

Quantum Broadcast Channels with Cooperating Decoders:

An Information-Theoretic Perspective on Quantum Repeaters

Uzi Pereg

Joint Work with Christian Deppe and Holger Boche
ISIT 2021

Institute for Communications Engineering
Technical University of Munich (TUM)



Motivation: Quantum Repeaters

- Attenuation in optical fibers poses a great challenge for long-distance quantum communication protocols.
 - Current applications: **quantum key distribution (QKD)**
→ Security based on one-time pad encryption

Motivation: Quantum Repeaters

- Attenuation in optical fibers poses a great challenge for long-distance quantum communication protocols.
 - Current applications: quantum key distribution (QKD)
 - Future implementation of the quantum internet and networks

Motivation: Quantum Repeaters

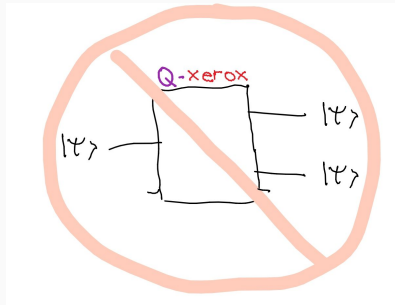
- Attenuation in optical fibers poses a great challenge for long-distance quantum communication protocols.
 - Current applications: quantum key distribution (QKD)
 - Future implementation of the quantum internet and networks
- Potential Solution: **Quantum repeaters** [Briegel et al., 1998]
 - The distance is divided into smaller segments with quantum repeaters at the intermediate stations.

Motivation: Quantum Repeaters

- Attenuation in optical fibers poses a great challenge for long-distance quantum communication protocols.
 - Current applications: quantum key distribution (QKD)
 - Future implementation of the quantum internet and networks
- Potential Solution: **Quantum repeaters** [Briegel et al., 1998]
 - The distance is divided into smaller segments with quantum repeaters at the intermediate stations.
 - Implementation: [van Loock et al., 2020]; quantum dots, trapped ions. [Rozpıfmmode et al.,2019] diamond color centers.

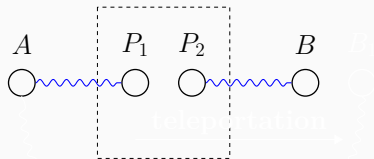
Motivation: Quantum Repeaters (Cont.)

- Straightforward amplification is not an option due to the **no-cloning theorem**, i.e. universal copying of quantum states stands in violation of quantum mechanics.



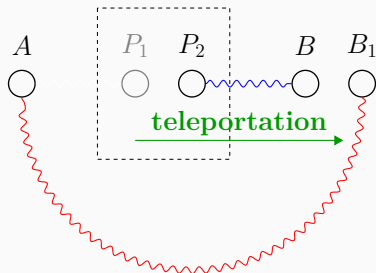
Motivation: Quantum Repeaters (Cont.)

- Basic scheme:
 - Use quantum communication and entanglement distillation to prepare $|\Phi_{AP_1}\rangle$ between the sender and the repeater, and $|\Phi_{P_2B}\rangle$ between the repeater and the receiver.



Motivation: Quantum Repeaters (Cont.)

- Basic scheme:
 - Use quantum communication and entanglement distillation to prepare $|\Phi_{AP_1}\rangle$ between the sender and the repeater, and $|\Phi_{P_2B}\rangle$ between the repeater and the receiver.
 - The repeater teleports the quantum state of P_1 onto B_1 thus swapping the entanglement; A and B_1 are now entangled at twice the distance.



Different categories for capacity of quantum channels:

Different categories for capacity of quantum channels:

- Classical capacity [Holevo 1998, Schumacher and Westmoreland 1997]
 - transmission of classical bits using a quantum channel

Different categories for capacity of quantum channels:

- Classical capacity [Holevo 1998, Schumacher and Westmoreland 1997]
 - transmission of classical bits using a quantum channel
- Quantum capacity [Lloyd 1998, Shor 2002, Devetak 2005]
 - transmission of qubits (= quantum bits)

Different categories for capacity of quantum channels:

- Classical capacity [Holevo 1998, Schumacher and Westmoreland 1997]
 - transmission of classical bits using a quantum channel
 - multi-letter formula 😞
- Quantum capacity [Lloyd 1998, Shor 2002, Devetak 2005]
 - transmission of qubits (= quantum bits)
 - multi-letter formula 😞

Background: Quantum Shannon Theory (Cont.)

- Entanglement-assisted capacity [Bennett et al. 1999]
 - Alice and Bob share entanglement resources
 - strictly higher capacity
 - single-letter formula 😊

Background: Quantum Shannon Theory (Cont.)

- Entanglement-assisted capacity [Bennett et al. 1999]
 - Alice and Bob share entanglement resources
 - strictly higher capacity
 - single-letter formula 😊
- Classical channel
 - Single user: entanglement resources do not help [Bennett et al., 1999]

Background: Quantum Shannon Theory (Cont.)

- Entanglement-assisted capacity [Bennett et al. 1999]
 - Alice and Bob share entanglement resources
 - strictly higher capacity
 - single-letter formula 😊
- Classical channel
 - Single user: entanglement resources do not help [Bennett et al., 1999]
 - MAC: entanglement resources between two transmitters can increase achievable rates! [Leditzky et al., 2020]
The channel is defined by a **pseudo-telepathy game** [Nötzel, 2019] [Winter, 2019] [Quek and Shor, 2017]

Background: Quantum Shannon Theory (Cont.)

- Entanglement-assisted capacity [Bennett et al. 1999]
 - Alice and Bob share entanglement resources
 - strictly higher capacity
 - single-letter formula 😊
- Classical channel
 - Single user: entanglement resources do not help [Bennett et al., 1999]
 - MAC: entanglement resources between two transmitters can increase achievable rates! [Leditzky et al., 2020]
The channel is defined by a **pseudo-telepathy game** [Nötzel, 2019] [Winter, 2019] [Quek and Shor, 2017]
 - Zero-error capacity [Leung et al., 2012]

Very partial list:

- Classical broadcast channel with cooperation [Dabora & Servetto, 2006] [Steinberg, 2015]
- Quantum broadcast channels [Yard, Hayden & Devetak, 2011]
 - Entanglement assistance [Dupuis, Hayden & Li 2010]
 - Hadamard BC [Wang, Das & Wilde, 2017]
- Classical-quantum relay channel [Savov & Wilde, 2015]
- Environment assistance [Smolin, Verstraete & Winter, 2005] [Winter, 2005]
- Repeater assistance [Pirandola, 2016] [Ghalaii and Pirandola, 2020]
- ...

we consider quantum broadcast channels in different settings of cooperation between two receivers.

- Entanglement resources
- Classical conferencing:
Receiver 1 can send classical messages to Receiver 2

we consider quantum broadcast channels in different settings of cooperation between two receivers.

- Entanglement resources
- Classical conferencing:
Receiver 1 can send classical messages to Receiver 2
- Quantum conferencing:
Receiver 1 can teleport a quantum state to Receiver 2

- Primitive relay channel: Receiver 1 “serves” Receiver 2
- Observations
 - tradeoff between repeater-aided and repeater-less communication
 - bottleneck behavior

- Definitions
- Entanglement Resources
- Classical Conferencing
- Quantum Conferencing
- Observations on Quantum Repeaters

The state ρ_A of a quantum system A is an Hermitian, positive semidefinite, unit-trace density matrix over \mathcal{H}_A .

Entropy

Given ρ_{AB} , define

$$H(A)_\rho \equiv -\text{Tr}(\rho_A \log \rho_A)$$

$$H(A|B)_\rho \equiv H(AB)_\rho - H(B)_\rho$$

Information Measures

- Mutual information $I(A; B)_\rho = H(A)_\rho + H(B)_\rho - H(AB)_\rho$
- Coherent information $I(A)B)_\rho = -H(A|B)_\rho$.

A quantum broadcast channel $\mathcal{N}_{A \rightarrow B_1 B_2}$ is a linear, completely positive, trace preserving map corresponding to a quantum physical evolution:

$$\rho_A \xrightarrow{\mathcal{N}} \rho_{B_1 B_2}$$

A quantum broadcast channel $\mathcal{N}_{A \rightarrow B_1 B_2}$ is a linear, completely positive, trace preserving map corresponding to a quantum physical evolution:

$$\rho_A \xrightarrow{\mathcal{N}} \rho_{B_1 B_2}$$

Interpretation

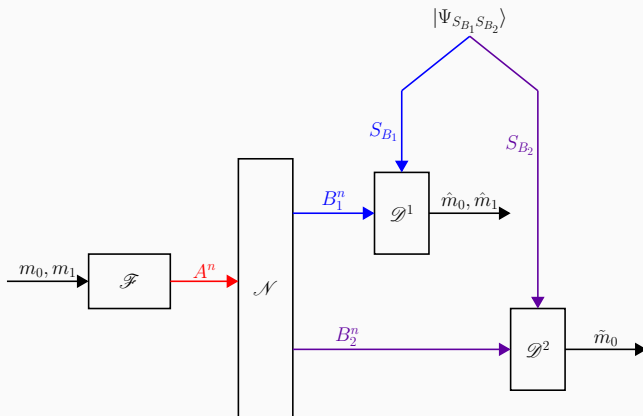
Alice — the transmitter

Bob 1 — the repeater

Bob 2 — the destination receiver

- Definitions
- Entanglement Resources
- Classical Conferencing
- Quantum Conferencing
- Observations on Quantum Repeaters

Coding with Entangled Decoders



Communication Scheme

Alice chooses a common message m_0 for both users and a private message m_1 for Bob 1.

Input: Alice prepares $\rho_{A^n}^{m_0, m_1} = \mathcal{F}(m_0, m_1)$, and transmits A^n .

Communication Scheme

Alice chooses a common message m_0 for both users and a private message m_1 for Bob 1.

Input: Alice prepares $\rho_{A^n}^{m_0, m_1} = \mathcal{F}(m_0, m_1)$, and transmits A^n .

Output: Bob 1 and Bob 2 receive B_1^n and B_2^n ,

$$\rho_{B_1^n B_2^n}^{m_0, m_1} = \mathcal{N}^{\otimes n}(\rho_{A^n}^{m_0, m_1})$$

Communication Scheme

Alice chooses a common message m_0 for both users and a private message m_1 for Bob 1.

Input: Alice prepares $\rho_{A^n}^{m_0, m_1} = \mathcal{F}(m_0, m_1)$, and transmits A^n .

Output: Bob 1 and Bob 2 receive B_1^n and B_2^n ,

$$\rho_{B_1^n B_2^n}^{m_0, m_1} = \mathcal{N}^{\otimes n}(\rho_{A^n}^{m_0, m_1})$$

Bob 1 receives B_1^n , combines with S_{B_1} , and performs the measurement Λ . Similarly, Bob 2 performs Γ on B_2^n , S_{B_2} .

BC-MAC Duality

- The duality between the broadcast/multiple-access channels is a useful property in the study of classical MIMO channels [Jindal et al., 2004]

BC-MAC Duality

- The duality between the broadcast/multiple-access channels is a useful property in the study of classical MIMO channels [Jindal et al., 2004]
- Recently, Leditzky et al. (2020) showed that entanglement between two transmitters can strictly increase the achievable rates for a MAC, even when the channel is classical (!)

magic square

BC-MAC Duality

- The duality between the broadcast/multiple-access channels is a useful property in the study of classical MIMO channels [Jindal et al., 2004]
- Recently, Leditzky et al. (2020) showed that entanglement between two transmitters can strictly increase the achievable rates for a MAC, even when the channel is classical (!)
- Does the dual property hold? That is, can entanglement between decoders increase the achievable rates?

magic square

BC-MAC Duality

- The duality between the broadcast/multiple-access channels is a useful property in the study of classical MIMO channels [Jindal et al., 2004]
- Recently, Leditzky et al. (2020) showed that entanglement between two transmitters can strictly increase the achievable rates for a MAC, even when the channel is classical (!)
- Does the dual property hold? That is, can entanglement between decoders increase the achievable rates?

Theorem

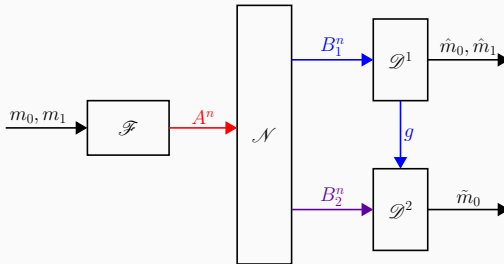
The capacity region of a broadcast channel with entangled decoders is the same as without entanglement resources.

Preprint available on [arXiv:2011.09233](https://arxiv.org/abs/2011.09233)

- Definitions
- Entanglement Resources
- **Classical Conferencing**
- Quantum Conferencing
- Observations on Quantum Repeaters

Classical Conferencing

Bob 1 can send a classical conferencing message $g \in [1 : 2^{nC_{12}}]$ to Bob 2:



Results: Classical Conferencing

Define

$$\mathcal{R}_{\text{Cl}}(\mathcal{N}) \triangleq \bigcup \left\{ (R_0, R_1) : \begin{array}{l} R_0 \leq I(X_0; B_2)_\rho + C_{12} \\ R_1 \leq I(X_1; B_1|X_0)_\rho \\ R_0 + R_1 \leq I(X_0, X_1; B_1)_\rho \end{array} \right\}$$

where the union is over the set of all distributions p_{X_0, X_1} , and state collection $\{\theta_A^{x_0, x_1}\}$,

$$\rho_{X_0 X_1 B} = \sum_{x_0 \in \mathcal{X}_0} \sum_{x_1 \in \mathcal{X}_1} p_{X_0, X_1}(x_0, x_1) |x_0\rangle\langle x_0| \otimes |x_1\rangle\langle x_1| \otimes \mathcal{N}(\theta_A^{x_0, x_1})$$

with $|\mathcal{X}_0| \leq |\mathcal{H}_A|^2 + 2$ and $|\mathcal{X}_1| \leq (|\mathcal{H}_A|^2 + 2)|\mathcal{H}_A|^2 + 1$.

Theorem

The classical capacity region of the quantum broadcast channel $\mathcal{N}_{A \rightarrow B_1 B_2}$ with conferencing and degraded message sets is given by

$$\mathbb{R}_{Cl}(\mathcal{N}) = \bigcup_{k=1}^{\infty} \frac{1}{k} \mathcal{R}_{Cl}(\mathcal{N}^{\otimes k})$$

For a Hadamard broadcast channel,

$$\mathbb{R}_{Cl}(\mathcal{N}) = \mathcal{R}_{Cl}(\mathcal{N})$$

Theorem

The classical capacity region of the quantum broadcast channel $\mathcal{N}_{A \rightarrow B_1 B_2}$ with conferencing and degraded message sets is given by

$$\mathbb{R}_{Cl}(\mathcal{N}) = \bigcup_{k=1}^{\infty} \frac{1}{k} \mathcal{R}_{Cl}(\mathcal{N}^{\otimes k})$$

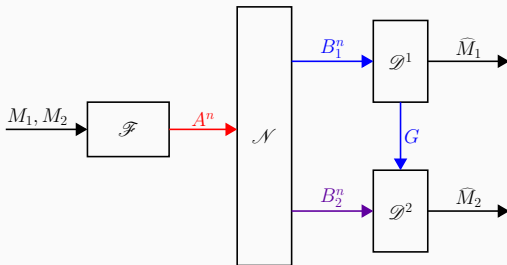
Proof Key Ideas

- Classical construction: “super-position coding” + binning
The bins are indexed by the conference message g .
- Quantum packing lemma (square-root measurement)
- Gentle measurement lemma to perform consecutive measurements without collasing the output [P., ISIT 2020]

- Definitions
- Entanglement Resources
- Classical Conferencing
- Quantum Conferencing
- Observations on Quantum Repeaters

Quantum Conferencing

Given entanglement resources, Bob 1 can teleport a quantum state to Bob 2 at a conferencing rate $C_{Q,12} = \frac{1}{2}C_{12}$.

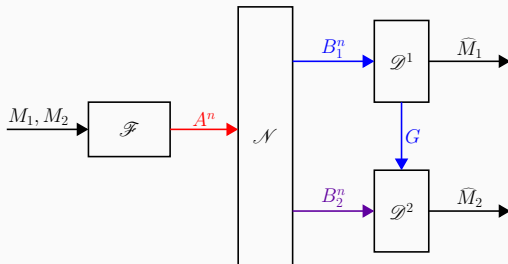


No-Cloning

- The receivers cannot recover a common quantum state. Thus, we consider two private messages M_1 and M_2 .

Quantum Conferencing

Given entanglement resources, Bob 1 can teleport a quantum state to Bob 2 at a conferencing rate $C_{Q,12} \frac{\text{qubits}}{\text{transmission}} = \frac{1}{2} C_{12} \frac{\text{cbits}}{\text{transmission}}$.



No-Cloning

- The receivers cannot recover a common quantum state. Thus, we consider two private messages M_1 and M_2 .

Subspace Transmission

Quantum communication is also referred to as entanglement transmission and can be extended to strong subspace transmission, where the entanglement between the message systems and their environment is also recovered.

Entanglement Generation

- By the **monogamy** property of quantum entanglement, Alice cannot generate a maximally entangled state with both Bob 1 and Bob 2 simultaneously.
- Alice can generate a GHZ state with Bob 1 and Bob 2, using $|\psi_{\bar{A}M_1M_2}\rangle = \frac{1}{\sqrt{d}} \sum_{x=1}^d |x\rangle \otimes |x\rangle \otimes |x\rangle$. [Yard et al., 2011]

Entanglement Generation

- By the **monogamy** property of quantum entanglement, Alice cannot generate a maximally entangled state with both Bob 1 and Bob 2 simultaneously.
- Alice can generate a GHZ state with Bob 1 and Bob 2, using $|\psi_{\bar{A}M_1M_2}\rangle = \frac{1}{\sqrt{d}} \sum_{x=1}^d |x\rangle \otimes |x\rangle \otimes |x\rangle$. [Yard et al., 2011]
- She can also generate two entangled pairs by preparing $|\Phi_{\bar{A}_1M_1}\rangle \otimes |\Phi_{\bar{A}_2M_2}\rangle$.

Theorem (achievable region)

A rate pair (Q_1, Q_2) is achievable with quantum conferencing if

$$Q_1 \leq I(\bar{A}_1 \rangle B_1)_\rho$$

$$Q_2 \leq I(\bar{A}_2 \rangle B_2)_\rho + C_{Q,12}$$

$$Q_1 + Q_2 \leq I(\bar{A}_1 \rangle B_1)_\rho + I(\bar{A}_2 \rangle B_2)_\rho$$

for some input state $\rho_{\bar{A}_1 \bar{A}_2 A}$, where $\rho_{\bar{A}_1 \bar{A}_2 B_1 B_2} = (\text{id}_{\bar{A}_1 \bar{A}_2} \otimes \mathcal{N})(\rho_{\bar{A}_1 \bar{A}_2 A})$.

Observations (1)

- The rate region above reflects a greedy approach, where using the conferencing link to increase the information rate of User 2 comes directly at the expense of User 1:

If $Q_2 = I(\bar{A}_2 \rangle B_2)_\rho + \Delta$, then $Q_1 \leq I(\bar{A}_1 \rangle B_1)_\rho - \Delta$.

Observations (2)

- For classical information, optimal performance is achieved using superposition coding, where Receiver 1 can recover the message of User 2 without necessarily “losing” rate.

Observations (2)

- For classical information, optimal performance is achieved using superposition coding, where Receiver 1 can recover the message of User 2 without necessarily “losing” rate.
- The quantum scheme does not involve superposition [Dupuis et al., 2010]. Without conferencing, it is impossible for Receiver 1 to decode the message of User 2 by the no-cloning theorem.

Observations (3)

- The setting of conferencing decoders imposes a chronological order: First Bob 1 receives and processes B_1^n , then Bob 1 sends the conference message to Bob 2, and at last, Bob 2 receives B_2^n and the conference message.

Observations (3)

- The setting of conferencing decoders imposes a chronological order: First Bob 1 receives and processes B_1^n , then Bob 1 sends the conference message to Bob 2, and at last, Bob 2 receives B_2^n and the conference message.
- Hence, Bob 1 *can* recover the state of M_2 and send it to Bob 2 using the conference link — while destroying the state in his location.

Theorem (outer bound)

If a rate pair (Q_1, Q_2) is achievable with quantum conferencing, then

$$Q_1 \leq \frac{1}{n} I(\bar{A}_1 \rangle B_1^n)_\rho$$

$$Q_2 \leq \frac{1}{n} I(\bar{A}_2 T \rangle B_2^n)_\rho + C_{Q,12}$$

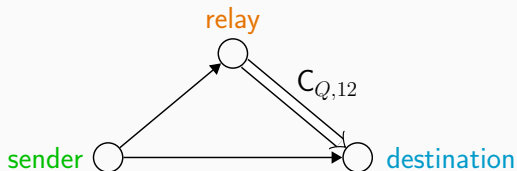
$$Q_1 + Q_2 \leq \frac{1}{n} I(\bar{A}_1 \rangle B_1^n)_\rho + \frac{1}{n} I(\bar{A}_2 \rangle B_1^n B_2^n)_\rho$$

for some input state $\rho_{T\bar{A}_1\bar{A}_2A^n}$, where

$$\rho_{T\bar{A}_1\bar{A}_2B_1^nB_2^n} = (\text{id}_{T\bar{A}_1\bar{A}_2} \otimes \mathcal{N}^{\otimes n})(\rho_{T\bar{A}_1\bar{A}_2A^n).$$

Quantum Relay Channel

Taking $Q_1 = 0$, the model reduces to the primitive relay channel.
Bob 1 is called a relay in this setting, because his only task is to help the transmission of information to Bob 2.



Theorem

The quantum capacity of the primitive relay channel $\mathcal{N}_{A \rightarrow B_1 B_2}^{\text{relay}}$ has the following bounds:

1) Cutset upper bound

$$C_Q(\mathcal{N}^{\text{relay}}) \leq \lim_{n \rightarrow \infty} \sup_{\rho_{\bar{A}TA^n}} \frac{1}{n} \min [I(\bar{A}T)B_2^n]_{\rho} + C_{Q,12}, I(\bar{A})B_1^n B_2^n]_{\rho}$$

with $\rho_{\bar{A}TB_1^n B_2^n} = (id_{\bar{A}T} \otimes \mathcal{N}^{\otimes n})(\rho_{ATA^n})$.

Theorem

The quantum capacity of the primitive relay channel $\mathcal{N}_{A \rightarrow B_1 B_2}^{\text{relay}}$ has the following bounds:

1) Cutset upper bound

$$C_Q(\mathcal{N}^{\text{relay}}) \leq \lim_{n \rightarrow \infty} \sup_{\rho_{\bar{A}TA^n}} \frac{1}{n} \min [I(\bar{A}T)B_2^n)_\rho + C_{Q,12}, I(\bar{A})B_1^n B_2^n)_\rho]$$

$$\text{with } \rho_{\bar{A}TB_1^n B_2^n} = (id_{\bar{A}T} \otimes \mathcal{N}^{\otimes n})(\rho_{ATA^n}).$$

2) Decode-forward lower bound

$$C_Q(\mathcal{N}^{\text{relay}}) \geq \max_{|\phi_{\bar{A}_1 \bar{A}_2 A}\rangle} [I(\bar{A}_2)B_2)_\rho + \min (I(\bar{A}_1)B_1)_\rho, C_{Q,12}])]$$

$$\text{with } \rho_{\bar{A}_1 \bar{A}_2 B_1 B_2} = (id_{\bar{A}_1 \bar{A}_2} \mathcal{N})(\phi_{\bar{A}_1 \bar{A}_2 A}).$$

Theorem

The quantum capacity of the primitive relay channel $\mathcal{N}_{A \rightarrow B_1 B_2}^{\text{relay}}$ has the following bounds:

3) Entanglement-formation lower bound

$$C_Q(\mathcal{N}^{\text{relay}}) \geq \max_{|\phi_{\bar{A}A}\rangle, \mathcal{F}_{B_1 \rightarrow \hat{B}_1} : E_F(\rho_{\hat{B}_1 \bar{A} B_2 E}) \leq C_{Q,12}} I(\bar{A} \rangle_{\hat{B}_1 B_2})_\phi$$

with $|\phi_{\bar{A} B_1 B_2 E}\rangle = (\mathbb{1} \otimes U_{A \rightarrow B_1 B_2 E}^{\mathcal{N}}) |\phi_{\bar{A} A}\rangle$,

$\rho_{\bar{A} \hat{B}_1 B_2 E} = \mathcal{F}_{B_1 \rightarrow \hat{B}_1}(\phi_{\bar{A} B_1 B_2 E})$, where

$$E_F(\rho_{\hat{B}_1 \bar{A} B_2 E}) \equiv \inf_{p_X(x), |\psi_{\hat{B}_1 \bar{A} B_2 E}^x\rangle} H(\hat{B}_1 | X)_\psi$$

is the **entanglement of formation** w.r.p. $\hat{B}_1 | \bar{A} B_2 E$.

- Achievability is based on channel simulation [Berta et al., 2013]

- Definitions
- Entanglement Resources
- Classical Conferencing
- Quantum Conferencing
- Observations on Quantum Repeaters

Observations (1)

- We view Alice, Bob 1, and Bob 2 as the sender, repeater, and destination receiver. In other words, the repeater is the quantum version of a relay.
- Our results show the tradeoff between **repeaterless** communication and relaying information through the repeater.

Observations (2)

- In the decode-forward lower bound: the term $I(A_2 \rangle B_2)_\rho$ corresponds to repeaterless communication, while $\min(I(A_1 \rangle B_1)_\rho, C_{Q,12})$ corresponds to quantum transmission via the repeater.
- Bottleneck flow: Due to the serial connection between the sender-repeater link $A \rightarrow B_1$ with the repeater-receiver link $B_1 \rightarrow B_2$, the throughput is dictated by the smaller rate.

Thank you