Finite blocklength converse bounds for quantum channels (arXiv:1210.4722)

Will Matthews (University of Cambridge)
Stephanie Wehner (National University of Singapore)

Introduction: Codes

Classical data over quantum channels.

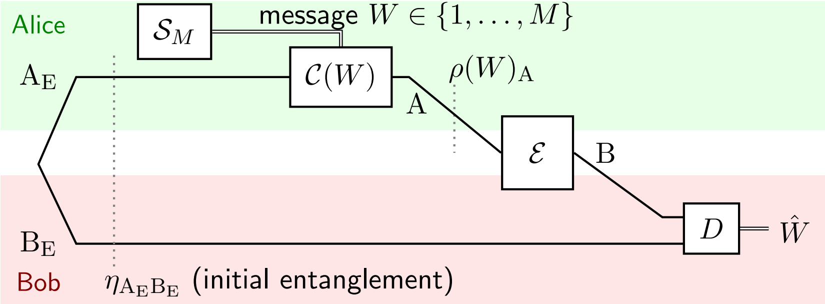
Entanglement-assisted (EA) code $\mathcal{Z}$ of **size** M:

For uniform source $\mathcal{S}_M$ $(\Pr(W = w|\mathcal{S}_M) = 1/M)$:
Average input $\rho_\mathrm{A} = \frac{1}{M}\sum_{w=1}^{M}\rho(w)_\mathrm{A}$.
Error probability $\epsilon = \Pr(\hat{W} \neq W|\mathcal{E}, \mathcal{Z}, \mathcal{S}_M)$.

Introduction: Codes

Classical data over quantum channels.

Entanglement-assisted (EA) code $\mathcal{Z}$ of **size** M:



For uniform source $\mathcal{S}_M$ $(\Pr(W = w|\mathcal{S}_M) = 1/M)$:

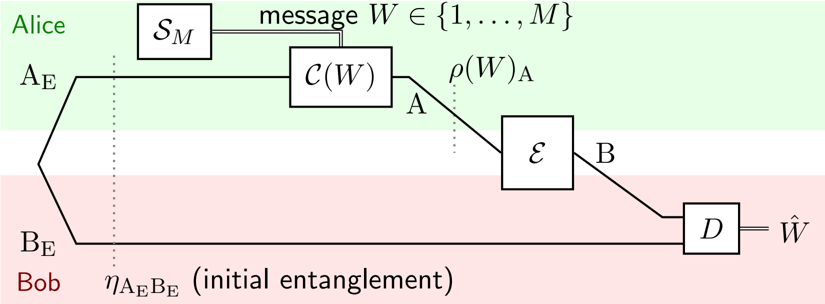
Average input $\rho_\mathrm{A} = \frac{1}{M}\sum_{w=1}^{M} \rho(w)_\mathrm{A}$.

Error probability $\epsilon = \Pr(\hat{W} \neq W|\mathcal{E}, \mathcal{Z}, \mathcal{S}_M)$.

Introduction: Codes

Classical data over quantum channels.

Entanglement-assisted (EA) code $\mathcal{Z}$ of **size** M:

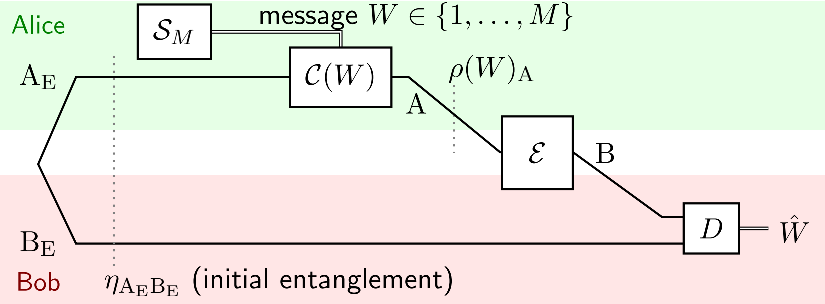


For uniform source $\mathcal{S}_M$ ($\mathrm{Pr}(W = w|\mathcal{S}_M) = 1/M$):
Average input $\rho_\mathrm{A} = \frac{1}{M}\sum_{w=1}^{M} \rho(w)_\mathrm{A}$.
Error probability $\epsilon = \mathrm{Pr}(\hat{W} \neq W|\mathcal{E}, \mathcal{Z}, \mathcal{S}_M)$.

Introduction: Codes

Classical data over quantum channels.

Entanglement-assisted (EA) code $\mathcal{Z}$ of **size** M:



For uniform source $\mathcal{S}_M$ $(\Pr(W = w|\mathcal{S}_M) = 1/M)$:

Average input $\rho_\mathrm{A} = \frac{1}{M}\sum_{w=1}^{M} \rho(w)_\mathrm{A}$.

Error probability $\epsilon = \Pr(\hat{W} \neq W|\mathcal{E}, \mathcal{Z}, \mathcal{S}_M)$.

Introduction: Code performance and capacities

- $M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$ denotes largest size of entanglement-assisted code with average input ρ and error probability ϵ for $\mathcal{E}$.
- $M_\epsilon^{\mathrm{E}}(\mathcal{E}) = \max_\rho M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$
- $M_\epsilon(\rho, \mathcal{E})$ and $M_\epsilon(\mathcal{E})$ denote the corresponding quantities for *unassisted* codes ($\eta_{\mathrm{A_E B_E}}$ separable).
- For a channel $\mathcal{E} = (\mathcal{E}^n)_{n \in \mathbb{N}}$, where $\mathcal{E}^n$ is CPTP map for n channel uses (taking states of A^n to states of B^n): $C^{\mathrm{E}}(\mathcal{E}) := \lim_{\epsilon \to 0} \lim_{n \to \infty} \frac{1}{n} \log M_\epsilon^{\mathrm{E}}(\mathcal{E}^n)$
- Asymptotics: For channels with i.i.d. uses $\mathcal{E}^n = \mathcal{E}^{\otimes n}$:
  - $C^{\mathrm{E}}(\mathcal{E})$ has single letter BSST formula (arXiv:quant-ph/0106052).
  - $C(\mathcal{E})$ is regularised Holevo bound.
  - Both reduce to Shannon capacity formula for classical channels.

Introduction: Code performance and capacities

- $M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$ denotes largest size of entanglement-assisted code with average input ρ and error probability ϵ for $\mathcal{E}$.
- $M_\epsilon^{\mathrm{E}}(\mathcal{E}) = \max_\rho M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$
- $M_\epsilon(\rho, \mathcal{E})$ and $M_\epsilon(\mathcal{E})$ denote the corresponding quantities for *unassisted* codes ($\eta_{\mathrm{A_E B_E}}$ separable).
- For a channel $\boldsymbol{\mathcal{E}} = (\mathcal{E}^n)_{n\in\mathbb{N}}$, where $\mathcal{E}^n$ is CPTP map for n channel uses (taking states of A^n to states of B^n): $C^{\mathrm{E}}(\boldsymbol{\mathcal{E}}) := \lim_{\epsilon\to 0} \lim_{n\to\infty} \frac{1}{n} \log M_\epsilon^{\mathrm{E}}(\mathcal{E}^n)$
- Asymptotics: For channels with i.i.d. uses $\mathcal{E}^n = \mathcal{E}^{\otimes n}$:
  - $C^{\mathrm{E}}(\boldsymbol{\mathcal{E}})$ has single letter BSST formula (arXiv:quant-ph/0106052).
  - $C(\boldsymbol{\mathcal{E}})$ is regularised Holevo bound.
  - Both reduce to Shannon capacity formula for classical channels.

Introduction: Code performance and capacities

- $M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$ denotes largest size of entanglement-assisted code with average input ρ and error probability ϵ for $\mathcal{E}$.
- $M_\epsilon^{\mathrm{E}}(\mathcal{E}) = \max_\rho M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$
- $M_\epsilon(\rho, \mathcal{E})$ and $M_\epsilon(\mathcal{E})$ denote the corresponding quantities for *unassisted* codes ($\eta_{\mathrm{A_E B_E}}$ separable).
- For a channel $\mathcal{E} = (\mathcal{E}^n)_{n \in \mathbb{N}}$, where $\mathcal{E}^n$ is CPTP map for n channel uses (taking states of A^n to states of B^n): $C^{\mathrm{E}}(\mathcal{E}) := \lim_{\epsilon \to 0} \lim_{n \to \infty} \frac{1}{n} \log M_\epsilon^{\mathrm{E}}(\mathcal{E}^n)$
- Asymptotics: For channels with i.i.d. uses $\mathcal{E}^n = \mathcal{E}^{\otimes n}$:
  - $C^{\mathrm{E}}(\mathcal{E})$ has single letter BSST formula (arXiv:quant-ph/0106052).
  - $C(\mathcal{E})$ is regularised Holevo bound.
  - Both reduce to Shannon capacity formula for classical channels.

Introduction: Code performance and capacities

- $M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$ denotes largest size of entanglement-assisted code with average input ρ and error probability ϵ for $\mathcal{E}$.
- $M_\epsilon^{\mathrm{E}}(\mathcal{E}) = \max_\rho M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$
- $M_\epsilon(\rho, \mathcal{E})$ and $M_\epsilon(\mathcal{E})$ denote the corresponding quantities for *unassisted* codes ($\eta_{\mathrm{A_E B_E}}$ separable).
- For a channel $\boldsymbol{\mathcal{E}} = (\mathcal{E}^n)_{n\in\mathbb{N}}$, where $\mathcal{E}^n$ is CPTP map for n channel uses (taking states of A^n to states of B^n): $C^{\mathrm{E}}(\boldsymbol{\mathcal{E}}) := \lim_{\epsilon\to 0} \lim_{n\to\infty} \frac{1}{n} \log M_\epsilon^{\mathrm{E}}(\mathcal{E}^n)$
- Asymptotics: For channels with i.i.d. uses $\mathcal{E}^n = \mathcal{E}^{\otimes n}$:
  - $C^{\mathrm{E}}(\mathcal{E})$ has single letter BSST formula (arXiv:quant-ph/0106052).
  - $C(\mathcal{E})$ is regularised Holevo bound.
  - Both reduce to Shannon capacity formula for classical channels.

Introduction: Code performance and capacities

- $M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$ denotes largest size of entanglement-assisted code with average input ρ and error probability ϵ for $\mathcal{E}$.
- $M_\epsilon^{\mathrm{E}}(\mathcal{E}) = \max_\rho M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$
- $M_\epsilon(\rho, \mathcal{E})$ and $M_\epsilon(\mathcal{E})$ denote the corresponding quantities for *unassisted* codes ($\eta_{\mathrm{A_E B_E}}$ separable).
- For a channel $\boldsymbol{\mathcal{E}} = (\mathcal{E}^n)_{n\in\mathbb{N}}$, where $\mathcal{E}^n$ is CPTP map for n channel uses (taking states of A^n to states of B^n): $C^{\mathrm{E}}(\boldsymbol{\mathcal{E}}) := \lim_{\epsilon\to 0} \lim_{n\to\infty} \frac{1}{n} \log M_\epsilon^{\mathrm{E}}(\mathcal{E}^n)$
- Asymptotics: For channels with i.i.d. uses $\mathcal{E}^n = \mathcal{E}^{\otimes n}$:
  - $C^{\mathrm{E}}(\mathcal{E})$ has single letter BSST formula (arXiv:quant-ph/0106052).
  - $C(\mathcal{E})$ is regularised Holevo bound.
  - Both reduce to Shannon capacity formula for classical channels.

Introduction: Code performance and capacities

- $M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$ denotes largest size of entanglement-assisted code with average input ρ and error probability ϵ for $\mathcal{E}$.
- $M_\epsilon^{\mathrm{E}}(\mathcal{E}) = \max_\rho M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$
- $M_\epsilon(\rho, \mathcal{E})$ and $M_\epsilon(\mathcal{E})$ denote the corresponding quantities for *unassisted* codes ($\eta_{\mathrm{A_E B_E}}$ separable).
- For a channel $\boldsymbol{\mathcal{E}} = (\mathcal{E}^n)_{n\in\mathbb{N}}$, where $\mathcal{E}^n$ is CPTP map for n channel uses (taking states of A^n to states of B^n): $C^{\mathrm{E}}(\boldsymbol{\mathcal{E}}) := \lim_{\epsilon\to 0} \lim_{n\to\infty} \frac{1}{n} \log M_\epsilon^{\mathrm{E}}(\mathcal{E}^n)$
- Asymptotics: For channels with i.i.d. uses $\mathcal{E}^n = \mathcal{E}^{\otimes n}$:
  - $C^{\mathrm{E}}(\boldsymbol{\mathcal{E}})$ has single letter BSST formula (arXiv:quant-ph/0106052).
  - $C(\boldsymbol{\mathcal{E}})$ is regularised Holevo bound.
  - Both reduce to Shannon capacity formula for classical channels.

Introduction: Code performance and capacities

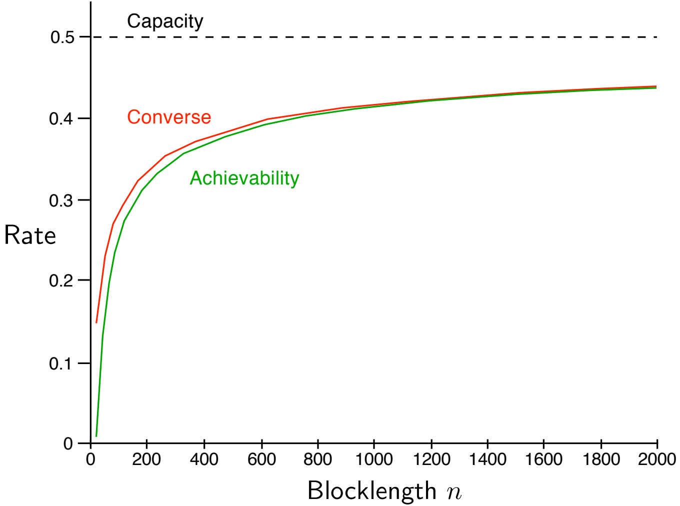
- $M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$ denotes largest size of entanglement-assisted code with average input ρ and error probability ϵ for $\mathcal{E}$.
- $M_\epsilon^{\mathrm{E}}(\mathcal{E}) = \max_\rho M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$
- $M_\epsilon(\rho, \mathcal{E})$ and $M_\epsilon(\mathcal{E})$ denote the corresponding quantities for *unassisted* codes ($\eta_{\mathrm{A_E B_E}}$ separable).
- For a channel $\boldsymbol{\mathcal{E}} = (\mathcal{E}^n)_{n\in\mathbb{N}}$, where $\mathcal{E}^n$ is CPTP map for n channel uses (taking states of A^n to states of B^n):
  $C^{\mathrm{E}}(\boldsymbol{\mathcal{E}}) := \lim_{\epsilon\to 0} \lim_{n\to\infty} \frac{1}{n} \log M_\epsilon^{\mathrm{E}}(\mathcal{E}^n)$
- Asymptotics: For channels with i.i.d. uses $\mathcal{E}^n = \mathcal{E}^{\otimes n}$:
  - $C^{\mathrm{E}}(\boldsymbol{\mathcal{E}})$ has single letter BSST formula (arXiv:quant-ph/0106052).
  - $C(\boldsymbol{\mathcal{E}})$ is regularised Holevo bound.
  - Both reduce to Shannon capacity formula for classical channels.

Introduction: Code performance and capacities

- $M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$ denotes largest size of entanglement-assisted code with average input ρ and error probability ϵ for $\mathcal{E}$.
- $M_\epsilon^{\mathrm{E}}(\mathcal{E}) = \max_\rho M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E})$
- $M_\epsilon(\rho, \mathcal{E})$ and $M_\epsilon(\mathcal{E})$ denote the corresponding quantities for *unassisted* codes ($\eta_{\mathrm{A_E B_E}}$ separable).
- For a channel $\boldsymbol{\mathcal{E}} = (\mathcal{E}^n)_{n\in\mathbb{N}}$, where $\mathcal{E}^n$ is CPTP map for n channel uses (taking states of A^n to states of B^n): $C^{\mathrm{E}}(\boldsymbol{\mathcal{E}}) := \lim_{\epsilon\to 0} \lim_{n\to\infty} \frac{1}{n} \log M_\epsilon^{\mathrm{E}}(\mathcal{E}^n)$
- Asymptotics: For channels with i.i.d. uses $\mathcal{E}^n = \mathcal{E}^{\otimes n}$:
  - $C^{\mathrm{E}}(\boldsymbol{\mathcal{E}})$ has single letter BSST formula (arXiv:quant-ph/0106052).
  - $C(\boldsymbol{\mathcal{E}})$ is regularised Holevo bound.
  - Both reduce to Shannon capacity formula for classical channels.

Background and motivation

Converse and achievability bounds[1] on the rate $\frac{1}{n} \log M_\epsilon(\mathcal{E}^n)$ when $\epsilon = 1/1000$ and $\boldsymbol{\mathcal{E}}$ is the BSC with $\Pr(\text{bit flip}) = 0.11$.



[1] Polyanskiy, Poor, Verdú. IEEE Trans. Inf. T., 56, 2307-2359

Background and motivation

- Datta & Hsieh (arXiv:1105.3321) give converse (and achievability) for $M_\epsilon^{\mathrm{E}}(\mathcal{E})$, but it has some disadvantages (diverges as $\epsilon \to 0$; not clear how to compute).
- Polyanskiy–Poor–Verdú gives a classical converse which relates coding to hypothesis testing. It is simple, and powerful enough to derive many important classical converse bounds, so we want a quantum generalisation.
- The converse in Wang & Renner (arXiv:1007.5456) for $M_\epsilon(\mathcal{E})$ is almost such a generalisation for unassisted codes (see also Hayashi's book).
- We obtain a hierarchy of bounds based on quantum hypothesis testing of a bipartite system with restricted measurements, including a novel converse for EA codes, and a generalisation of Wang-Renner converse for unassisted codes.

Background and motivation

- Datta & Hsieh (arXiv:1105.3321) give converse (and achievability) for $M_\epsilon^{\mathrm{E}}(\mathcal{E})$, but it has some disadvantages (diverges as $\epsilon \to 0$; not clear how to compute).
- Polyanskiy–Poor–Verdú gives a classical converse which relates coding to hypothesis testing. It is simple, and powerful enough to derive many important classical converse bounds, so we want a quantum generalisation.
- The converse in Wang & Renner (arXiv:1007.5456) for $M_\epsilon(\mathcal{E})$ is almost such a generalisation for unassisted codes (see also Hayashi's book).
- We obtain a hierarchy of bounds based on quantum hypothesis testing of a bipartite system with restricted measurements, including a novel converse for EA codes, and a generalisation of Wang-Renner converse for unassisted codes.

Background and motivation

- Datta & Hsieh (arXiv:1105.3321) give converse (and achievability) for $M_\epsilon^{\mathrm{E}}(\mathcal{E})$, but it has some disadvantages (diverges as $\epsilon \to 0$; not clear how to compute).
- Polyanskiy–Poor–Verdú gives a classical converse which relates coding to hypothesis testing. It is simple, and powerful enough to derive many important classical converse bounds, so we want a quantum generalisation.
- The converse in Wang & Renner (arXiv:1007.5456) for $M_\epsilon(\mathcal{E})$ is almost such a generalisation for unassisted codes (see also Hayashi's book).
- We obtain a hierarchy of bounds based on quantum hypothesis testing of a bipartite system with restricted measurements, including a novel converse for EA codes, and a generalisation of Wang-Renner converse for unassisted codes.

Background and motivation

- Datta & Hsieh (arXiv:1105.3321) give converse (and achievability) for $M_\epsilon^{\mathrm{E}}(\mathcal{E})$, but it has some disadvantages (diverges as $\epsilon \to 0$; not clear how to compute).
- Polyanskiy–Poor–Verdú gives a classical converse which relates coding to hypothesis testing. It is simple, and powerful enough to derive many important classical converse bounds, so we want a quantum generalisation.
- The converse in Wang & Renner (arXiv:1007.5456) for $M_\epsilon(\mathcal{E})$ is almost such a generalisation for unassisted codes (see also Hayashi's book).
- We obtain a hierarchy of bounds based on quantum hypothesis testing of a bipartite system with restricted measurements, including a novel converse for EA codes, and a generalisation of Wang-Renner converse for unassisted codes.

Background: Quantum hypothesis testing

H_0: State is τ_0. H_1: State is τ_1.

Test T for H_0: The element of a binary POVM $\{T, \mathbb{1} - T\}$ for the outcome "accept H_0".

$$\alpha(T) := \mathrm{Pr}(\text{reject } H_0 | T, H_0) = 1 - \mathrm{Tr}\tau_0 T \quad \text{(false negative)},$$
$$\beta(T) := \mathrm{Pr}(\text{accept } H_0 | T, H_1) = \mathrm{Tr}\tau_1 T \quad \text{(false positive)}.$$

For a class of tests Ω we define

$$\beta_\epsilon^\Omega(\tau_0, \tau_1) := \min_{T \in \Omega} \beta(T, \tau_1), \text{ subject to } \alpha(T, \tau_0) \le \epsilon.$$

Background: Quantum hypothesis testing

H_0: State is τ_0. H_1: State is τ_1.

Test T for H_0: The element of a binary POVM $\{T, \mathbb{1} - T\}$ for the outcome "accept H_0".

$$\alpha(T) := \Pr(\text{reject } H_0 | T, H_0) = 1 - \mathrm{Tr}\tau_0 T \quad \text{(false negative)},$$
$$\beta(T) := \Pr(\text{accept } H_0 | T, H_1) = \mathrm{Tr}\tau_1 T \quad \text{(false positive)}.$$

For a class of tests $\mathbf{\Omega}$ we define

$$\beta_\epsilon^{\mathbf{\Omega}}(\tau_0, \tau_1) := \min_{T \in \mathbf{\Omega}} \beta(T, \tau_1), \text{ subject to } \alpha(T, \tau_0) \leq \epsilon.$$

Background: Quantum hypothesis testing

H_0: State is τ_0. H_1: State is τ_1.

Test T for H_0: The element of a binary POVM $\{T, \mathbb{1} - T\}$ for the outcome "accept H_0".

$$\alpha(T) := \mathrm{Pr}(\text{reject } H_0 | T, H_0) = 1 - \mathrm{Tr}\tau_0 T \quad \text{(false negative)},$$
$$\beta(T) := \mathrm{Pr}(\text{accept } H_0 | T, H_1) = \mathrm{Tr}\tau_1 T \quad \text{(false positive)}.$$

For a class of tests $\boldsymbol{\Omega}$ we define

$$\beta_\epsilon^{\boldsymbol{\Omega}}(\tau_0, \tau_1) := \min_{T \in \boldsymbol{\Omega}} \beta(T, \tau_1), \text{ subject to } \alpha(T, \tau_0) \le \epsilon.$$

Background: Quantum hypothesis testing

H_0: State is τ_0. H_1: State is τ_1.

Test T for H_0: The element of a binary POVM $\{T, \mathbb{1} - T\}$ for the outcome "accept H_0".

$$\alpha(T) := \Pr(\text{reject } H_0 | T, H_0) = 1 - \mathrm{Tr}\tau_0 T \quad \text{(false negative)},$$
$$\beta(T) := \Pr(\text{accept } H_0 | T, H_1) = \mathrm{Tr}\tau_1 T \quad \text{(false positive)}.$$

For a class of tests $\mathbf{\Omega}$ we define

$$\beta_\epsilon^{\mathbf{\Omega}}(\tau_0, \tau_1) := \min_{T \in \mathbf{\Omega}} \beta(T, \tau_1), \text{ subject to } \alpha(T, \tau_0) \leq \epsilon.$$

Background: Classes of test for bipartite system

- $\mathbf{L}$: *Local tests* - Test on joint outcome of local measurements (coordinated only by shared randomness).
- $\mathbf{LC1}$: One-way communication from Alice to Bob.
- $\mathbf{PPT}$: $0 \leq \Gamma_{\mathrm{B}}[T_{\tilde{\mathrm{A}}\mathrm{B}}] \leq \mathbb{1}$.
- $\mathbf{ALL}$: All tests. Symbol omitted e.g. $\beta_\epsilon = \beta_\epsilon^{\mathbf{ALL}}$.

$$\mathbf{L} \subset \mathbf{LC1} \subset \mathbf{PPT} \subset \mathbf{ALL}.$$

Background: Classes of test for bipartite system

- $\mathbf{L}$: *Local tests* - Test on joint outcome of local measurements (coordinated only by shared randomness).
- $\mathbf{LC1}$: One-way communication from Alice to Bob.
- $\mathbf{PPT}$: $0 \leq \Gamma_{\mathrm{B}}[T_{\tilde{\mathrm{A}}\mathrm{B}}] \leq \mathbb{1}$.
- $\mathbf{ALL}$: All tests. Symbol omitted e.g. $\beta_\epsilon = \beta_\epsilon^{\mathbf{ALL}}$.

$$\mathbf{L} \subset \mathbf{LC1} \subset \mathbf{PPT} \subset \mathbf{ALL}.$$

Background: Classes of test for bipartite system

- $\mathbf{L}$: *Local tests* - Test on joint outcome of local measurements (coordinated only by shared randomness).
- $\mathbf{LC1}$: One-way communication from Alice to Bob.
- $\mathbf{PPT}$: $0 \leq \Gamma_{\mathrm{B}}[T_{\tilde{\mathrm{A}}\mathrm{B}}] \leq \mathbb{1}$.
- $\mathbf{ALL}$: All tests. Symbol omitted e.g. $\beta_\epsilon = \beta_\epsilon^{\mathbf{ALL}}$.

$$\mathbf{L} \subset \mathbf{LC1} \subset \mathbf{PPT} \subset \mathbf{ALL}.$$

Background: Classes of test for bipartite system

- $\mathbf{L}$: *Local tests* - Test on joint outcome of local measurements (coordinated only by shared randomness).
- $\mathbf{LC1}$: One-way communication from Alice to Bob.
- $\mathbf{PPT}$: $0 \leq \Gamma_{\mathrm{B}}[T_{\tilde{\mathrm{A}}\mathrm{B}}] \leq \mathbb{1}$.
- $\mathbf{ALL}$: All tests. Symbol omitted e.g. $\beta_\epsilon = \beta_\epsilon^{\mathbf{ALL}}$.

$$\mathbf{L} \subset \mathbf{LC1} \subset \mathbf{PPT} \subset \mathbf{ALL}.$$

Background: Classes of test for bipartite system

- $\mathbf{L}$: *Local tests* - Test on joint outcome of local measurements (coordinated only by shared randomness).
- $\mathbf{LC1}$: One-way communication from Alice to Bob.
- $\mathbf{PPT}$: $0 \leq \Gamma_{\mathrm{B}}[T_{\tilde{\mathrm{A}}\mathrm{B}}] \leq \mathbb{1}$.
- $\mathbf{ALL}$: All tests. Symbol omitted e.g. $\beta_\epsilon = \beta_\epsilon^{\mathbf{ALL}}$.

$$\mathbf{L} \subset \mathbf{LC1} \subset \mathbf{PPT} \subset \mathbf{ALL}.$$

Background: Classes of test for bipartite system

- $\mathbf{L}$: *Local tests* - Test on joint outcome of local measurements (coordinated only by shared randomness).
- $\mathbf{LC1}$: One-way communication from Alice to Bob.
- $\mathbf{PPT}$: $0 \leq \Gamma_{\mathrm{B}}[T_{\tilde{\mathrm{A}}\mathrm{B}}] \leq \mathbb{1}$.
- $\mathbf{ALL}$: All tests. Symbol omitted e.g. $\beta_\epsilon = \beta_\epsilon^{\mathbf{ALL}}$.

$$\mathbf{L} \subset \mathbf{LC1} \subset \mathbf{PPT} \subset \mathbf{ALL}.$$

Main idea: Codes to tests

From a **CPTP map** $\mathcal{E}$ and an **EA code** with average input state ρ_A and error ϵ when used with $\mathcal{E}$ we construct:

The **state** $\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}} := \mathcal{E}_{\mathrm{B}|\mathrm{A}}[\psi_{\tilde{\mathrm{A}}\mathrm{A}}]$ given by $\mathcal{E}$ acting on a certain purification of ρ: $\psi_{\tilde{\mathrm{A}}\mathrm{A}} := \rho_\mathrm{A}^{\frac{1}{2}}\tilde{\Phi}_{\mathrm{A}\tilde{\mathrm{A}}}\rho_\mathrm{A}^{\frac{1}{2}}$, ($\tilde{\Phi}_{\mathrm{A}\tilde{\mathrm{A}}} := \sum_{ij} |i\rangle_{\tilde{\mathrm{A}}}|i\rangle_\mathrm{A}\langle j|_{\tilde{\mathrm{A}}}\langle j|_\mathrm{A}$).

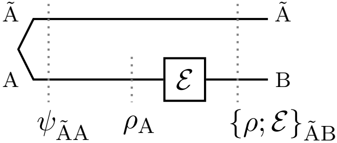
A **test** $T_{\tilde{\mathrm{A}}\mathrm{B}}$ such that $\mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}T_{\tilde{\mathrm{A}}\mathrm{B}} = 1-\epsilon.$

Unassisted codes map to **local tests.**

Main idea: Codes to tests

From a **CPTP map** $\mathcal{E}$ and an **EA code** with average input state ρ_{A} and error ϵ when used with $\mathcal{E}$ we construct:

The **state** $\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}} := \mathcal{E}_{\mathrm{B}|\mathrm{A}}[\psi_{\tilde{\mathrm{A}}\mathrm{A}}]$ given by $\mathcal{E}$ acting on a certain purification of ρ: $\psi_{\tilde{\mathrm{A}}\mathrm{A}} := \rho_{\mathrm{A}}^{\frac{1}{2}}\tilde{\Phi}_{\mathrm{A}\tilde{\mathrm{A}}}\rho_{\mathrm{A}}^{\frac{1}{2}}$, ($\tilde{\Phi}_{\mathrm{A}\tilde{\mathrm{A}}} := \sum_{ij}|i\rangle_{\tilde{\mathrm{A}}}|i\rangle_{\mathrm{A}}\langle j|_{\tilde{\mathrm{A}}}\langle j|_{\mathrm{A}}$).



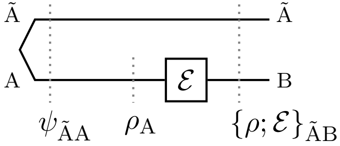
A **test** $T_{\tilde{\mathrm{A}}\mathrm{B}}$ such that $\mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}T_{\tilde{\mathrm{A}}\mathrm{B}} = 1-\epsilon.$

Unassisted codes map to **local tests.**

Main idea: Codes to tests

From a **CPTP map** $\mathcal{E}$ and an **EA code** with average input state ρ_{A} and error ϵ when used with $\mathcal{E}$ we construct:

The **state** $\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}} := \mathcal{E}_{\mathrm{B}|\mathrm{A}}[\psi_{\tilde{\mathrm{A}}\mathrm{A}}]$ given by $\mathcal{E}$ acting on a certain purification of ρ: $\psi_{\tilde{\mathrm{A}}\mathrm{A}} := \rho_{\mathrm{A}}^{\frac{1}{2}}\tilde{\Phi}_{\mathrm{A}\tilde{\mathrm{A}}}\rho_{\mathrm{A}}^{\frac{1}{2}}$, $(\tilde{\Phi}_{\mathrm{A}\tilde{\mathrm{A}}} := \sum_{ij} |i\rangle_{\tilde{\mathrm{A}}}|i\rangle_{\mathrm{A}}\langle j|_{\tilde{\mathrm{A}}}\langle j|_{\mathrm{A}})$.



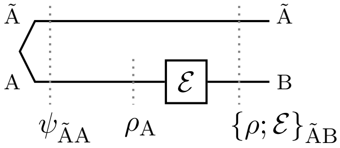
A **test** $T_{\tilde{\mathrm{A}}\mathrm{B}}$ such that $\mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}T_{\tilde{\mathrm{A}}\mathrm{B}} = 1-\epsilon.$

Unassisted codes map to **local tests.**

Main idea: Codes to tests

From a **CPTP map** $\mathcal{E}$ and an **EA code** with average input state ρ_{A} and error ϵ when used with $\mathcal{E}$ we construct:

The **state** $\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}} := \mathcal{E}_{\mathrm{B}|\mathrm{A}}[\psi_{\tilde{\mathrm{A}}\mathrm{A}}]$ given by $\mathcal{E}$ acting on a certain purification of ρ: $\psi_{\tilde{\mathrm{A}}\mathrm{A}} := \rho_{\mathrm{A}}^{\frac{1}{2}}\tilde{\Phi}_{\mathrm{A}\tilde{\mathrm{A}}}\rho_{\mathrm{A}}^{\frac{1}{2}}$, ($\tilde{\Phi}_{\mathrm{A}\tilde{\mathrm{A}}} := \sum_{ij}|i\rangle_{\tilde{\mathrm{A}}}|i\rangle_{\mathrm{A}}\langle j|_{\tilde{\mathrm{A}}}\langle j|_{\mathrm{A}}$).



A **test** $T_{\tilde{\mathrm{A}}\mathrm{B}}$ such that $\mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}T_{\tilde{\mathrm{A}}\mathrm{B}} = 1-\epsilon.$

Unassisted codes map to **local tests.**

Suppose there exists a code of size M, average input ρ, with error ϵ for $\mathcal{E}$, which maps to a test $T_{\tilde{A}B}$ in class $\mathbf{\Omega}$.

H_0: State is $\{\rho;\mathcal{E}\}_{\tilde{A}B}$ H_1: State is $\rho^*_{\tilde{A}}\sigma_B$

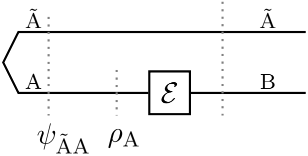
• $\alpha(T_{\tilde{A}B}) = 1 - \mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{A}B}T_{\tilde{A}B} = \epsilon$.
For a CPTP map $\mathcal{F}$ with constant output σ_B the success probability is $1/M$, so
• $\beta(T_{\tilde{A}B}) = \mathrm{Tr}\rho^*_{\tilde{A}}\sigma_B T_{\tilde{A}B} = 1/M$.

Therefore $\forall\sigma_B : \beta^{\mathbf{\Omega}}_\epsilon(\{\rho;\mathcal{E}\}_{\tilde{A}B}, \rho^*_{\tilde{A}}\sigma_B) \le 1/M$, or

$$M \le B^{\mathbf{\Omega}}_\epsilon(\rho,\mathcal{E}) := \left(\max_\sigma \beta^{\mathbf{\Omega}}_\epsilon(\{\rho;\mathcal{E}\}_{\tilde{A}B}, \rho^*_{\tilde{A}}\sigma_B)\right)^{-1}$$

Suppose there exists a code of size M, average input ρ, with error ϵ for $\mathcal{E}$, which maps to a test $T_{\tilde{\mathrm{A}}\mathrm{B}}$ in class $\mathbf{\Omega}$.

H_0: State is $\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}$



H_1: State is $\rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}}$

- $\alpha(T_{\tilde{\mathrm{A}}\mathrm{B}}) = 1 - \mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}} T_{\tilde{\mathrm{A}}\mathrm{B}} = \epsilon.$

For a CPTP map $\mathcal{F}$ with constant output σ_{B} the success probability is $1/M$, so

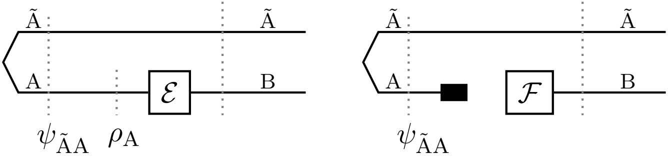
- $\beta(T_{\tilde{\mathrm{A}}\mathrm{B}}) = \mathrm{Tr}\rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}} T_{\tilde{\mathrm{A}}\mathrm{B}} = 1/M.$

Therefore $\forall \sigma_{\mathrm{B}} : \beta^{\mathbf{\Omega}}_{\epsilon}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}}) \le 1/M$, or

$$M \le B^{\mathbf{\Omega}}_{\epsilon}(\rho,\mathcal{E}) := \left(\max_{\sigma} \beta^{\mathbf{\Omega}}_{\epsilon}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})\right)^{-1}$$

Suppose there exists a code of size M, average input ρ, with error ϵ for $\mathcal{E}$, which maps to a test $T_{\tilde{A}B}$ in class $\mathbf{\Omega}$.

H_0: State is $\{\rho;\mathcal{E}\}_{\tilde{A}B}$ H_1: State is $\rho^*_{\tilde{A}}\sigma_B$



- $\alpha(T_{\tilde{A}B}) = 1 - \mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{A}B}T_{\tilde{A}B} = \epsilon$.

For a CPTP map $\mathcal{F}$ with constant output σ_B
the success probability is $1/M$, so

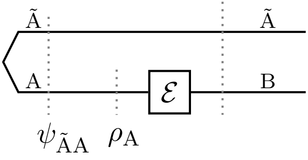
- $\beta(T_{\tilde{A}B}) = \mathrm{Tr}\rho^*_{\tilde{A}}\sigma_B T_{\tilde{A}B} = 1/M$.

Therefore $\forall\sigma_B : \beta^{\mathbf{\Omega}}_\epsilon(\{\rho;\mathcal{E}\}_{\tilde{A}B}, \rho^*_{\tilde{A}}\sigma_B) \le 1/M$, or

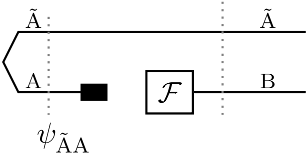
$$M \le B^{\mathbf{\Omega}}_\epsilon(\rho,\mathcal{E}) := \left(\max_\sigma \beta^{\mathbf{\Omega}}_\epsilon(\{\rho;\mathcal{E}\}_{\tilde{A}B}, \rho^*_{\tilde{A}}\sigma_B)\right)^{-1}$$

Suppose there exists a code of size M, average input ρ, with error ϵ for $\mathcal{E}$, which maps to a test $T_{\tilde{A}B}$ in class $\mathbf{\Omega}$.

H_0: State is $\{\rho;\mathcal{E}\}_{\tilde{A}B}$



H_1: State is $\rho^*_{\tilde{A}}\sigma_B$



- $\alpha(T_{\tilde{A}B}) = 1 - \mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{A}B}T_{\tilde{A}B} = \epsilon$.

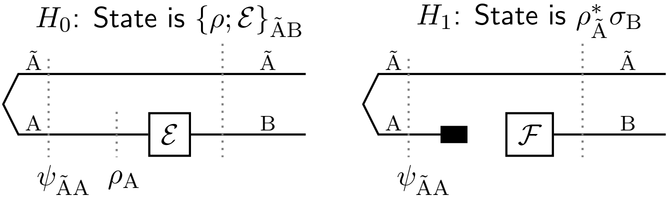
For a CPTP map $\mathcal{F}$ with constant output σ_B the success probability is $1/M$, so

- $\beta(T_{\tilde{A}B}) = \mathrm{Tr}\rho^*_{\tilde{A}}\sigma_B T_{\tilde{A}B} = 1/M$.

Therefore $\forall\sigma_B : \beta^{\mathbf{\Omega}}_\epsilon(\{\rho;\mathcal{E}\}_{\tilde{A}B}, \rho^*_{\tilde{A}}\sigma_B) \leq 1/M$, or

$$M \leq B^{\mathbf{\Omega}}_\epsilon(\rho,\mathcal{E}) := \left(\max_\sigma \beta^{\mathbf{\Omega}}_\epsilon(\{\rho;\mathcal{E}\}_{\tilde{A}B}, \rho^*_{\tilde{A}}\sigma_B)\right)^{-1}$$

Suppose there exists a code of size M, average input ρ, with error ϵ for $\mathcal{E}$, which maps to a test $T_{\tilde{\mathrm{A}}\mathrm{B}}$ in class $\mathbf{\Omega}$.



- $\alpha(T_{\tilde{\mathrm{A}}\mathrm{B}}) = 1 - \mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}} T_{\tilde{\mathrm{A}}\mathrm{B}} = \epsilon$.

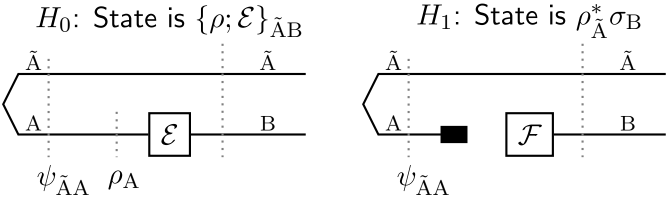
For a CPTP map $\mathcal{F}$ with constant output σ_{B}
the success probability is $1/M$, so

- $\beta(T_{\tilde{\mathrm{A}}\mathrm{B}}) = \mathrm{Tr}\rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}} T_{\tilde{\mathrm{A}}\mathrm{B}} = 1/M$.

Therefore $\forall \sigma_{\mathrm{B}} : \beta^{\mathbf{\Omega}}_{\epsilon}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}}) \leq 1/M$, or

$$M \leq B^{\mathbf{\Omega}}_{\epsilon}(\rho,\mathcal{E}) := \left(\max_{\sigma} \beta^{\mathbf{\Omega}}_{\epsilon}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})\right)^{-1}$$

Suppose there exists a code of size M, average input ρ, with error ϵ for $\mathcal{E}$, which maps to a test $T_{\tilde{A}B}$ in class $\mathbf{\Omega}$.



- $\alpha(T_{\tilde{A}B}) = 1 - \mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{A}B}T_{\tilde{A}B} = \epsilon$.

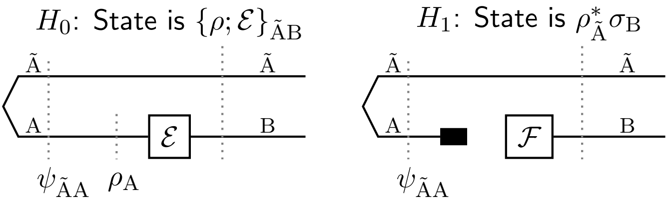
For a CPTP map $\mathcal{F}$ with constant output σ_B
the success probability is $1/M$, so

- $\beta(T_{\tilde{A}B}) = \mathrm{Tr}\rho^*_{\tilde{A}}\sigma_B T_{\tilde{A}B} = 1/M$.

Therefore $\forall \sigma_B : \beta^{\mathbf{\Omega}}_{\epsilon}(\{\rho;\mathcal{E}\}_{\tilde{A}B}, \rho^*_{\tilde{A}}\sigma_B) \le 1/M$, or

$$M \le B^{\mathbf{\Omega}}_{\epsilon}(\rho,\mathcal{E}) := \left(\max_{\sigma} \beta^{\mathbf{\Omega}}_{\epsilon}(\{\rho;\mathcal{E}\}_{\tilde{A}B}, \rho^*_{\tilde{A}}\sigma_B)\right)^{-1}$$

Suppose there exists a code of size M, average input ρ, with error ϵ for $\mathcal{E}$, which maps to a test $T_{\tilde{A}B}$ in class $\mathbf{\Omega}$.



- $\alpha(T_{\tilde{A}B}) = 1 - \mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{A}B}T_{\tilde{A}B} = \epsilon$.

For a CPTP map $\mathcal{F}$ with constant output σ_B the success probability is $1/M$, so

- $\beta(T_{\tilde{A}B}) = \mathrm{Tr}\rho^*_{\tilde{A}}\sigma_B T_{\tilde{A}B} = 1/M$.

Therefore $\forall\sigma_B : \beta^{\mathbf{\Omega}}_\epsilon(\{\rho;\mathcal{E}\}_{\tilde{A}B}, \rho^*_{\tilde{A}}\sigma_B) \leq 1/M$, or

$$M \leq B^{\mathbf{\Omega}}_\epsilon(\rho,\mathcal{E}) := \left(\max_\sigma \beta^{\mathbf{\Omega}}_\epsilon(\{\rho;\mathcal{E}\}_{\tilde{A}B}, \rho^*_{\tilde{A}}\sigma_B)\right)^{-1}$$

The main bounds

$$B_\epsilon^{\mathbf{\Omega}}(\rho, \mathcal{E}) := \left(\max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho; \mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}} \sigma_{\mathrm{B}}) \right)^{-1}$$

Defining $B_\epsilon^{\mathbf{\Omega}}(\mathcal{E}) := \max_\rho B^{\mathbf{\Omega}}(\rho, \mathcal{E})$ we have:
For entanglement-assisted codes: $M_\epsilon^{\mathrm{E}}(\rho, \mathcal{E}) \leq B_\epsilon(\rho, \mathcal{E})$, and

$$M_\epsilon^{\mathrm{E}}(\mathcal{E}) \leq B_\epsilon(\mathcal{E});$$

For unassisted codes: Since these map to local tests, for any class $\mathbf{\Omega}$ containing $\mathbf{L}$, $M_\epsilon(\rho, \mathcal{E}) \leq B_\epsilon^{\mathbf{\Omega}}(\rho, \mathcal{E})$, and

$$M_\epsilon(\mathcal{E}) \leq B_\epsilon^{\mathbf{\Omega}}(\mathcal{E}).$$

The main bounds

$$B_\epsilon^{\mathbf{\Omega}}(\rho,\mathcal{E}) := \left(\max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})\right)^{-1}$$

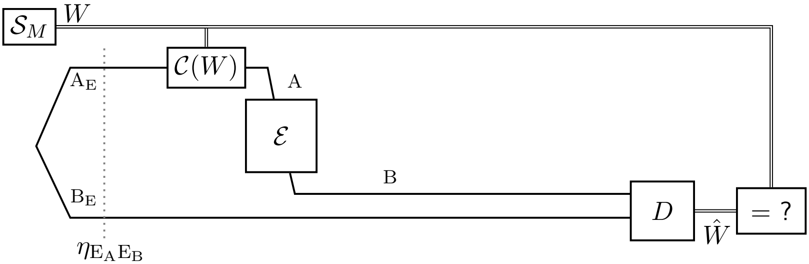
Defining $B_\epsilon^{\mathbf{\Omega}}(\mathcal{E}) := \max_\rho B^{\mathbf{\Omega}}(\rho,\mathcal{E})$ we have:
For entanglement-assisted codes: $M_\epsilon^{\mathrm{E}}(\rho,\mathcal{E}) \leq B_\epsilon(\rho,\mathcal{E})$, and

$$M_\epsilon^{\mathrm{E}}(\mathcal{E}) \leq B_\epsilon(\mathcal{E});$$

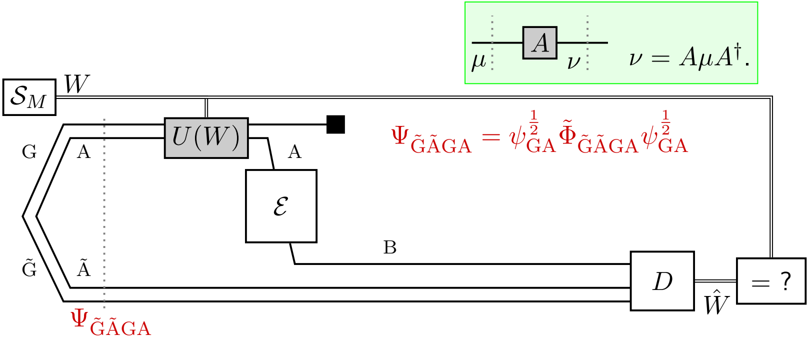
For unassisted codes: Since these map to local tests, for any class $\mathbf{\Omega}$ containing $\mathbf{L}$, $M_\epsilon(\rho,\mathcal{E}) \leq B_\epsilon^{\mathbf{\Omega}}(\rho,\mathcal{E})$, and

$$M_\epsilon(\mathcal{E}) \leq B_\epsilon^{\mathbf{\Omega}}(\mathcal{E}).$$

Constructing the test

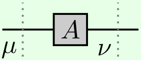


Constructing the test

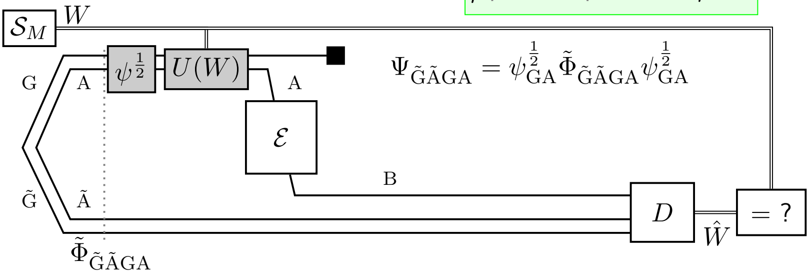


Constructing the test

$$\rho_{\mathrm{A}} = \frac{1}{M}\sum_w \mathrm{Tr}_{\mathrm{G}} U(w)_{\mathrm{GA}} \psi_{\mathrm{GA}} U(w)^{\dagger}_{\mathrm{GA}}$$



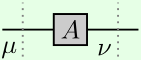
$$\nu = A\mu A^{\dagger}.$$



$$\Psi_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}\mathrm{GA}} = \psi^{\frac{1}{2}}_{\mathrm{GA}} \tilde{\Phi}_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}\mathrm{GA}} \psi^{\frac{1}{2}}_{\mathrm{GA}}$$

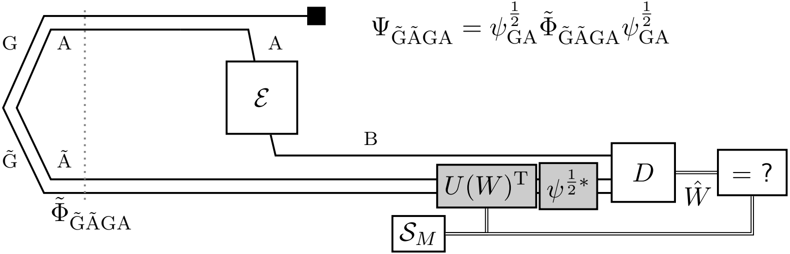
Constructing the test

$$\rho_{\mathrm{A}} = \frac{1}{M}\sum_w \mathrm{Tr}_{\mathrm{G}} U(w)_{\mathrm{GA}}\psi_{\mathrm{GA}}U(w)^{\dagger}_{\mathrm{GA}}$$



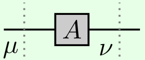
$\nu = A\mu A^{\dagger}$.

$$\Psi_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}\mathrm{GA}} = \psi^{\frac{1}{2}}_{\mathrm{GA}}\tilde{\Phi}_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}\mathrm{GA}}\psi^{\frac{1}{2}}_{\mathrm{GA}}$$



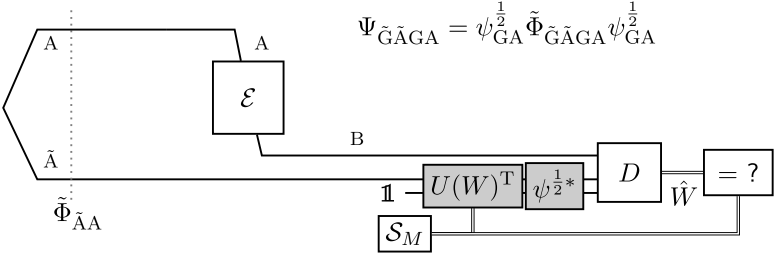
Constructing the test

$$\rho_{\mathrm{A}} = \frac{1}{M} \sum_w \mathrm{Tr}_{\mathrm{G}} U(w)_{\mathrm{GA}} \psi_{\mathrm{GA}} U(w)^{\dagger}_{\mathrm{GA}}$$



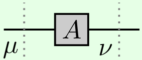
$\nu = A\mu A^{\dagger}.$

$$\Psi_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}\mathrm{GA}} = \psi^{\frac{1}{2}}_{\mathrm{GA}} \tilde{\Phi}_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}\mathrm{GA}} \psi^{\frac{1}{2}}_{\mathrm{GA}}$$



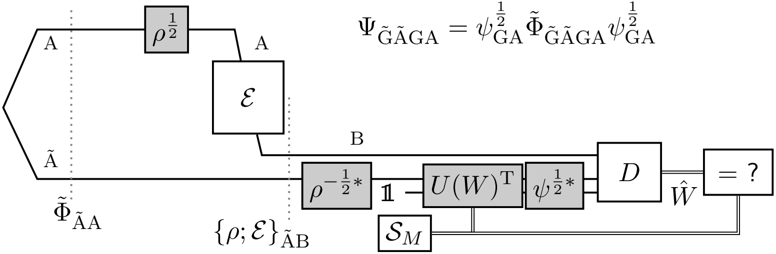
Constructing the test

$$\rho_{\mathrm{A}} = \frac{1}{M}\sum_w \mathrm{Tr}_{\mathrm{G}} U(w)_{\mathrm{GA}} \psi_{\mathrm{GA}} U(w)^{\dagger}_{\mathrm{GA}}$$



$\nu = A\mu A^{\dagger}$.

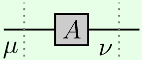
$$\Psi_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}\mathrm{GA}} = \psi^{\frac{1}{2}}_{\mathrm{GA}} \tilde{\Phi}_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}\mathrm{GA}} \psi^{\frac{1}{2}}_{\mathrm{GA}}$$



$$1 - \epsilon = \mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}} T_{\tilde{\mathrm{A}}\mathrm{B}}$$

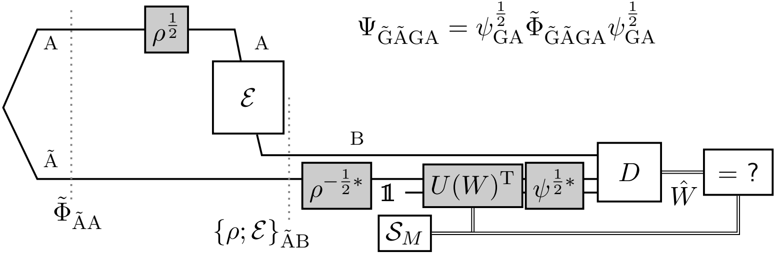
Constructing the test

$\rho_{\mathrm{A}} = \frac{1}{M}\sum_w \mathrm{Tr}_{\mathrm{G}} U(w)_{\mathrm{GA}} \psi_{\mathrm{GA}} U(w)^{\dagger}_{\mathrm{GA}}$



$\nu = A\mu A^{\dagger}$.

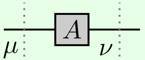
$\Psi_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}\mathrm{GA}} = \psi^{\frac{1}{2}}_{\mathrm{GA}} \tilde{\Phi}_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}\mathrm{GA}} \psi^{\frac{1}{2}}_{\mathrm{GA}}$



$1 - \epsilon = \mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}} T_{\tilde{\mathrm{A}}\mathrm{B}}$ where, with $K(w)_{\mathrm{GA}} := U(w)_{\mathrm{GA}} \psi^{\frac{1}{2}}_{\mathrm{GA}}$,

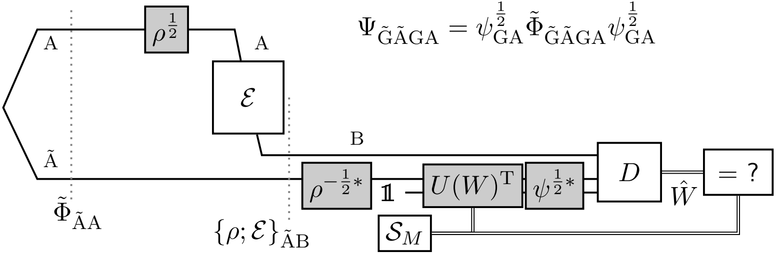
Constructing the test

$$\rho_{\mathrm{A}} = \frac{1}{M}\sum_w \mathrm{Tr}_{\mathrm{G}} U(w)_{\mathrm{GA}}\psi_{\mathrm{GA}}U(w)^{\dagger}_{\mathrm{GA}}$$



$\nu = A\mu A^{\dagger}$.

$$\Psi_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}\mathrm{GA}} = \psi^{\frac{1}{2}}_{\mathrm{GA}}\tilde{\Phi}_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}\mathrm{GA}}\psi^{\frac{1}{2}}_{\mathrm{GA}}$$



$1-\epsilon = \mathrm{Tr}\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}T_{\tilde{\mathrm{A}}\mathrm{B}}$ where, with $K(w)_{\mathrm{GA}} := U(w)_{\mathrm{GA}}\psi^{\frac{1}{2}}_{\mathrm{GA}}$,

$$T_{\tilde{\mathrm{A}}\mathrm{B}} = \frac{1}{M}\sum_{w=1}^{M}\rho_{\tilde{\mathrm{A}}}^{-\frac{1}{2}*}(\mathrm{Tr}_{\tilde{\mathrm{G}}}K(w)^{*}_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}}D(w)_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}\mathrm{B}}K(w)^{\mathrm{T}}_{\tilde{\mathrm{G}}\tilde{\mathrm{A}}})\rho_{\tilde{\mathrm{A}}}^{-\frac{1}{2}*}$$

Properties of the bounds

- They reduce to the PPV converse for classical channels.
- Entanglement-assisted bound:
  - Can recover converse part of BSST.
  - $B_\epsilon(\mathcal{E})^{-1}$ is given by an SDP which generalises the linear program formulation of the PPV converse (Matthews arXiv:1109.5417)
- Bounds for unassisted codes:
  - The upper bound for $M_\epsilon(\mathcal{E})$ in Wang-Renner (arXiv:1007.5456) is equivalent to $\mathbf{\Omega} = \mathbf{LC1}$ and fixing $\sigma = \mathcal{E}[\rho]$, which is no stronger than $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$ and can be worse.
  - $\mathbf{L}$ bound can be stronger (but less nice in other ways).
  - $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$, and hence $B_\epsilon^{\mathbf{L}}(\mathcal{E})$ can recover Holevo bound (see WR).
  - $B_\epsilon^{\mathbf{PPT}}(\mathcal{E})^{-1}$ is given by a semidefinite program (SDP).

Properties of the bounds

- They reduce to the PPV converse for classical channels.
- Entanglement-assisted bound:
  - Can recover converse part of BSST.
  - $B_\epsilon(\mathcal{E})^{-1}$ is given by an SDP which generalises the linear program formulation of the PPV converse (Matthews arXiv:1109.5417)
- Bounds for unassisted codes:
  - The upper bound for $M_\epsilon(\mathcal{E})$ in Wang-Renner (arXiv:1007.5456) is equivalent to $\mathbf{\Omega} = \mathbf{LC1}$ and fixing $\sigma = \mathcal{E}[\rho]$, which is no stronger than $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$ and can be worse.
  - $\mathbf{L}$ bound can be stronger (but less nice in other ways).
  - $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$, and hence $B_\epsilon^{\mathbf{L}}(\mathcal{E})$ can recover Holevo bound (see WR).
  - $B_\epsilon^{\mathbf{PPT}}(\mathcal{E})^{-1}$ is given by a semidefinite program (SDP).

Properties of the bounds

- They reduce to the PPV converse for classical channels.
- Entanglement-assisted bound:
  - Can recover converse part of BSST.
  - $B_\epsilon(\mathcal{E})^{-1}$ is given by an SDP which generalises the linear program formulation of the PPV converse (Matthews arXiv:1109.5417)
- Bounds for unassisted codes:
  - The upper bound for $M_\epsilon(\mathcal{E})$ in Wang-Renner (arXiv:1007.5456) is equivalent to $\mathbf{\Omega} = \mathbf{LC1}$ and fixing $\sigma = \mathcal{E}[\rho]$, which is no stronger than $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$ and can be worse.
  - $\mathbf{L}$ bound can be stronger (but less nice in other ways).
  - $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$, and hence $B_\epsilon^{\mathbf{L}}(\mathcal{E})$ can recover Holevo bound (see WR).
  - $B_\epsilon^{\mathbf{PPT}}(\mathcal{E})^{-1}$ is given by a semidefinite program (SDP).

Properties of the bounds

- They reduce to the PPV converse for classical channels.
- Entanglement-assisted bound:
  - Can recover converse part of BSST.
  - $B_\epsilon(\mathcal{E})^{-1}$ is given by an SDP which generalises the linear program formulation of the PPV converse (Matthews arXiv:1109.5417)
- Bounds for unassisted codes:
  - The upper bound for $M_\epsilon(\mathcal{E})$ in Wang-Renner (arXiv:1007.5456) is equivalent to $\mathbf{\Omega} = \mathbf{LC1}$ and fixing $\sigma = \mathcal{E}[\rho]$, which is no stronger than $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$ and can be worse.
  - $\mathbf{L}$ bound can be stronger (but less nice in other ways).
  - $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$, and hence $B_\epsilon^{\mathbf{L}}(\mathcal{E})$ can recover Holevo bound (see WR).
  - $B_\epsilon^{\mathbf{PPT}}(\mathcal{E})^{-1}$ is given by a semidefinite program (SDP).

Properties of the bounds

- They reduce to the PPV converse for classical channels.
- Entanglement-assisted bound:
  - Can recover converse part of BSST.
  - $B_\epsilon(\mathcal{E})^{-1}$ is given by an SDP which generalises the linear program formulation of the PPV converse (Matthews arXiv:1109.5417)
- Bounds for unassisted codes:
  - The upper bound for $M_\epsilon(\mathcal{E})$ in Wang-Renner (arXiv:1007.5456) is equivalent to $\mathbf{\Omega} = \mathbf{LC1}$ and fixing $\sigma = \mathcal{E}[\rho]$, which is no stronger than $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$ and can be worse.
  - $\mathbf{L}$ bound can be stronger (but less nice in other ways).
  - $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$, and hence $B_\epsilon^{\mathbf{L}}(\mathcal{E})$ can recover Holevo bound (see WR).
  - $B_\epsilon^{\mathbf{PPT}}(\mathcal{E})^{-1}$ is given by a semidefinite program (SDP).

Properties of the bounds

- They reduce to the PPV converse for classical channels.
- Entanglement-assisted bound:
  - Can recover converse part of BSST.
  - $B_\epsilon(\mathcal{E})^{-1}$ is given by an SDP which generalises the linear program formulation of the PPV converse (Matthews arXiv:1109.5417)
- Bounds for unassisted codes:
  - The upper bound for $M_\epsilon(\mathcal{E})$ in Wang-Renner (arXiv:1007.5456) is equivalent to $\mathbf{\Omega} = \mathbf{LC1}$ and fixing $\sigma = \mathcal{E}[\rho]$, which is no stronger than $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$ and can be worse.
  - $\mathbf{L}$ bound can be stronger (but less nice in other ways).
  - $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$, and hence $B_\epsilon^{\mathbf{L}}(\mathcal{E})$ can recover Holevo bound (see WR).
  - $B_\epsilon^{\mathbf{PPT}}(\mathcal{E})^{-1}$ is given by a semidefinite program (SDP).

Properties of the bounds

- They reduce to the PPV converse for classical channels.
- Entanglement-assisted bound:
  - Can recover converse part of BSST.
  - $B_\epsilon(\mathcal{E})^{-1}$ is given by an SDP which generalises the linear program formulation of the PPV converse (Matthews arXiv:1109.5417)
- Bounds for unassisted codes:
  - The upper bound for $M_\epsilon(\mathcal{E})$ in Wang-Renner (arXiv:1007.5456) is equivalent to $\mathbf{\Omega} = \mathbf{LC1}$ and fixing $\sigma = \mathcal{E}[\rho]$, which is no stronger than $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$ and can be worse.
  - $\mathbf{L}$ bound can be stronger (but less nice in other ways).
  - $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$, and hence $B_\epsilon^{\mathbf{L}}(\mathcal{E})$ can recover Holevo bound (see WR).
  - $B_\epsilon^{\mathbf{PPT}}(\mathcal{E})^{-1}$ is given by a semidefinite program (SDP).

Properties of the bounds

- They reduce to the PPV converse for classical channels.
- Entanglement-assisted bound:
  - Can recover converse part of BSST.
  - $B_\epsilon(\mathcal{E})^{-1}$ is given by an SDP which generalises the linear program formulation of the PPV converse (Matthews arXiv:1109.5417)
- Bounds for unassisted codes:
  - The upper bound for $M_\epsilon(\mathcal{E})$ in Wang-Renner (arXiv:1007.5456) is equivalent to $\mathbf{\Omega} = \mathbf{LC1}$ and fixing $\sigma = \mathcal{E}[\rho]$, which is no stronger than $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$ and can be worse.
  - $\mathbf{L}$ bound can be stronger (but less nice in other ways).
  - $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$, and hence $B_\epsilon^{\mathbf{L}}(\mathcal{E})$ can recover Holevo bound (see WR).
  - $B_\epsilon^{\mathbf{PPT}}(\mathcal{E})^{-1}$ is given by a semidefinite program (SDP).

Properties of the bounds

- They reduce to the PPV converse for classical channels.
- Entanglement-assisted bound:
  - Can recover converse part of BSST.
  - $B_\epsilon(\mathcal{E})^{-1}$ is given by an SDP which generalises the linear program formulation of the PPV converse (Matthews arXiv:1109.5417)
- Bounds for unassisted codes:
  - The upper bound for $M_\epsilon(\mathcal{E})$ in Wang-Renner (arXiv:1007.5456) is equivalent to $\mathbf{\Omega} = \mathbf{LC1}$ and fixing $\sigma = \mathcal{E}[\rho]$, which is no stronger than $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$ and can be worse.
  - $\mathbf{L}$ bound can be stronger (but less nice in other ways).
  - $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$, and hence $B_\epsilon^{\mathbf{L}}(\mathcal{E})$ can recover Holevo bound (see WR).
  - $B_\epsilon^{\mathbf{PPT}}(\mathcal{E})^{-1}$ is given by a semidefinite program (SDP).

Properties of the bounds

- They reduce to the PPV converse for classical channels.
- Entanglement-assisted bound:
  - Can recover converse part of BSST.
  - $B_\epsilon(\mathcal{E})^{-1}$ is given by an SDP which generalises the linear program formulation of the PPV converse (Matthews arXiv:1109.5417)
- Bounds for unassisted codes:
  - The upper bound for $M_\epsilon(\mathcal{E})$ in Wang-Renner (arXiv:1007.5456) is equivalent to $\mathbf{\Omega} = \mathbf{LC1}$ and fixing $\sigma = \mathcal{E}[\rho]$, which is no stronger than $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$ and can be worse.
  - $\mathbf{L}$ bound can be stronger (but less nice in other ways).
  - $B_\epsilon^{\mathbf{LC1}}(\mathcal{E})$, and hence $B_\epsilon^{\mathbf{L}}(\mathcal{E})$ can recover Holevo bound (see WR).
  - $B_\epsilon^{\mathbf{PPT}}(\mathcal{E})^{-1}$ is given by a semidefinite program (SDP).

Properties of the bounds[2]

$$B_\epsilon^{\mathbf{\Omega}}(\mathcal{E}) = \left(\min_\rho \max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})\right)^{-1}$$

- $\beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})$ is
  - Concave in σ.
  - Convex in ρ if $\mathbf{LC1} \subseteq \mathbf{\Omega}$.
- $\max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})$ is also convex in ρ.

These properties allow simplification given symmetry:

- For a **group covariant map** $\forall g \in G : \mathcal{E}[U_g \rho U_g^\dagger] = V_g \mathcal{E}[\rho] V_g^\dagger$, we can restrict to group *invariant* ρ and σ in the optimisations.
- For permutation covariant channels: Poly(n) size SDP for EA converse ($\mathbf{\Omega} = \mathbf{ALL}$).

[2]See Y. Polyanskiy's study of classical bound on his website. To appear in IEEE Trans. Inf. T.

Properties of the bounds[2]

$$B_\epsilon^{\mathbf{\Omega}}(\mathcal{E}) = \left(\min_\rho \max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}}) \right)^{-1}$$

- $\beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})$ is
  - Concave in σ.
  - Convex in ρ if $\mathbf{LC1} \subseteq \mathbf{\Omega}$.
- $\max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})$ is also convex in ρ.

These properties allow simplification given symmetry:

- For a **group covariant map** $\forall g \in G : \mathcal{E}[U_g \rho U_g^\dagger] = V_g \mathcal{E}[\rho] V_g^\dagger$, we can restrict to group *invariant* ρ and σ in the optimisations.
- For permutation covariant channels: Poly(n) size SDP for EA converse ($\mathbf{\Omega} = \mathbf{ALL}$).

[2] See Y. Polyanskiy's study of classical bound on his website. To appear in IEEE Trans. Inf. T.

Properties of the bounds[2]

$$B_\epsilon^{\mathbf{\Omega}}(\mathcal{E}) = \left(\min_\rho \max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})\right)^{-1}$$

- $\beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})$ is
  - Concave in σ.
  - Convex in ρ if $\mathbf{LC1} \subseteq \mathbf{\Omega}$.
- $\max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})$ is also convex in ρ.

These properties allow simplification given symmetry:

- For a **group covariant map** $\forall g \in G : \mathcal{E}[U_g \rho U_g^\dagger] = V_g \mathcal{E}[\rho] V_g^\dagger$, we can restrict to group *invariant* ρ and σ in the optimisations.
- For permutation covariant channels: Poly(n) size SDP for EA converse ($\mathbf{\Omega} = \mathbf{ALL}$).

[2]See Y. Polyanskiy's study of classical bound on his website. To appear in IEEE Trans. Inf. T.

Properties of the bounds[2]

$$B_\epsilon^{\mathbf{\Omega}}(\mathcal{E}) = \left(\min_{\rho} \max_{\sigma} \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}}) \right)^{-1}$$

- $\beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})$ is
  - Concave in σ.
  - Convex in ρ if $\mathbf{LC1} \subseteq \mathbf{\Omega}$.
- $\max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})$ is also convex in ρ.

These properties allow simplification given symmetry:

- For a **group covariant map** $\forall g \in G : \mathcal{E}[U_g \rho U_g^\dagger] = V_g \mathcal{E}[\rho] V_g^\dagger$, we can restrict to group *invariant* ρ and σ in the optimisations.
- For permutation covariant channels: Poly(n) size SDP for EA converse ($\mathbf{\Omega} = \mathbf{ALL}$).

[2] See Y. Polyanskiy's study of classical bound on his website. To appear in IEEE Trans. Inf. T.

Properties of the bounds[2]

$$B_\epsilon^{\mathbf{\Omega}}(\mathcal{E}) = \left(\min_\rho \max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})\right)^{-1}$$

- $\beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})$ is
  - Concave in σ.
  - Convex in ρ if $\mathbf{LC1} \subseteq \mathbf{\Omega}$.
- $\max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})$ is also convex in ρ.

These properties allow simplification given symmetry:

- For a **group covariant map** $\forall g \in G : \mathcal{E}[U_g \rho U_g^\dagger] = V_g \mathcal{E}[\rho] V_g^\dagger$, we can restrict to group *invariant* ρ and σ in the optimisations.
- For permutation covariant channels: Poly(n) size SDP for EA converse ($\mathbf{\Omega} = \mathbf{ALL}$).

---

[2] See Y. Polyanskiy's study of classical bound on his website. To appear in IEEE Trans. Inf. T.

Properties of the bounds[2]

$$B_\epsilon^{\mathbf{\Omega}}(\mathcal{E}) = \left(\min_\rho \max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho_{\tilde{\mathrm{A}}}^{*}\sigma_{\mathrm{B}})\right)^{-1}$$

- $\beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho_{\tilde{\mathrm{A}}}^{*}\sigma_{\mathrm{B}})$ is
  - Concave in σ.
  - Convex in ρ if $\mathbf{LC1} \subseteq \mathbf{\Omega}$.
- $\max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho_{\tilde{\mathrm{A}}}^{*}\sigma_{\mathrm{B}})$ is also convex in ρ.

These properties allow simplification given symmetry:

- For a **group covariant map** $\forall g \in G : \mathcal{E}[U_g \rho U_g^\dagger] = V_g \mathcal{E}[\rho] V_g^\dagger$, we can restrict to group *invariant* ρ and σ in the optimisations.
- For permutation covariant channels: Poly(n) size SDP for EA converse ($\mathbf{\Omega} = \mathbf{ALL}$).

[2] See Y. Polyanskiy's study of classical bound on his website. To appear in IEEE Trans. Inf. T.

Properties of the bounds[2]

$$B_\epsilon^{\mathbf{\Omega}}(\mathcal{E}) = \left(\min_\rho \max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}}) \right)^{-1}$$

- $\beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})$ is
  - Concave in σ.
  - Convex in ρ if $\mathbf{LC1} \subseteq \mathbf{\Omega}$.
- $\max_\sigma \beta_\epsilon^{\mathbf{\Omega}}(\{\rho;\mathcal{E}\}_{\tilde{\mathrm{A}}\mathrm{B}}, \rho^*_{\tilde{\mathrm{A}}}\sigma_{\mathrm{B}})$ is also convex in ρ.

These properties allow simplification given symmetry:

- For a **group covariant map** $\forall g \in G : \mathcal{E}[U_g \rho U_g^\dagger] = V_g \mathcal{E}[\rho] V_g^\dagger$, we can restrict to group *invariant* ρ and σ in the optimisations.
- For permutation covariant channels: Poly(n) size SDP for EA converse ($\mathbf{\Omega} = \mathbf{ALL}$).

[2]See Y. Polyanskiy's study of classical bound on his website. To appear in IEEE Trans. Inf. T.

Example: EA coding over the depolarising channel

- d-dimensional depolarising channel:
  $\mathcal{D}[\tau] = (1-p)\tau + p\mathrm{Tr}(\tau)\mu$,
  where $\mu = \mathbb{1}/d$ is the maximally mixed state.
- $\mathcal{D}^{\otimes n}$ has the covariance group $S_n \ltimes \mathrm{U}(d)^{\times n}$
- Only G invariant ρ and σ are the maximally mixed states.
- $\{\mu^{\otimes n}; \mathcal{D}^{\otimes n}\} = \phi(p)^{\otimes n}$ where $\phi(p) := (1-p)\phi_{\tilde{\mathrm{A}}\mathrm{B}} + p\mu_{\tilde{\mathrm{A}}}\mu_{\mathrm{B}}$,
  where ϕ is the $U \otimes U^*$ invariant maximally entangled state.
- $M_\epsilon^{\mathrm{E}}(\mathcal{D}^{\otimes n}) \leq B_\epsilon(\mathcal{E}) = \beta_\epsilon((\phi(p)^{\otimes n})_{\tilde{\mathrm{A}}^n\mathrm{B}^n} \| (\mu^{\otimes n})_{\tilde{\mathrm{A}}^n}(\mu^{\otimes n})_{\mathrm{B}^n})^{-1}$
- Since the arguments commute, and there are only two distinct eigenvalues (eigenprojectors ϕ and $\mathbb{1} - \phi$), the problem is equivalent to classical hypothesis testing between two differently biased coins, based on n tosses.

Example: EA coding over the depolarising channel

- d-dimensional depolarising channel:
  $\mathcal{D}[\tau] = (1-p)\tau + p\mathrm{Tr}(\tau)\mu$,
  where $\mu = \mathbb{1}/d$ is the maximally mixed state.
- $\mathcal{D}^{\otimes n}$ has the covariance group $S_n \ltimes \mathrm{U}(d)^{\times n}$
- Only G invariant ρ and σ are the maximally mixed states.
- $\{\mu^{\otimes n}; \mathcal{D}^{\otimes n}\} = \phi(p)^{\otimes n}$ where $\phi(p) := (1-p)\phi_{\tilde{\mathrm{A}}\mathrm{B}} + p\mu_{\tilde{\mathrm{A}}}\mu_{\mathrm{B}}$,
  where ϕ is the $U \otimes U^*$ invariant maximally entangled state.
- $M_\epsilon^{\mathrm{E}}(\mathcal{D}^{\otimes n}) \leq B_\epsilon(\mathcal{E}) = \beta_\epsilon((\phi(p)^{\otimes n})_{\tilde{\mathrm{A}}^n\mathrm{B}^n} \| (\mu^{\otimes n})_{\tilde{\mathrm{A}}^n}(\mu^{\otimes n})_{\mathrm{B}^n})^{-1}$
- Since the arguments commute, and there are only two distinct eigenvalues (eigenprojectors ϕ and $\mathbb{1} - \phi$), the problem is equivalent to classical hypothesis testing between two differently biased coins, based on n tosses.

Example: EA coding over the depolarising channel

- d-dimensional depolarising channel:
  $\mathcal{D}[\tau] = (1-p)\tau + p\mathrm{Tr}(\tau)\mu$,
  where $\mu = \mathbb{1}/d$ is the maximally mixed state.
- $\mathcal{D}^{\otimes n}$ has the covariance group $S_n \ltimes \mathrm{U}(d)^{\times n}$
- Only G invariant ρ and σ are the maximally mixed states.
- $\{\mu^{\otimes n}; \mathcal{D}^{\otimes n}\} = \phi(p)^{\otimes n}$ where $\phi(p) := (1-p)\phi_{\tilde{\mathrm{A}}\mathrm{B}} + p\mu_{\tilde{\mathrm{A}}}\mu_{\mathrm{B}}$,
  where ϕ is the $U \otimes U^*$ invariant maximally entangled state.
- $M_\epsilon^{\mathrm{E}}(\mathcal{D}^{\otimes n}) \leq B_\epsilon(\mathcal{E}) = \beta_\epsilon((\phi(p)^{\otimes n})_{\tilde{\mathrm{A}}^n\mathrm{B}^n} \| (\mu^{\otimes n})_{\tilde{\mathrm{A}}^n}(\mu^{\otimes n})_{\mathrm{B}^n})^{-1}$
- Since the arguments commute, and there are only two distinct eigenvalues (eigenprojectors ϕ and $\mathbb{1} - \phi$), the problem is equivalent to classical hypothesis testing between two differently biased coins, based on n tosses.

Example: EA coding over the depolarising channel

- d-dimensional depolarising channel:
  $\mathcal{D}[\tau] = (1-p)\tau + p\mathrm{Tr}(\tau)\mu$,
  where $\mu = \mathbb{1}/d$ is the maximally mixed state.
- $\mathcal{D}^{\otimes n}$ has the covariance group $S_n \ltimes \mathrm{U}(d)^{\times n}$
- Only G invariant ρ and σ are the maximally mixed states.
- $\{\mu^{\otimes n}; \mathcal{D}^{\otimes n}\} = \phi(p)^{\otimes n}$ where $\phi(p) := (1-p)\phi_{\tilde{\mathrm{A}}\mathrm{B}} + p\mu_{\tilde{\mathrm{A}}}\mu_{\mathrm{B}}$,
  where ϕ is the $U \otimes U^*$ invariant maximally entangled state.
- $M_\epsilon^{\mathrm{E}}(\mathcal{D}^{\otimes n}) \leq B_\epsilon(\mathcal{E}) = \beta_\epsilon((\phi(p)^{\otimes n})_{\tilde{\mathrm{A}}^n\mathrm{B}^n} \| (\mu^{\otimes n})_{\tilde{\mathrm{A}}^n}(\mu^{\otimes n})_{\mathrm{B}^n})^{-1}$
- Since the arguments commute, and there are only two distinct eigenvalues (eigenprojectors ϕ and $\mathbb{1} - \phi$), the problem is equivalent to classical hypothesis testing between two differently biased coins, based on n tosses.

Example: EA coding over the depolarising channel

- d-dimensional depolarising channel:
  $\mathcal{D}[\tau] = (1-p)\tau + p\mathrm{Tr}(\tau)\mu$,
  where $\mu = \mathbb{1}/d$ is the maximally mixed state.
- $\mathcal{D}^{\otimes n}$ has the covariance group $S_n \ltimes \mathrm{U}(d)^{\times n}$
- Only G invariant ρ and σ are the maximally mixed states.
- $\{\mu^{\otimes n}; \mathcal{D}^{\otimes n}\} = \phi(p)^{\otimes n}$ where $\phi(p) := (1-p)\phi_{\tilde{\mathrm{A}}\mathrm{B}} + p\mu_{\tilde{\mathrm{A}}}\mu_{\mathrm{B}}$,
  where ϕ is the $U \otimes U^*$ invariant maximally entangled state.
- $M_\epsilon^{\mathrm{E}}(\mathcal{D}^{\otimes n}) \leq B_\epsilon(\mathcal{E}) = \beta_\epsilon((\phi(p)^{\otimes n})_{\tilde{\mathrm{A}}^n\mathrm{B}^n} \| (\mu^{\otimes n})_{\tilde{\mathrm{A}}^n}(\mu^{\otimes n})_{\mathrm{B}^n})^{-1}$
- Since the arguments commute, and there are only two distinct eigenvalues (eigenprojectors ϕ and $\mathbb{1} - \phi$), the problem is equivalent to classical hypothesis testing between two differently biased coins, based on n tosses.

Example: EA coding over the depolarising channel

- d-dimensional depolarising channel:
  $\mathcal{D}[\tau] = (1-p)\tau + p\mathrm{Tr}(\tau)\mu$,
  where $\mu = \mathbb{1}/d$ is the maximally mixed state.
- $\mathcal{D}^{\otimes n}$ has the covariance group $S_n \ltimes \mathrm{U}(d)^{\times n}$
- Only G invariant ρ and σ are the maximally mixed states.
- $\{\mu^{\otimes n}; \mathcal{D}^{\otimes n}\} = \phi(p)^{\otimes n}$ where $\phi(p) := (1-p)\phi_{\tilde{\mathrm{A}}\mathrm{B}} + p\mu_{\tilde{\mathrm{A}}}\mu_{\mathrm{B}}$,
  where ϕ is the $U \otimes U^*$ invariant maximally entangled state.
- $M_\epsilon^{\mathrm{E}}(\mathcal{D}^{\otimes n}) \leq B_\epsilon(\mathcal{E}) = \beta_\epsilon((\phi(p)^{\otimes n})_{\tilde{\mathrm{A}}^n\mathrm{B}^n} \| (\mu^{\otimes n})_{\tilde{\mathrm{A}}^n}(\mu^{\otimes n})_{\mathrm{B}^n})^{-1}$
- Since the arguments commute, and there are only two distinct eigenvalues (eigenprojectors ϕ and $\mathbb{1} - \phi$), the problem is equivalent to classical hypothesis testing between two differently biased coins, based on n tosses.

Example: EA coding over the depolarising channel

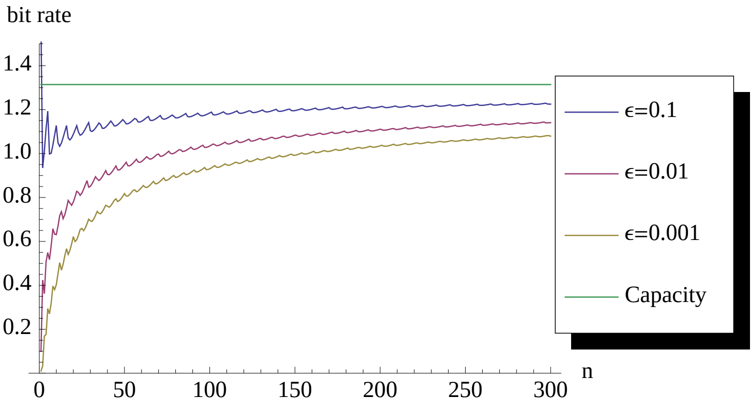


Figure: The upper bound on the rate for entanglement assisted codes over the p=0.15 depolarising channel for three different error probabilities.

Summary and outlook

- We have generalised a powerful converse for classical channel coding to a hierarchy of bounds for quantum channel coding based on hypothesis testing with restricted measurements.
- Application to proving security in the noisy-storage model of quantum cryptography (see paper).
- Almost closed form expressions for other simple channels?
- Relationship to Datta-Hsieh bound?
- Investigate PPT bound for unassisted codes.
- "Matching" achievability bounds?
- Second order asymptotics for EA coding over i.i.d. channels (converse part of Strassen-like result) using results of next talk?

Summary and outlook

- We have generalised a powerful converse for classical channel coding to a hierarchy of bounds for quantum channel coding based on hypothesis testing with restricted measurements.
- Application to proving security in the noisy-storage model of quantum cryptography (see paper).
- Almost closed form expressions for other simple channels?
- Relationship to Datta-Hsieh bound?
- Investigate PPT bound for unassisted codes.
- "Matching" achievability bounds?
- Second order asymptotics for EA coding over i.i.d. channels (converse part of Strassen-like result) using results of next talk?

Summary and outlook

- We have generalised a powerful converse for classical channel coding to a hierarchy of bounds for quantum channel coding based on hypothesis testing with restricted measurements.
- Application to proving security in the noisy-storage model of quantum cryptography (see paper).
- Almost closed form expressions for other simple channels?
- Relationship to Datta-Hsieh bound?
- Investigate PPT bound for unassisted codes.
- "Matching" achievability bounds?
- Second order asymptotics for EA coding over i.i.d. channels (converse part of Strassen-like result) using results of next talk?

Summary and outlook

- We have generalised a powerful converse for classical channel coding to a hierarchy of bounds for quantum channel coding based on hypothesis testing with restricted measurements.
- Application to proving security in the noisy-storage model of quantum cryptography (see paper).
- Almost closed form expressions for other simple channels?
- Relationship to Datta-Hsieh bound?
- Investigate PPT bound for unassisted codes.
- "Matching" achievability bounds?
- Second order asymptotics for EA coding over i.i.d. channels (converse part of Strassen-like result) using results of next talk?

Summary and outlook

- We have generalised a powerful converse for classical channel coding to a hierarchy of bounds for quantum channel coding based on hypothesis testing with restricted measurements.
- Application to proving security in the noisy-storage model of quantum cryptography (see paper).
- Almost closed form expressions for other simple channels?
- Relationship to Datta-Hsieh bound?
- Investigate PPT bound for unassisted codes.
- "Matching" achievability bounds?
- Second order asymptotics for EA coding over i.i.d. channels (converse part of Strassen-like result) using results of next talk?

Summary and outlook

- We have generalised a powerful converse for classical channel coding to a hierarchy of bounds for quantum channel coding based on hypothesis testing with restricted measurements.
- Application to proving security in the noisy-storage model of quantum cryptography (see paper).
- Almost closed form expressions for other simple channels?
- Relationship to Datta-Hsieh bound?
- Investigate PPT bound for unassisted codes.
- “Matching” achievability bounds?
- Second order asymptotics for EA coding over i.i.d. channels (converse part of Strassen-like result) using results of next talk?

Summary and outlook

- We have generalised a powerful converse for classical channel coding to a hierarchy of bounds for quantum channel coding based on hypothesis testing with restricted measurements.
- Application to proving security in the noisy-storage model of quantum cryptography (see paper).
- Almost closed form expressions for other simple channels?
- Relationship to Datta-Hsieh bound?
- Investigate PPT bound for unassisted codes.
- "Matching" achievability bounds?
- Second order asymptotics for EA coding over i.i.d. channels (converse part of Strassen-like result) using results of next talk?

Summary and outlook

- We have generalised a powerful converse for classical channel coding to a hierarchy of bounds for quantum channel coding based on hypothesis testing with restricted measurements.
- Application to proving security in the noisy-storage model of quantum cryptography (see paper).
- Almost closed form expressions for other simple channels?
- Relationship to Datta-Hsieh bound?
- Investigate PPT bound for unassisted codes.
- “Matching” achievability bounds?
- Second order asymptotics for EA coding over i.i.d. channels (converse part of Strassen-like result) using results of next talk?