log d$
- For separable states σ_{AB}, $\mathrm{H}_2(A|B)_\sigma \geqslant 0$[5]
- $\mathrm{H}_2(A|B)_\rho < 0 \Rightarrow \rho_{AB}$ must be entangled
- Trivializing system B ($\rho_B = 1$), we get the collision entropy

$$\mathrm{H}_2\left(A\right)_\rho = -\log \mathrm{Tr}\,\rho_A^2$$

[4] Marco Tomamichel. *Quantum Information Processing with Finite Resources: Mathematical Foundations*. Vol. 5. Springer, 2015.

[5] Mario Berta, Patrick J Coles, and Stephanie Wehner. "Entanglement-assisted guessing of complementary measurement outcomes". In: *Physical Review A* 90.6 (2014), p. 062127.

Conditional collision entropy

- Let ρ_{AB} be a quantum state on system AB
- The conditional collision entropy is defined as[4]

$$\mathrm{H}_2(A|B)_\rho = -\log \mathrm{Tr}\left[\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}\right]$$

- $\mathbb{1}_A$ is the identity operator
- $-\log d \leqslant \mathrm{H}_2(A|B)_\rho \leqslant \log d$
- For separable states σ_{AB}, $\mathrm{H}_2(A|B)_\sigma \geqslant 0$[5]
- $\mathrm{H}_2(A|B)_\rho < 0 \Rightarrow \rho_{AB}$ must be entangled
- Trivializing system B ($\rho_B = 1$), we get the collision entropy

$$\mathrm{H}_2(A)_\rho = -\log \mathrm{Tr}\, \rho_A^2$$

[4] Marco Tomamichel. *Quantum Information Processing with Finite Resources: Mathematical Foundations*. Vol. 5. Springer, 2015.

[5] Mario Berta, Patrick J Coles, and Stephanie Wehner. "Entanglement-assisted guessing of complementary measurement outcomes". In: *Physical Review A* 90.6 (2014), p. 062127.

Conditional collision entropy

- Let ρ_{AB} be a quantum state on system AB
- The conditional collision entropy is defined as[4]

$$\mathrm{H}_2(A|B)_\rho = -\log \mathrm{Tr}\left[\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}\right]$$

- $\mathbb{1}_A$ is the identity operator
- $-\log d \leqslant \mathrm{H}_2(A|B)_\rho \leqslant \log d$
- For separable states σ_{AB}, $\mathrm{H}_2(A|B)_\sigma \geqslant 0$[5]
- $\mathrm{H}_2(A|B)_\rho < 0 \Rightarrow \rho_{AB}$ must be entangled
- Trivializing system B ($\rho_B = 1$), we get the collision entropy

$$\mathrm{H}_2\left(A\right)_\rho = -\log \mathrm{Tr}\, \rho_A^2$$

[4] Marco Tomamichel. *Quantum Information Processing with Finite Resources: Mathematical Foundations*. Vol. 5. Springer, 2015.

[5] Mario Berta, Patrick J Coles, and Stephanie Wehner. "Entanglement-assisted guessing of complementary measurement outcomes". In: *Physical Review A* 90.6 (2014), p. 062127.

Conditional collision entropy

- Let ρ_{AB} be a quantum state on system AB
- The conditional collision entropy is defined as[4]

$$\mathrm{H}_2(A|B)_\rho = -\log \mathrm{Tr}\left[\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}\right]$$

- $\mathbb{1}_A$ is the identity operator
- $-\log d \leqslant \mathrm{H}_2(A|B)_\rho \leqslant \log d$
- For separable states σ_{AB}, $\mathrm{H}_2(A|B)_\sigma \geqslant 0$[5]
- $\mathrm{H}_2(A|B)_\rho < 0 \Rightarrow \rho_{AB}$ must be entangled
- Trivializing system B ($\rho_B = 1$), we get the collision entropy

$$\mathrm{H}_2\left(A\right)_\rho = -\log \mathrm{Tr}\,\rho_A^2$$

[4] Marco Tomamichel. *Quantum Information Processing with Finite Resources: Mathematical Foundations*. Vol. 5. Springer, 2015.

[5] Mario Berta, Patrick J Coles, and Stephanie Wehner. "Entanglement-assisted guessing of complementary measurement outcomes". In: *Physical Review A* 90.6 (2014), p. 062127.

Conditional collision entropy

- Let ρ_{AB} be a quantum state on system AB
- The conditional collision entropy is defined as[4]

$$\mathrm{H}_2(A|B)_\rho = -\log \mathrm{Tr}\left[\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}\right]$$

- $\mathbb{1}_A$ is the identity operator
- $-\log d \leqslant \mathrm{H}_2(A|B)_\rho \leqslant \log d$
- For separable states σ_{AB}, $\mathrm{H}_2(A|B)_\sigma \geqslant 0$[5]
- $\mathrm{H}_2(A|B)_\rho < 0 \Rightarrow \rho_{AB}$ must be entangled
- Trivializing system B ($\rho_B = 1$), we get the collision entropy

$$\mathrm{H}_2\left(A\right)_\rho = -\log \mathrm{Tr}\,\rho_A^2$$

[4] Marco Tomamichel. *Quantum Information Processing with Finite Resources: Mathematical Foundations*. Vol. 5. Springer, 2015.

[5] Mario Berta, Patrick J Coles, and Stephanie Wehner. "Entanglement-assisted guessing of complementary measurement outcomes". In: *Physical Review A* 90.6 (2014), p. 062127.

Conditional collision entropy

- Let ρ_{AB} be a quantum state on system AB
- The conditional collision entropy is defined as[4]

$$\mathrm{H}_2(A|B)_\rho = -\log \mathrm{Tr}\left[\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}\rho_{AB}(\mathbb{1}_A \otimes \rho_B)^{-1/2}\right]$$

- $\mathbb{1}_A$ is the identity operator
- $-\log d \leqslant \mathrm{H}_2(A|B)_\rho \leqslant \log d$
- For separable states σ_{AB}, $\mathrm{H}_2(A|B)_\sigma \geqslant 0$[5]
- $\mathrm{H}_2(A|B)_\rho < 0 \Rightarrow \rho_{AB}$ must be entangled
- Trivializing system B ($\rho_B = 1$), we get the collision entropy

$$\mathrm{H}_2\left(A\right)_\rho = -\log \mathrm{Tr}\,\rho_A^2$$

[4] Marco Tomamichel. *Quantum Information Processing with Finite Resources: Mathematical Foundations*. Vol. 5. Springer, 2015.

[5] Mario Berta, Patrick J Coles, and Stephanie Wehner. "Entanglement-assisted guessing of complementary measurement outcomes". In: *Physical Review A* 90.6 (2014), p. 062127.

Outline

Post-measurement state for a MUM

- Let $\mathcal{P}^{(\theta)} = \{P_x^{(\theta)}\}_{x\in[d]}$ be a MUM in A
- Measuring ρ_{AB} on A by $\mathcal{P}^{(\theta)}$, we get a cq. state

$$\omega_{X^{(\theta)}B} = \sum_{x=1}^{d} |x\rangle\langle x|_X \otimes \mathrm{Tr}_A\left[\left(P_x^{(\theta)} \otimes \mathbb{1}_B\right)\rho_{AB}\right] \qquad (1)$$

- Register X stores the measurement outcome
- $\mathrm{Tr}_A[(P_x^{(\theta)} \otimes \mathbb{1}_B)\rho_{AB}]$ is the post-measurement state (unnormalized) left on system B
- $\mathrm{Tr}[(P_x^{(\theta)} \otimes \mathbb{1}_B)\rho_{AB}]$ is probability that the outcome is x

Post-measurement state for a MUM

- Let $\mathcal{P}^{(\theta)} = \{P_x^{(\theta)}\}_{x\in[d]}$ be a MUM in A
- Measuring ρ_{AB} on A by $\mathcal{P}^{(\theta)}$, we get a cq. state

$$\omega_{X^{(\theta)}B} = \sum_{x=1}^{d} |x\rangle\langle x|_X \otimes \mathrm{Tr}_A \left[\left(P_x^{(\theta)} \otimes \mathbb{1}_B\right) \rho_{AB}\right] \qquad (1)$$

- Register X stores the measurement outcome
- $\mathrm{Tr}_A[(P_x^{(\theta)} \otimes \mathbb{1}_B)\rho_{AB}]$ is the post-measurement state (unnormalized) left on system B
- $\mathrm{Tr}[(P_x^{(\theta)} \otimes \mathbb{1}_B)\rho_{AB}]$ is probability that the outcome is x

Post-measurement state for a MUM

- Let $\mathcal{P}^{(\theta)} = \{P_x^{(\theta)}\}_{x\in[d]}$ be a MUM in A
- Measuring ρ_{AB} on A by $\mathcal{P}^{(\theta)}$, we get a cq. state

$$\omega_{X^{(\theta)}B} = \sum_{x=1}^{d} |x\rangle\langle x|_X \otimes \mathrm{Tr}_A\left[\left(P_x^{(\theta)} \otimes \mathbb{1}_B\right)\rho_{AB}\right] \tag{1}$$

- Register X stores the measurement outcome
- $\mathrm{Tr}_A[(P_x^{(\theta)} \otimes \mathbb{1}_B)\rho_{AB}]$ is the post-measurement state (unnormalized) left on system B
- $\mathrm{Tr}[(P_x^{(\theta)} \otimes \mathbb{1}_B)\rho_{AB}]$ is probability that the outcome is x

Post-measurement state for a MUM

- Let $\mathcal{P}^{(\theta)} = \{P_x^{(\theta)}\}_{x \in [d]}$ be a MUM in A
- Measuring ρ_{AB} on A by $\mathcal{P}^{(\theta)}$, we get a cq. state

$$\omega_{X^{(\theta)}B} = \sum_{x=1}^{d} |x\rangle\langle x|_X \otimes \mathrm{Tr}_A \left[\left(P_x^{(\theta)} \otimes \mathbb{1}_B \right) \rho_{AB} \right] \qquad (1)$$

- Register X stores the measurement outcome
- $\mathrm{Tr}_A[(P_x^{(\theta)} \otimes \mathbb{1}_B)\rho_{AB}]$ is the post-measurement state (unnormalized) left on system B
- $\mathrm{Tr}[(P_x^{(\theta)} \otimes \mathbb{1}_B)\rho_{AB}]$ is probability that the outcome is x

Post-measurement state for complete set of MUMs

- Let $\{\mathcal{P}^{(\theta)}\}_{\theta\in[d+1]}$ be a complete set of MUMs on system A
- Define the following cq. state

$$\omega_{XB\Theta} = \frac{1}{d+1}\sum_{\theta=1}^{d+1}\sum_{x=1}^{d} |x\rangle\langle x|_X \otimes \mathrm{Tr}_A\left[\left(P_x^{(\theta)}\otimes \mathbb{1}_B\right)\rho_{AB}\right]\otimes|\theta\rangle\langle\theta|_\Theta \quad (2)$$

- Θ indicates which MUM has been performed
- $\omega_{XB\Theta}$ is a uniform mixing of $\omega_{X^{(\theta)}B}$: $\omega_{XB\Theta=\theta} = \omega_{X^{(\theta)}B}$
- Conditional collision entropy of $\omega_{XB\Theta}$, with partition $X{:}B\Theta$

$$\mathrm{H}_2\left(X|B\Theta\right)_\omega = -\log\left(\frac{1}{d+1}\sum_{\theta,x}\mathrm{Tr}_B\left\{\mathrm{Tr}_A[P_x^{(\theta)}\widetilde{\rho}_{AB}]^2\right\}\right)$$

where $\widetilde{\rho}_{AB} = \rho_B^{-1/4}\rho_{AB}\rho_B^{-1/4}$

Post-measurement state for complete set of MUMs

- Let $\{\mathcal{P}^{(\theta)}\}_{\theta\in[d+1]}$ be a complete set of MUMs on system A
- Define the following cq. state

$$\omega_{XB\Theta} = \frac{1}{d+1}\sum_{\theta=1}^{d+1}\sum_{x=1}^{d} |x\rangle\langle x|_X \otimes \mathrm{Tr}_A\left[\left(P_x^{(\theta)} \otimes \mathbb{1}_B\right)\rho_{AB}\right] \otimes |\theta\rangle\langle\theta|_\Theta \quad (2)$$

- Θ indicates which MUM has been performed
- $\omega_{XB\Theta}$ is a uniform mixing of $\omega_{X^{(\theta)}B}$: $\omega_{XB\Theta=\theta} = \omega_{X^{(\theta)}B}$
- Conditional collision entropy of $\omega_{XB\Theta}$, with partition $X{:}B\Theta$

$$\mathrm{H}_2\left(X|B\Theta\right)_\omega = -\log\left(\frac{1}{d+1}\sum_{\theta,x}\mathrm{Tr}_B\left\{\mathrm{Tr}_A[P_x^{(\theta)}\widetilde{\rho}_{AB}]^2\right\}\right)$$

where $\widetilde{\rho}_{AB} = \rho_B^{-1/4}\rho_{AB}\rho_B^{-1/4}$

Post-measurement state for complete set of MUMs

- Let $\{\mathcal{P}^{(\theta)}\}_{\theta\in[d+1]}$ be a complete set of MUMs on system A
- Define the following cq. state

$$\omega_{XB\Theta} = \frac{1}{d+1}\sum_{\theta=1}^{d+1}\sum_{x=1}^{d} |x\rangle\langle x|_X \otimes \mathrm{Tr}_A\left[\left(P_x^{(\theta)}\otimes \mathbb{1}_B\right)\rho_{AB}\right]\otimes|\theta\rangle\langle\theta|_\Theta \quad (2)$$

- Θ indicates which MUM has been performed
- $\omega_{XB\Theta}$ is a uniform mixing of $\omega_{X^{(\theta)}B}$: $\omega_{XB\Theta=\theta} = \omega_{X^{(\theta)}B}$
- Conditional collision entropy of $\omega_{XB\Theta}$, with partition $X{:}B\Theta$

$$\mathrm{H}_2\left(X|B\Theta\right)_\omega = -\log\left(\frac{1}{d+1}\sum_{\theta,x}\mathrm{Tr}_B\left\{\mathrm{Tr}_A[P_x^{(\theta)}\widetilde{\rho}_{AB}]^2\right\}\right)$$

where $\widetilde{\rho}_{AB} = \rho_B^{-1/4}\rho_{AB}\rho_B^{-1/4}$

Post-measurement state for complete set of MUMs

- Let $\{\mathcal{P}^{(\theta)}\}_{\theta \in [d+1]}$ be a complete set of MUMs on system A
- Define the following cq. state

$$\omega_{XB\Theta} = \frac{1}{d+1} \sum_{\theta=1}^{d+1} \sum_{x=1}^{d} |x\rangle\langle x|_X \otimes \mathrm{Tr}_A \left[\left(P_x^{(\theta)} \otimes \mathbb{1}_B \right) \rho_{AB} \right] \otimes |\theta\rangle\langle\theta|_\Theta \quad (2)$$

- Θ indicates which MUM has been performed
- $\omega_{XB\Theta}$ is a uniform mixing of $\omega_{X^{(\theta)}B}$: $\omega_{XB\Theta=\theta} = \omega_{X^{(\theta)}B}$
- Conditional collision entropy of $\omega_{XB\Theta}$, with partition $X{:}B\Theta$

$$\mathrm{H}_2 \left(X|B\Theta \right)_\omega = -\log \left(\frac{1}{d+1} \sum_{\theta,x} \mathrm{Tr}_B \left\{ \mathrm{Tr}_A [P_x^{(\theta)} \widetilde{\rho}_{AB}]^2 \right\} \right)$$

where $\widetilde{\rho}_{AB} = \rho_B^{-1/4} \rho_{AB} \rho_B^{-1/4}$

Post-measurement state for complete set of MUMs

- Let $\{\mathcal{P}^{(\theta)}\}_{\theta\in[d+1]}$ be a complete set of MUMs on system A
- Define the following cq. state

$$\omega_{XB\Theta} = \frac{1}{d+1}\sum_{\theta=1}^{d+1}\sum_{x=1}^{d} |x\rangle\langle x|_X \otimes \mathrm{Tr}_A\left[\left(P_x^{(\theta)}\otimes \mathbb{1}_B\right)\rho_{AB}\right]\otimes|\theta\rangle\langle\theta|_\Theta \quad (2)$$

- Θ indicates which MUM has been performed
- $\omega_{XB\Theta}$ is a uniform mixing of $\omega_{X^{(\theta)}B}$: $\omega_{XB\Theta=\theta} = \omega_{X^{(\theta)}B}$
- Conditional collision entropy of $\omega_{XB\Theta}$, with partition $X{:}B\Theta$

$$\mathrm{H}_2\left(X|B\Theta\right)_\omega = -\log\left(\frac{1}{d+1}\sum_{\theta,x}\mathrm{Tr}_B\left\{\mathrm{Tr}_A[P_x^{(\theta)}\widetilde{\rho}_{AB}]^2\right\}\right)$$

where $\widetilde{\rho}_{AB} = \rho_B^{-1/4}\rho_{AB}\rho_B^{-1/4}$

Theorem (An equality relation for complete set of MUMs)

Let $\{\mathcal{P}^{(\theta)}\}_{\theta\in[d+1]}$ *be a complete set of MUMs on system* A*. For arbitrary quantum state* ρ_{AB}*, it holds that*

$$\mathrm{H}_2\left(A|B\Theta\right)_\omega = \log\left(d+1\right) - \log\left(f(\kappa) + g(\kappa)2^{-\,\mathrm{H}_2(A|B)_\rho}\right), \quad (3)$$

where $\omega_{XB\Theta}$ *is defined in Eq.* (2)*, and the coefficients are given by*

$$f(\kappa) = 1 + \frac{1-\kappa}{d-1}, \quad g(\kappa) = \frac{\kappa d - 1}{d-1}.$$

- When $\kappa = 1$, Eq. (3) recovers the main result of [2][6]

$$\mathrm{H}_2\left(A|B\Theta\right)_\omega = \log\left(d+1\right) - \log\left(1 + 2^{-\,\mathrm{H}_2(A|B)_\rho}\right)$$

[6] Mario Berta, Patrick J Coles, and Stephanie Wehner. "Entanglement-assisted guessing of complementary measurement outcomes". In: *Physical Review A* 90.6 (2014), p. 062127.

Outline

Pretty-good state discrimination

- **State discrimination:** Let $\mathcal{S} = \{p_i, \rho_i\}$ be a state ensemble. Sample σ from $\mathcal{S}$. What is the index i of σ?
- Perform a measurement $\mathcal{M} = \{M_i\}$ to extract index: if the measurement outcome is i, then assert $\sigma \equiv \rho_i$
- Finding optimal measurement is a complex optimization problem[7]
- **Pretty-good measurement**[8] $\mathcal{M}^{\mathrm{pg}} = \{M_i\}$ of $\mathcal{S}$: $M_i = \rho^{-1/2}(p_i\rho_i)\rho^{-1/2}$, where $\rho = \sum_i p_i\rho_i$
- Pretty-good guessing probability

$$\mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = \sum_i p_i^2 \operatorname{Tr}[\rho^{-1/2}\rho_i\rho^{-1/2}\rho_i]$$

- $\mathcal{S}$ is equivalent to a cq. state $\rho_{XB} = \sum_i p_i|i\rangle\langle i| \otimes \rho_i^B$
- Operational interpretation of the conditional collision entropy[9]

$$\mathrm{P}^{\mathrm{pg}}(X|B)_\rho \equiv \mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = 2^{-\mathrm{H}_2(X|B)_\rho}$$

[7] Joonwoo Bae and Leong-Chuan Kwek. "Quantum state discrimination and its applications". In: *Journal of Physics A: Mathematical and Theoretical* 48.8 (2015), p. 083001.

[8] Paul Hausladen and William K Wootters. "A 'pretty good'measurement for distinguishing quantum states". In: *Journal of Modern Optics* 41.12 (1994), pp. 2385–2390.

[9] Harry Buhrman et al. "Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment". In: *Physical Review A* 78.2 (2008), p. 022316.

Pretty-good state discrimination

- **State discrimination:** Let $\mathcal{S} = \{p_i, \rho_i\}$ be a state ensemble. Sample σ from $\mathcal{S}$. What is the index i of σ?
- Perform a measurement $\mathcal{M} = \{M_i\}$ to extract index: if the measurement outcome is i, then assert $\sigma \equiv \rho_i$
- Finding optimal measurement is a complex optimization problem[7]
- **Pretty-good measurement**[8] $\mathcal{M}^{\mathrm{pg}} = \{M_i\}$ of $\mathcal{S}$: $M_i = \rho^{-1/2}(p_i\rho_i)\rho^{-1/2}$, where $\rho = \sum_i p_i\rho_i$
- Pretty-good guessing probability

$$\mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = \sum_i p_i^2 \operatorname{Tr}[\rho^{-1/2}\rho_i\rho^{-1/2}\rho_i]$$

- $\mathcal{S}$ is equivalent to a cq. state $\rho_{XB} = \sum_i p_i|i\rangle\langle i| \otimes \rho_i^B$
- Operational interpretation of the conditional collision entropy[9]

$$\mathrm{P}^{\mathrm{pg}}(X|B)_\rho \equiv \mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = 2^{-\mathrm{H}_2(X|B)_\rho}$$

---

[7] Joonwoo Bae and Leong-Chuan Kwek. "Quantum state discrimination and its applications". In: *Journal of Physics A: Mathematical and Theoretical* 48.8 (2015), p. 083001.

[8] Paul Hausladen and William K Wootters. "A 'pretty good'measurement for distinguishing quantum states". In: *Journal of Modern Optics* 41.12 (1994), pp. 2385–2390.

[9] Harry Buhrman et al. "Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment". In: *Physical Review A* 78.2 (2008), p. 022316.

Pretty-good state discrimination

- **State discrimination:** Let $\mathcal{S} = \{p_i, \rho_i\}$ be a state ensemble. Sample σ from $\mathcal{S}$. What is the index i of σ?
- Perform a measurement $\mathcal{M} = \{M_i\}$ to extract index: if the measurement outcome is i, then assert $\sigma \equiv \rho_i$
- Finding optimal measurement is a complex optimization problem[7]
- **Pretty-good measurement**[8] $\mathcal{M}^{\mathrm{pg}} = \{M_i\}$ of $\mathcal{S}$: $M_i = \rho^{-1/2}(p_i\rho_i)\rho^{-1/2}$, where $\rho = \sum_i p_i\rho_i$
- Pretty-good guessing probability

$$\mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = \sum_i p_i^2 \,\mathrm{Tr}[\rho^{-1/2}\rho_i\rho^{-1/2}\rho_i]$$

- $\mathcal{S}$ is equivalent to a cq. state $\rho_{XB} = \sum_i p_i|i\rangle\langle i| \otimes \rho_i^B$
- Operational interpretation of the conditional collision entropy[9]

$$\mathrm{P}^{\mathrm{pg}}(X|B)_\rho \equiv \mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = 2^{-\mathrm{H}_2(X|B)_\rho}$$

[7] Joonwoo Bae and Leong-Chuan Kwek. "Quantum state discrimination and its applications". In: *Journal of Physics A: Mathematical and Theoretical* 48.8 (2015), p. 083001.

[8] Paul Hausladen and William K Wootters. "A 'pretty good'measurement for distinguishing quantum states". In: *Journal of Modern Optics* 41.12 (1994), pp. 2385–2390.

[9] Harry Buhrman et al. "Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment". In: *Physical Review A* 78.2 (2008), p. 022316.

Pretty-good state discrimination

- **State discrimination:** Let $\mathcal{S} = \{p_i, \rho_i\}$ be a state ensemble. Sample σ from $\mathcal{S}$. What is the index i of σ?
- Perform a measurement $\mathcal{M} = \{M_i\}$ to extract index: if the measurement outcome is i, then assert $\sigma \equiv \rho_i$
- Finding optimal measurement is a complex optimization problem[7]
- **Pretty-good measurement**[8] $\mathcal{M}^{\mathrm{pg}} = \{M_i\}$ of $\mathcal{S}$: $M_i = \rho^{-1/2}(p_i\rho_i)\rho^{-1/2}$, where $\rho = \sum_i p_i\rho_i$
- Pretty-good guessing probability

$$\mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = \sum_i p_i^2 \,\mathrm{Tr}[\rho^{-1/2}\rho_i\rho^{-1/2}\rho_i]$$

- $\mathcal{S}$ is equivalent to a cq. state $\rho_{XB} = \sum_i p_i |i\rangle\langle i| \otimes \rho_i^B$
- Operational interpretation of the conditional collision entropy[9]

$$\mathrm{P}^{\mathrm{pg}}(X|B)_\rho \equiv \mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = 2^{-\,\mathrm{H}_2(X|B)_\rho}$$

[7] Joonwoo Bae and Leong-Chuan Kwek. "Quantum state discrimination and its applications". In: *Journal of Physics A: Mathematical and Theoretical* 48.8 (2015), p. 083001.

[8] Paul Hausladen and William K Wootters. "A 'pretty good'measurement for distinguishing quantum states". In: *Journal of Modern Optics* 41.12 (1994), pp. 2385–2390.

[9] Harry Buhrman et al. "Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment". In: *Physical Review A* 78.2 (2008), p. 022316.

Pretty-good state discrimination

- **State discrimination:** Let $\mathcal{S} = \{p_i, \rho_i\}$ be a state ensemble. Sample σ from $\mathcal{S}$. What is the index i of σ?
- Perform a measurement $\mathcal{M} = \{M_i\}$ to extract index: if the measurement outcome is i, then assert $\sigma \equiv \rho_i$
- Finding optimal measurement is a complex optimization problem[7]
- **Pretty-good measurement**[8] $\mathcal{M}^{\mathrm{pg}} = \{M_i\}$ of $\mathcal{S}$: $M_i = \rho^{-1/2}(p_i\rho_i)\rho^{-1/2}$, where $\rho = \sum_i p_i\rho_i$
- Pretty-good guessing probability

$$\mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = \sum_i p_i^2 \,\mathrm{Tr}[\rho^{-1/2}\rho_i\rho^{-1/2}\rho_i]$$

- $\mathcal{S}$ is equivalent to a cq. state $\rho_{XB} = \sum_i p_i|i\rangle\langle i| \otimes \rho_i^B$
- Operational interpretation of the conditional collision entropy[9]

$$\mathrm{P}^{\mathrm{pg}}(X|B)_\rho \equiv \mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = 2^{-\mathrm{H}_2(X|B)_\rho}$$

[7] Joonwoo Bae and Leong-Chuan Kwek. "Quantum state discrimination and its applications". In: *Journal of Physics A: Mathematical and Theoretical* 48.8 (2015), p. 083001.

[8] Paul Hausladen and William K Wootters. "A 'pretty good'measurement for distinguishing quantum states". In: *Journal of Modern Optics* 41.12 (1994), pp. 2385–2390.

[9] Harry Buhrman et al. "Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment". In: *Physical Review A* 78.2 (2008), p. 022316.

Pretty-good state discrimination

- **State discrimination:** Let $\mathcal{S} = \{p_i, \rho_i\}$ be a state ensemble. Sample σ from $\mathcal{S}$. What is the index i of σ?
- Perform a measurement $\mathcal{M} = \{M_i\}$ to extract index: if the measurement outcome is i, then assert $\sigma \equiv \rho_i$
- Finding optimal measurement is a complex optimization problem[7]
- **Pretty-good measurement**[8] $\mathcal{M}^{\mathrm{pg}} = \{M_i\}$ of $\mathcal{S}$: $M_i = \rho^{-1/2}(p_i\rho_i)\rho^{-1/2}$, where $\rho = \sum_i p_i\rho_i$
- Pretty-good guessing probability

$$\mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = \sum_i p_i^2 \,\mathrm{Tr}[\rho^{-1/2}\rho_i\rho^{-1/2}\rho_i]$$

- $\mathcal{S}$ is equivalent to a cq. state $\rho_{XB} = \sum_i p_i |i\rangle\langle i| \otimes \rho_i^B$
- Operational interpretation of the conditional collision entropy[9]

$$\mathrm{P}^{\mathrm{pg}}(X|B)_\rho \equiv \mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = 2^{-\mathrm{H}_2(X|B)_\rho}$$

[7] Joonwoo Bae and Leong-Chuan Kwek. "Quantum state discrimination and its applications". In: *Journal of Physics A: Mathematical and Theoretical* 48.8 (2015), p. 083001.

[8] Paul Hausladen and William K Wootters. "A 'pretty good'measurement for distinguishing quantum states". In: *Journal of Modern Optics* 41.12 (1994), pp. 2385–2390.

[9] Harry Buhrman et al. "Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment". In: *Physical Review A* 78.2 (2008), p. 022316.

Pretty-good state discrimination

- **State discrimination:** Let $\mathcal{S} = \{p_i, \rho_i\}$ be a state ensemble. Sample σ from $\mathcal{S}$. What is the index i of σ?
- Perform a measurement $\mathcal{M} = \{M_i\}$ to extract index: if the measurement outcome is i, then assert $\sigma \equiv \rho_i$
- Finding optimal measurement is a complex optimization problem[7]
- **Pretty-good measurement**[8] $\mathcal{M}^{\mathrm{pg}} = \{M_i\}$ of $\mathcal{S}$: $M_i = \rho^{-1/2}(p_i\rho_i)\rho^{-1/2}$, where $\rho = \sum_i p_i\rho_i$
- Pretty-good guessing probability

$$\mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = \sum_i p_i^2 \,\mathrm{Tr}[\rho^{-1/2}\rho_i\rho^{-1/2}\rho_i]$$

- $\mathcal{S}$ is equivalent to a cq. state $\rho_{XB} = \sum_i p_i |i\rangle\langle i| \otimes \rho_i^B$
- Operational interpretation of the conditional collision entropy[9]

$$\mathrm{P}^{\mathrm{pg}}(X|B)_\rho \equiv \mathrm{P}^{\mathrm{pg}}(\mathcal{S}) = 2^{-\,\mathrm{H}_2(X|B)_\rho}$$

[7] Joonwoo Bae and Leong-Chuan Kwek. "Quantum state discrimination and its applications". In: *Journal of Physics A: Mathematical and Theoretical* 48.8 (2015), p. 083001.

[8] Paul Hausladen and William K Wootters. "A 'pretty good'measurement for distinguishing quantum states". In: *Journal of Modern Optics* 41.12 (1994), pp. 2385–2390.

[9] Harry Buhrman et al. "Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment". In: *Physical Review A* 78.2 (2008), p. 022316.

Pretty-good guessing for a complete set of MUMs

- Each MUM induces a cq. state of the form

$$\omega_{X^{(\theta)}B} = \sum_{x=1}^{d} |x\rangle\langle x| \otimes \mathrm{Tr}_A \left[\left(P_x^{(\theta)} \otimes \mathbb{1}_B \right) \rho_{AB} \right]$$

- How well can Bob guess x?
  - He can guess "pretty-good": $\mathrm{P}^{\mathrm{pg}}(X^{(\theta)}|B)_\omega$
- How well can Bob guess x for a complete set of MUMs, on average?
- *Totally* determined by the quantum collision entropy of ρ_{AB}

Lemma

Let $\{\mathcal{P}^{(\theta)}\}_{\theta \in [d+1]}$ be a complete set of MUMs on system A. For arbitrary quantum state ρ_{AB}, it holds that

$$\sum_{\theta=1}^{d+1} \mathrm{P}^{\mathrm{pg}} \left(X^{(\theta)} \middle| B \right)_\omega = f(\kappa) + g(\kappa) 2^{-\mathrm{H}_2(A|B)_\rho}.$$

Pretty-good guessing for a complete set of MUMs

- Each MUM induces a cq. state of the form

$$\omega_{X^{(\theta)}B} = \sum_{x=1}^{d} |x\rangle\langle x| \otimes \mathrm{Tr}_A \left[\left(P_x^{(\theta)} \otimes \mathbb{1}_B \right) \rho_{AB} \right]$$

- How well can Bob guess x?
  - He can guess "pretty-good": $\mathrm{P}^{\mathrm{pg}}(X^{(\theta)}|B)_\omega$
- How well can Bob guess x for a complete set of MUMs, on average?
- *Totally* determined by the quantum collision entropy of ρ_{AB}

Lemma
Let $\{\mathcal{P}^{(\theta)}\}_{\theta \in [d+1]}$ be a complete set of MUMs on system A. For arbitrary quantum state ρ_{AB}, it holds that

$$\sum_{\theta=1}^{d+1} \mathrm{P}^{\mathrm{pg}} \left(X^{(\theta)} \middle| B \right)_\omega = f(\kappa) + g(\kappa) 2^{-\mathrm{H}_2(A|B)_\rho}.$$

Pretty-good guessing for a complete set of MUMs

- Each MUM induces a cq. state of the form

$$\omega_{X^{(\theta)}B} = \sum_{x=1}^{d} |x\rangle\langle x| \otimes \mathrm{Tr}_A \left[\left(P_x^{(\theta)} \otimes \mathbb{1}_B \right) \rho_{AB} \right]$$

- How well can Bob guess x?
  - He can guess "pretty-good": $\mathrm{P}^{\mathrm{pg}}(X^{(\theta)}|B)_\omega$
- How well can Bob guess x for a complete set of MUMs, on average?
- *Totally* determined by the quantum collision entropy of ρ_{AB}

Lemma

Let $\{\mathcal{P}^{(\theta)}\}_{\theta\in[d+1]}$ be a complete set of MUMs on system A. For arbitrary quantum state ρ_{AB}, it holds that

$$\sum_{\theta=1}^{d+1} \mathrm{P}^{\mathrm{pg}} \left(X^{(\theta)} \middle| B \right)_\omega = f(\kappa) + g(\kappa) 2^{-\mathrm{H}_2(A|B)_\rho}.$$

Pretty-good guessing for a complete set of MUMs

- Each MUM induces a cq. state of the form

$$\omega_{X^{(\theta)}B} = \sum_{x=1}^{d} |x\rangle\langle x| \otimes \mathrm{Tr}_A \left[\left(P_x^{(\theta)} \otimes \mathbb{1}_B \right) \rho_{AB} \right]$$

- How well can Bob guess x?
  - He can guess "pretty-good": $\mathrm{P}^{\mathrm{pg}}(X^{(\theta)}|B)_\omega$
- How well can Bob guess x for a complete set of MUMs, on average?
- *Totally* determined by the quantum collision entropy of ρ_{AB}

Lemma

Let $\{\mathcal{P}^{(\theta)}\}_{\theta \in [d+1]}$ *be a complete set of MUMs on system* A*. For arbitrary quantum state* ρ_{AB}*, it holds that*

$$\sum_{\theta=1}^{d+1} \mathrm{P}^{\mathrm{pg}} \left(X^{(\theta)} \middle| B \right)_\omega = f(\kappa) + g(\kappa) 2^{-\mathrm{H}_2(A|B)_\rho}.$$

Lower bound on sum of uncertainties

- Uncertainty relations are commonly expressed as lower bound on the sum of uncertainties

Lemma

Let $\{\mathcal{P}^{(\theta)}\}_{\theta \in [d+1]}$ be a complete set of MUMs on system A. For arbitrary quantum state ρ_{AB}, it holds that

$$\frac{1}{d+1} \sum_{\theta=1}^{d+1} \mathrm{H}_2 \left(X^{(\theta)} \middle| B \right)_\omega \geqslant \log(d+1) - \log\left(f(\kappa) + g(\kappa) 2^{-\mathrm{H}_2(A|B)_\rho} \right), \quad (4)$$

- Trivializing system B, Eq. (4) reduces to

$$\frac{1}{d+1} \sum_{\theta=1}^{d+1} \mathrm{H}_2 \left(X^{(\theta)} \right)_\omega \geqslant \log(d+1) - \log\left(f(\kappa) + g(\kappa) \operatorname{Tr}[\rho_A^2] \right)$$

- This is a uncertainty relation without memory
- Recovers a special case ($\alpha = 2$) of **Proposition 3** in [9][10]

[10] Alexey E Rastegin. "On uncertainty relations and entanglement detection with mutually unbiased measurements". In: *Open Systems & Information Dynamics* 22.01 (2015), p. 1550005.

Lower bound on sum of uncertainties

- Uncertainty relations are commonly expressed as lower bound on the sum of uncertainties

Lemma

Let $\{\mathcal{P}^{(\theta)}\}_{\theta\in[d+1]}$ *be a complete set of MUMs on system* A*. For arbitrary quantum state* ρ_{AB}*, it holds that*

$$\frac{1}{d+1}\sum_{\theta=1}^{d+1} \mathrm{H}_2\left(X^{(\theta)}\middle|B\right)_\omega \geqslant \log\left(d+1\right) - \log\left(f(\kappa)+g(\kappa)2^{-\,\mathrm{H}_2(A|B)_\rho}\right), \tag{4}$$

- Trivializing system B, Eq. (4) reduces to

$$\frac{1}{d+1}\sum_{\theta=1}^{d+1} \mathrm{H}_2\left(X^{(\theta)}\right)_\omega \geqslant \log\left(d+1\right) - \log\left(f(\kappa)+g(\kappa)\,\mathrm{Tr}[\rho_A^2]\right)$$

- This is a uncertainty relation without memory
- Recovers a special case ($\alpha = 2$) of **Proposition 3** in [9][10]

[10] Alexey E Rastegin. "On uncertainty relations and entanglement detection with mutually unbiased measurements". In: *Open Systems & Information Dynamics* 22.01 (2015), p. 1550005.

Lower bound on sum of uncertainties

- Uncertainty relations are commonly expressed as lower bound on the sum of uncertainties

Lemma

Let $\{\mathcal{P}^{(\theta)}\}_{\theta\in[d+1]}$ be a complete set of MUMs on system A. For arbitrary quantum state ρ_{AB}, it holds that

$$\frac{1}{d+1}\sum_{\theta=1}^{d+1} \mathrm{H}_2\left(X^{(\theta)}\middle|B\right)_\omega \geqslant \log(d+1) - \log\left(f(\kappa) + g(\kappa)2^{-\mathrm{H}_2(A|B)_\rho}\right), \qquad (4)$$

- Trivializing system B, Eq. (4) reduces to

$$\frac{1}{d+1}\sum_{\theta=1}^{d+1} \mathrm{H}_2\left(X^{(\theta)}\right)_\omega \geqslant \log(d+1) - \log\left(f(\kappa) + g(\kappa)\,\mathrm{Tr}[\rho_A^2]\right)$$

- This is a uncertainty relation without memory
- Recovers a special case ($\alpha = 2$) of **Proposition 3** in [9][10]

[10] Alexey E Rastegin. "On uncertainty relations and entanglement detection with mutually unbiased measurements". In: *Open Systems & Information Dynamics* 22.01 (2015), p. 1550005.

Lower bound on sum of uncertainties

- Uncertainty relations are commonly expressed as lower bound on the sum of uncertainties

Lemma

Let $\{\mathcal{P}^{(\theta)}\}_{\theta\in[d+1]}$ be a complete set of MUMs on system A. For arbitrary quantum state ρ_{AB}, it holds that

$$\frac{1}{d+1}\sum_{\theta=1}^{d+1} \mathrm{H}_2\left(X^{(\theta)}\middle|B\right)_{\omega} \geqslant \log\left(d+1\right) - \log\left(f(\kappa) + g(\kappa)2^{-\mathrm{H}_2(A|B)_\rho}\right), \tag{4}$$

- Trivializing system B, Eq. (4) reduces to

$$\frac{1}{d+1}\sum_{\theta=1}^{d+1} \mathrm{H}_2\left(X^{(\theta)}\right)_{\omega} \geqslant \log\left(d+1\right) - \log\left(f(\kappa) + g(\kappa)\,\mathrm{Tr}[\rho_A^2]\right)$$

- This is a uncertainty relation without memory
- Recovers a special case ($\alpha = 2$) of **Proposition 3** in [9][10]

[10] Alexey E Rastegin. "On uncertainty relations and entanglement detection with mutually unbiased measurements". In: *Open Systems & Information Dynamics* 22.01 (2015), p. 1550005.

An entanglement detection method

- Let $\{\mathcal{P}^{(\theta)}\}_{\theta\in[d+1]}$ be a complete set of MUMs on A
- Let $\{\mathcal{Q}^{(\theta)}\}_{\theta\in[d+1]}$ be an arbitrary set of $d+1$ measurements on B
- If Alice performs $\mathcal{P}^{(\theta)}$, Bob performs $\mathcal{Q}^{(\theta)}$. They get

$$\omega_{X^{(\theta)}Y^{(\theta)}} = \sum_{x,y=1}^{d} \mathrm{Tr}\left[\left(P_x^{(\theta)} \otimes Q_y^{(\theta)}\right)\rho_{AB}\right] |x\rangle\langle x| \otimes |y\rangle\langle y|.$$

- $\omega_{X^{(\theta)}Y^{(\theta)}}$ can be evaluated from measurement statistics

Lemma

For arbitrary separable quantum state ρ_{AB}, it holds that

$$\frac{1}{d+1}\sum_{\theta=1}^{d+1} \mathrm{H}_2\left(X^{(\theta)}\middle|Y^{(\theta)}\right)_\omega \geqslant \log(d+1) - \log\left(f(\kappa)+g(\kappa)\right).$$

An entanglement detection method (cont.)

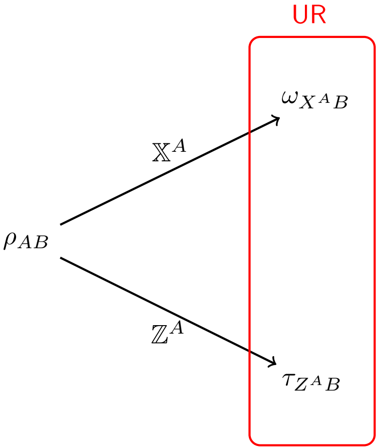
- How does the detection method work?
- Suppose now there exists a source producing states ρ_{AB}
- Alice and Bob sample from the source and gather statistics
- They estimate the joint distribution for each pair $\{\mathcal{P}^{(\theta)}, \mathcal{Q}^{(\theta)}\}$
- They evaluate the sum of (classical) conditional collision entropies
- According to the above lemma, the source is entangled if

$$\frac{1}{d+1}\sum_{\theta=1}^{d+1} \mathrm{H}_2\left(X^{(\theta)}\middle|Y^{(\theta)}\right)_{\omega} < \log\left(d+1\right) - \log\left(f(\kappa)+g(\kappa)\right). \quad (5)$$

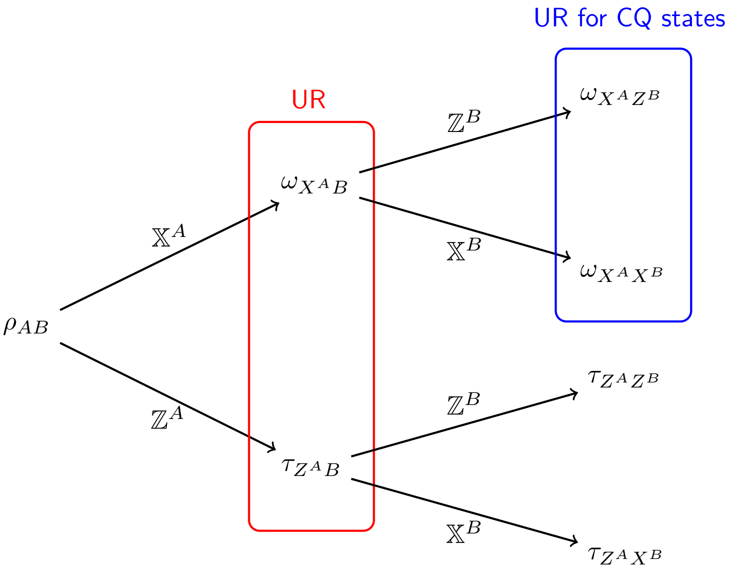
- The choice of measurements $\{\mathcal{Q}^{(\theta)}\}$ on system B is arbitrary
- For best detection criterion, minimize the LHS. of Eq. (5) by optimizing over all possible measurements $\{\mathcal{Q}^{(\theta)}\}$

Outline

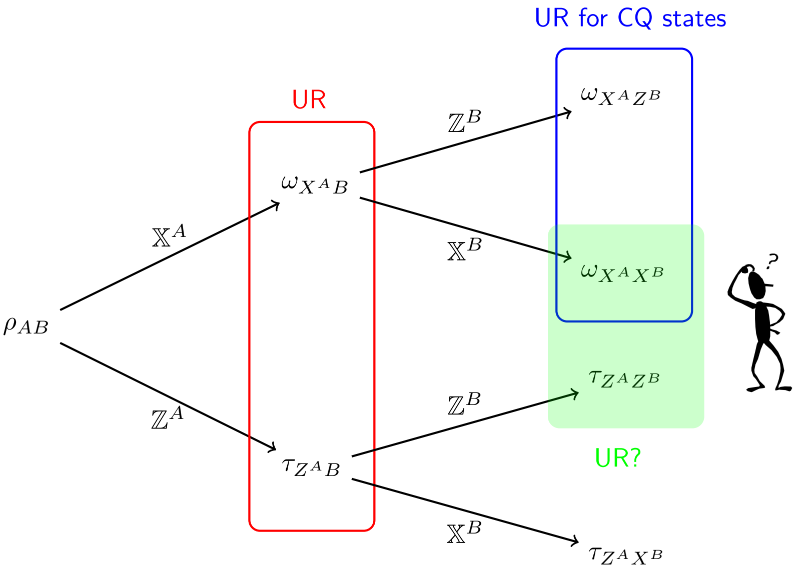
A unified view



A unified view (cont.)



A unified view (cont.)



CQC conjecture

- Let $\mathbb{X}^A$ and $\mathbb{Z}^A$ be complementary on A
- Let $\mathbb{X}^B$ and $\mathbb{Z}^B$ be complementary on B
- $\mathbb{X}^A \otimes \mathbb{X}^B$ and $\mathbb{Z}^A \otimes \mathbb{Z}^B$ induce two classical states

$$\begin{aligned}
\omega_{X^A X^B} &= \sum_{ij} p_{ij} |x_i^A\rangle\langle x_i^A| \otimes |x_j^B\rangle\langle x_j^B| \\
p_{ij} &= \langle x_i^A x_j^B | \rho_{AB} | x_i^A x_j^B \rangle \\
\tau_{Z^A Z^B} &= \sum_{mn} q_{mn} |z_m^A\rangle\langle z_m^A| \otimes |z_n^B\rangle\langle z_n^B| \\
q_{mn} &= \langle z_m^A z_n^B | \rho_{AB} | z_m^A z_n^B \rangle
\end{aligned}$$

- The complementary-quantum correlation conjecture (CQC)[11]

$$\mathrm{I}\left(X^A{:}X^B\right)_\omega + \mathrm{I}\left(Z^A{:}Z^B\right)_\tau \leqslant \mathrm{I}(A{:}B)_\rho$$

- $\mathrm{I}(A{:}B)$ is the mutual information quantifying the correlation between A and B

[11] James Schneeloch, Curtis J Broadbent, and John C Howell. "Uncertainty Relation for Mutual Information". In: *Physical Review A* 90.6 (2014), p. 062119.

CQC conjecture

- Let $\mathbb{X}^A$ and $\mathbb{Z}^A$ be complementary on A
- Let $\mathbb{X}^B$ and $\mathbb{Z}^B$ be complementary on B
- $\mathbb{X}^A \otimes \mathbb{X}^B$ and $\mathbb{Z}^A \otimes \mathbb{Z}^B$ induce two classical states

$$
\begin{aligned}
\omega_{X^A X^B} &= \sum_{ij} p_{ij} |x_i^A\rangle\langle x_i^A| \otimes |x_j^B\rangle\langle x_j^B| \\
p_{ij} &= \langle x_i^A x_j^B | \rho_{AB} | x_i^A x_j^B \rangle \\
\tau_{Z^A Z^B} &= \sum_{mn} q_{mn} |z_m^A\rangle\langle z_m^A| \otimes |z_n^B\rangle\langle z_n^B| \\
q_{mn} &= \langle z_m^A z_n^B | \rho_{AB} | z_m^A z_n^B \rangle
\end{aligned}
$$

- The complementary-quantum correlation conjecture (CQC)[11]

$$
\mathrm{I}\left(X^A{:}X^B\right)_\omega + \mathrm{I}\left(Z^A{:}Z^B\right)_\tau \leqslant \mathrm{I}(A{:}B)_\rho
$$

- $\mathrm{I}(A{:}B)$ is the mutual information quantifying the correlation between A and B

[11] James Schneeloch, Curtis J Broadbent, and John C Howell. "Uncertainty Relation for Mutual Information". In: *Physical Review A* 90.6 (2014), p. 062119.

CQC conjecture

- Let $\mathbb{X}^A$ and $\mathbb{Z}^A$ be complementary on A
- Let $\mathbb{X}^B$ and $\mathbb{Z}^B$ be complementary on B
- $\mathbb{X}^A \otimes \mathbb{X}^B$ and $\mathbb{Z}^A \otimes \mathbb{Z}^B$ induce two classical states

$$\begin{aligned}
\omega_{X^A X^B} &= \sum_{ij} p_{ij} |x_i^A\rangle\langle x_i^A| \otimes |x_j^B\rangle\langle x_j^B| \\
p_{ij} &= \langle x_i^A x_j^B | \rho_{AB} | x_i^A x_j^B \rangle \\
\tau_{Z^A Z^B} &= \sum_{mn} q_{mn} |z_m^A\rangle\langle z_m^A| \otimes |z_n^B\rangle\langle z_n^B| \\
q_{mn} &= \langle z_m^A z_n^B | \rho_{AB} | z_m^A z_n^B \rangle
\end{aligned}$$

- The complementary-quantum correlation conjecture (CQC)[11]

$$\mathrm{I}\left(X^A{:}X^B\right)_\omega + \mathrm{I}\left(Z^A{:}Z^B\right)_\tau \leqslant \mathrm{I}(A{:}B)_\rho$$

- $\mathrm{I}(A{:}B)$ is the mutual information quantifying the correlation between A and B

[11] James Schneeloch, Curtis J Broadbent, and John C Howell. "Uncertainty Relation for Mutual Information". In: *Physical Review A* 90.6 (2014), p. 062119.

CQC conjecture

- Let $\mathbb{X}^A$ and $\mathbb{Z}^A$ be complementary on A
- Let $\mathbb{X}^B$ and $\mathbb{Z}^B$ be complementary on B
- $\mathbb{X}^A \otimes \mathbb{X}^B$ and $\mathbb{Z}^A \otimes \mathbb{Z}^B$ induce two classical states

$$\begin{aligned} \omega_{X^A X^B} &= \sum_{ij} p_{ij} |x_i^A\rangle\langle x_i^A| \otimes |x_j^B\rangle\langle x_j^B| \\ p_{ij} &= \langle x_i^A x_j^B | \rho_{AB} | x_i^A x_j^B \rangle \\ \tau_{Z^A Z^B} &= \sum_{mn} q_{mn} |z_m^A\rangle\langle z_m^A| \otimes |z_n^B\rangle\langle z_n^B| \\ q_{mn} &= \langle z_m^A z_n^B | \rho_{AB} | z_m^A z_n^B \rangle \end{aligned}$$

- The complementary-quantum correlation conjecture (CQC)[11]

$$\mathrm{I}\left(X^A{:}X^B\right)_\omega + \mathrm{I}\left(Z^A{:}Z^B\right)_\tau \leqslant \mathrm{I}(A{:}B)_\rho$$

- $\mathrm{I}(A{:}B)$ is the mutual information quantifying the correlation between A and B

[11] James Schneeloch, Curtis J Broadbent, and John C Howell. "Uncertainty Relation for Mutual Information". In: *Physical Review A* 90.6 (2014), p. 062119.

CQC conjecture

- Let $\mathbb{X}^A$ and $\mathbb{Z}^A$ be complementary on A
- Let $\mathbb{X}^B$ and $\mathbb{Z}^B$ be complementary on B
- $\mathbb{X}^A \otimes \mathbb{X}^B$ and $\mathbb{Z}^A \otimes \mathbb{Z}^B$ induce two classical states

$$\begin{aligned}
\omega_{X^A X^B} &= \sum_{ij} p_{ij} |x_i^A\rangle\langle x_i^A| \otimes |x_j^B\rangle\langle x_j^B| \\
p_{ij} &= \langle x_i^A x_j^B | \rho_{AB} | x_i^A x_j^B \rangle \\
\tau_{Z^A Z^B} &= \sum_{mn} q_{mn} |z_m^A\rangle\langle z_m^A| \otimes |z_n^B\rangle\langle z_n^B| \\
q_{mn} &= \langle z_m^A z_n^B | \rho_{AB} | z_m^A z_n^B \rangle
\end{aligned}$$

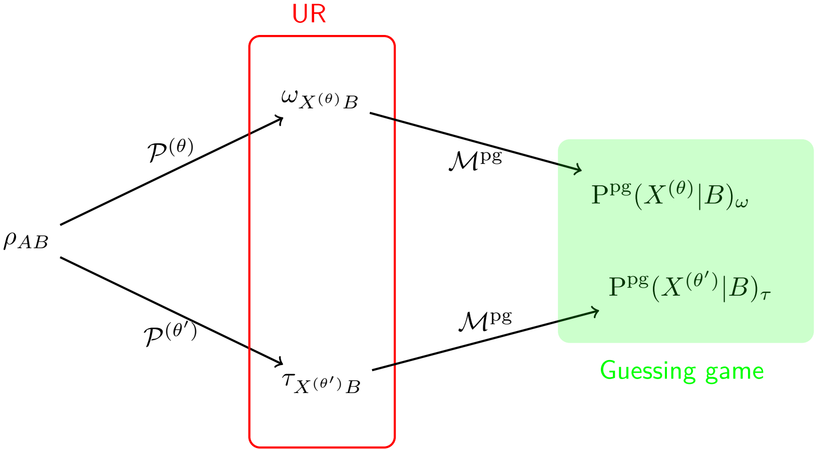
- The complementary-quantum correlation conjecture (CQC)[11]

$$\mathrm{I}\left(X^A{:}X^B\right)_\omega + \mathrm{I}\left(Z^A{:}Z^B\right)_\tau \leqslant \mathrm{I}(A{:}B)_\rho$$

- $\mathrm{I}(A{:}B)$ is the mutual information quantifying the correlation between A and B

[11] James Schneeloch, Curtis J Broadbent, and John C Howell. "Uncertainty Relation for Mutual Information". In: *Physical Review A* 90.6 (2014), p. 062119.

Our work fits into the unified view



Summary

- **What have done?**
  - An equality relation for complete set of MUMs
  - Conditional collision entropy as uncertainty measure
  - Some corollaries from the equality relation
    1. Bound on pretty-good guessing probabilities
    2. An uncertainty relation expressed as sum of uncertainties
    3. An entanglement detection method
- **What to do?**
  - Bounds on pretty-good guessing probabilities for a set of MUMs
  - Uncertainty relations for a set of MUMs
  - Finally, the CQC conjecture!

Summary

- **What have done?**
  - An equality relation for complete set of MUMs
  - Conditional collision entropy as uncertainty measure
  - Some corollaries from the equality relation
    1. Bound on pretty-good guessing probabilities
    2. An uncertainty relation expressed as sum of uncertainties
    3. An entanglement detection method
- **What to do?**
  - Bounds on pretty-good guessing probabilities for a set of MUMs
  - Uncertainty relations for a set of MUMs
  - Finally, the CQC conjecture!

Thank you !

Any questions ?

Bibliography I

Joonwoo Bae and Leong-Chuan Kwek. "Quantum state discrimination and its applications". In: *Journal of Physics A: Mathematical and Theoretical* 48.8 (2015), p. 083001.

Mario Berta, Patrick J Coles, and Stephanie Wehner. "Entanglement-assisted guessing of complementary measurement outcomes". In: *Physical Review A* 90.6 (2014), p. 062127.

Mario Berta et al. "The uncertainty principle in the presence of quantum memory". In: *Nature Physics* 6.9 (2010), pp. 659–662.

Harry Buhrman et al. "Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment". In: *Physical Review A* 78.2 (2008), p. 022316.

Patrick J Coles et al. "Entropic uncertainty relations and their applications". In: *Reviews of Modern Physics* 89.1 (2017), p. 015002.

Bibliography II

- Matthew A Graydon and DM Appleby. "Quantum conical designs". In: *Journal of Physics A: Mathematical and Theoretical* 49.8 (2016), p. 085301.
- Paul Hausladen and William K Wootters. "A 'pretty good' measurement for distinguishing quantum states". In: *Journal of Modern Optics* 41.12 (1994), pp. 2385–2390.
- Amir Kalev and Gilad Gour. "Mutually unbiased measurements in finite dimensions". In: *New Journal of Physics* 16.5 (2014), p. 053038.
- Alexey E Rastegin. "On uncertainty relations and entanglement detection with mutually unbiased measurements". In: *Open Systems & Information Dynamics* 22.01 (2015), p. 1550005.
- James Schneeloch, Curtis J Broadbent, and John C Howell. "Uncertainty Relation for Mutual Information". In: *Physical Review A* 90.6 (2014), p. 062119.
- Marco Tomamichel. *Quantum Information Processing with Finite Resources: Mathematical Foundations*. Vol. 5. Springer, 2015.