



UNIVERSITY OF  
**ILLINOIS**  
URBANA-CHAMPAIGN

# Post-selection techniques and applications in QKD and channel coding

Anna Honeycutt, Max Gold, Sharjeel Ahmad

2nd December 2025

# Introduction

The *post-selection techniques* details a representation-theoretic methodology to bound norms on distance measures between channels. This helps us compute how well one channel can *simulate* another.

We discuss

1. The foundation of this technique and its applications to QKD [CKR09].
2. Its application to channel coding theorems, and the elements of the simulations discussed in these theorems [BCR11].

# Part I: Post-Selection Technique for Quantum Channels

$$\|\Delta\|_{\diamond} := \max_{\|X\|_1 \leq 1} \|(\Delta \otimes \mathbb{1})X\|_1$$

Given the action of the actual protocol,  $\mathcal{E}$ , and ideal functionality of the protocol,  $\mathcal{F}$ , we can quantify the distance  $\|\mathcal{E} - \mathcal{F}\|_{\diamond}$

Example: single shot discrimination of two channels  $\{\mathcal{E}, \mathcal{F}\}$  with equal prior probability

$$p_{succ} = \frac{1}{2} + \frac{1}{4} \|\mathcal{E} - \mathcal{F}\|_{\diamond}$$

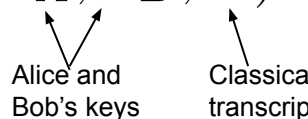
$\mathcal{E}$  and  $\mathcal{F}$  identical:  $\|\mathcal{E} - \mathcal{F}\|_{\diamond} \rightarrow 0$ ,  $p_{succ} \rightarrow \frac{1}{2}$

$\mathcal{E}$  and  $\mathcal{F}$  perfectly distinguishable:  $\|\mathcal{E} - \mathcal{F}\|_{\diamond} \rightarrow 2$ ,  $p_{succ} \rightarrow 1$

Alice and Bob share  $n$  entangled pairs on  $\mathcal{H}^A \otimes \mathcal{H}^B$

Application of local measurements followed by classical post-processing generates a key of  $l$  bits

Generated by map  $\mathcal{E} : (\mathcal{H}^A \otimes \mathcal{H}^B)^{\otimes n} \rightarrow (S_A, S_B, C)$



Alice and Bob's keys      Classical transcript

Define a map  $S : (S_A, S_B, C) \rightarrow (S'_A, S'_B)$ , where  $(S'_A, S'_B)$  are identical, uniformly distributed keys

**Ideal map:**  $\mathcal{F} = S \circ \mathcal{E}$

$\mathcal{E}$  is  $\epsilon$ -secure if  $\|\mathcal{E} - \mathcal{F}\|_{\diamond} \leq \epsilon$

$$\|\Delta\|_{\diamond} := \max_{\|X\|_1 \leq 1} \|(\Delta \otimes \mathbb{1})X\|_1$$

**Theorem 1:** If for any permutation  $\pi$  there exists a CPTP map  $\mathcal{K}_{\pi}$  such that  $\Delta \circ \pi = \mathcal{K}_{\pi} \circ \Delta$ , then

$$\|\Delta\|_{\diamond} \leq g_{n,d} \|(\Delta \otimes \mathbb{1})(\tau_{\mathcal{H}^n \mathcal{R}})\|_1$$

where  $g_{n,d} = \binom{n + d^2 - 1}{n} \leq (n + 1)^{d^2 - 1}$  and  $d = \dim(\mathcal{H})$ .

[CKR09]

de Finetti state  $\tau_{\mathcal{H}^n} = \int \sigma_{\mathcal{H}}^{\otimes n} \mu(\sigma_{\mathcal{H}})$

Recall  $\|\Delta\|_{\diamond} := \max_{\|X\|_1 \leq 1} \|(\Delta \otimes \mathbb{1})X\|_1$ . We want to show, for an arbitrary input state  $\rho_{\mathcal{H}^n \mathcal{R}'}$ ,

$$\|(\Delta \otimes \mathbb{1})\rho_{\mathcal{H}^n \mathcal{R}'}\|_1 \leq g_{n,d} \|(\Delta \otimes \mathbb{1})\tau_{\mathcal{H}^n \mathcal{R}}\|_1$$

Recall  $\|\Delta\|_{\diamond} := \max_{\|X\|_1 \leq 1} \|(\Delta \otimes \mathbb{1})X\|_1$ . We want to show, for an arbitrary input state  $\rho_{\mathcal{H}^n \mathcal{R}'}$ ,

$$\|(\Delta \otimes \mathbb{1})\rho_{\mathcal{H}^n \mathcal{R}'}\|_1 \leq g_{n,d} \|(\Delta \otimes \mathbb{1})\tau_{\mathcal{H}^n \mathcal{R}}\|_1$$

- If  $\Delta$  is permutation invariant (satisfies Theorem 1), then it is sufficient to consider inputs  $\bar{\rho}_{\mathcal{H}^n \mathcal{K}^n}$

with support on  $Sym^n(\mathcal{H} \otimes \mathcal{K})$ :  $\|(\Delta \otimes \mathbb{1})\rho_{\mathcal{H}^n \mathcal{R}'}\|_1 \leq \|(\Delta \otimes \mathbb{1})\bar{\rho}_{\mathcal{H}^n \mathcal{K}^n}\|_1$

Recall  $\|\Delta\|_{\diamond} := \max_{\|X\|_1 \leq 1} \|(\Delta \otimes \mathbb{1})X\|_1$ . We want to show, for an arbitrary input state  $\rho_{\mathcal{H}^n \mathcal{R}'}$ ,

$$\|(\Delta \otimes \mathbb{1})\rho_{\mathcal{H}^n \mathcal{R}'}\|_1 \leq g_{n,d} \|(\Delta \otimes \mathbb{1})\tau_{\mathcal{H}^n \mathcal{R}}\|_1$$

- If  $\Delta$  is permutation invariant (satisfies Theorem 1), then it is sufficient to consider inputs  $\bar{\rho}_{\mathcal{H}^n \mathcal{K}^n}$

with support on  $Sym^n(\mathcal{H} \otimes \mathcal{K})$ :  $\|(\Delta \otimes \mathbb{1})\rho_{\mathcal{H}^n \mathcal{R}'}\|_1 \leq \|(\Delta \otimes \mathbb{1})\bar{\rho}_{\mathcal{H}^n \mathcal{K}^n}\|_1$

- *Lemma 2:* for any such  $\bar{\rho}_{\mathcal{H}^n \mathcal{K}^n}$ , there exists a trace non-increasing map  $T$  such that

$$\bar{\rho}_{\mathcal{H}^n \mathcal{K}^n} = g_{n,d}(\mathbb{1} \otimes T)\tau_{\mathcal{H}^n \mathcal{K}^n \mathcal{N}}, \text{ where } \tau_{\mathcal{H}^n \mathcal{K}^n} = \int \sigma_{\mathcal{H}\mathcal{K}}^{\otimes n} d(\sigma_{\mathcal{H}\mathcal{K}}):$$

$$\begin{aligned} \|(\Delta \otimes \mathbb{1})\bar{\rho}_{\mathcal{H}^n \mathcal{K}^n}\|_1 &= g_{n,d} \|(\Delta \otimes T)\tau_{\mathcal{H}^n \mathcal{K}^n \mathcal{N}}\|_1 \\ &\leq g_{n,d} \|(\Delta \otimes \mathbb{1})\tau_{\mathcal{H}^n \mathcal{K}^n \mathcal{N}}\|_1 \end{aligned}$$

**Theorem 1:** If for any permutation  $\pi$  there exists a CPTP map  $\mathcal{K}_\pi$  such that  $\Delta \circ \pi = \mathcal{K}_\pi \circ \Delta$ , then

$$\|\Delta\|_\diamond \leq g_{n,d} \|(\Delta \otimes \mathbb{1})(\tau_{\mathcal{H}^n \mathcal{R}})\|_1$$

$\mathcal{E}$  is  $\epsilon$ -secure whenever:  $\|((\mathcal{E} - \mathcal{F}) \otimes \mathbb{1})(\tau_{\mathcal{H}^n \mathcal{R}})\|_1 \leq \bar{\epsilon} := \epsilon(n+1)^{-(d^2-1)}$

**Collective attack:** Eve attacks each signal independently and identically

- Secure against collective attacks if  $\|((\mathcal{E} - \mathcal{F}) \otimes \mathbb{1})(\sigma_{\mathcal{H}\mathcal{K}}^{\otimes n})\|_1 \leq \bar{\epsilon}$

for any pure  $\sigma_{\mathcal{H}\mathcal{K}}$

- $\bar{\epsilon}$ -security against collective attacks implies  $\epsilon$ -security against general attacks

# Part II: The Quantum Reverse Shannon Theorem (QRST)

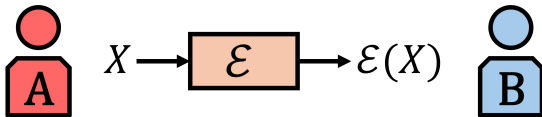
Application of the post-selection technique in a channel coding theorem  
(and the intuition behind quantum state splitting)

# Classical channel coding theorems

## Shannon's Noisy Channel Coding Theorem [Sha48]

- The asymptotic capacity of a noisy channel,  $\mathcal{E}$ , to communicate over a distribution of inputs,  $X$ ,

$$C(\mathcal{E}) := \max_X \{H(X) + H(\mathcal{E}(X)) - H(X, \mathcal{E}(X))\}$$

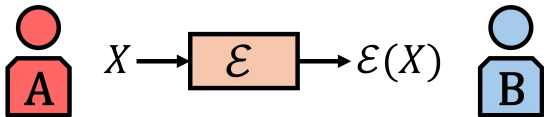


# Classical channel coding theorems

## Shannon's Noisy Channel Coding Theorem [Sha48]

- The asymptotic capacity of a noisy channel,  $\mathcal{E}$ , to communicate over a distribution of inputs,  $X$ ,

$$C(\mathcal{E}) := \max_X \{H(X) + H(\mathcal{E}(X)) - H(X, \mathcal{E}(X))\}$$



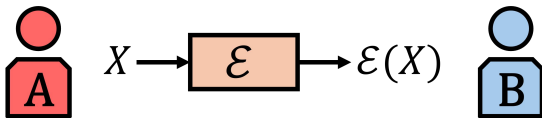
- For a transmission rate,  $R < C(\mathcal{E})$ , there exists an error-correcting code yielding arbitrarily small error.
- Shannon showed that *shared randomness* does not increase  $C(\mathcal{E})$

# Classical channel coding theorems

## Shannon's Noisy Channel Coding Theorem [Sha48]

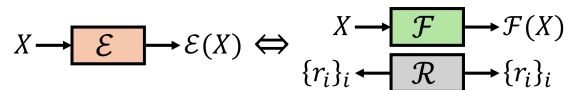
- The asymptotic capacity of a noisy channel,  $\mathcal{E}$ , to communicate over a distribution of inputs,  $X$ ,

$$C(\mathcal{E}) := \max_X \{H(X) + H(\mathcal{E}(X)) - H(X, \mathcal{E}(X))\}$$



- For a transmission rate,  $R < C(\mathcal{E})$ , there exists an error-correcting code yielding arbitrarily small error.
- Shannon showed that *shared randomness* does not increase  $C(\mathcal{E})$

## The Classical Reverse Shannon Theorem (CRST) [Ben+02]



- Given free shared randomness, a (noise) channel  $\mathcal{E}$  can be *simulated* by a (noiseless) channel  $\mathcal{F}$  with a capacity,

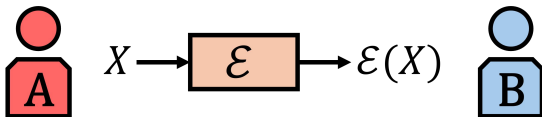
$$C_R(\mathcal{E}, \mathcal{F}) := \frac{C(\mathcal{E})}{C(\mathcal{F})}$$

# Classical channel coding theorems

## Shannon's Noisy Channel Coding Theorem [Sha48]

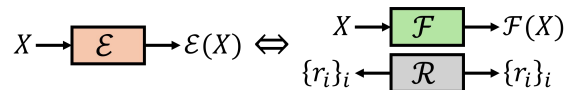
- The asymptotic capacity of a noisy channel,  $\mathcal{E}$ , to communicate over a distribution of inputs,  $X$ ,

$$C(\mathcal{E}) := \max_X \{H(X) + H(\mathcal{E}(X)) - H(X, \mathcal{E}(X))\}$$



- For a transmission rate,  $R < C(\mathcal{E})$ , there exists an error-correcting code yielding arbitrarily small error.
- Shannon showed that *shared randomness* does not increase  $C(\mathcal{E})$

## The Classical Reverse Shannon Theorem (CRST) [Ben+02]



- Given free shared randomness, a (noise) channel  $\mathcal{E}$  can be *simulated* by a (noiseless) channel  $\mathcal{F}$  with a capacity,

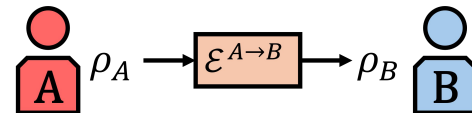
$$C_R(\mathcal{E}, \mathcal{F}) := \frac{C(\mathcal{E})}{C(\mathcal{F})}$$

- The Shannon capacity is the only parameter needed to characterize a classical channel.
- $C(\mathcal{E})n + \mathcal{O}(n)$  uses of  $\mathcal{F}$  are needed to simulate  $n$  uses of  $\mathcal{E}$ , with shared randomness that scales linearly in  $n$  [Win02].

# The Quantum Reverse Shannon Theorem (QRST)

- The CRST motivates applications of *entanglement-assisted classical capacity* of a channel  $\mathcal{E}$  [Ben+02], given as,

$$C_E(\mathcal{E}) := \max_{\rho} \{H(\rho) + H(\mathcal{E}(\rho)) - H((\mathcal{E} \otimes \text{id})\Phi_{\rho})\}$$



# The Quantum Reverse Shannon Theorem (QRST)

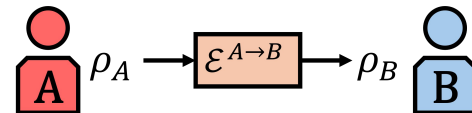
- The CRST motivates applications of *entanglement-assisted classical capacity* of a channel  $\mathcal{E}$  [Ben+02], given as,

$$C_E(\mathcal{E}) := \max_{\rho} \{H(\rho) + H(\mathcal{E}(\rho)) - H((\mathcal{E} \otimes \text{id})\Phi_{\rho})\}$$

- QRST: Given unlimited *shared entanglement*,  $\mathcal{E}$  can be simulated by  $\mathcal{F}$  with a capacity,

$$C_E(\mathcal{E}, \mathcal{F}) := \frac{C_E(\mathcal{E})}{C_E(\mathcal{F})}$$

- Proved originally in [Ben+14] (orig. ver. [Ben+09]).
  - Orig. ver. only worked for I.I.D. sources (via Homer Simpson protocol).
  - For general inputs, requires discussing *entanglement spread*.



# The Quantum Reverse Shannon Theorem (QRST)

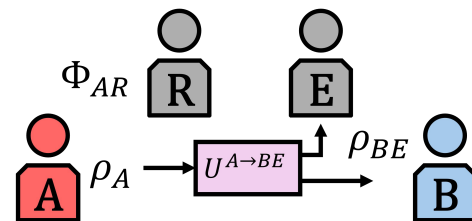
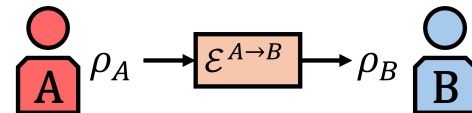
- The CRST motivates applications of *entanglement-assisted classical capacity* of a channel  $\mathcal{E}$  [Ben+02], given as,

$$C_E(\mathcal{E}) := \max_{\rho} \{H(\rho) + H(\mathcal{E}(\rho)) - H((\mathcal{E} \otimes \text{id})\Phi_{\rho})\}$$

- QRST: Given unlimited *shared entanglement*,  $\mathcal{E}$  can be simulated by  $\mathcal{F}$  with a capacity,

$$C_E(\mathcal{E}, \mathcal{F}) := \frac{C_E(\mathcal{E})}{C_E(\mathcal{F})}$$

- Proved originally in [Ben+14] (orig. ver. [Ben+09]).
  - Orig. ver. only worked for I.I.D. sources (via Homer Simpson protocol).
  - For general inputs, requires discussing *entanglement spread*.



$$\rho_A = \text{Tr}_R[\Phi_{AR}]$$

$$\rho_{BE} = U^{A \rightarrow BE} \rho_A (U^{A \rightarrow BE})^\dagger$$

$$\rho_B = \text{Tr}_E[\rho_{BE}]$$

# *One-shot* information theory

- [BCR11] proves their result of the QRST in the one-shot setting.
- The *smooth conditional min-entropy* and the *smooth max-information* are defined in terms of their unsmooth variants as:

$$H_{\min}(A|B)_\rho := - \inf_{\sigma_B} D_{\max}(\rho_{AB} || \mathbb{I}_A \otimes \sigma_B) .$$

$$I_{\max}(A : B)_\rho := \inf_{\sigma_B} D_{\max}(\rho_{AB} || \rho_A \otimes \rho_B)$$

# One-shot information theory

- [BCR11] proves their result of the QRST in the one-shot setting.
- The *smooth conditional min-entropy* and the *smooth max-information* are defined in terms of their unsmooth variants as:

$$\mathcal{B}^\epsilon(\rho) := \{\bar{\rho} \in \mathcal{S}_{\leq}(\mathcal{H}) : P(\rho, \bar{\rho}) \leq \epsilon\}$$

$$P(\rho, \sigma) := \sqrt{1 - (F(\rho, \sigma) + \sqrt{(1 - \text{tr}\rho)(1 - \text{tr}\sigma)})^2}$$

$$H_{\min}(A|B)_\rho := -\inf_{\sigma_B} D_{\max}(\rho_{AB} || \mathbb{I}_A \otimes \sigma_B)$$

$$I_{\max}(A : B)_\rho := \inf_{\sigma_B} D_{\max}(\rho_{AB} || \rho_A \otimes \rho_B)$$

# One-shot information theory

- [BCR11] proves their result of the QRST in the one-shot setting.
- The *smooth conditional min-entropy* and the *smooth max-information* are defined in terms of their unsmooth variants as:

$$\mathcal{B}^\epsilon(\rho) := \{\bar{\rho} \in \mathcal{S}_{\leq}(\mathcal{H}) : P(\rho, \bar{\rho}) \leq \epsilon\}$$

$$P(\rho, \sigma) := \sqrt{1 - (F(\rho, \sigma) + \sqrt{(1 - \text{tr}\rho)(1 - \text{tr}\sigma)})^2}$$

$$H_{\min}(A|B)_\rho := -\inf_{\sigma_B} D_{\max}(\rho_{AB} || \mathbb{I}_A \otimes \sigma_B) \rightarrow H_{\min}^\epsilon(A|B)_\rho := \sup_{\bar{\rho}_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})} H_{\min}(A|B)_{\bar{\rho}}$$

$$I_{\max}(A : B)_\rho := \inf_{\sigma_B} D_{\max}(\rho_{AB} || \rho_A \otimes \rho_B) \rightarrow I_{\max}^\epsilon(A : B)_\rho := \inf_{\bar{\rho}_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})} I_{\max}(A : B)_{\bar{\rho}}$$

# One-shot information theory

- [BCR11] proves their result of the QRST in the one-shot setting.
- The *smooth conditional min-entropy* and the *smooth max-information* are defined in terms of their unsmooth variants as:

$$\mathcal{B}^\epsilon(\rho) := \{\bar{\rho} \in \mathcal{S}_{\leq}(\mathcal{H}) : P(\rho, \bar{\rho}) \leq \epsilon\}$$

$$P(\rho, \sigma) := \sqrt{1 - (F(\rho, \sigma) + \sqrt{(1 - \text{tr}\rho)(1 - \text{tr}\sigma)})^2}$$

$$H_{\min}(A|B)_\rho := -\inf_{\sigma_B} D_{\max}(\rho_{AB} || \mathbb{I}_A \otimes \sigma_B) \rightarrow H_{\min}^\epsilon(A|B)_\rho := \sup_{\bar{\rho}_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})} H_{\min}(A|B)_{\bar{\rho}}$$

$$I_{\max}(A : B)_\rho := \inf_{\sigma_B} D_{\max}(\rho_{AB} || \rho_A \otimes \rho_B) \rightarrow I_{\max}^\epsilon(A : B)_\rho := \inf_{\bar{\rho}_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})} I_{\max}(A : B)_{\bar{\rho}}$$

- In the QRST there is an operational interpretation of these entropies:  $I$  is a bound on the quantum communication cost of a  $\epsilon$ -error *quantum state splitting protocol*.

Given a joint pure state consisting of a sender (Alice), receiver (Bob) and a reference system:  $\rho_{ABR}$

**Quantum State Merging:** How much of a given resource is needed in order to move the A-part from Alice to Bob so that the final global state (including R) is unchanged. Given that the A-part is initially with Alice.

Resource:

- Quantum Communication
- Shared Entanglement
- Embezzling States
- Classical Communication

Given a joint pure state consisting of a sender (Alice), receiver (Bob) and a reference system:  $\rho_{AA'R}$

**Quantum State Splitting:** How much of a given resource is needed in order to move the  $A'$ -part from Alice to Bob so that the final global state (including  $R$ ) is unchanged. Given that the  $AA'$  part is initially with Alice.

Why does the reference system matter?

- The reference system is the mathematical device that holds all coherence, entanglement, and correlations that the protocol must maintain
- Because the protocol is required to match the full pure state (including  $R$ ), it must act coherently—preserving superpositions and entanglement through every step

Maximally entangled states (MES) as a free resource is insufficient to prove the Quantum Reverse Shannon Theorem because of entanglement spread

## Entanglement Spread:

- In a coherent protocol applied to superpositions of different branches, different branches may require different amounts of entanglement
- There is no way using only local operations to produce a coherent superposition of different MES sizes (local operations cannot coherently change Schmidt Rank)
- This inability is the entanglement spread obstruction

For example:  $|\Phi_{d_1}\rangle \rightarrow \alpha |\Phi_{d_1}\rangle + \beta |\Phi_{d_2}\rangle$  is not possible using LO

Where  $|\Phi_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d |i, i\rangle$

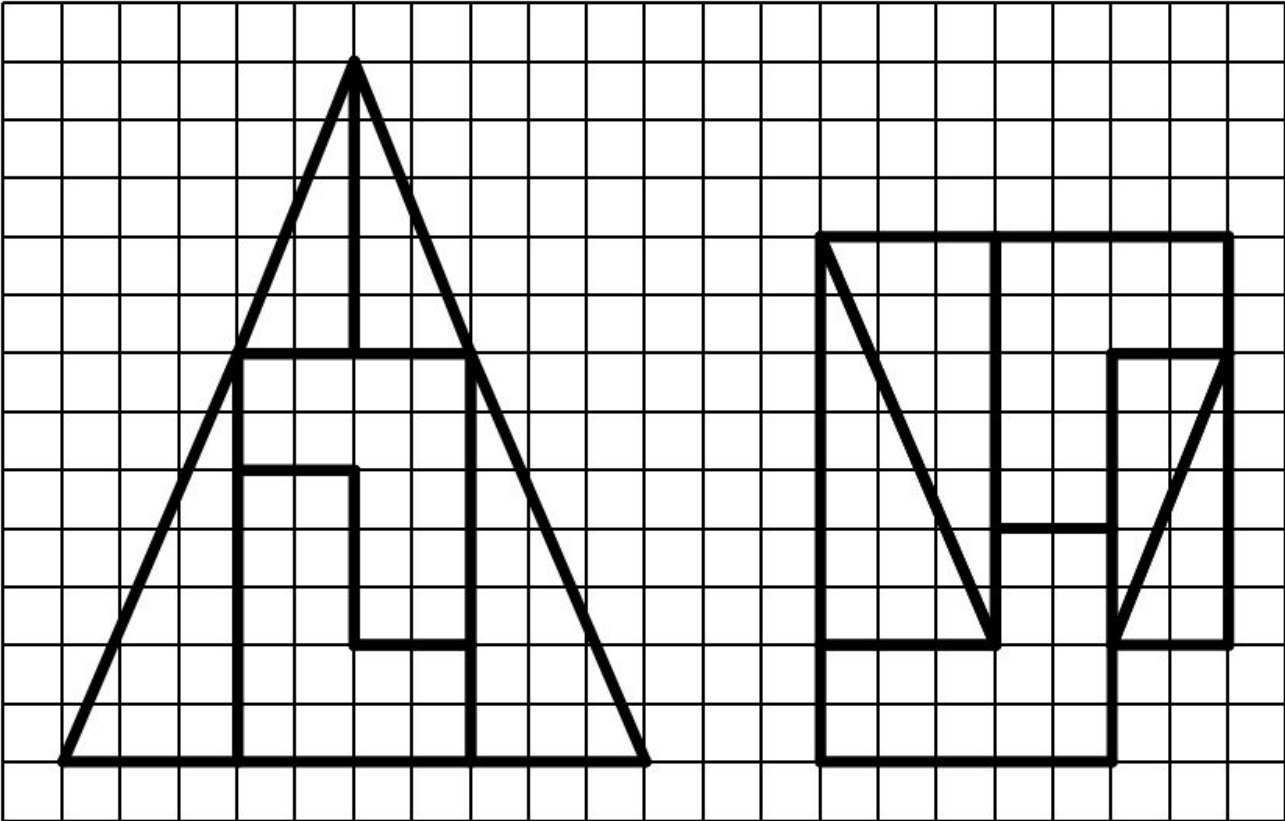
**Definition:** An  $\delta$ -ebit embezzling state  $\mu_{AB}$  is a bipartite state such that there exists some local isometries  $X_A, X_B$  with:

$$(X_A \otimes X_B)\mu_{AB}(X_A \otimes X_B)^\dagger \approx_\delta \mu_{AB} \otimes |\phi\rangle_{A'B'}$$

Where  $|\phi\rangle_{A'B'}$  denotes an ebit

So you can “embezzle” an ebit(s) out of  $\mu$  with an arbitrarily small error and without any coherent classical communication. More simply:

$$\mu_{AB} \rightarrow \mu_{AB} \otimes |\phi\rangle_{A'B'} \text{ with error } \leq \delta$$



Let  $\rho_{AR}$  be given, and split  $A$  into subsystems  $A_1A_2$ . Consider applying a Haar-random unitary  $U$  on  $A$  and then tracing out  $A_2$ . If the output of dimension  $|A_1|$  satisfies:

$$\log |A_1| \leq \frac{1}{2} \left( \log |A| + H_{\min}(A | R)_\rho \right) - \log \frac{1}{\epsilon}$$

Then averaging over  $U$  yields:

$$\int dU \left\| \sigma_{A_1R}(U) - \frac{I_{A_1}}{|A_1|} \otimes \rho_R \right\|_1 \leq \epsilon$$

Here  $\sigma_{A_1R}(U) = \text{tr}_{A_2} [(U \otimes I_R) \rho_{AR} (U^\dagger \otimes I_R)]$

**Main Result:** after an appropriate (random) unitary and discarding  $A_2$ , the remainder  $A_1$  is nearly maximally mixed and uncorrelated with  $R$ .  $A_1$  is decoupled from the reference.

The lemma quantifies the required size of  $A_1$  in terms of the min-entropy  $H_{\min}(A|R)$  and the total size  $\log|A|$ . The minimum entropy encodes the correlations with  $R$ .

Role in the state merging protocol:

- To merge  $A$  into Bob, we find a unitary that decouples a part of  $A$  from  $R$
- the remaining part can be sent to Bob and the purification argument reconstructs the desired state while producing entanglement
- theorem quantifies how large the discarded subsystem must be to effect decoupling, connecting to  $H_{\min}$

A CPTP map is an  $\epsilon$ -error state merging of  $|\rho\rangle_{ABR}$  if after local operations + sending  $q$  qubits from Alice to Bob, the output approximates:  $\rho_{BB'R} \otimes |\phi_L\rangle_{A_1B_1}$

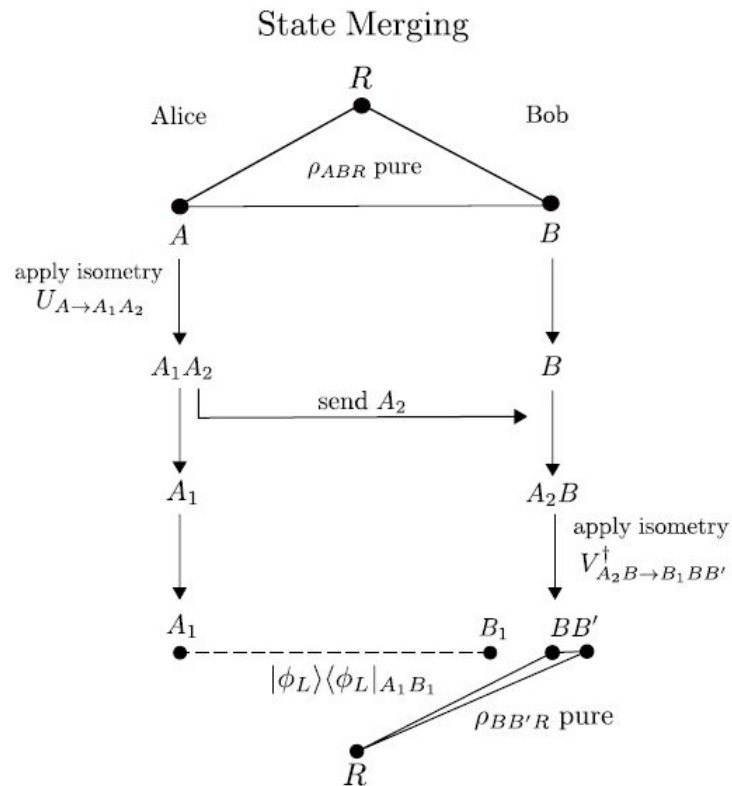
This yields a quantum communication cost of

$$q = \left\lceil \frac{1}{2} \left[ H_0(A)_\rho - H_{\min}(A | R)_\rho \right] + 2 \log \left( \frac{1}{\epsilon} \right) \right\rceil$$

And an entanglement gain of

$$e = \left\lfloor \frac{1}{2} \left[ H_0(A)_\rho + H_{\min}(A | R)_\rho \right] - 2 \log \left( \frac{1}{\epsilon} \right) \right\rfloor$$

where  $H_0(A)_\rho = \log \text{rank}(\rho_A)$



# One-Shot Quantum State Splitting with MES



A CPTP map is an  $\epsilon$ -error state merging of  $|\rho\rangle_{AA'R}$  if after local operations + sending  $q$  qubits from Alice to Bob, the output approximates:  $\rho_{ABR}$

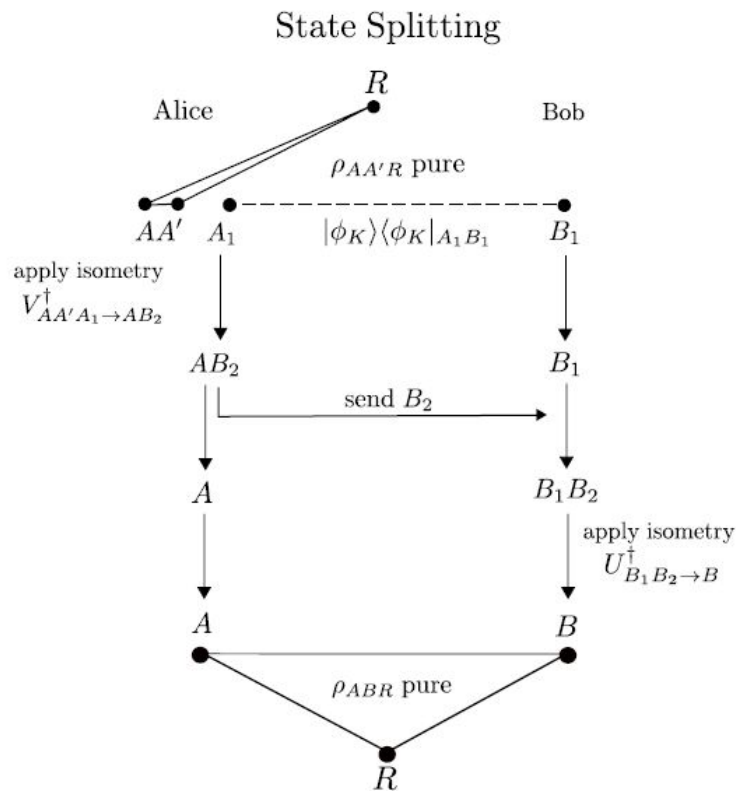
This yields a quantum communication cost of

$$q = \left\lceil \frac{1}{2} \left[ H_0(A')_{\rho} - H_{\min}(A' | R)_{\rho} \right] + 2 \log \left( \frac{1}{\epsilon} \right) \right\rceil$$

And an entanglement cost of

$$e = \left\lceil \frac{1}{2} \left[ H_0(A')_{\rho} + H_{\min}(A' | R)_{\rho} \right] - 2 \log \left( \frac{1}{\epsilon} \right) \right\rceil$$

where  $H_0(A')_{\rho} = \log \text{rank}(\rho_{A'})$



**Theorem:** Any  $\varepsilon$ -error state splitting protocol must satisfy:

$$q \geq \frac{1}{2} I_{\max}^{\varepsilon'}(A' : R)_{\rho}$$

Intuition:

- Max-information measures how correlated the reference and a given subsystem are in the sense relevant to one-shot tasks
- If Bob ends up highly correlated with  $R$  (as required by success), Alice must have communicated enough qubits to increase Bob's information about  $R$
- Sending  $q$  qubits can at most double the max-information by  $2q$  leading to the lower bound

**Theorem:** There exists an  $\left(\epsilon + \epsilon' + \delta \log |A'| + |A'|^{-1/2}\right)$  - error quantum state splitting protocol with a  $\delta$ -bit embezzling state for a quantum communication cost of:

$$q \leq \frac{1}{2} I_{\max}^{\epsilon'}(A' : R)_{\rho} + 2 * \log \frac{1}{\epsilon} + 4 + \log \log |A'|$$

Explanation:

- $\frac{1}{2} I_{\max}^{\epsilon'}(A' : R)_{\rho}$  quantity controlling the communication cost in one-shot splitting i.e., how much must be transferred
- $2 \log (1/\epsilon)$  typical tail / smoothing overhead from the decoupling / one-shot arguments
- $4 + \log \log |A'|$  small finite-size additive overheads: constant bookkeeping, plus the cost to coherently send the index register for the decomposition

The two tasks are time-reversals of each other

For any pure state  $|AA'R\rangle$

- Splitting transfers  $A'$  from Alice  $\rightarrow$  Bob using communication
- Merging transfers  $A$  from Alice  $\rightarrow$  Bob while generating entanglement

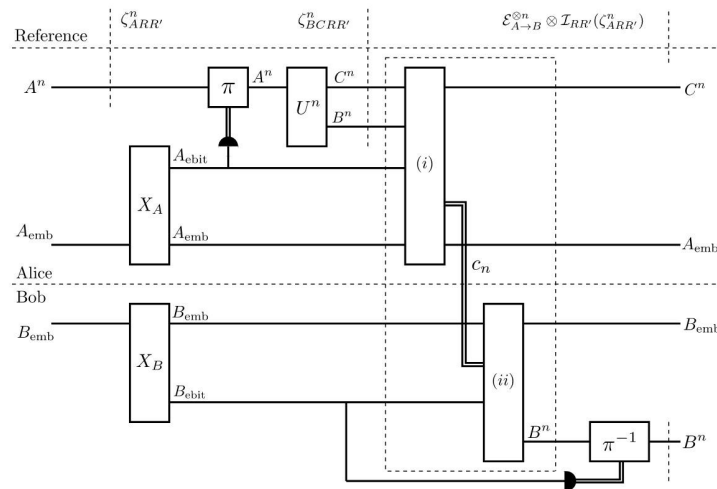
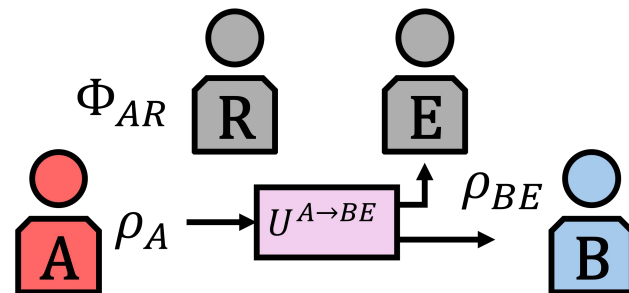
Algebraic Duality:

- If merging requires cost  $q$  and generates entanglement  $e$
- then splitting requires cost  $q$  and consumes entanglement  $e$

The protocols are literally inverses once enriched with embezzling states

# Proof of the QRST

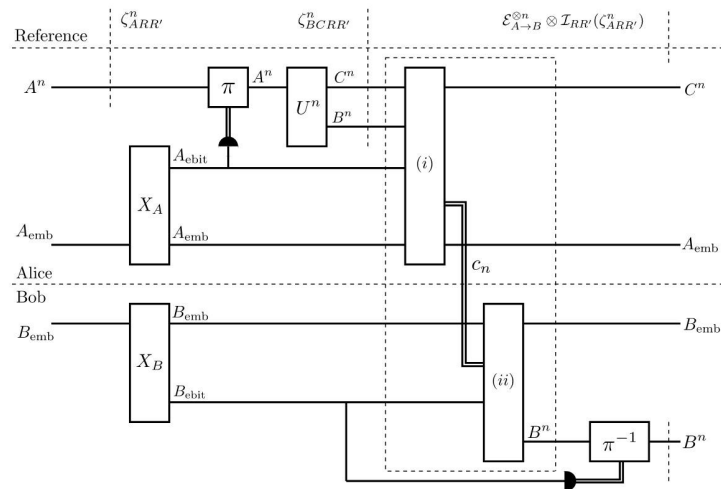
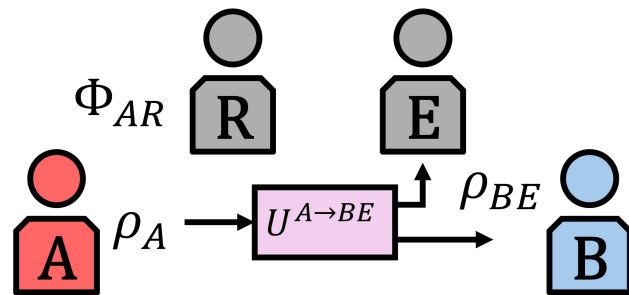
- Concept: Demonstrate one-shot Shannon simulation, where (1) **A** simulates the isometry locally, and (2) utilize quantum state splitting to optimally transfer to **B**.



# Proof of the QRST

- Concept: Demonstrate one-shot Shannon simulation, where (1) **A** simulates the isometry locally, and (2) utilize quantum state splitting to optimally transfer to **B**.
- Given a de Finetti input, simulate

$$\zeta_{BCRR'}^{\otimes n} = (U_{A \rightarrow BC}^{\otimes n} \otimes \mathbb{I}_{RR'}) \zeta_{ARR'}^{\otimes n} (U_{A \rightarrow BC}^{\otimes n} \otimes \mathbb{I}_{RR'})^\dagger$$



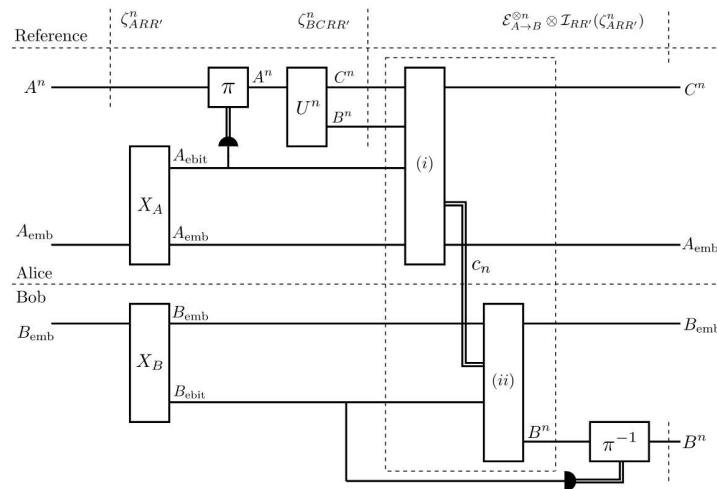
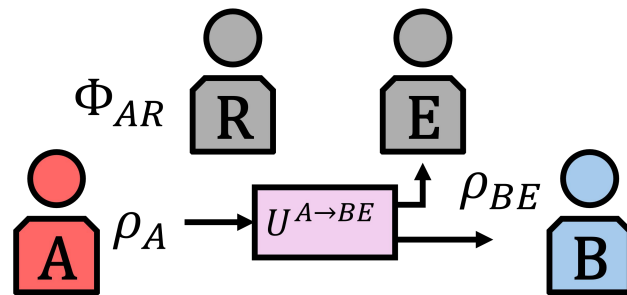
# Proof of the QRST

- Concept: Demonstrate one-shot Shannon simulation, where (1) **A** simulates the isometry locally, and (2) utilize quantum state splitting to optimally transfer to **B**.
- Given a de Finetti input, simulate

$$\zeta_{BCRR'}^{\otimes n} = (U_{A \rightarrow BC}^{\otimes n} \otimes \mathbb{I}_{RR'}) \zeta_{ARR'}^{\otimes n} (U_{A \rightarrow BC}^{\otimes n} \otimes \mathbb{I}_{RR'})^\dagger$$

- On the right: (i) state splitting, (ii) teleportation. Bounded classical communication goes as

$$\frac{1}{2} c_n = q_n \leq \frac{1}{2} I_{\max}^\epsilon(B : RR') (\mathcal{E}^{\otimes n} \otimes \text{id})(\zeta^{\otimes n}) + \chi$$



# Proof of the QRST

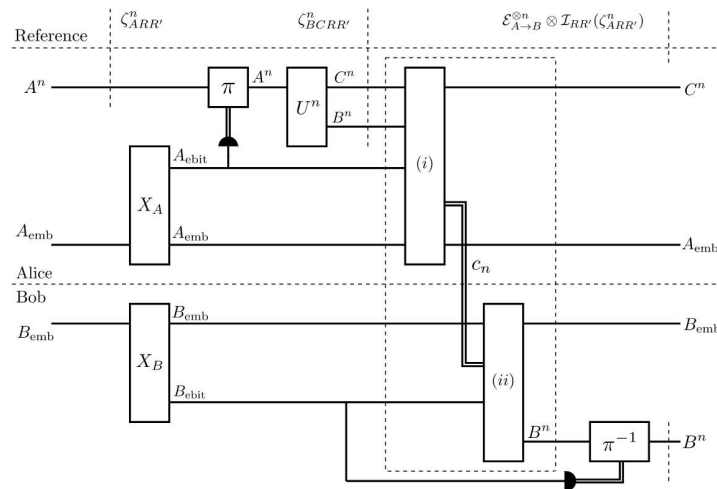
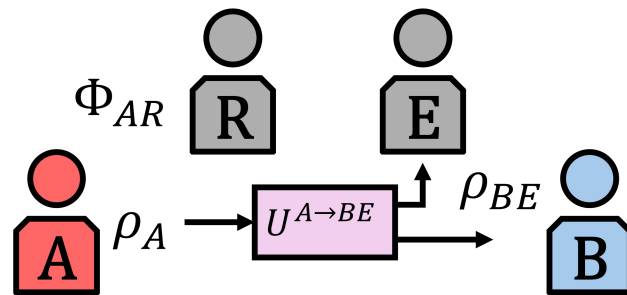
- Concept: Demonstrate one-shot Shannon simulation, where (1) **A** simulates the isometry locally, and (2) utilize quantum state splitting to optimally transfer to **B**.
- Given a de Finetti input, simulate

$$\zeta_{BCRR'}^{\otimes n} = (U_{A \rightarrow BC}^{\otimes n} \otimes \mathbb{I}_{RR'}) \zeta_{ARR'}^{\otimes n} (U_{A \rightarrow BC}^{\otimes n} \otimes \mathbb{I}_{RR'})^\dagger$$

- On the right: (i) state splitting, (ii) teleportation. Bounded classical communication goes as

$$\frac{1}{2} c_n = q_n \leq \frac{1}{2} I_{\max}^\epsilon(B : RR') (\mathcal{E}^{\otimes n} \otimes \text{id})(\zeta^{\otimes n}) + \chi$$

- Simulations involves only local operations on **A**'s and **B**'s side, classical communication, and access to embezzling states.



# Application of the post-selection technique

- The one-shot reverse Shannon simulation  $\mathcal{P}$  realizes  $\mathcal{E}$ , if

$$\left\| \mathcal{E}_{A \rightarrow B}^{\otimes n} - \mathcal{P}_{A \rightarrow B}^n \right\|_{\diamond} \leq \beta$$

# Application of the post-selection technique

- The one-shot reverse Shannon simulation  $\mathcal{P}$  realizes  $\mathcal{E}$ , if

$$\|\mathcal{E}_{A \rightarrow B}^{\otimes n} - \mathcal{P}_{A \rightarrow B}^n\|_{\diamond} \leq \beta$$

- Assuming a permutation-invariant simulation, the post-selection technique lets us simplify that above to

$$\|((\mathcal{E}_{A \rightarrow B}^{\otimes n} - \mathcal{P}_{A \rightarrow B}^n) \otimes \text{id}_{RR'}) (\zeta_{ARR'}^{\otimes n})\|_1 \leq \beta(n+1)^{-|A|^2-1}$$

- This technique extends the results of the QRST on de Finetti inputs to general inputs.

# Sources

- [Sha48] - 10.1002/j.1538-7305.1949.tb00928.x
- [Ben+02] - 10.48550/arXiv.quant-ph/0106052
- [Win02] - 10.48550/arXiv.quant-ph/0208131
- [vDH03] - 10.1103/PhysRevA.67.060302
- [CKR09] - 10.1103/PhysRevLett.102.020504
- [BCR11] - 10.1007/s00220-011-1309-7
- [Ben+14] - 10.1109/TIT.2014.2309968

Questions?