Catalytic Decoupling

Christian Majenz
QMATH, University of Copenhagen
Joint work with Mario Berta, Frédéric Dupuis, Renato Renner and Matthias Christandl
(arXiv:1605.00514)

Beyond IID Workshop, Institut d'Estudis Catalans, Barcelona

22.07.2016

Structure

Introduction

Decoupling

- Idea: Get rid of correlations by locally applying a noisy operation

Decoupling

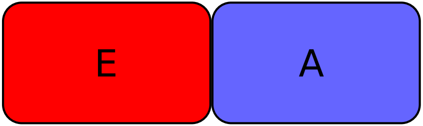
- Idea: Get rid of correlations by locally applying a noisy operation
- most used operations: partial trace, projective measurement

Decoupling

- Idea: Get rid of correlations by locally applying a noisy operation
- most used operations: partial trace, projective measurement

Decoupling by partial trace:

- bipartite system AE

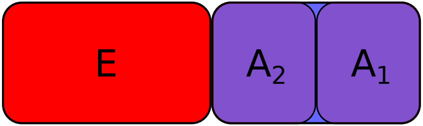


Decoupling

- Idea: Get rid of correlations by locally applying a noisy operation
- most used operations: partial trace, projective measurement

Decoupling by partial trace:

- bipartite system AE
- divide system A into two parts, $A \cong A_1 \otimes A_2$

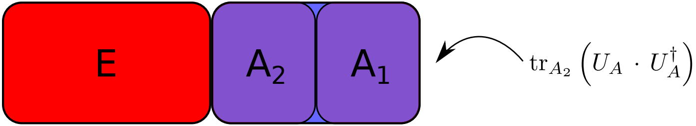


Decoupling

- Idea: Get rid of correlations by locally applying a noisy operation
- most used operations: partial trace, projective measurement

Decoupling by partial trace:

- bipartite system AE
- divide system A into two parts, $A \cong A_1 \otimes A_2$
- apply a unitary

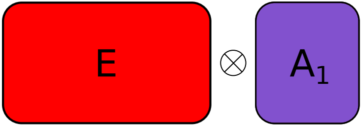


Decoupling

- Idea: Get rid of correlations by locally applying a noisy operation
- most used operations: partial trace, projective measurement

Decoupling by partial trace:

- bipartite system AE
- divide system A into two parts, $A \cong A_1 \otimes A_2$
- apply a unitary
- trace out A_2

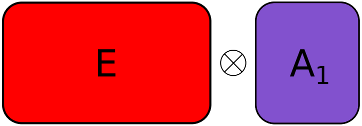


Decoupling

- Idea: Get rid of correlations by locally applying a noisy operation
- most used operations: partial trace, projective measurement

Decoupling by partial trace:

- bipartite system AE
- divide system A into two parts, $A \cong A_1 \otimes A_2$
- apply a unitary
- trace out A_2
- how big do we have to choose A_2?



Applications:

Applications:

- Quantum state merging (Horodecki, Oppenheim, Winter), "mother protocol" (Abeyesinghe et al.)
- Quantum state redistribution (Devetak, Yard)
- Channel coding
- Quantum thermodynamics
- Solid state physics
- Black hole radiation

...

Smooth Rényi entropies

- $\rho, \sigma \in \mathcal{B}(\mathcal{H})$, $\rho, \sigma > 0$, $\mathrm{tr}\rho = 1$

Smooth Rényi entropies

- $\rho, \sigma \in \mathcal{B}(\mathcal{H})$, $\rho, \sigma > 0$, $\mathrm{tr}\rho = 1$

  max-relative entropy $D_{\max}(\rho\|\sigma) = \min\left\{\lambda \in \mathbb{R}\middle| 2^\lambda \sigma \geq \rho\right\}$

Smooth Rényi entropies

- $\rho, \sigma \in \mathcal{B}(\mathcal{H})$, $\rho, \sigma > 0$, $\mathrm{tr}\rho = 1$

  max-relative entropy $D_{\max}(\rho\|\sigma) = \min\left\{\lambda \in \mathbb{R} \middle| 2^{\lambda}\sigma \geq \rho\right\}$

- bipartite state ρ_{AB}
  conditional min-entropy
  $H_{\min}(A|B)_{\rho} = \max_{\sigma}(-D_{\max}(\rho_{AB}\|\mathbb{1}_A \otimes \sigma_B))$

Smooth Rényi entropies

- $\rho, \sigma \in \mathcal{B}(\mathcal{H})$, $\rho, \sigma > 0$, $\mathrm{tr}\rho = 1$

  max-relative entropy $D_{\max}(\rho\|\sigma) = \min\left\{\lambda \in \mathbb{R}\middle|2^{\lambda}\sigma \geq \rho\right\}$
- bipartite state ρ_{AB}
  conditional min-entropy
  $H_{\min}(A|B)_\rho = \max_\sigma(-D_{\max}(\rho_{AB}\|\mathbb{1}_A \otimes \sigma_B))$
- conditional max-entropy defined via purification ρ_{ABC},
  $H_{\max}(A|B)_\rho = -H_{\min}(A|C)$

Smooth Rényi entropies

- $\rho, \sigma \in \mathcal{B}(\mathcal{H})$, $\rho, \sigma > 0$, $\mathrm{tr}\rho = 1$

  max-relative entropy $D_{\mathrm{max}}(\rho\|\sigma) = \min\left\{\lambda \in \mathbb{R} \middle| 2^{\lambda}\sigma \geq \rho\right\}$
- bipartite state ρ_{AB}
  conditional min-entropy
  $H_{\mathrm{min}}(A|B)_{\rho} = \max_{\sigma}(-D_{\mathrm{max}}(\rho_{AB}\|\mathbb{1}_A \otimes \sigma_B))$
- conditional max-entropy defined via purification ρ_{ABC},
  $H_{\mathrm{max}}(A|B)_{\rho} = -H_{\mathrm{min}}(A|C)$
- smooth versions $H_x^{\varepsilon}(A|B)_{\rho}$ by taking max / min over ε-Ball

Smooth Rényi entropies

- $\rho, \sigma \in \mathcal{B}(\mathcal{H})$, $\rho, \sigma > 0$, $\mathrm{tr}\rho = 1$

  max-relative entropy $D_{\max}(\rho\|\sigma) = \min\left\{\lambda \in \mathbb{R} \middle| 2^{\lambda}\sigma \geq \rho\right\}$
- bipartite state ρ_{AB}
  conditional min-entropy
  $H_{\min}(A|B)_{\rho} = \max_{\sigma}(-D_{\max}(\rho_{AB}\|\mathbb{1}_A \otimes \sigma_B))$
- conditional max-entropy defined via purification ρ_{ABC},
  $H_{\max}(A|B)_{\rho} = -H_{\min}(A|C)$
- smooth versions $H_x^{\varepsilon}(A|B)_{\rho}$ by taking max / min over ε-Ball
- max-mutual information:
  $I_{\max}(A:B)_{\rho} = \min_{\sigma} D_{\max}(\rho_{AB}\|\rho_A \otimes \sigma_B)$

Smooth Rényi entropies

- $\rho, \sigma \in \mathcal{B}(\mathcal{H})$, $\rho, \sigma > 0$, $\mathrm{tr}\rho = 1$

  max-relative entropy $D_{\mathrm{max}}(\rho\|\sigma) = \mathrm{min}\left\{\lambda \in \mathbb{R} \middle| 2^{\lambda}\sigma \geq \rho\right\}$
- bipartite state ρ_{AB}
  conditional min-entropy
  $H_{\mathrm{min}}(A|B)_\rho = \mathrm{max}_\sigma(-D_{\mathrm{max}}(\rho_{AB}\|\mathbb{1}_A \otimes \sigma_B))$
- conditional max-entropy defined via purification ρ_{ABC},
  $H_{\mathrm{max}}(A|B)_\rho = -H_{\mathrm{min}}(A|C)$
- smooth versions $H^{\varepsilon}_{x}(A|B)_\rho$ by taking max / min over ε-Ball
- max-mutual information:
  $I_{\mathrm{max}}(A : B)_\rho = \mathrm{min}_\sigma\, D_{\mathrm{max}}(\rho_{AB}\|\rho_A \otimes \sigma_B)$
- $I^{\varepsilon}_{\mathrm{max}}(A : B)_\rho = \mathrm{min}_{\tilde{\rho}}\, I_{\mathrm{max}}(A : B)_{\tilde{\rho}}$

One shot secoupling

Theorem (General one shot decoupling; Dupuis, Berta, Wullschleger, Renner (DBWR))

Let $\varepsilon > 0$*,* ρ_{AE} *a bipartite quantum state, and let* $\mathcal{T}_{A\to B}$ *be a quantum channel with Choi-Jamiołkowski representation* $\tau_{AB} = J(\mathcal{T})$ *such that* $tr(\tau_{AB}) \leqslant 1$*. Then, we have that*

$$\int_{\mathrm{U}(A)} \left\| \mathcal{T}_{A\to B}(U_A \rho_{AE} U_A^\dagger) - \tau_B \otimes \rho_E \right\|_1 dU \\ \leq 2^{-\frac{1}{2} H_{\min}^{\varepsilon}(A|E)_\rho - \frac{1}{2} H_{\min}^{\varepsilon}(A|B)_\tau} + 12\varepsilon \ ,$$

where $\int \cdot \, dU$ *denotes the integral over the Haar measure over the full unitary group on* $\mathcal{H}_A$*.*

One shot secoupling

Theorem (General one shot decoupling; Dupuis, Berta, Wullschleger, Renner (DBWR))

Let $\varepsilon > 0$, ρ_{AE} a bipartite quantum state, and let $\mathcal{T}_{A\to B}$ be a quantum channel with Choi-Jamiołkowski representation $\tau_{AB} = J(\mathcal{T})$ such that $tr(\tau_{AB}) \leqslant 1$. Then, we have that

$$\int_{\mathrm{U}(A)} \left\| \mathcal{T}_{A\to B}(U_A \rho_{AE} U_A^\dagger) - \tau_B \otimes \rho_E \right\|_1 dU$$
$$\leq 2^{-\frac{1}{2} H_{\min}^{\varepsilon}(A|E)_\rho - \frac{1}{2} H_{\min}^{\varepsilon}(A|B)_\tau} + 12\varepsilon \ ,$$

where $\int \cdot \, dU$ denotes the integral over the Haar measure over the full unitary group on $\mathcal{H}_A$.

One shot secoupling

Theorem (General one shot decoupling; Dupuis, Berta, Wullschleger, Renner (DBWR))

Let $\varepsilon > 0$, ρ_{AE} a bipartite quantum state, and let $\mathcal{T}_{A\to B}$ be a quantum channel with Choi-Jamiołkowski representation $\tau_{AB} = J(\mathcal{T})$ such that $tr(\tau_{AB}) \leqslant 1$. Then, we have that

$$\int_{\mathrm{U}(A)} \left\| \mathcal{T}_{A\to B}(U_A \rho_{AE} U_A^\dagger) - \tau_B \otimes \rho_E \right\|_1 dU$$
$$\leq 2^{-\frac{1}{2} H_{\min}^{\varepsilon}(A|E)_\rho - \frac{1}{2} H_{\min}^{\varepsilon}(A|B)_\tau} + 12\varepsilon \ ,$$

where $\int \cdot\, dU$ denotes the integral over the Haar measure over the full unitary group on $\mathcal{H}_A$.

One shot decoupling by partial trace

Theorem

Let ρ_{AE} be a bipartite quantum state, and let $\mathcal{H}_A \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ such that

$$\log|A_2| \geq \frac{1}{2}\left(H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho\right) - \mathcal{O}\left(\log\frac{1}{\varepsilon}\right).$$

Then, we have

$$\int_{\mathrm{U}(A)} P\left(tr_{A_2}\left(U_A \rho_{AE} U_A^\dagger\right), \frac{1_{A_1}}{|A_1|} \otimes \rho_E\right) \mathrm{d}\, U_A \leq \mathcal{O}(\varepsilon).$$

One shot decoupling by partial trace

Theorem

Let ρ_{AE} be a bipartite quantum state, and let $\mathcal{H}_A \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ such that

$$\log |A_2| \geq \frac{1}{2} \left(H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho \right) - \mathcal{O}\left(\log \frac{1}{\varepsilon} \right).$$

Then, we have

$$\int_{\mathrm{U}(A)} P\left(tr_{A_2}\left(U_A \rho_{AE} U_A^\dagger \right), \frac{1_{A_1}}{|A_1|} \otimes \rho_E \right) \mathrm{d}\, U_A \leq \mathcal{O}\left(\varepsilon\right).$$

One shot decoupling by partial trace

Theorem

Let ρ_{AE} be a bipartite quantum state, and let $\mathcal{H}_A \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ such that

$$\log |A_2| \geq \frac{1}{2} \left(H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho \right) - \mathcal{O}\left(\log \frac{1}{\varepsilon} \right).$$

Then, we have

$$\int_{\mathrm{U}(A)} P\left(tr_{A_2}\left(U_A \rho_{AE} U_A^\dagger \right), \frac{1_{A_1}}{|A_1|} \otimes \rho_E \right) \mathrm{d}\, U_A \leq \mathcal{O}\left(\varepsilon\right).$$

One shot decoupling by partial trace

$\approx$Theorem

Let $\rho_{AE} = {\rho'_{A'B'}}^{\otimes n}$ be a bipartite i.i.d. quantum state, and let $\mathcal{H}_A \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ such that

$$\log |A_2| \geq \frac{1}{2} I(E:A)_\rho - \mathcal{O}\left(\log \frac{1}{\varepsilon}\right).$$

Then, we have

$$\int_{\mathrm{U}(A)} P\left(tr_{A_2}\left(U_A \rho_{AE} U_A^\dagger\right), \frac{1_{A_1}}{|A_1|} \otimes \rho_E\right) \mathrm{d}\, U_A \leq \mathcal{O}(\varepsilon).$$

One shot decoupling by partial trace

Theorem

Let ρ_{AE} be a bipartite quantum state, and let $\mathcal{H}_A \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ such that

$$\log |A_2| \geq \frac{1}{2} \left(H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho \right) - \mathcal{O}\left(\log \frac{1}{\varepsilon} \right).$$

Then, we have

$$\int_{\mathrm{U}(A)} P\left(tr_{A_2}\left(U_A \rho_{AE} U_A^\dagger \right), \frac{1_{A_1}}{|A_1|} \otimes \rho_E \right) \mathrm{d}\, U_A \leq \mathcal{O}\left(\varepsilon\right).$$

Example

$$H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho$$

Example

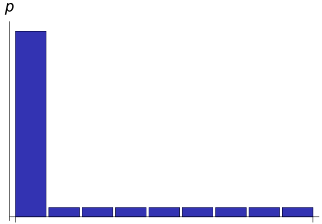
$H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho$

- Take $\mathcal{H}_A = \mathbb{C}^{n+1}$ and E trivial

Example

$H^{\varepsilon}_{\max}(A)_{\rho} - H^{\varepsilon}_{\min}(A|E)_{\rho}$

- Take $\mathcal{H}_A = \mathbb{C}^{n+1}$ and E trivial
- $\rho_A = \mathrm{diag}(p_0, ..., p_n)$, $p_i = \frac{1-p_0}{n}$ for $i \geq 1$



Example

$H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho$

- Take $\mathcal{H}_A = \mathbb{C}^{n+1}$ and E trivial
- $\rho_A = \mathrm{diag}(p_0, ..., p_n)$, $p_i = \frac{1-p_0}{n}$ for $i \geq 1$

$\Rightarrow$ $H^{\varepsilon}_{\min}(A) = -\log(p_0 - \varepsilon)$

Example

$H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho$

- Take $\mathcal{H}_A = \mathbb{C}^{n+1}$ and E trivial
- $\rho_A = \mathrm{diag}(p_0, ..., p_n)$, $p_i = \frac{1-p_0}{n}$ for $i \geq 1$

$\Rightarrow$ $H^{\varepsilon}_{\min}(A) = -\log(p_0 - \varepsilon)$

$H^{\varepsilon}_{\max}(A) \geq \log n - \log \frac{1}{1-\varepsilon^2-\sqrt{p_0}}$

Example

$H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho$

- Take $\mathcal{H}_A = \mathbb{C}^{n+1}$ and E trivial
- $\rho_A = \mathrm{diag}(p_0, ..., p_n)$, $p_i = \frac{1-p_0}{n}$ for $i \geq 1$

$\Rightarrow$ $H^{\varepsilon}_{\min}(A) = -\log(p_0 - \varepsilon)$

$H_{\max}(A) \geq \log n - \log \frac{1}{1-\varepsilon^2-\sqrt{p_0}}$

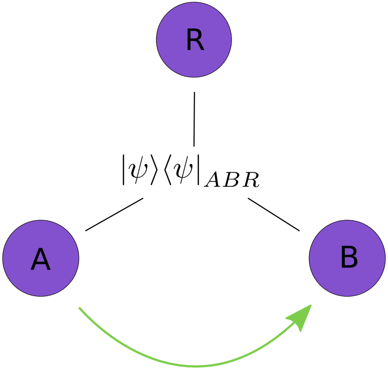
$\Rightarrow$ $H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho \approx \log n$,

while A should be considered decoupled from the trivial E

Coherent state merging (FQSW)

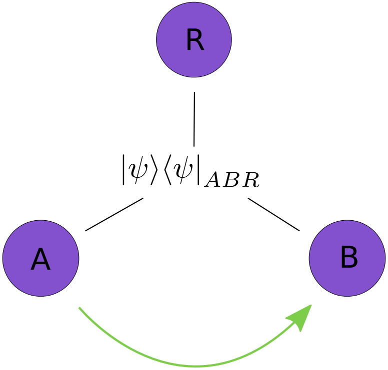
Coherent state merging (FQSW)

- Alice, Bob and a referee share a pure quantum state $|\psi\rangle\langle\psi|_{ABR}$.



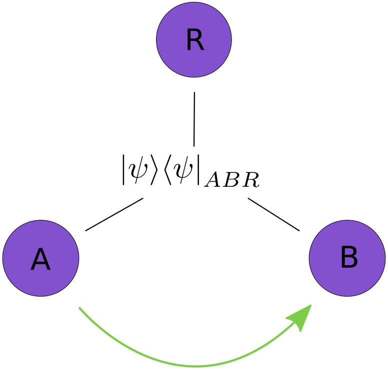
Coherent state merging (FQSW)

- Alice, Bob and a referee share a pure quantum state $|\psi\rangle\langle\psi|_{ABR}$.
- their task: Alice has to send her part of the state to Bob



Coherent state merging (FQSW)

- Alice, Bob and a referee share a pure quantum state $|\psi\rangle\langle\psi|_{ABR}$.
- their task: Alice has to send her part of the state to Bob
- the correlations with R have to remain intact



Coherent state merging (FQSW)

- Alice, Bob and a referee share a pure quantum state $|\psi\rangle\langle\psi|_{ABR}$.
- their task: Alice has to send her part of the state to Bob
- the correlations with R have to remain intact

Protocol:

Coherent state merging (FQSW)

- Alice, Bob and a referee share a pure quantum state $|\psi\rangle\langle\psi|_{ABR}$.
- their task: Alice has to send her part of the state to Bob
- the correlations with R have to remain intact

Protocol:

1. Alice runs decoupling from R: She splits $A \cong A_1 A_2$, and applies a random unitary

Coherent state merging (FQSW)

- Alice, Bob and a referee share a pure quantum state $|\psi\rangle\langle\psi|_{ABR}$.
- their task: Alice has to send her part of the state to Bob
- the correlations with R have to remain intact

Protocol:

1. Alice runs decoupling from R: She splits $A \cong A_1 A_2$, and applies a random unitary
2. Alice sends A_2 to Bob

Coherent state merging (FQSW)

- Alice, Bob and a referee share a pure quantum state $|\psi\rangle\langle\psi|_{ABR}$.
- their task: Alice has to send her part of the state to Bob
- the correlations with R have to remain intact

Protocol:

1. Alice runs decoupling from R: She splits $A \cong A_1 A_2$, and applies a random unitary
2. Alice sends A_2 to Bob

$\Rightarrow$ Joint state of Alice and referee: $\rho_{A_1 R} \approx \tau_{A_1} \otimes \rho_R$

Coherent state merging (FQSW)

- Alice, Bob and a referee share a pure quantum state $|\psi\rangle\langle\psi|_{ABR}$.
- their task: Alice has to send her part of the state to Bob
- the correlations with R have to remain intact

Protocol:

1. Alice runs decoupling from R: She splits $A \cong A_1 A_2$, and applies a random unitary
2. Alice sends A_2 to Bob

$\Rightarrow$ Joint state of Alice and referee: $\rho_{A_1 R} \approx \tau_{A_1} \otimes \rho_R$

3. Bob has purification of this state,

Coherent state merging (FQSW)

- Alice, Bob and a referee share a pure quantum state $|\psi\rangle\langle\psi|_{ABR}$.
- their task: Alice has to send her part of the state to Bob
- the correlations with R have to remain intact

Protocol:

1. Alice runs decoupling from R: She splits $A \cong A_1 A_2$, and applies a random unitary
2. Alice sends A_2 to Bob

$\Rightarrow$ Joint state of Alice and referee: $\rho_{A_1 R} \approx \tau_{A_1} \otimes \rho_R$

3. Bob has purification of this state,

- Uhlmanns theorem: Bob can recover AB

Coherent state merging (FQSW)

- Alice, Bob and a referee share a pure quantum state $|\psi\rangle\langle\psi|_{ABR}$.
- their task: Alice has to send her part of the state to Bob
- the correlations with R have to remain intact

Protocol:

1. Alice runs decoupling from R: She splits $A \cong A_1 A_2$, and applies a random unitary
2. Alice sends A_2 to Bob

$\Rightarrow$ Joint state of Alice and referee: $\rho_{A_1 R} \approx \tau_{A_1} \otimes \rho_R$

3. Bob has purification of this state,

- Uhlmanns theorem: Bob can recover AB

  quantum communication cost:
  $q(A:R)_\psi = \frac{1}{2}(H^\varepsilon_{\max}(A)_\psi - H^\varepsilon_{\min}(A|R)_\psi)$

Coherent state merging (FQSW)

- Alice, Bob and a referee share a pure quantum state $|\psi\rangle\langle\psi|_{ABR}$.
- their task: Alice has to send her part of the state to Bob
- the correlations with R have to remain intact

Protocol:

1. Alice runs decoupling from R: She splits $A \cong A_1 A_2$, and applies a random unitary
2. Alice sends A_2 to Bob

$\Rightarrow$ Joint state of Alice and referee: $\rho_{A_1 R} \approx \tau_{A_1} \otimes \rho_R$

3. Bob has purification of this state,

- Uhlmanns theorem: Bob can recover AB

quantum communication cost:
$q(A:R)_\psi = \frac{1}{2}(H^\varepsilon_{\max}(A)_\psi - H^\varepsilon_{\min}(A|R)_\psi)$
suboptimal (example)

Previous work

- One shot quantum communication with arbitrary entangled resources:

Previous work

- One shot quantum communication with arbitrary entangled resources:
- One shot coherent state merging possible with $q(A:R)_\psi = \frac{1}{2} I_{\max}(A:R) + \log\log|A| + \mathcal{O}\left(\log\frac{1}{\varepsilon}\right)$ (Berta, Christandl, Renner, BCR)

Previous work

- One shot quantum communication with arbitrary entangled resources:
- One shot coherent state merging possible with $q(A:R)_\psi = \frac{1}{2} I_{\max}(A:R) + \log\log|A| + \mathcal{O}\left(\log\frac{1}{\varepsilon}\right)$ (Berta, Christandl, Renner, BCR)

... uses standard decoupling and embezzling states (van Dam and Hayden)

Previous work

- One shot quantum communication with arbitrary entangled resources:
- One shot coherent state merging possible with $q(A:R)_\psi = \frac{1}{2} I_{\max}(A:R) + \log\log|A| + \mathcal{O}\left(\log\frac{1}{\varepsilon}\right)$ (Berta, Christandl, Renner, BCR)

... uses standard decoupling and embezzling states (van Dam and Hayden)

- One shot state merging possible with $q(A:R)_\psi = \frac{1}{2}(I_{\max}(A:R) + \log\log I_{\max}(A:R)) + \mathcal{O}\left(\log\frac{1}{\varepsilon}\right)$ (Anshu, Devabathini, Jain, ADJ)

Previous work

- One shot quantum communication with arbitrary entangled resources:
- One shot coherent state merging possible with $q(A:R)_\psi = \frac{1}{2} I_{\max}(A:R) + \log\log|A| + \mathcal{O}\left(\log \frac{1}{\varepsilon}\right)$ (Berta, Christandl, Renner, BCR)

... uses standard decoupling and embezzling states (van Dam and Hayden)

- One shot state merging possible with $q(A:R)_\psi = \frac{1}{2}(I_{\max}(A:R) + \log\log I_{\max}(A:R)) + \mathcal{O}\left(\log \frac{1}{\varepsilon}\right)$ (Anshu, Devabathini, Jain, ADJ)

... uses different technique called convex split lemma.

Catalytic decoupling

Catalytic decoupling

- Generalize decoupling twofold:

Catalytic decoupling

- Generalize decoupling twofold:
- drop randomization condition

Catalytic decoupling

- Generalize decoupling twofold:
- drop randomization condition
- allow free mixed ancillary states

Catalytic decoupling

- Generalize decoupling twofold:
  - drop randomization condition
  - allow free mixed ancillary states

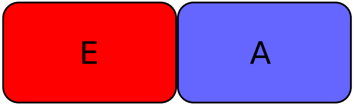
In pictures, step by step:

Catalytic decoupling

- Generalize decoupling twofold:
  - drop randomization condition
  - allow free mixed ancillary states

In pictures, step by step:

- Bipartite system AE

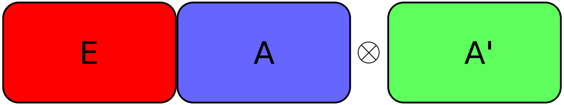


Catalytic decoupling

- Generalize decoupling twofold:
  - drop randomization condition
  - allow free mixed ancillary states

In pictures, step by step:

- Bipartite system AE
- add ancillary system A' in a fixed state

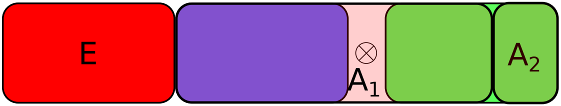


Catalytic decoupling

- Generalize decoupling twofold:
  - drop randomization condition
  - allow free mixed ancillary states

In pictures, step by step:

- Bipartite system AE
- add ancillary system A' in a fixed state
- divide system AA' into two parts, $AA' \cong A_1 \otimes A_2$

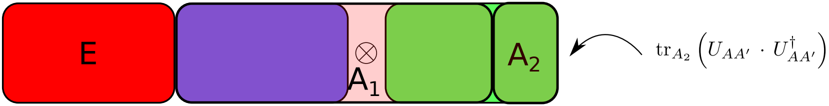


Catalytic decoupling

- Generalize decoupling twofold:
  - drop randomization condition
  - allow free mixed ancillary states

In pictures, step by step:

- Bipartite system AE
- add ancillary system A' in a fixed state
- divide system AA' into two parts, $AA' \cong A_1 \otimes A_2$
- apply a unitary

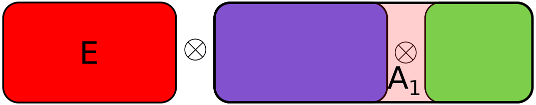


Catalytic decoupling

- Generalize decoupling twofold:
- drop randomization condition
- allow free mixed ancillary states

In pictures, step by step:

- Bipartite system AE
- add ancillary system A' in a fixed state
- divide system AA' into two parts, $AA' \cong A_1 \otimes A_2$
- apply a unitary
- trace out A_2

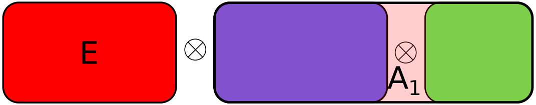


Catalytic decoupling

- Generalize decoupling twofold:
- drop randomization condition
- allow free mixed ancillary states

In pictures, step by step:

- Bipartite system AE
- add ancillary system A' in a fixed state
- divide system AA' into two parts, $AA' \cong A_1 \otimes A_2$
- apply a unitary
- trace out A_2
- how big do we have to choose A_2 here?



Definitions

- Quantum state ρ_{AE}

Definitions

- Quantum state ρ_{AE}
- minimal remainder system size $R^{\varepsilon}(A:E)_{\rho}$ for standard decoupling:

$$
\begin{aligned}
&R^{\varepsilon}(A:E)_{\rho} \\
&= \min \left\{ r \in \mathbb{R} \middle| \exists \mathcal{H}_A \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} : \log|A_2| = r,\ \min_{\omega} P(\rho_{A_1 E}, \omega_{A_1} \otimes \omega_E) \leq \varepsilon \right\}
\end{aligned}
$$

Definitions

- Quantum state ρ_{AE}
- minimal remainder system size $R^{\varepsilon}(A:E)_{\rho}$ for standard decoupling:

$$R^{\varepsilon}(A:E)_{\rho} = \min\left\{ r \in \mathbb{R} \middle| \exists \mathcal{H}_A \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} : \log|A_2| = r,\ \min_{\omega} P(\rho_{A_1 E}, \omega_{A_1} \otimes \omega_E) \leq \varepsilon \right\}$$

! we just ask for a product state, no randomizing

Definitions

- Quantum state ρ_{AE}
- minimal remainder system size $R^\varepsilon(A:E)_\rho$ for standard decoupling:

$$R^\varepsilon(A:E)_\rho$$
$$= \min\left\{ r \in \mathbb{R} \middle| \exists \mathcal{H}_A \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} : \log|A_2| = r,\ \min_\omega P(\rho_{A_1E}, \omega_{A_1} \otimes \omega_E) \leq \varepsilon \right\}$$

! we just ask for a product state, no randomizing

- minimal remainder system size $R_c^\varepsilon(A:E)_\rho$ for catalytic decoupling:

$$R_c^\varepsilon(A:E)_\rho = \inf_{\rho'_{A'}} R^\varepsilon(AA':E)_{\rho\otimes\rho'}$$

Definitions

- Quantum state ρ_{AE}
- minimal remainder system size $R^{\varepsilon}(A:E)_{\rho}$ for standard decoupling:

$$R^{\varepsilon}(A:E)_{\rho}$$
$$= \min\left\{ r \in \mathbb{R} \middle| \exists \mathcal{H}_A \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2} : \log|A_2| = r,\ \min_{\omega} P(\rho_{A_1E}, \omega_{A_1} \otimes \omega_E) \leq \varepsilon \right\}$$

! we just ask for a product state, no randomizing

- minimal remainder system size $R_c^{\varepsilon}(A:E)_{\rho}$ for catalytic decoupling:

$$R_c^{\varepsilon}(A:E)_{\rho} = \inf_{\rho'_{A'}} R^{\varepsilon}(AA':E)_{\rho\otimes\rho'}$$

- Claim: $R_c^{\varepsilon}(A:E)_{\rho} = \frac{1}{2} I_{\max}^{\varepsilon}(A:E)_{\rho}$ essentially.

Converse

Converse

- Observation: $R_c^\varepsilon(A:E)_\rho \leq R^\varepsilon(A:E)_\rho$ (trivial ancilla)

Converse

- Observation: $R_c^\varepsilon(A:E)_\rho \leq R^\varepsilon(A:E)_\rho$ (trivial ancilla)
  Want $R_c^\varepsilon(A:E)_\rho \geq \frac{1}{2} I_{\max}^\varepsilon(A:E)_\rho$. Ingredients:

Converse

- Observation: $R_c^\varepsilon(A:E)_\rho \leq R^\varepsilon(A:E)_\rho$ (trivial ancilla)

  Want $R_c^\varepsilon(A:E)_\rho \geq \frac{1}{2} I_{\max}^\varepsilon(A:E)_\rho$. Ingredients:

(1) non-locking of $I_{\max}^\varepsilon$: $I_{\max}^\varepsilon(A:BC)_\rho \leq I_{\max}^\varepsilon(A:B)_\rho + 2\log|C|$ (Berta, Christandl, Renner)

Converse

- Observation: $R_c^\varepsilon(A:E)_\rho \leq R^\varepsilon(A:E)_\rho$ (trivial ancilla)
  Want $R_c^\varepsilon(A:E)_\rho \geq \frac{1}{2} I_{\max}^\varepsilon(A:E)_\rho$. Ingredients:

(1) non-locking of $I_{\max}^\varepsilon$: $I_{\max}^\varepsilon(A:BC)_\rho \leq I_{\max}^\varepsilon(A:B)_\rho + 2\log|C|$ (Berta, Christandl, Renner)

(2) for ρ_{AB}, σ_E: $I_{\max}^\varepsilon(A:B)_\rho = I_{\max}^\varepsilon(A:BE)_{\rho\otimes\sigma}$ (from monotonicity under CPTP-maps, BCR)

Converse

- Observation: $R_c^\varepsilon(A:E)_\rho \leq R^\varepsilon(A:E)_\rho$ (trivial ancilla)
  Want $R_c^\varepsilon(A:E)_\rho \geq \frac{1}{2} I_{\max}^\varepsilon(A:E)_\rho$. Ingredients:

(1) non-locking of $I_{\max}^\varepsilon$: $I_{\max}^\varepsilon(A:BC)_\rho \leq I_{\max}^\varepsilon(A:B)_\rho + 2\log|C|$ (Berta, Christandl, Renner)

(2) for ρ_{AB}, σ_E: $I_{\max}^\varepsilon(A:B)_\rho = I_{\max}^\varepsilon(A:BE)_{\rho\otimes\sigma}$ (from monotonicity under CPTP-maps, BCR)

For a state ρ_{AE}, suppose $\rho'_{A'}$ and $\mathcal{H}_A \otimes \mathcal{H}_{A'} \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ achieve catalytic decoupling of A from E with error ε.

$$I_{\max}^\varepsilon(E:A)_\rho$$

Converse

- Observation: $R_c^\varepsilon(A:E)_\rho \leq R^\varepsilon(A:E)_\rho$ (trivial ancilla)
  Want $R_c^\varepsilon(A:E)_\rho \geq \frac{1}{2} I_{\max}^\varepsilon(A:E)_\rho$. Ingredients:

(1) non-locking of $I_{\max}^\varepsilon$: $I_{\max}^\varepsilon(A:BC)_\rho \leq I_{\max}^\varepsilon(A:B)_\rho + 2\log|C|$ (Berta, Christandl, Renner)

(2) for ρ_{AB}, σ_E: $I_{\max}^\varepsilon(A:B)_\rho = I_{\max}^\varepsilon(A:BE)_{\rho\otimes\sigma}$ (from monotonicity under CPTP-maps, BCR)

For a state ρ_{AE}, suppose $\rho'_{A'}$ and $\mathcal{H}_A \otimes \mathcal{H}_{A'} \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ achieve catalytic decoupling of A from E with error ε.

$$I_{\max}^\varepsilon(E:A)_\rho \overset{(2)}{=} I_{\max}^\varepsilon(E:AA')_{\rho\otimes\rho'}$$

Converse

- Observation: $R_c^\varepsilon(A:E)_\rho \leq R^\varepsilon(A:E)_\rho$ (trivial ancilla)
  Want $R_c^\varepsilon(A:E)_\rho \geq \frac{1}{2} I_{\max}^\varepsilon(A:E)_\rho$. Ingredients:

(1) non-locking of $I_{\max}^\varepsilon$: $I_{\max}^\varepsilon(A:BC)_\rho \leq I_{\max}^\varepsilon(A:B)_\rho + 2\log|C|$ (Berta, Christandl, Renner)

(2) for ρ_{AB}, σ_E: $I_{\max}^\varepsilon(A:B)_\rho = I_{\max}^\varepsilon(A:BE)_{\rho\otimes\sigma}$ (from monotonicity under CPTP-maps, BCR)

For a state ρ_{AE}, suppose $\rho'_{A'}$ and $\mathcal{H}_A \otimes \mathcal{H}_{A'} \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ achieve catalytic decoupling of A from E with error ε.

$$I_{\max}^\varepsilon(E:A)_\rho \stackrel{(2)}{=} I_{\max}^\varepsilon(E:AA')_{\rho\otimes\rho'}$$

$$= I_{\max}^\varepsilon(E:A_1A_2)_{\rho\otimes\rho'}$$

Converse

- Observation: $R_c^\varepsilon(A:E)_\rho \leq R^\varepsilon(A:E)_\rho$ (trivial ancilla)
  Want $R_c^\varepsilon(A:E)_\rho \geq \frac{1}{2} I_{\max}^\varepsilon(A:E)_\rho$. Ingredients:

(1) non-locking of $I_{\max}^\varepsilon$: $I_{\max}^\varepsilon(A:BC)_\rho \leq I_{\max}^\varepsilon(A:B)_\rho + 2\log|C|$ (Berta, Christandl, Renner)

(2) for ρ_{AB}, σ_E: $I_{\max}^\varepsilon(A:B)_\rho = I_{\max}^\varepsilon(A:BE)_{\rho\otimes\sigma}$ (from monotonicity under CPTP-maps, BCR)

For a state ρ_{AE}, suppose $\rho'_{A'}$ and $\mathcal{H}_A \otimes \mathcal{H}_{A'} \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ achieve catalytic decoupling of A from E with error ε.

$$I_{\max}^\varepsilon(E:A)_\rho \overset{(2)}{=} I_{\max}^\varepsilon(E:AA')_{\rho\otimes\rho'}$$
$$= I_{\max}^\varepsilon(E:A_1A_2)_{\rho\otimes\rho'} \overset{(1)}{\leq} I_{\max}^\varepsilon(E:A_1)_{\rho\otimes\rho'} + 2\log|A_2|$$

Converse

- Observation: $R_c^\varepsilon(A:E)_\rho \leq R^\varepsilon(A:E)_\rho$ (trivial ancilla)
  Want $R_c^\varepsilon(A:E)_\rho \geq \frac{1}{2} I_{\max}^\varepsilon(A:E)_\rho$. Ingredients:

(1) non-locking of $I_{\max}^\varepsilon$: $I_{\max}^\varepsilon(A:BC)_\rho \leq I_{\max}^\varepsilon(A:B)_\rho + 2\log|C|$ (Berta, Christandl, Renner)

(2) for ρ_{AB}, σ_E: $I_{\max}^\varepsilon(A:B)_\rho = I_{\max}^\varepsilon(A:BE)_{\rho\otimes\sigma}$ (from monotonicity under CPTP-maps, BCR)

For a state ρ_{AE}, suppose $\rho'_{A'}$ and $\mathcal{H}_A \otimes \mathcal{H}_{A'} \cong \mathcal{H}_{A_1} \otimes \mathcal{H}_{A_2}$ achieve catalytic decoupling of A from E with error ε.

$$
\begin{aligned}
& I_{\max}^\varepsilon(E:A)_\rho \overset{(2)}{=} I_{\max}^\varepsilon(E:AA')_{\rho\otimes\rho'} \\
=& I_{\max}^\varepsilon(E:A_1A_2)_{\rho\otimes\rho'} \overset{(1)}{\leq} I_{\max}^\varepsilon(E:A_1)_{\rho\otimes\rho'} + 2\log|A_2| \\
\overset{(2)}{=}& 2\log|A_2|
\end{aligned}
$$

Achievability

Achievability

Theorem (CM, Berta, Dupuis, Renner, Christandl)

Let $\rho_{AE} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_E)$ be a quantum state. Then, for any $0 < \delta \leq \varepsilon$ catalytic decoupling with error ε can be achieved with remainder system size

$$\log |A_2| \leq \frac{1}{2}\left(I_{\max}^{\varepsilon-\delta}(E;A)_\rho + \left\{ \log\log I_{\max}^{\varepsilon-\delta}(E;A)_\rho \right\}_+ \right) + \mathcal{O}(\log \frac{1}{\delta}),$$

where we define $\{x\}_+$ to be equal to x if $x \in \mathbb{R}_{\geq 0}$ and 0 otherwise.

Achievability

Theorem (CM, Berta, Dupuis, Renner, Christandl)

Let $\rho_{AE} \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_E)$ *be a quantum state. Then, for any* $0 < \delta \leq \varepsilon$ *catalytic decoupling with error* ε *can be achieved with remainder system size*

$$\log |A_2| \leq \frac{1}{2}\left(I_{\max}^{\varepsilon-\delta}(E;A)_\rho + \left\{ \log\log I_{\max}^{\varepsilon-\delta}(E;A)_\rho \right\}_+ \right) + \mathcal{O}(\log \frac{1}{\delta}),$$

where we define $\{x\}_+$ *to be equal to* x *if* $x \in \mathbb{R}_{\geq 0}$ *and* 0 *otherwise.*

- Two proofs, one using the techniques from Anshu et al. and Berta et al. respectively

i.i.d

i.i.d

- $I_{\max}^{\varepsilon}$ has the AEP (BCR):

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} I_{\max}^{\varepsilon}(A:B)_{\rho^{\otimes n}} = I(A:B)_{\rho}$$

i.i.d

- $I_{\max}^{\varepsilon}$ has the AEP (BCR):

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} I_{\max}^{\varepsilon}(A:B)_{\rho^{\otimes n}} = I(A:B)_{\rho}$$

! asymptotically the ancilla becomes unnecessary, usual randomization condition becomes redundant

i.i.d

- $I^{\varepsilon}_{\max}$ has the AEP (BCR):

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} I^{\varepsilon}_{\max}(A:B)_{\rho^{\otimes n}} = I(A:B)_{\rho}$$

! asymptotically the ancilla becomes unnecessary, usual randomization condition becomes redundant

- tightness of characterization allows derivation of a 2nd order term:

i.i.d

- $I^{\varepsilon}_{\max}$ has the AEP (BCR):

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} I^{\varepsilon}_{\max}(A:B)_{\rho^{\otimes n}} = I(A:B)_{\rho}$$

! asymptotically the ancilla becomes unnecessary, usual randomization condition becomes redundant

- tightness of characterization allows derivation of a 2nd order term:
- $D^{\varepsilon}_{\max}(\rho^{\otimes n} \| \sigma^{\otimes n}) = nD(\rho\|\sigma) + \sqrt{nV(\rho\|\sigma)}\Phi^{-1}(\varepsilon) + \mathcal{O}(\log n)$ (Tomamichel and Hayashi)

i.i.d

- $I^{\varepsilon}_{\max}$ has the AEP (BCR):

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}I^{\varepsilon}_{\max}(A:B)_{\rho^{\otimes n}} = I(A:B)_{\rho}$$

! asymptotically the ancilla becomes unnecessary, usual randomization condition becomes redundant

- tightness of characterization allows derivation of a 2nd order term:
- $D^{\varepsilon}_{\max}(\rho^{\otimes n}\|\sigma^{\otimes n}) = nD(\rho\|\sigma) + \sqrt{nV(\rho\|\sigma)}\Phi^{-1}(\varepsilon) + \mathcal{O}(\log n)$ (Tomamichel and Hayashi)
- along the lines of of TH's derivation for source coding with quantum side information we get

$$R^{\varepsilon}_{c}(A:E)_{\rho^{\otimes}} = nI(A:E) + \sqrt{nV_I(A:E)_{\rho}}\Phi^{-1}(\varepsilon) + \mathcal{O}(\log n)$$

One shot coherent state merging (BCR)

One shot coherent state merging (BCR)

Now: easy!

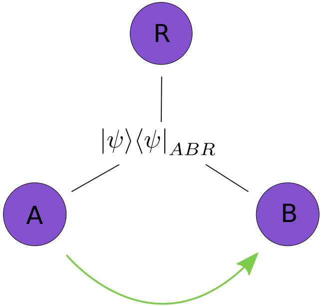
One shot coherent state merging (BCR)

Now: easy! Difficult parts hidden in achievability of CD.

One shot coherent state merging (BCR)

Now: easy! Difficult parts hidden in achievability of CD.

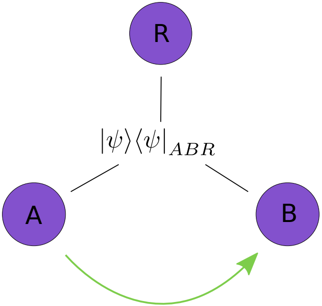
- Alice, Bob and a referee share a pure quantum state $|\psi\rangle\langle\psi|_{ABR}$.
- their task: Alice has to send her part of the state to Bob



One shot coherent state merging (BCR)

Now: easy! Difficult parts hidden in achievability of CD.

- Alice, Bob and a referee share a pure quantum state $|\psi\rangle\langle\psi|_{ABR}$.
- their task: Alice has to send her part of the state to Bob
- Alice needs ancilla – give purification to Bob $\Rightarrow$ entangled resource!



One shot coherent state merging (BCR)

Now: easy! Difficult parts hidden in achievability of CD.

Protocol:

One shot coherent state merging (BCR)

Now: easy! Difficult parts hidden in achievability of CD.

Protocol:

1. Alice runs catalytic decoupling from R: She splits $AA' \cong A_1 A_2$, and applies unitary

One shot coherent state merging (BCR)

Now: easy! Difficult parts hidden in achievability of CD.

Protocol:

1. Alice runs catalytic decoupling from R: She splits $AA' \cong A_1 A_2$, and applies unitary
2. Alice sends A_2 to Bob

One shot coherent state merging (BCR)

Now: easy! Difficult parts hidden in achievability of CD.

Protocol:

1. Alice runs catalytic decoupling from R: She splits $AA' \cong A_1 A_2$, and applies unitary
2. Alice sends A_2 to Bob

$\Rightarrow$ Joint state of Alice and referee: $\rho_{A_1 R} \approx \omega_{A_1} \otimes \rho_R$

One shot coherent state merging (BCR)

Now: easy! Difficult parts hidden in achievability of CD.

Protocol:

1. Alice runs catalytic decoupling from R: She splits $AA' \cong A_1 A_2$, and applies unitary
2. Alice sends A_2 to Bob

$\Rightarrow$ Joint state of Alice and referee: $\rho_{A_1 R} \approx \omega_{A_1} \otimes \rho_R$

3. Bob has purification of this state,

One shot coherent state merging (BCR)

Now: easy! Difficult parts hidden in achievability of CD.

Protocol:

1. Alice runs catalytic decoupling from R: She splits $AA' \cong A_1 A_2$, and applies unitary
2. Alice sends A_2 to Bob

$\Rightarrow$ Joint state of Alice and referee: $\rho_{A_1 R} \approx \omega_{A_1} \otimes \rho_R$

3. Bob has purification of this state,

   Uhlmanns theorem: Bob can recover AB

One shot coherent state merging (BCR)

Now: easy! Difficult parts hidden in achievability of CD.

Protocol:

1. Alice runs catalytic decoupling from R: She splits $AA' \cong A_1A_2$, and applies unitary
2. Alice sends A_2 to Bob

$\Rightarrow$ Joint state of Alice and referee: $\rho_{A_1R} \approx \omega_{A_1} \otimes \rho_R$

3. Bob has purification of this state,

   Uhlmanns theorem: Bob can recover AB

- quantum communication cost: $q(A:R)_\psi \approx \frac{1}{2} I^{\varepsilon}_{\max}(R:A)_\psi$

One shot coherent state merging (BCR)

Now: easy! Difficult parts hidden in achievability of CD.

Protocol:

1. Alice runs catalytic decoupling from R: She splits $AA' \cong A_1 A_2$, and applies unitary
2. Alice sends A_2 to Bob

$\Rightarrow$ Joint state of Alice and referee: $\rho_{A_1 R} \approx \omega_{A_1} \otimes \rho_R$

3. Bob has purification of this state,

   Uhlmanns theorem: Bob can recover AB

- quantum communication cost: $q(A:R)_\psi \approx \frac{1}{2} I_{\max}^{\varepsilon}(R:A)_\psi$

! optimal

Local erasure of correlations

Local erasure of correlations

Model by Groismann, Popescu and Winter

Local erasure of correlations

Model by Groismann, Popescu and Winter

def. Random unitary channel

$$\Lambda(X) = \frac{1}{N}\sum_{i=1}^{N} U_i X U_i^\dagger$$

Local erasure of correlations

Model by Groismann, Popescu and Winter

def. Random unitary channel

$$\Lambda(X) = \frac{1}{N} \sum_{i=1}^{N} U_i X U_i^\dagger$$

- Given ρ_{AE}, how many unitaries do we need to get $\Lambda_A \otimes \mathrm{id}_E(\rho_{AE}) =_\varepsilon \omega_A \otimes \rho_E$

Local erasure of correlations

Model by Groismann, Popescu and Winter

def. Random unitary channel

$$\Lambda(X) = \frac{1}{N}\sum_{i=1}^{N} U_i X U_i^\dagger$$

- Given ρ_{AE}, how many unitaries do we need to get $\Lambda_A \otimes \mathrm{id}_E(\rho_{AE}) =_\varepsilon \omega_A \otimes \rho_E$
- GPW: rate $= I(A:E)$ in i.i.d. scenario

Local erasure of correlations

Model by Groismann, Popescu and Winter

def. Random unitary channel

$$\Lambda(X) = \frac{1}{N} \sum_{i=1}^{N} U_i X U_i^\dagger$$

- Given ρ_{AE}, how many unitaries do we need to get $\Lambda_A \otimes \mathrm{id}_E(\rho_{AE}) =_\varepsilon \omega_A \otimes \rho_E$
- GPW: rate$=I(A:E)$ in i.i.d. scenario

! "Catalytic local erasure of correlations" equivalent to catalytic decoupling

Local erasure of correlations

Model by Groismann, Popescu and Winter

def. Random unitary channel

$$\Lambda(X) = \frac{1}{N}\sum_{i=1}^{N} U_i X U_i^\dagger$$

- Given ρ_{AE}, how many unitaries do we need to get $\Lambda_A \otimes \mathrm{id}_E(\rho_{AE}) =_\varepsilon \omega_A \otimes \rho_E$
- GPW: rate= $I(A:E)$ in i.i.d. scenario

! "Catalytic local erasure of correlations" equivalent to catalytic decoupling

⇒ One-shot local erasure of correlations can be done with $2^{I_{\max}^{\varepsilon}(E:A)}$ unitaries using an ancilla

Proofs

Proof ingredient

Lemma (Convex split lemma; Anshu, Devabathini, Jain)

Let $\rho \in \mathcal{B}(\mathcal{H}_A \otimes \mathcal{H}_E)$ *and* $\sigma \in \mathcal{B}(\mathcal{H}_E)$ *be quantum states,* $k = D_{max}(\rho_{AE} \| \rho_A \otimes \sigma_E)$ *and* $0 < \delta < \frac{1}{6}$*. Define*

$$n = \begin{cases} 1 & k \leq 3\delta \\ \left\lceil \frac{8 \cdot 2^k \log\left(\frac{k}{\delta}\right)}{\delta^3} \right\rceil & \text{else} \end{cases} .$$

Then the state

$$\tau_{AE_1 \dots E_n} = \frac{1}{n} \sum_{j=1}^{n} \rho_{AE_j} \otimes \left(\sigma^{\otimes (n-1)}\right)_{E_{j^c}} \tag{1}$$

is almost product,

$$I(A; E_1 \dots E_n)_\tau \leq 3\delta \quad \text{as well as} \quad P\left(\tau_A \otimes \tau_{E_1 \dots E_n}, \tau_{AE_1 \dots E_n}\right) \leq \sqrt{6\delta}.$$

1. Proof sketch

1. Proof sketch

Abstracted from ADJ's state merging protocol.

1. Proof sketch

Abstracted from ADJ's state merging protocol.

- Let σ_A be a minimizer in $I^{\varepsilon}_{\max}(E:A)_\rho = \min_{\tilde{\rho}} \min_\sigma D_{\max}(\rho_{AE} \| \sigma_A \otimes \rho_E)$.

1. Proof sketch

Abstracted from ADJ's state merging protocol.

- Let σ_A be a minimizer in $I^{\varepsilon}_{\max}(E:A)_\rho = \min_{\tilde{\rho}} \min_{\sigma} D_{\max}(\rho_{AE} \| \sigma_A \otimes \rho_E)$.
- want to use the convex split lemma $\Rightarrow$ ancilla state $\sigma_A^{\otimes(n-1)}$, where n is determined by the max-mutual information

1. Proof sketch

Abstracted from ADJ's state merging protocol.

- Let σ_A be a minimizer in $I_{\max}^{\varepsilon}(E:A)_\rho = \min_{\tilde{\rho}} \min_\sigma D_{\max}(\rho_{AE} \| \sigma_A \otimes \rho_E)$.
- want to use the convex split lemma $\Rightarrow$ ancilla state $\sigma_A^{\otimes(n-1)}$, where n is determined by the max-mutual information

$\rightarrow$ n A-systems

1. Proof sketch

Abstracted from ADJ's state merging protocol.

- Let σ_A be a minimizer in $I^{\varepsilon}_{\max}(E:A)_\rho = \min_{\tilde{\rho}} \min_\sigma D_{\max}(\rho_{AE} \| \sigma_A \otimes \rho_E)$.
- want to use the convex split lemma $\Rightarrow$ ancilla state $\sigma_A^{\otimes(n-1)}$, where n is determined by the max-mutual information

$\rightarrow$ n A-systems

- want unitary operation:

1. Proof sketch

Abstracted from ADJ's state merging protocol.

- Let σ_A be a minimizer in $I^{\varepsilon}_{\max}(E:A)_\rho = \min_{\tilde{\rho}} \min_\sigma D_{\max}(\rho_{AE} \| \sigma_A \otimes \rho_E)$.
- want to use the convex split lemma $\Rightarrow$ ancilla state $\sigma_A^{\otimes(n-1)}$, where n is determined by the max-mutual information

$\rightarrow$ n A-systems

- want unitary operation:

\- take another ancilla $\mathbb{1}_n/n$

1. Proof sketch

Abstracted from ADJ's state merging protocol.

- Let σ_A be a minimizer in $I^{\varepsilon}_{\max}(E:A)_\rho = \min_{\tilde\rho} \min_\sigma D_{\max}(\rho_{AE} \| \sigma_A \otimes \rho_E)$.
- want to use the convex split lemma $\Rightarrow$ ancilla state $\sigma_A^{\otimes(n-1)}$, where n is determined by the max-mutual information

$\rightarrow$ n A-systems

- want unitary operation:

- take another ancilla $\mathbb{1}_n/n$
- controlled on this ancilla being in state ℓ, swap the first and ℓth A-system

1. Proof sketch

Abstracted from ADJ's state merging protocol.

- Let σ_A be a minimizer in $I^{\varepsilon}_{\max}(E:A)_\rho = \min_{\tilde\rho}\min_\sigma D_{\max}(\rho_{AE}\|\sigma_A\otimes\rho_E)$.
- want to use the convex split lemma $\Rightarrow$ ancilla state $\sigma_A^{\otimes(n-1)}$, where n is determined by the max-mutual information

$\rightarrow$ n A-systems

- want unitary operation:
  - take another ancilla $\mathbb{1}_n/n$
  - controlled on this ancilla being in state ℓ, swap the first and ℓth A-system
- convex split lemma $\Rightarrow$ tracing out the second ancilla yields product state

1. Proof sketch

Abstracted from ADJ's state merging protocol.

- Let σ_A be a minimizer in $I_{\max}^{\varepsilon}(E:A)_\rho = \min_{\tilde\rho} \min_\sigma D_{\max}(\rho_{AE} \| \sigma_A \otimes \rho_E)$.
- want to use the convex split lemma $\Rightarrow$ ancilla state $\sigma_A^{\otimes(n-1)}$, where n is determined by the max-mutual information

→ n A-systems

- want unitary operation:
  - take another ancilla $\mathbb{1}_n/n$
  - controlled on this ancilla being in state ℓ, swap the first and ℓth A-system
- convex split lemma $\Rightarrow$ tracing out the second ancilla yields product state

! but: $\log|A_2|$ still a factor 2 two large.

1. Proof sketch (ctd.)

- A_2 is classical

1. Proof sketch (ctd.)

- A_2 is classical

→ superdense coding?

1. Proof sketch (ctd.)

- A_2 is classical

$\rightarrow$ superdense coding?

- let ρ_{CQ} cq-state, $\mathcal{H}_C = \mathcal{H}_{C'}^{\otimes 2}$

1. Proof sketch (ctd.)

- A_2 is classical

→ superdense coding?

- let ρ_{CQ} cq-state, $\mathcal{H}_C = \mathcal{H}_{C'}^{\otimes 2}$
- decoupling formulation of superdense coding:

1. Proof sketch (ctd.)

- A_2 is classical

→ superdense coding?

- let ρ_{CQ} cq-state, $\mathcal{H}_C = \mathcal{H}_{C'}^{\otimes 2}$
- decoupling formulation of superdense coding:
- rotate standard basis of C to Bell basis

1. Proof sketch (ctd.)

- A_2 is classical

$\rightarrow$ superdense coding?

- let ρ_{CQ} cq-state, $\mathcal{H}_C = \mathcal{H}_{C'}^{\otimes 2}$
- decoupling formulation of superdense coding:
- rotate standard basis of C to Bell basis
- trace out one of the C's

1. Proof sketch (ctd.)

- A_2 is classical

→ superdense coding?

- let ρ_{CQ} cq-state, $\mathcal{H}_C = \mathcal{H}_{C'}^{\otimes 2}$
- decoupling formulation of superdense coding:
- rotate standard basis of C to Bell basis
- trace out one of the C's

$\Rightarrow$ $\rho_{C'Q} = \tau_{C'} \otimes \rho_Q$

2. Proof sketch (rougher)

2. Proof sketch (rougher)

Abstracted from BCR's state merging protocol.

2. Proof sketch (rougher)

Abstracted from BCR's state merging protocol.

- Idea: if $\rho_A \approx \tau_A$ then $I^{\varepsilon}_{\max}(A:E)_\rho \approx H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho$

2. Proof sketch (rougher)

Abstracted from BCR's state merging protocol.

- Idea: if $\rho_A \approx \tau_A$ then $I^{\varepsilon}_{\max}(A:E)_\rho \approx H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho$

$\Rightarrow$ DBWR's one-shot decoupling is enough!

2. Proof sketch (rougher)

Abstracted from BCR's state merging protocol.

- Idea: if $\rho_A \approx \tau_A$ then $I^{\varepsilon}_{\max}(A:E)_\rho \approx H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho$

$\Rightarrow$ DBWR's one-shot decoupling is enough!

- partition $\mathcal{H}_A$ into subspaces where this holds

2. Proof sketch (rougher)

Abstracted from BCR's state merging protocol.

- Idea: if $\rho_A \approx \tau_A$ then $I^{\varepsilon}_{\text{max}}(A:E)_\rho \approx H^{\varepsilon}_{\text{max}}(A)_\rho - H^{\varepsilon}_{\text{min}}(A|E)_\rho$

$\Rightarrow$ DBWR's one-shot decoupling is enough!

- partition $\mathcal{H}_A$ into subspaces where this holds
- apply the decoupling unitaries in superposition

2. Proof sketch (rougher)

Abstracted from BCR's state merging protocol.

- Idea: if $\rho_A \approx \tau_A$ then $I^{\varepsilon}_{\max}(A:E)_\rho \approx H^{\varepsilon}_{\max}(A)_\rho - H^{\varepsilon}_{\min}(A|E)_\rho$

$\Rightarrow$ DBWR's one-shot decoupling is enough!

- partition $\mathcal{H}_A$ into subspaces where this holds
- apply the decoupling unitaries in superposition
- use half an embezzling state (van Dam and Hayden) to "unembezzle" maximally mixed states of different sizes

Open Problems

Open Problems

- $I_{\max}^{\varepsilon}$ has the AEP (BCR):

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} I_{\max}^{\varepsilon}(A:B)_{\rho^{\otimes n}} = I(A:B)_{\rho}$$

Open Problems

- $I^{\varepsilon}_{\max}$ has the AEP (BCR):

$$\lim_{\varepsilon\to 0}\lim_{n\to\infty}\frac{1}{n}I^{\varepsilon}_{\max}(A:B)_{\rho^{\otimes n}} = I(A:B)_{\rho}$$

$\Rightarrow$ ancilla becomes unnecessary for i.i.d. $\rightarrow$ standard decoupling

Open Problems

- $I_{\max}^{\varepsilon}$ has the AEP (BCR):

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} I_{\max}^{\varepsilon}(A:B)_{\rho^{\otimes n}} = I(A:B)_{\rho}$$

$\Rightarrow$ ancilla becomes unnecessary for i.i.d. $\rightarrow$ standard decoupling

- our protocol: ancilla size $\sim n$

Open Problems

- $I_{\max}^{\varepsilon}$ has the AEP (BCR):

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} I_{\max}^{\varepsilon}(A:B)_{\rho^{\otimes n}} = I(A:B)_{\rho}$$

$\Rightarrow$ ancilla becomes unnecessary for i.i.d. $\rightarrow$ standard decoupling

- our protocol: ancilla size $\sim n$
- Is the ancilla necessary at all?

Open Problems

- $I_{\max}^{\varepsilon}$ has the AEP (BCR):

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} I_{\max}^{\varepsilon}(A:B)_{\rho^{\otimes n}} = I(A:B)_{\rho}$$

$\Rightarrow$ ancilla becomes unnecessary for i.i.d. $\to$ standard decoupling

- our protocol: ancilla size $\sim n$
- Is the ancilla necessary at all?
- if so, still huge ancilla, size $2^{I_{\max}(E:A)} \log |A|$. trade-offs? converse?

Open Problems

- $I_{\max}^{\varepsilon}$ has the AEP (BCR):

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} I_{\max}^{\varepsilon}(A : B)_{\rho^{\otimes n}} = I(A : B)_\rho$$

$\Rightarrow$ ancilla becomes unnecessary for i.i.d. $\rightarrow$ standard decoupling

- our protocol: ancilla size $\sim n$
- Is the ancilla necessary at all?
- if so, still huge ancilla, size $2^{I_{\max}(E:A)} \log |A|$. trade-offs? converse?
- especially: finite block length regime?

Summary

- We defined catalytic decoupling
- We characterized it, unifying two techniques in one-shot quantum communication
- second order asymptotics for i.i.d.
- Applications: local erasure of correlations, decoupling proof of one-shot coherent state merging

As this is the last talk: A big "Thank you" to the organizers for the great workshop!

Questions?