

Communication with Unreliable Entanglement Assistance

Uzi Pereg^{1,2}, Christian Deppe¹, and Holger Boche^{2,3,4}

¹Institute for Communications Engineering, Technical University of Munich

²Munich Center for Quantum Science and Technology (MCQST)

³Theoretical Information Technology, Technical University of Munich

⁴Cyber Security in the Age of Large-Scale Adversaries
Exzellenzcluster (CASA)

May 10, 2022

Abstract

Entanglement resources can increase transmission rates substantially. Unfortunately, entanglement is a fragile resource that is quickly degraded by decoherence effects. In order to generate entanglement for optical communication, the transmitter and the receiver first prepare entangled spin-photon pairs locally, and then the photon at the transmitter is sent to the receiver through an optical fiber or free space. Without feedback, the transmitter does not know whether the entangled photon has reached the receiver. The present work introduces a new model of unreliable entanglement assistance, whereby the communication system operates whether entanglement assistance is present or not. While the sender is ignorant, the receiver knows whether the entanglement generation was successful. In the case of a failure, the receiver decodes less information. In this manner, the effective transmission rate is adapted according to the assistance status. Regularized formulas are derived for the classical and quantum capacity regions with unreliable entanglement assistance, characterizing the tradeoff between the unassisted rate and the excess rate that can be obtained from entanglement assistance.

Keywords

Channel capacity, entanglement assistance, quantum communication, Shannon theory.

Email: uzi.pereg@tum.de, christian.deppe@tum.de, boche@tum.de

Introduction

Quantum channels represent the physical evolution of a non-isolated system and provide a mathematical description for a noisy transmission medium, such as an optical fiber. The channel capacity is the ultimate characteristic for communication throughput, *i.e.* the optimal transmission rate with an asymptotically vanishing error for a given noisy channel. Generally speaking, quantum communication and security protocols can be categorized as either entanglement-assisted or unassisted. Entanglement resources are instrumental in a wide variety of quantum network frameworks, such as physical-layer security¹, interferometry², sensor networks^{3;4}, and communication complexity⁵. Furthermore, the data rate can be significantly higher when the communicating parties are provided with entangled particles^{6;7}, as has recently been demonstrated in experiments⁸. Unfortunately, entanglement is a fragile resource that is quickly degraded by decoherence effects⁹.

In order to generate entanglement in an optical communication system, the transmitter may prepare an entangled pair of photons locally, and then send one of them to the receiver¹⁰. Such generation protocols are not always successful, as photons are easily absorbed before reaching the destination. Therefore, practical systems require a back channel, to inform the transmitter whether the entanglement has been established to a satisfying degree of quality. In the case of a failure, the protocol is to be repeated. The backward transmission may result in a delay, which in turn leads to a further degradation of the entanglement resources. In this work, we propose a new principle of operation: Communication with unreliable entanglement assistance. In our model, the communication system operates on a rate that is adapted to the status of the entanglement assistance, whether the assistance exists or not. Hence, feedback and repetition are not required.

Driven by new applications such as Industry 4.0, Vehicle-to-Everything (V2X), and the Tactile Internet¹¹, future communication systems such as those beyond the fifth generation of mobile networks (5G) will significantly differ from both existing wireless and wired networks. Quantum communication networks are expected to play an important role in the communication infrastructure of the modern digital society. Such systems will have a more involved network structure and will impose more diverse and challenging quality-of-service (QoS) requirements on the network resilience and reliability, service availability, delay, security, privacy, and many others. Some of these new requirements can only be met by using quantum communication¹². The deployment requirements will go beyond those of the traditional systems, *e.g.* the Tactile Internet will allow not only the control of data, but also of physical and virtual objects. With such critical applications comes the need to address the trustworthiness of the system and its services.

Resilience and reliability are core elements of trustworthiness and have been identified as key challenges for future communication systems¹³. Furthermore, resilience and reliability cannot necessarily be verified automatically on digital hardware, *i.e.* on Turing machines¹⁴. It is not Turing decidable whether an attacker can perform a denial-of-service attack or not. Thus, it is also not Turing decidable whether a communication system is trustworthy or not¹³. Therefore, it is fundamentally important to achieve entirely new approaches for resilience by design and for reliability by design. Here, we develop the theory for reliabil-

ity by design for entanglement-assisted point-to-point quantum communication systems.

Communication through quantum channels can carry classical or quantum information. For classical communication, the Holevo-Schumacher-Westmoreland (HSW) Theorem provides a regularized formula for the classical capacity of a quantum channel without assistance^{15;16}. Although calculation of such a formula is intractable in general, it provides computable lower bounds, and there are special cases where the capacity can be computed exactly. The reason for this difficulty is that the Holevo information is super-additive¹⁷. A similar difficulty occurs with transmission of quantum information. The regularized formula for the quantum capacity is given in terms of the coherent information¹⁸. The entanglement-assisted classical capacity and quantum capacity of a noisy quantum channel were fully characterized by Bennett *et al.*^{6;7} in terms of the quantum mutual information, in analogy to Shannon's capacity formula for a classical channel¹⁹. The tradeoff between transmission, leakage, key, and entanglement rates is studied extensively in the literature as well²⁰⁻²⁸.

The theory of uncertain cooperation was first introduced to classical information theory in 2014 by Steinberg²⁹, and further investigated by Huleihel and Steinberg³⁰. Our framework is inspired by Steinberg's model²⁹. The classical models of unreliable cooperation mainly focus on dynamic resources in multi-user settings, such as the multiple-access channel³¹ and the broadcast channel³²⁻³⁴. Other approaches for unreliable communication links include the outage analysis^{35;36}, automatic repeat request (ARQ)^{37;38}, and cognitive radios³⁹. Our focus here, however, is on a point-to-point quantum channel and the reliability of static resources.

In this paper, we consider communication of either classical or quantum information over a quantum channel, while Alice and Bob are provided with *unreliable* entanglement resources, as the communicating parties are uncertain about the availability of entanglement assistance. Specifically, Alice wishes to send two messages, at rates R and R' . She encodes both messages using her share of the entanglement resources, as she does not know whether Bob will have access to the entangled resources. Bob has two decoding procedures. If the entanglement assistance has failed to reach Bob's location, he performs a decoding operation to recover the first message alone. Hence, the communication system operates on a rate R . Whereas if Bob has entanglement assistance, he decodes both messages, hence the overall transmission rate is $R + R'$. In other words, R is a *guaranteed rate*, and R' is the *excess rate* of information that entanglement assistance provides. We define the capacity region as the set of all rate pairs (R, R') that can be achieved with asymptotically vanishing decoding errors. We establish a regularized characterization for the classical and quantum capacity regions. We are developing reliability by design. If the entanglement resource is unreliable, then the rate R can be guaranteed regardless. For the applications mentioned above, this is of central importance, because absolutely critical data can be transmitted at rate R and the communication does not break down.

The communication design makes a compromise. In general terms, the extreme options are to use the entanglement resources to the fullest extent, or ignore them completely. A communication protocol that relies heavily on the entanglement resources reaps the benefits of entanglement to a high extent, if the assistance is present. However, if the entanglement generation fails, then the transmission rate will be very low. That is, the excess rate R' will be close

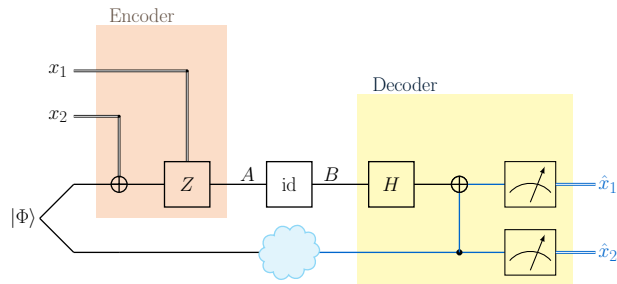


Figure 1: Super-dense coding with unreliable entanglement assistance. The blue lines indicate the bits and qubits that are affected when the entanglement resources fail to reach Bob's location.

to optimal, while the guaranteed rate R will be low. If the designer decides to sacrifice excess rate and reduce R' , *i.e.* reduce the gain from the entanglement resources, then we can guarantee a higher transmission rate. Our results characterize the optimal tradeoff.

Consider the simple scenario of a noiseless qubit channel $\text{id}_{A \rightarrow B}$, for which we have two elementary communication methods:

1. Send one classical bit of information.
2. Employ the super-dense coding protocol in order to send two classical bits, as illustrated in Figure 1.

The first method is optimal without assistance, while the second is optimal when entanglement assistance is present. If Alice follows the super-dense coding protocol, but the entanglement resources do not reach Bob's location, then Bob measures a qubit that has no correlation with the information bits. In the framework of unreliable entanglement assistance, Method 2 achieves a zero guaranteed rate and an excess rate of two information bits per transmission. Suppose that Alice employs time division: She sends $(1 - \lambda)n$ transmissions using Method 1, and λn transmissions following Method 2, where $0 \leq \lambda \leq 1$. Hence, the communication system operates on a guaranteed rate of $R = 1 - \lambda$ information bits per transmission, and an excess rate of $R' = 2\lambda$ information bits per transmission. We show that the time division region is optimal for the noiseless qubit channel. Nevertheless, we demonstrate that time division can be strictly sub-optimal for a noisy channel.

1 Definitions and Related Work

1.1 Notation and Information Measures

The quantum state of a system A is a density operator ρ on the Hilbert space \mathcal{H}_A . The set of all such density operators is denoted by $\mathcal{S}(\mathcal{H}_A)$. A measurement of a quantum system is a set of operators $\{\Lambda_j\}$ that forms a positive operator-valued measure (POVM), *i.e.* $\Lambda_j \succeq 0$ and $\sum_j \Lambda_j = \mathbb{1}$, where $\mathbb{1}$ is the identity operator.

According to the Born rule, if the system is in state ρ , then the probability of the measurement outcome j is given by $\text{Tr}(\Lambda_j \rho)$. The trace distance between two density operators ρ and σ is $\|\rho - \sigma\|_1$, where $\|F\|_1 = \text{Tr}(\sqrt{F^\dagger F})$.

Given a bipartite state ρ_{AB} on $\mathcal{H}_A \otimes \mathcal{H}_B$, define the quantum mutual information as

$$I(A; B)_\rho = H(\rho_A) + H(\rho_B) - H(\rho_{AB}), \quad (1)$$

where $H(\rho) \equiv -\text{Tr}[\rho \log(\rho)]$ is the von Neumann entropy of the state ρ . Furthermore, conditional quantum entropy and mutual information are defined by $H(A|B)_\rho = H(\rho_{AB}) - H(\rho_B)$ and $I(A; B|C)_\rho = H(A|C)_\rho + H(B|C)_\rho - H(A, B|C)_\rho$, respectively. The coherent information is then defined as

$$I(A)B)_\rho = -H(A|B)_\rho. \quad (2)$$

The maximally entangled state between two systems of dimension d is denoted by $|\Phi_{AB}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle_A \otimes |j\rangle_B$, where $\{|j\rangle_A\}$ and $\{|j\rangle_B\}$ are respective orthonormal bases.

We also use the following notation conventions. Calligraphic letters $\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \dots$ are used for finite sets. Lowercase letters x, y, z, \dots represent constants and values of classical random variables, and uppercase letters X, Y, Z, \dots represent random variables. We use $x^j = (x_1, x_2, \dots, x_j)$ to denote a sequence of letters from \mathcal{X} , and $[i : j]$ for the index set $\{i, i+1, \dots, j\}$, where $j > i$.

1.2 Quantum Channel

A quantum channel maps a state at the sender system to a state at the receiver system. Formally, a quantum channel $\mathcal{N}_{A \rightarrow B} : \mathcal{S}(\mathcal{H}_A) \rightarrow \mathcal{S}(\mathcal{H}_B)$ is defined by a linear, completely positive, trace preserving map $\mathcal{N}_{A \rightarrow B}$. In the Stinespring representation, a quantum channel is specified by $\mathcal{N}_{A \rightarrow B}(\rho_A) = \text{Tr}_E(U \rho_A U^\dagger)$, where the operator U is an isometry, *i.e.* $U^\dagger U = \mathbf{1}$. We assume that the quantum channel has a product form: If $A^n = (A_1, \dots, A_n)$ are sent through n channel uses, then the input state ρ_{A^n} undergoes the tensor product mapping $\mathcal{N}_{A^n \rightarrow B^n} \equiv \mathcal{N}_{A \rightarrow B}^{\otimes n}$. The sender and the receiver are often referred to as Alice and Bob.

1.3 Coding with Unreliable Assistance

We give coding definitions for communication with unreliable entanglement resources. We denote Alice and Bob's entangled systems by G_A and G_B , respectively.

1.3.1 Classical Codes

Definition 1. A $(2^{nR}, 2^{nR'}, n)$ classical code with unreliable entanglement assistance consists of the following: Two message sets $[1 : 2^{nR}]$ and $[1 : 2^{nR'}]$, where $2^{nR}, 2^{nR'}$ are assumed to be integers, a pure entangled state Ψ_{G_A, G_B} , a collection of encoding maps $\mathcal{F}_{G_A \rightarrow A^n}^{m, m'} : \mathcal{S}(\mathcal{H}_{G_A}) \rightarrow \mathcal{S}(\mathcal{H}_A^{\otimes n})$ for $m \in [1 : 2^{nR}]$ and $m' \in [1 : 2^{nR'}]$, and two decoding POVMs $\mathcal{D}_{B^n G_B} = \{D_{m, m'}\}$ and $\mathcal{D}_{B^n}^* = \{D_m^*\}$. We denote the code by $(\mathcal{F}, \Psi, \mathcal{D}, \mathcal{D}^*)$.

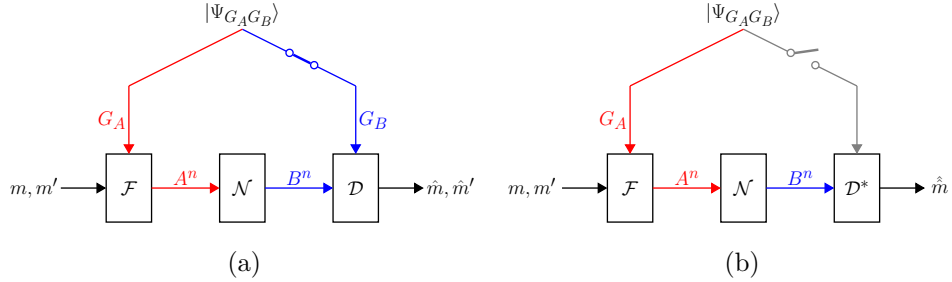


Figure 2: Illustration of unreliable entanglement assistance that is controlled by an imaginary switch. The quantum systems of Alice and Bob are marked in red and blue, respectively. Alice encodes the messages m and m' by applying the encoding map $\mathcal{F}_{G_A \rightarrow A^n}^{m, m'}$ to the system G_A , which is entangled with G_B . The model assumes that entanglement assistance may fail to reach Bob. Thus, there are two scenarios: (a) “On”: Bob performs a measurement $\mathcal{D}_{B^n G_B}$ in order to estimate m and m' . (b) “Off”: Bob performs a measurement $\mathcal{D}_{B^n}^*$ to estimate m , and does not recover m' , as he cannot access G_B .

The communication scheme is depicted in Figure 2. The sender Alice has the systems G_A, A^n and the receiver Bob has the system B^n , and *possibly* G_B as well, where G_A and G_B are entangled. The model captures two scenarios, *i.e.* when entanglement assistance is present or absent. This is illustrated in Figure 2 by an imaginary switch that controls the assistance. Without assistance, Bob is only required to decode one message, and given entanglement assistance, he should recover both messages.

Specifically, Alice chooses two classical messages, $m \in [1 : 2^{nR}]$ and $m' \in [1 : 2^{nR'}]$. She applies the encoding channel $\mathcal{F}_{G_A \rightarrow A^n}^{m, m'}$ to her share of the entangled state Ψ_{G_A, G_B} , and then transmits A^n over n channel uses of $\mathcal{N}_{A \rightarrow B}$. Bob receives the channel output B^n . If the entanglement assistance is present, *i.e.* Bob has access to the entanglement resource G_B , then he should recover both messages. He combines the output with the entangled system G_B , and performs the POVM $\mathcal{D}_{B^n G_B} = \{D_{m, m'}\}$ to obtain an estimate (\hat{m}, \hat{m}') .

Otherwise, if entanglement assistance is absent, then Bob does not have G_B , and he is only required to recover m . Hence, he performs the measurement $\mathcal{D}_{B^n} = \{D_m^*\}$ to obtain an estimate \hat{m} of the first message alone. In the presence of entanglement assistance, the conditional probability of error given that the messages m and m' were sent, is

$$P_{e|m, m'}^{(n)}(\mathcal{F}, \Psi, \mathcal{D}) = 1 - \text{Tr}[D_{m, m'}(\mathcal{N}_{A \rightarrow B}^{\otimes n} \otimes \text{id})(\mathcal{F}^{m, m'} \otimes \text{id})(\Psi_{G_A, G_B})] \quad (3)$$

and without assistance,

$$P_{e|m, m'}^{*(n)}(\mathcal{F}, \Psi, \mathcal{D}^*) = 1 - \text{Tr}[D_m^* \mathcal{N}_{A \rightarrow B}^{\otimes n} \mathcal{F}^{m, m'}(\Psi_{G_A})]. \quad (4)$$

Notice that the encoded input remains the same, since Alice does not know whether entanglement assistance is present or not. Therefore, the error depends on m and m' in both cases.

Given $\varepsilon > 0$, we say that the code is a $(2^{nR}, 2^{nR'}, n, \varepsilon)$ classical code if the error probabilities are bounded by ε . That is, $P_{e|m, m'}^{(n)}(\mathcal{F}, \Psi, \mathcal{D}) \leq \varepsilon$ and

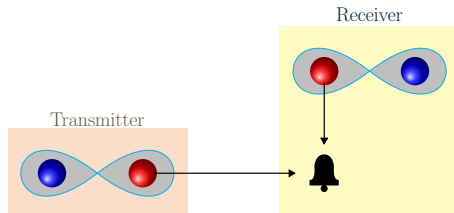


Figure 3: Heralded entanglement generation.

$P_{e|m,m'}^{*(n)}(\mathcal{F}, \Psi, \mathcal{D}^*) \leq \varepsilon$ for all $m \in [1 : 2^{nR}]$ and $m' \in [1 : 2^{nR'}]$. A rate pair (R, R') is called achievable if for every $\varepsilon > 0$ and sufficiently large n , there exists a $(2^{nR}, 2^{nR'}, n, \varepsilon)$ code with unreliable entanglement assistance.

The classical capacity region $\mathcal{C}_{\text{EA}^*}(\mathcal{N})$ with unreliable entanglement assistance is defined as the set of achievable rate pairs.

Remark 1. It is important to note that unreliable assistance is *not* equivalent to noisy assistance, which was considered by Zhuang *et al.*²⁶. In particular, we do not associate a statistical model to the availability of the entanglement resources. Instead, we consider a rate region that reflects the tradeoff between the guaranteed rate and the excess rate. The guaranteed rate R corresponds to information that Bob recovers whether the entanglement assistance is present or not, while the excess rate R' represents the additional information that is sent if entanglement assistance is present. In other words, the rate R represents the worst-case scenario, whereas R' is associated with the best-case scenario. As opposed to the average performance that is considered in the statistical model²⁶, we provide a worst-case best-case performance analysis. We would also like to emphasize that we only account for two extreme cases, *i.e.* either the *entire* entanglement resources are available or not at all.

Remark 2. In practical systems, heralded entanglement generation guarantees that Bob knows whether the procedure was successful or not. Thus, our assumption that Bob knows whether the entangled resource is present or absent is a practical one. Specifically, in optical communication, both Alice and Bob prepare an entangled photon pair or spin-photon pair locally, see Figure 3. Let us denote the pairs by $|\Phi_{G_A P_A}\rangle$ and $|\Phi_{G_B P_B}\rangle$, respectively, where P_A and P_B represent photons. In order to generate entanglement with Bob, Alice transmits the photon P_A . If the photon transmission was successful, then Bob has the two photons P_A and P_B in his lab, as well as the quantum system G_B . In this case, a Bell measurement on P_A and P_B eliminates the photons, but the remaining systems of Alice and Bob, G_A and G_B , become entangled. If the photon has not reached Bob, then the measurement outcome indicates so.

1.3.2 Quantum Codes

Next, we give a definition of a quantum code with unreliable entanglement assistance.

Definition 2. A $(2^{nQ}, 2^{nQ'}, n)$ quantum code with unreliable entanglement assistance consists of the following: A product Hilbert space $\mathcal{H}_M \otimes \mathcal{H}_{\bar{M}}$ with dimensions $|\mathcal{H}_M| = 2^{nQ}$ and $|\mathcal{H}_{\bar{M}}| = 2^{n(Q+Q')}$, a pure entangled state Ψ_{G_A, G_B} ,

an encoding channel $\mathcal{F}_{G_A M \bar{M} \rightarrow A^n} : \mathcal{S}(\mathcal{H}_{G_A} \otimes \mathcal{H}_M \otimes \mathcal{H}_{\bar{M}}) \rightarrow \mathcal{S}(\mathcal{H}_A^{\otimes n})$, and two decoding channels $\mathcal{D}_{B^n G_B \rightarrow \bar{M}} : \mathcal{S}(\mathcal{H}_B^{\otimes n} \otimes \mathcal{H}_{G_B}) \rightarrow \mathcal{S}(\mathcal{H}_{\bar{M}})$ and $\mathcal{D}_{B^n \rightarrow \hat{M}}^* : \mathcal{S}(\mathcal{H}_B^{\otimes n}) \rightarrow \mathcal{S}(\mathcal{H}_{\hat{M}})$.

The sender Alice has the systems G_A, M, \bar{M}, A^n and the receiver Bob has the systems B^n, \hat{M}, \bar{M} , and possibly G_B , where G_A and G_B are entangled. We think of M and \bar{M} as quantum message systems. Alice has a product state $\theta_M \otimes \xi_{\bar{M}}$. Let $|\theta_{MK}\rangle \otimes |\xi_{\bar{M}\bar{K}}\rangle$ be a purification of Alice's state, while K, \bar{K} are arbitrary purifying systems. Alice encodes the input state by applying the encoding channel $\mathcal{F}_{G_A M \bar{M} \rightarrow A^n}$ to M, \bar{M} , and to her share of the entangled state Ψ_{G_A, G_B} , and transmits the system A^n over n channel uses of $\mathcal{N}_{A \rightarrow B}$. Bob receives the channel output systems B^n . If the entanglement assistance is present, then he combines the output with the entangled system G_B , and applies the decoding channel $\mathcal{D}_{B^n G_B \rightarrow \bar{M}}$. Otherwise, if entanglement assistance is absent, then he performs $\mathcal{D}_{B^n \rightarrow \hat{M}}^*$.

Given $\varepsilon > 0$, the code is said to be a $(2^{nQ}, 2^{nQ'}, n, \varepsilon)$ quantum code with unreliable entanglement assistance if the trace distance between the original state and the resulting state at the receiver is bounded by ε in each scenario, *i.e.*

$$\frac{1}{2} \left\| \xi_{\bar{M}\bar{K}} - \mathcal{D}_{A \rightarrow B}^{\otimes n} \mathcal{F}(\theta_{MK} \otimes \xi_{\bar{M}\bar{K}} \otimes \Psi_{G_A, G_B}) \right\|_1 \leq \varepsilon, \quad (5)$$

and

$$\frac{1}{2} \left\| \theta_{MK} - \mathcal{D}_{A \rightarrow B}^{\otimes n} \mathcal{F}(\theta_{MK} \otimes \xi_{\bar{M}\bar{K}} \otimes \Psi_{G_A}) \right\|_1 \leq \varepsilon, \quad (6)$$

where $\|\cdot\|_1$ denotes the trace norm. Observe that the second error depends on the entangled state only through the reduced state of G_A , since the receiver does not have access to G_B in the scenario of absent assistance. A rate pair (Q, Q') is said to be achievable if for every $\varepsilon > 0$ and sufficiently large n , there exists a $(2^{nQ}, 2^{nQ'}, n, \varepsilon)$ code with unreliable entanglement assistance. The quantum capacity region $\mathcal{Q}_{\text{EA}^*}(\mathcal{N})$ is defined in a similar manner as before.

In the following remark, we discuss the relation between the classical and quantum formulations above. In many communication models in the literature, it does not matter whether the messages are chosen by the sender Alice, or given to her by an external source. However, in the quantum model, there is a fundamental distinction between the general task of sub-space transmission and remote state preparation, as we explain below.

Remark 3. In the classical code in Definition 1, if entanglement assistance is present, then Bob decodes the composite message $\bar{m} = (m, m')$. Hence, the overall transmission rate with entanglement assistance is $R_{EA} = R + R'$. In the quantum code in Definition 2, M and \bar{M} are two independent systems of dimensions 2^{nQ} and $2^{n(Q+Q')}$. Hence, the overall quantum rate with entanglement assistance is $Q_{EA} = Q + Q'$. In some applications of quantum error correction, Alice receives the system M from another source, and does not prepare it herself. While Alice can perform any operation on this system, she does not necessarily know its state in this case. Due to the no-cloning theorem, Alice cannot duplicate a general state of M either. Thus, our definition of quantum transmission with unreliable entanglement describes a more restricted problem.

1.4 Related Work

We briefly review known results without assistance and with reliable entanglement assistance. We denote the corresponding classical and quantum capacities with reliable entanglement assistance by $C_{\text{EA}}(\mathcal{N})$ and $Q_{\text{EA}}(\mathcal{N})$, and without assistance by $C(\mathcal{N})$ and $Q(\mathcal{N})$, respectively.

Define the following information measures: The channel Holevo information

$$\begin{aligned}\chi(\mathcal{N}) &\equiv \max_{p_X(x), |\psi_A^x\rangle} I(X; B)_\omega, \\ \omega_{XB} &\equiv \sum_{x \in \mathcal{X}} p_X(x) |x\rangle\langle x| \otimes \mathcal{N}(\psi_A^x), \quad |\mathcal{X}| \leq |\mathcal{H}_A|^2,\end{aligned}\tag{7}$$

and the channel coherent information

$$\begin{aligned}I_c(\mathcal{N}) &\equiv \max_{|\phi_{A_1A}\rangle} I(A_1; B)_\omega, \\ \omega_{A_1B} &\equiv (\text{id} \otimes \mathcal{N})(|\phi_{A_1A}\rangle\langle\phi_{A_1A}|), \quad |\mathcal{H}_{A_1}| \leq |\mathcal{H}_A|.\end{aligned}\tag{8}$$

Observe that the Holevo information is maximized over ensembles of pure states, while the quantum capacity is maximized over entangled states. We will see the implications of those properties in the results section. The classical capacity theorem and the quantum capacity theorem are given below.

Theorem 1. The *classical capacity* of a quantum channel $\mathcal{N}_{A \rightarrow B}$ without assistance is given by^{15;16}

$$C(\mathcal{N}) = \lim_{k \rightarrow \infty} \frac{1}{k} \chi(\mathcal{N}^{\otimes k}).\tag{9}$$

Theorem 2. The *quantum capacity* of a quantum channel $\mathcal{N}_{A \rightarrow B}$ without assistance is given by^{18;41–43}

$$Q(\mathcal{N}) = \lim_{k \rightarrow \infty} \frac{1}{k} I_c(\mathcal{N}^{\otimes k}).\tag{10}$$

Next, consider communication with reliable entanglement assistance. The entanglement-assisted capacity formula turns out to be the quantum analog of Shannon's classical formula^{6;7}. Define

$$\begin{aligned}I(\mathcal{N}) &= \max_{|\phi_{A_1A}\rangle} I(A_1; B)_\omega, \\ \omega_{A_1B} &\equiv (\text{id} \otimes \mathcal{N})(|\phi_{A_1A}\rangle\langle\phi_{A_1A}|), \quad |\mathcal{H}_{A_1}| \leq |\mathcal{H}_A|.\end{aligned}\tag{11}$$

Theorem 3. The classical capacity and the quantum capacity of a quantum channel $\mathcal{N}_{A \rightarrow B}$ with reliable entanglement assistance are given by^{6;7}

$$C_{\text{EA}}(\mathcal{N}) = I(\mathcal{N}),\tag{12}$$

$$Q_{\text{EA}}(\mathcal{N}) = \frac{1}{2} I(\mathcal{N}).\tag{13}$$

The classical capacity and the quantum capacity have different units, *i.e.* $C_{\text{EA}}(\mathcal{N})$ is measured in classical information bits per channel use, whereas

$Q_{\text{EA}}(\mathcal{N})$ in information *qubits* per channel use. Nonetheless, the capacity values satisfy $Q_{\text{EA}}(\mathcal{N}) = \frac{1}{2}C_{\text{EA}}(\mathcal{N})$, given reliable entanglement assistance. This relation can be inferred from the fundamental single-unit protocols. Specifically, super-dense coding⁴⁴ is a well known communication protocol whereby two classical bits are transmitted using a single use of a noiseless qubit channel and a maximally entangled pair. In the other direction, by employing the teleportation protocol⁴⁵, qubits can be sent at half the rate of classical bits given entanglement resources.

2 Results

We establish a regularized characterization for the capacity region with unreliable entanglement assistance, for the transmission of either classical information or quantum information.

2.1 Classical Communication

Let $\mathcal{N}_{A \rightarrow B}$ be a given channel, and define

$$\mathcal{R}_{\text{EA}^*}(\mathcal{N}) = \bigcup_{p_X, \varphi_{A_0 A_1}, \mathcal{F}^{(x)}} \left\{ (R, R') : \begin{array}{l} R \leq I(X; B)_\omega \\ R' \leq I(A_1; B|X)_\omega \end{array} \right\} \quad (14)$$

with

$$\omega_{X A_1 A} = \sum_{x \in \mathcal{X}} p_X(x) |x\rangle\langle x| \otimes (\text{id} \otimes \mathcal{F}_{A_0 \rightarrow A}^{(x)})(\varphi_{A_1 A_0}), \quad (15)$$

$$\omega_{X A_1 B} = (\text{id} \otimes \mathcal{N}_{A \rightarrow B})(\omega_{X A_1 A}). \quad (16)$$

Intuitively, the classical variable X is associated with the classical message m , which Bob decodes whether there is entanglement assistance or not. The reference system A_0 can be thought of as Alice's share of the entanglement resources. Since the resources are pre-shared before communication takes place, the entangled state φ is non-correlated with the messages. Alice encodes the message m' using the encoding operator $\mathcal{F}^{(x)}$. Before we state the capacity theorem, we give the following lemma. The property below simplifies the computation of the above region and the achievability proof as well.

Lemma 4. The union in (14) is exhausted by pure states $|\phi_{A_0 A_1}\rangle$ and with the cardinality of $|\mathcal{X}| \leq |\mathcal{H}_A|^2 + 1$.

The restriction to pure states is based on state purification, while the alphabet bound follows from the Fenchel-Eggleston-Carathéodory lemma⁴⁶, using similar arguments that Yard *et al.*⁴⁷ use. The details are given in Appendix B. Our main result on classical communication with unreliable entanglement assistance is stated below.

Theorem 5. The classical capacity region of a quantum channel $\mathcal{N}_{A \rightarrow B}$ with unreliable entanglement assistance satisfies

$$\mathcal{C}_{\text{EA}^*}(\mathcal{N}) = \bigcup_{n=1}^{\infty} \frac{1}{n} \mathcal{R}_{\text{EA}^*}(\mathcal{N}^{\otimes n}). \quad (17)$$

The proof of Theorem 5 is given in Appendix C. In general, there is a trade-off between the rates R and R' , and we cannot necessarily achieve the maximum rate for both of them simultaneously. Intuitively, the excess rate R' that is provided by entanglement assistance depends on the level of entanglement between the ancilla A_1 and the channel input A , or equivalently, on how entanglement-breaking the encoding map is. We give a more precise explanation below.

In the region formula in (14), we have a union over the probability distributions p_X , states $\varphi_{A_0A_1}$, and collections of mappings $\{\mathcal{F}_{A_0 \rightarrow A}^{(x)}\}_{x \in \mathcal{X}}$. The boundary of this region is attained by optimizing over these objects. Observe that in order for R' to achieve the entanglement-assisted capacity, we may set $\varphi_{A_0A_1}$ as the entangled state that attains the maximum in (11), and take $\mathcal{F}_{A_0 \rightarrow A}^{(x)}$ to be the identity map. Since the output has no correlation with X , this assignment achieves the rate pair $(R, R') = (0, C_{\text{EA}}(\mathcal{N}))$ (cf. (11) and (14)).

To maximize the unassisted rate, set an encoding channel $\mathcal{F}_{A_0 \rightarrow A}^{(x)}$ that outputs the pure state $|\psi_A^x\rangle$ that is optimal in (7), *i.e.*

$$\mathcal{F}^{(x)}(\varphi_{A_1A_0}) = \varphi_{A_1} \otimes \psi_A^x. \quad (18)$$

Such an assignment achieves $(R, R') = (\chi(\mathcal{N}), 0)$ (cf. (7) and (14)). In other words, the Holevo information is achieved for an entanglement-breaking encoder.

To illustrate our results, we give an example.

Example 1. Consider the qubit depolarizing channel

$$\mathcal{N}(\rho) = (1 - \varepsilon)\rho + \varepsilon \frac{\mathbb{1}}{2}, \quad (19)$$

with $\varepsilon \in [0, 1]$. The classical capacity without assistance is given by $C(\mathcal{N}) = 1 - H_2\left(\frac{\varepsilon}{2}\right)$, and it is achieved with a symmetric distribution over the ensemble $\{|0\rangle, |1\rangle\}$, where $H_2(t) \equiv -t \log(t) - (1-t) \log(1-t)$ is the binary entropy function⁴⁸. On the other hand, the classical capacity with reliable entanglement assistance is given by $C_{\text{EA}}(\mathcal{N}) = 2 - H\left(1 - \frac{3\varepsilon}{4}, \frac{\varepsilon}{4}, \frac{\varepsilon}{4}, \frac{\varepsilon}{4}\right)$, and it is achieved with a maximally entangled input state⁶.

A natural compromise is to mix the strategies above. Let Z be an independent random bit that chooses between the strategies, where $Z \sim \text{Bernoulli}(\lambda)$ for a given $\lambda \in [0, 1]$. That is, we define $\mathcal{F}^{(x,z)}$ by $\mathcal{F}^{(x,0)}(\rho_A) = \psi_A^x$ and $\mathcal{F}^{(x,1)} = \text{id}$. Plugging $\tilde{X} \equiv (X, Z)$, we obtain the time-division achievable region,

$$\mathcal{R}_{\text{EA}^*}(\mathcal{N}) \supseteq \bigcup_{0 \leq \lambda \leq 1} \left\{ (R, R') : \begin{array}{l} R \leq (1 - \lambda)C(\mathcal{N}) \\ R' \leq \lambda C_{\text{EA}}(\mathcal{N}) \end{array} \right\}. \quad (20)$$

Next, we numerically compute an achievable region that outperforms the time-division bound. Instead of using a classical mixture of the strategies, we use quantum superposition. Define a non-normalized vector,

$$|u_\beta\rangle \equiv \sqrt{1 - \beta}|0\rangle \otimes |0\rangle + \sqrt{\beta}|1\rangle \otimes |\Phi\rangle. \quad (21)$$

Then, set

$$|\phi_{A_0A_1}\rangle \equiv \frac{1}{\|u_\beta\|} |u_\beta\rangle, \quad (22)$$

$$p_X = \left(\frac{1}{2}, \frac{1}{2}\right), \quad (23)$$

$$\mathcal{F}^{(x)}(\rho) \equiv X^x \rho X^x, \quad (24)$$

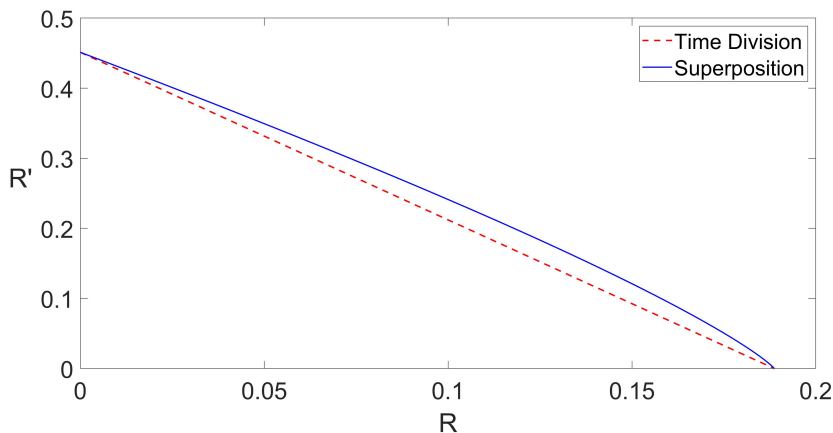


Figure 4: Achievable classical rate regions for the depolarizing channel with unreliable entanglement assistance, for a depolarization probability $\varepsilon = \frac{1}{2}$.

where X is the bitflip Pauli operator. Observe that for $\beta = 0$, the input state is $\mathcal{F}^{(x)}(|0\rangle\langle 0|) = |x\rangle\langle x|$, which achieves the classical capacity without assistance. On the other hand, for $\beta = 1$, the parameter x chooses one of two Bell states.

Figure 4 depicts the resulting region for a depolarization probability of $\varepsilon = \frac{1}{2}$. The triangular region below the dashed red line is the time-division bound, which is obtained by a classical mixture, whereas the solid blue line indicates the achievable region corresponding to the superposition state $\frac{|u_\beta\rangle}{\|u_\beta\|}$, as in (21).

For a noiseless qubit channel, time division is optimal.

Corollary 6. The classical capacity region of a noiseless qubit channel with unreliable entanglement assistance is given by the time-division region, *i.e.*

$$\mathcal{C}_{\text{EA}^*}(\text{id}) = \bigcup_{0 \leq \lambda \leq 1} \left\{ (R, R') : \begin{array}{l} R \leq 1 - \lambda \\ R' \leq 2\lambda \end{array} \right\}. \quad (25)$$

Proof. As explained in the introduction, to achieve the rate pair $(R, R') = (1 - \lambda, 2\lambda)$, Alice and Bob simply perform super-dense coding repeatedly, over a fraction of λ of the block, and communicate over the 0-1 basis in the remaining part. To show the converse part, let $(R, R') \in \frac{1}{n} \mathcal{R}_{\text{EA}^*}(\mathcal{N}^{\otimes n})$ (see (16)), hence

$$\begin{aligned} R &\leq \frac{1}{n} I(X; B^n)_\omega = \frac{1}{n} [H(B^n)_\omega - H(B^n|X)_\omega] \\ &\leq 1 - \frac{1}{n} H(B^n|X)_\omega \end{aligned} \quad (26)$$

and

$$\begin{aligned} R' &\leq \frac{1}{n} I(A_1; B^n|X)_\omega \\ &\leq \frac{1}{n} \cdot 2H(B^n|X)_\omega. \end{aligned} \quad (27)$$

The last inequality holds since the quantum conditional entropy satisfies $|H(B|A)_\rho| \leq H(B)_\rho$ in general, hence $H(B^n|A_1X)_\omega = \sum_x p_X(x)H(B^n|A_1, X=x)_\omega \geq -\sum_x p_X(x)H(B^n|X=x)_\omega = -H(B^n|X)_\omega$. The converse part for the corollary follows, as we define $\lambda \equiv \frac{1}{n}H(B^n|X)_\omega$. \square

2.2 Quantum Communication

Consider quantum communication over $\mathcal{N}_{A \rightarrow B}$ with unreliable entanglement assistance. Define

$$\mathcal{L}_{\text{EA}^*}(\mathcal{N}) = \bigcup_{\varphi_{A_1 A_2 A}} \left\{ (Q, Q') : \begin{array}{l} Q \leq \min\{I(A_1|B)_\omega, H(A_1|A_2)_\omega\}, \\ Q + Q' \leq \frac{1}{2}I(A_2; B)_\omega \end{array} \right\} \quad (28)$$

with

$$\omega_{A_1 A_2 B} = (\text{id} \otimes \mathcal{N}_{A \rightarrow B})(\varphi_{A_1 A_2 A}). \quad (29)$$

Theorem 7. The quantum capacity region of a quantum channel $\mathcal{N}_{A \rightarrow B}$ with unreliable entanglement assistance satisfies

$$\mathcal{Q}_{\text{EA}^*}(\mathcal{N}) = \bigcup_{n=1}^{\infty} \frac{1}{n} \mathcal{L}_{\text{EA}^*}(\mathcal{N}^{\otimes n}). \quad (30)$$

The proof of Theorem 7 is given in Appendix D.

3 Summary and Discussion

We summarize our results and compare the techniques in our work and in previous works. We consider communication over a quantum channel $\mathcal{N}_{A \rightarrow B}$, where Alice and Bob are provided with *unreliable* entanglement resources. Suppose that Alice wishes to send two messages, at rates R and R' . She encodes both messages using her share of the entanglement resources, as she does not know whether Bob will have access to the entangled resources. Bob has two decoding procedures. If the entanglement assistance has failed to reach Bob's location, he performs a decoding operation to recover the first message alone. Hence, the communication system operates on a rate R . Whereas if Bob has entanglement assistance, he decodes both messages, hence the overall transmission rate is $R + R'$. In other words, R is a *guaranteed rate*, and R' is the *excess rate* of information that entanglement assistance provides. The communication setting is illustrated in Figure 2, in which the resource uncertainty is represented by the unknown position of a switch.

We define the capacity region as the set of all rate pairs (R, R') that can be achieved with asymptotically vanishing decoding errors.

In the transmission of quantum information, Alice chooses a product state $\theta_M \otimes \xi_{\bar{M}}$ over Hilbert spaces of dimension $|\mathcal{H}_M| = 2^{nQ}$ and $|\mathcal{H}_{\bar{M}}| = 2^{n(Q+Q')}$. Alice encodes the input state by applying the encoding channel $\mathcal{F}_{G_A M \bar{M} \rightarrow A^n}$ to M, \bar{M} , and to her share of the entangled state Ψ_{G_A, G_B} , and transmits the system A^n over n channel uses of $\mathcal{N}_{A \rightarrow B}$. Bob receives the channel output systems B^n . If the entanglement assistance is present, then he applies the decoding channel

\mathcal{D} to the joint output $B^n G_B$ in order to recover ξ_M . Otherwise, if entanglement assistance is absent, then he performs \mathcal{D}^* on B^n in order to recover θ_M .

We have established a regularized characterization for the classical and quantum capacity regions. The communication design makes a compromise. We have seen that the unassisted rate is high when the channel input is in a pure state. Such an assignment achieves $(R, R') = (\chi(\mathcal{N}), 0)$, where $\chi(\mathcal{N})$ is the Holevo information of the channel. On the other hand, high excess rates are achieved when the encoder preserves the entanglement between the input system and the ancilla (see (14)). Such an encoding operation achieves the rate pair $(R, R') = (0, C_{\text{EA}}(\mathcal{N}))$, where $C_{\text{EA}}(\mathcal{N})$ is the entanglement-assisted capacity. Time division between these coding strategies achieves the rate pairs $(R, R') = ((1 - \lambda)\chi(\mathcal{N}), \lambda C_{\text{EA}}(\mathcal{N}))$, for $0 \leq \lambda \leq 1$.

In the simple scenario of classical communication over a noiseless qubit channel, we have shown that the optimal strategy is to perform time division between super-dense coding and unassisted transmission over the 0-1 basis (see Figure 1). For the noiseless qubit channel, the classical capacity region with unreliable entanglement assistance is thus $\mathcal{C}_{\text{EA}^*}(\mathcal{N}) = \bigcup_{0 \leq \lambda \leq 1} \{(R, R') : R \leq 1 - \lambda, R' \leq 2\lambda\}$. On the other hand, for the depolarizing channel, time division is strictly sub-optimal.

Next, we discuss capacity computation, the cloud superposition-coding interpretation of our results, the side-information interpretation, and the consequences on the quantum broadcast channel with one-sided entanglement assistance.

3.1 Computing Channel Capacities

For communication system design nowadays, it is crucial to evaluate the current performance and how close it is to the optimum^{49;50}. Classical commercial systems today already employ sophisticated error correction codes with near-Shannon limit performance^{51;52}. At the time of writing, a realization of a full-scale quantum communication system that approaches the Shannon-theoretic limits does not exist, and we can only hope that future systems of quantum communication will reach this level of maturity. Given a specific quantum channel, e.g. an optical fiber channel with specific parameters, a practitioner is usually interested in computing the channel capacity as a number. For such practical purposes, a regularized characterization as in Theorems 1-2 and 5-7 is not necessarily a problem (see a further explanation in Remark 7 by the authors²⁸). Yet, in Shannon theory, it is generally considered desirable to establish a single-letter computable capacity formula^{53;54}. Beyond computability, the disadvantage of a regularized multi-letter formula of the form $\lim_{n \rightarrow \infty} \frac{1}{n} \mathbf{F}(\mathcal{N}^{\otimes n})$, is that such characterization is not unique (see⁵⁵Section 13.1.3).

Under practical encoding constraints⁵⁴, regularized capacity results yield computable formulas. Encoding constraints are particularly relevant when the transmitter has access to a cluster of multiple small or moderate-size quantum computers without interaction between them, and also in nearest-neighbor qubit architectures^{56;57}. Consider classical communication without assistance, as in Theorem 1, and suppose that the encoder's quantum systems A^n are partitioned into sub-blocks of a small size b , such that the input state has the form $\rho_{A^n} = \rho_{A_1^b} \otimes \rho_{A_{b+1}^{2b}} \otimes \cdots \otimes \rho_{A_{n-b+1}^b}$. As recently observed⁵⁴, the capacity of a quantum

channel $\mathcal{N}_{A \rightarrow B}$ under an encoding constraint $b > 0$, is given by

$$C(\mathcal{N}, b) = \frac{1}{b} \chi(\mathcal{N}^{\otimes b}). \quad (31)$$

This formula is computable, since $b > 0$ is assumed to be a small constant. This trivial observation and its consequences can be extended to other models as well.

Another shortcoming of our results is that we do not have a bound on the dimension of the ancillas A_0 , A_1 , and A_2 . One could always compute an achievable region by simply choosing the dimension of A_ℓ , $\ell \in \{1, 2, 3\}$. However, the optimal rates cannot be computed with absolute precision in general. A similar difficulty appears in other quantum models such as broadcast communication⁵⁸ Section VIII, the wiretap channel⁵⁹ Remark 5, squashed entanglement⁶⁰ Section 1, and state-dependent channels^{61,28} Section V.

3.2 Superposition-Coding Interpretation

Our model has a deep relation to the quantum broadcast channel. Before we give the precise formulation, we point out a heuristic connection. The characterization of the classical capacity region in Theorem 5 clearly resembles the classical superposition-coding region of the broadcast channel without assistance⁶² (see Theorem 2 therein). The difference is that here the encoding involves quantum operations. Nevertheless, we can portray a similar metaphorical image: Let m be an index over 2^{nR} clouds. Recall that the region formula in (14) involves an ancillary state $\varphi_{A_0 A_1}$ and a collection of encoding mappings $\{\mathcal{F}_{A_0 \rightarrow A}^{(x)}\}_{x \in \mathcal{X}}$. Each cloud center is associated with a classical codeword $x^n(m)$, and at the center of each cloud there is the state $\otimes_{i=1}^n \mathcal{F}^{x_i(m)}(\varphi)$. Applying random Pauli operators that encode the message m' takes us from the cloud center to a satellite on the cloud that depends on both m and m' . The channel input is the satellite state. Bob decodes in two steps. First, Bob recovers the cloud, *i.e.* he estimates m . If the entanglement assistance is absent, then Bob quits after the first step. Otherwise, if Bob has entanglement assistance, then he continues to decode the satellite m' .

3.3 Side Information Interpretation

We mentioned in the previous section that our classical coding scheme can be interpreted as a superposition code. Consider the second decoding step for the message m' . As the message m has already been estimated, we can think of $x^n(m)$ as side information for this decoding operation. Thus, it is not surprising that the bound on the excess rate R' in (14) has a similar form as in the capacity formula for a quantum channel with classical side information at the encoder and the decoder (see⁶³ Corollary 12).

For the quantum capacity region, we point out a connection to quantum side information. A quantum state-dependent channel $(\mathcal{P}_{SA \rightarrow B}, |\theta_{SS_0}\rangle)$ is defined by a linear, completely positive, trace preserving map $\mathcal{P}_{SA \rightarrow B}$ and a fixed quantum state $|\theta_{SS_0}\rangle$ ^{61;64}. We refer to the system S as a quantum channel state. Given quantum side information, the encoder has access to the system S_0 , which is entangled with the channel state system S . This model can be interpreted as if the channel is entangled with the systems S and S_0 . The quantum capacity

with quantum side information and no assistance is given by the regularization of the following formula (see²⁸Theorem 11),

$$L(\mathcal{P}) = \sup_{\varphi_{A_1 S A} : \varphi_S = \theta_S} \min\{I(A_1|B)_\omega, H(A_1|S)_\varphi\}, \quad (32)$$

with $\omega_{A_1 B} = \mathcal{P}_{SA \rightarrow B}(\varphi_{A_1 S A})$. Thus, we interpret the guaranteed rate Q in (28) as the quantum coding rate, given a channel state A_2 .

3.4 The Broadcast Channel with One-Sided Assistance

Beyond the heuristic connection above, the mathematical formulation of our problem is close to that of a broadcast channel with one-sided assistance. Let $\mathcal{N}_{A \rightarrow B_1 B_2}^{\text{broadcast}}$ be a quantum broadcast channel with two receivers, Bob 1 and Bob 2. Suppose that Alice wishes to send a common message $m_0 \in [1 : 2^{nR_0}]$ to both users and a dedicated message $m_1 \in [1 : 2^{nR_1}]$ to the first user alone. That is, Bob 1 decodes both m_0 and m_1 , while Bob 2 is only required to decode m_0 . This model is referred to as the broadcast channel with degraded message sets⁶². Now, assume that Alice and Bob 1 share reliable entanglement resources $\Psi_{G_A, G_{B_1}}$, while Bob 2 has no resources at all.

The error criterion is the probability that at least one of the receivers decodes erroneously. However, it is sufficient to consider each receiver separately, since the coding performance depends on the broadcast channel $\mathcal{N}_{A \rightarrow B_1 B_2}^{\text{broadcast}}$ only through the marginals $\mathcal{N}_{A \rightarrow B_1}^{(1)}$ and $\mathcal{N}_{A \rightarrow B_2}^{(2)}$ ⁶⁵,

$$\mathcal{N}^{(1)}(\rho_A) \equiv \text{Tr}_{B_2}(\mathcal{N}^{\text{broadcast}}(\rho_A)), \quad (33)$$

$$\mathcal{N}^{(2)}(\rho_A) \equiv \text{Tr}_{B_1}(\mathcal{N}^{\text{broadcast}}(\rho_A)). \quad (34)$$

Hence, achievable rate pairs (R_0, R_1) can be defined in terms of the following error probabilities,

$$P_{e1|m_0, m_1}^{(n)}(\mathcal{F}, \Psi, \mathcal{D}^{(1)}) = 1 - \text{Tr}[D_{m_0, m_1}^{(1)}(\mathcal{N}_{A \rightarrow B_1}^{(1)\otimes n} \otimes \text{id})(\mathcal{F}^{m_0, m_1} \otimes \text{id})(\Psi_{G_A, G_{B_1}})] \quad (35)$$

for Bob 1, and

$$P_{e2|m_0, m_1}^{(n)}(\mathcal{F}, \Psi, \mathcal{D}^{(2)}) = 1 - \text{Tr}[D_m^{(2)} \mathcal{N}_{A \rightarrow B_2}^{(2)\otimes n} \mathcal{F}^{m_0, m_1}(\Psi_{G_A})] \quad (36)$$

for Bob 2, where $\mathcal{F}_{G_A \rightarrow A^n}^{m_0, m_1}$ is the encoding map, while $\mathcal{D}_{G_{B_1} B_1^n}^{(1)} = \{D_{m_0, m_1}^{(1)}\}$ and $\mathcal{D}_{B_2^n}^{(2)} = \{D_{m_0}^{(2)}\}$ are the decoding maps of Bob 1 and Bob 2, respectively.

Observe that the error definitions above are analogous to those of the classical capacity region with unreliable entanglement assistance in Section 1, where m and m' are replaced by m_0 and m_1 , respectively. Although, the error probabilities for the broadcast channel depend on two different channels, $\mathcal{N}^{(1)}$ and $\mathcal{N}^{(2)}$. The same methods as we used in this paper show that the classical capacity region of the quantum broadcast channel with one-sided entanglement assistance is given by the regularization of the following formula,

$$\mathcal{R}_2(\mathcal{N}^{\text{broadcast}}) = \bigcup_{p_X, \varphi_{A_0 A_1}, \mathcal{F}^{(x)}} \left\{ \begin{array}{l} (R_0, R_1) : R_0 \leq I(X; B_2)_\omega \\ R_1 \leq I(A_1; B_1|X)_\omega \\ R_0 + R_1 \leq I(XA_1; B_1)_\omega \end{array} \right\} \quad (37)$$

with

$$\omega_{XA_1A} = \sum_{x \in \mathcal{X}} p_X(x) |x\rangle\langle x| \otimes (\text{id} \otimes \mathcal{F}_{A_0 \rightarrow A}^{(x)})(\varphi_{A_1A_0}), \quad (38)$$

$$\omega_{XA_1B_1B_2} = (\text{id} \otimes \mathcal{N}_{A \rightarrow B_1B_2}^{\text{broadcast}})(\rho_{XA_1A}). \quad (39)$$

It is now natural to wonder whether this similarity extends to the quantum capacity. However, in the transmission of quantum information, Bob 1 and Bob 2 cannot recover a common state due to the no-cloning theorem. That is, quantum communication with degraded message sets is not well defined (see ⁶⁵Section III.C). Yet, the techniques of Dupuis *et al.* ^{58;66} for the quantum broadcast channel with dedicated messages were useful in our proof in Appendix D, for the quantum capacity theorem with unreliable entanglement assistance.

Data Availability

No data sets were generated during this study

Competing interests

The authors declare no competing interests.

Grant information

U. Pereg and H. Boche were supported by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany’s Excellence Strategy – EXC-2111 – 390814868. In addition, U. Pereg, C. Deppe, and H. Boche were supported by the German Federal Ministry of Education and Research (BMBF) through Grants 16KISQ028 (Pereg, Deppe) and 16KISQ020 (Boche). This work of H. Boche was supported in part by the BMBF within the national initiative for “Post Shannon Communication (NewCom)” under Grant 16KIS1003K, and in part by the DFG within the Gottfried Wilhelm Leibniz Prize under Grant BO 1734/20-1 and within Germany’s Excellence Strategy EXC-2092 – 390781972. U. Pereg was also supported by the Israel CHE Fellowship for Quantum Science and Technology.

Acknowledgments

The authors wish to thank Christoph Becher (Universität des Saarlandes) for useful discussions, Elizabeth Söder for the English review, and Mohammad J. Salariseddigh for his technical support in preparing the figures.

A Information-Theoretic Tools

In this section, we give the basic information-theoretic tools that will be used in the achievability proofs later on.

A.1 Quantum Packing Lemma

To prove achievability for the classical capacity theorem, we will use the quantum packing lemma. Standard method-of-types concepts are defined as usual^{55,54}. We briefly introduce the notation and basic properties while the detailed definitions can be found in the references⁵⁴. In particular, given a density operator $\rho = \sum_x p_X(x) |x\rangle\langle x|$ on the Hilbert space \mathcal{H}_A , we let $\mathcal{A}^\delta(p_X)$ denote the δ -typical set that is associated with p_X , and $\Pi_{A^n}^\delta(\rho)$ the projector onto the corresponding subspace. The following inequalities follow from well-known properties of δ -typical sets⁶⁷,

$$\mathrm{Tr}(\Pi^\delta(\rho)\rho^{\otimes n}) \geq 1 - \varepsilon \quad (40)$$

$$2^{-n(H(\rho)+c\delta)}\Pi^\delta(\rho) \preceq \Pi^\delta(\rho)\rho^{\otimes n}\Pi^\delta(\rho) \preceq 2^{-n(H(\rho)-c\delta)} \quad (41)$$

$$\mathrm{Tr}(\Pi^\delta(\rho)) \leq 2^{n(H(\rho)+c\delta)} \quad (42)$$

where $c > 0$ is a constant. Furthermore, for $\sigma_B = \sum_x p_X(x)\rho_B^x$, let $\Pi_{B^n}^\delta(\sigma_B|x^n)$ denote the projector corresponding to the conditional δ -typical set given the sequence x^n . Similarly⁵⁵,

$$\mathrm{Tr}(\Pi^\delta(\sigma_B|x^n)\rho_{B^n}^{x^n}) \geq 1 - \varepsilon' \quad (43)$$

$$\begin{aligned} 2^{-n(H(B|X')_\sigma+c'\delta)}\Pi^\delta(\sigma_B|x^n) &\preceq \Pi^\delta(\sigma_B|x^n)\rho_{B^n}^{x^n}\Pi^\delta(\sigma_B|x^n) \\ &\preceq 2^{-n(H(B|X')_\sigma-c'\delta)} \end{aligned} \quad (44)$$

$$\mathrm{Tr}(\Pi^\delta(\sigma_B|x^n)) \leq 2^{n(H(B|X')_\sigma+c'\delta)} \quad (45)$$

where $c' > 0$ is a constant, $\rho_{B^n}^{x^n} = \bigotimes_{i=1}^n \rho_{B_i}^{x_i}$, and the classical random variable X' is distributed according to the type of x^n . If $x^n \in \mathcal{A}^\delta(p_X)$, then

$$\mathrm{Tr}(\Pi^\delta(\sigma_B)\rho_{B^n}^{x^n}) \geq 1 - \varepsilon' \quad (46)$$

as well (see⁵⁵ Property 15.2.7).

The lemma below is a simplified version of the quantum packing lemma in⁶⁸. *Lemma 8* (Quantum Packing Lemma⁶⁸). Let

$$\rho = \sum_{x \in \mathcal{X}} p_X(x)\rho_x, \quad (47)$$

where $\{p_X(x), \rho_x\}_{x \in \mathcal{X}}$ is a given ensemble. Furthermore, suppose that there is a code projector Π and codeword projectors Π_{x^n} , $x^n \in \mathcal{A}^\delta(p_X)$, that satisfy for every $\alpha > 0$ and sufficiently large n ,

$$\mathrm{Tr}(\Pi\rho_{x^n}) \geq 1 - \alpha \quad (48)$$

$$\mathrm{Tr}(\Pi_{x^n}\rho_{x^n}) \geq 1 - \alpha \quad (49)$$

$$\mathrm{Tr}(\Pi_{x^n}) \leq 2^{nd} \quad (50)$$

$$\Pi\rho^{\otimes n}\Pi \preceq 2^{-n(D-\alpha)}\Pi \quad (51)$$

for some $0 < d < D$ with $\rho_{x^n} \equiv \bigotimes_{i=1}^n \rho_{x_i}$. Then, there exist codewords $x^n(m)$, $m \in [1 : 2^{nR}]$, and a POVM $\{\Lambda_m\}_{m \in [1:2^{nR}]}$, such that

$$\mathrm{Tr}(\Lambda_m\rho_{x^n(m)}) \geq 1 - 2^{-n[D-d-R-\varepsilon_n(\alpha)]} \quad (52)$$

for all $m \in [1 : 2^{nR}]$, where $\varepsilon_n(\alpha)$ tends to zero as $n \rightarrow \infty$ and $\alpha \rightarrow 0$.

A.2 The Decoupling Theorem

To prove achievability for the quantum capacity theorem, we will use the decoupling theorem⁶⁶. Before we state the theorem, we give an intuitive explanation in the spirit of⁵⁵ Section 24.10. Consider a quantum channel $\mathcal{N}_{A \rightarrow B}$ without entanglement assistance. Let $|\theta_{MK}\rangle$ be a purification of the quantum message state θ_M , where K is Alice's reference system. Suppose that $|\psi_{KE^n E^n J_1}\rangle$ is a purification of the joint state of Alice's reference system K , the channel output B^n , and Bob's environment E^n , with a purifying system J_1 . Observe that if the reduced state $\psi_{KE^n J_1}$ is a product state, i.e. $\psi_{KE^n J_1} = \theta_K \otimes \omega_{E^n J_1}$, then it has a purification of the form $|\theta_{MK}\rangle \otimes |\omega_{E^n J_1 J_2}\rangle$. Since all purifications are related by isometries⁵⁵ Theorem 5.1.1, there exists an isometry $D_{B^n \rightarrow M J_2}$ such that $|\theta_{MK}\rangle \otimes |\omega_{E^n J_1 J_2}\rangle = D_{B^n \rightarrow M J_2} |\psi_{KE^n E^n J_1}\rangle$. Tracing out K , E^n , J_1 , and J_2 , it follows that there exists a decoding map $\mathcal{D}_{B^n \rightarrow M}$ that recovers the message state, i.e. $\theta_M = \mathcal{D}_{B^n \rightarrow M}(\psi_{B^n})$. Therefore, in order to show that there exists a reliable coding scheme, it is sufficient to encode in such a manner that approximately decouples between Alice's reference system and Bob's environment, i.e., such that $\psi_{KE^n J_1} \approx \theta_K \otimes \omega_{E^n J_1}$.

We will make use of the following definitions from⁶⁹. Define the conditional min-entropy by

$$\begin{aligned} H_{\min}(\rho_{AB}|\sigma_B) &= -\log \inf \{ \lambda \in \mathbb{R} : \rho_{AB} \preceq \lambda \cdot (\mathbb{1}_A \otimes \sigma_B) \} \\ H_{\min}(A|B)_\rho &= \sup_{\sigma_B} H_{\min}(\rho_{AB}|\sigma_B), \end{aligned} \quad (53)$$

where the supremum is over quantum states of the system B . In general, the conditional min-entropy is bounded by

$$-\log |\mathcal{H}_B| \leq H_{\min}(A|B)_\rho \leq \log |\mathcal{H}_A|. \quad (54)$$

To see this, observe that if we choose $\sigma_B = \frac{\mathbb{1}_B}{|\mathcal{H}_B|}$, then the matrix inequality $\rho_{AB} \preceq \lambda(\mathbb{1}_A \otimes \sigma_B)$ holds for $\lambda = |\mathcal{H}_B|$, hence $H_{\min}(\rho_{AB}|\sigma_B) \geq -\log |\mathcal{H}_B|$. As for the upper bound, the matrix inequality implies that $1 = \text{Tr}(\rho_{AB}) \leq \lambda |\mathcal{H}_A| \text{Tr}(\sigma_B) = \lambda |\mathcal{H}_A|$, hence $H_{\min}(\rho_{AB}|\sigma_B) \leq \log |\mathcal{H}_A|$. Furthermore, the lower bound is saturated when the joint state of A and B is $|\Phi_{AB}\rangle$, whereas the upper bound for a product state $\frac{\mathbb{1}_A}{|\mathcal{H}_A|} \otimes \rho_B$.

Then, define the smoothed min-entropy by

$$H_{\min}^\varepsilon(A|B)_\rho = \max_{\sigma_{AB} : d_F(\rho_{AB}, \sigma_{AB}) \leq \varepsilon} H_{\min}^\varepsilon(A|B)_\sigma \quad (55)$$

for arbitrarily small $\varepsilon > 0$, where $d_F(\rho, \sigma) = \sqrt{1 - \|\sqrt{\rho}\sqrt{\sigma}\|_1^2}$ is the fidelity distance between the states. As for the von Neumann entropy, conditioning cannot increase the smoothed min-entropy, i.e. $H_{\min}^\varepsilon(A|BC)_\rho \leq H_{\min}^\varepsilon(A|B)_\rho$ ⁶⁹ Lemma 3.1.7. The theorem below follows from Dupuis' results (see⁶⁶ Lemma 2.3 and Theorem 3.8).

Theorem 9 (Decoupling Theorem⁶⁶). Let $\theta_{A_1 K}$ be a quantum state, $\mathcal{T}_{A_1 \rightarrow E}$ a quantum channel, and $\varepsilon > 0$ arbitrary. Define

$$\omega_{AE} = \mathcal{T}_{A_1 \rightarrow E}(\Phi_{A_1 A}). \quad (56)$$

Then,

$$\int_{\mathbb{U}_{A_1}} \|\mathcal{T}_{A_1 \rightarrow E}(U_{A_1} \rho_{A_1 K}) - \omega_E \otimes \theta_K\|_1 dU_{A_1} \leq 2^{-\frac{1}{2}[H_{\min}^\varepsilon(A|E)_\omega + H_{\min}^\varepsilon(A_1|K)_\rho]} + 8\varepsilon \quad (57)$$

where the integral is over the Haar measure on all unitaries U_A .

The decoupling theorem shows that by choosing a unitary U_A uniformly at random, we can approximately decouple between E and K provided that $H_{\min}^\varepsilon(A|E)_\omega > -H_{\min}^\varepsilon(A_1|K)_\rho$. Uhlmann's theorem⁷⁰ is often used along with the decoupling approach to establish the existence of proper encoding and decoding operations.

Theorem 10 (Uhlmann's theorem^{70 66} Corollary 3.2). For every pair of pure states $|\psi_{AB}\rangle$ and $|\theta_{AC}\rangle$ that satisfy $\|\psi_A - \theta_A\|_1 \leq \varepsilon$, there exists an isometry $F_{B \rightarrow C}$ such that $\|(\mathbb{1} \otimes F_{B \rightarrow C})\psi_{AB} - \theta_{AC}\|_1 \leq 2\sqrt{\varepsilon}$.

B Proof of Lemma 4

Consider the region $\mathcal{R}_{\text{EA}^*}(\mathcal{N})$ as defined in (14). Fix $\varphi_{A_0 A_1}$, $p_X(x)$, and $\{\mathcal{F}_{A_0 \rightarrow A}^{(x)}\}$. Let

$$R = I(X; B)_\omega, \quad (58)$$

$$R' = I(A_1; B|X)_\omega. \quad (59)$$

We prove the lemma using similar techniques as in Pereg^{54;71}. It is easy to see that pure states are sufficient, as every quantum state $\varphi_{A_0 A_1}$ has a purification $|\phi_{A_0 J_0 A_1}\rangle$. Since A_0 is arbitrary, we can extend it and obtain the same characterization when A_0 is replaced by $\bar{A}_0 = (A_0, J_0)$.

To bound the alphabet size of the random variable X , we use the Fenchel-Eggleston-Carathéodory lemma⁴⁶ and similar arguments as in previous works^{47;54}. Having fixed $\varphi_{A_0 A_1}$ and $\{\mathcal{F}_{A_0 \rightarrow A}^{(x)}\}$, define

$$\omega_A^x \equiv \mathcal{F}_{A_0 \rightarrow A}^{(x)}(\varphi_{A_0}). \quad (60)$$

Every quantum state ρ_A has a unique and real parametric representation $u(\rho_A)$ of dimension $|\mathcal{H}_A|^2 - 1$ (see⁵⁴ Appendix B-B). Then, define a map $g : \mathcal{X} \rightarrow \mathbb{R}^{|\mathcal{H}_A|^2 + 1}$ by

$$g(x) = (u(\omega_A^x), H(B|X = x)_\omega, I(A_1; B|X = x)_\omega). \quad (61)$$

The map g can be extended to probability distributions as follows:

$$G : p_X \mapsto \sum_{x \in \mathcal{X}} p_X(x) g(x) = (u(\omega_A), H(B|X)_\omega, I(A_1; B|X)_\omega), \quad (62)$$

as $\omega_A = \sum_x p_X(x) \omega_A^x$. According to the Fenchel-Eggleston-Carathéodory lemma⁴⁶, any point in the convex closure of a connected compact set within \mathbb{R}^d belongs to the convex hull of d points in the set. Since the map G is linear, it maps the set of distributions on \mathcal{X} to a connected compact set in $\mathbb{R}^{|\mathcal{H}_A|^2 + 1}$. Thus, for every p_X , there exists a probability distribution $p_{\bar{X}}$ on a subset $\bar{\mathcal{X}} \subseteq \mathcal{X}$

of size $|\mathcal{H}_A|^2 + 1$, such that $G(p_{\bar{X}}) = G(p_X)$. We deduce that the cardinality of X can be restricted to $|\mathcal{X}| \leq |\mathcal{H}_A|^2 + 1$, while preserving ω_A , and thus, the output state $\omega_B \equiv \mathcal{N}(\omega_A)$ as well, and the mutual informations $I(X; B)_\omega = H(B)_\rho - H(B|X)_\omega$ and $I(A_1; B|X)_\omega$.

This completes the proof of the lemma. \square

C Proof of Theorem 5

Consider classical communication over a quantum channel $\mathcal{N}_{A \rightarrow B}$ with unreliable entanglement assistance.

C.1 Achievability Proof

We show that for every $\varepsilon_0, \delta_0 > 0$, there exists a $(2^{n(R-\delta_0)}, 2^{n(R'-\delta_0)}, n, \varepsilon_0)$ code with unreliable entanglement assistance, provided that $(R, R') \in \mathcal{R}_{\text{EA}^*}(\mathcal{N})$. To this end, we will use the quantum packing lemma⁶⁸, as presented in Subsection A.1 of the previous appendix. Recall that by Lemma 4, it suffices to consider pure states. Then, let $|\phi_{G_1 G_2}\rangle$ be a pure entangled state on $\mathcal{H}_{A_0} \otimes \mathcal{H}_{A_0}$, and $\mathcal{F}^{(x)}$ be a quantum channel acting on $\mathcal{S}(\mathcal{H}_{A_0})$ (see (14)-(16)). Suppose that Alice and Bob share $|\phi_{G_1 G_2}\rangle^{\otimes n}$.

As we explain below, we can restrict ourselves to isometric encoding maps. For a moment, let us denote the channel input by S , and consider the channel $\mathcal{N}_{S \rightarrow B}$. In the derivation below, we will use the encoding channel $\mathcal{F}_{A_0 \rightarrow S}^{(x)}$. Every quantum channel $\mathcal{F}_{A_0 \rightarrow S}^{(x)}$ has an isometric extension $F_{A_0 \rightarrow S\check{S}}^{(x)}$. Since it is an encoding mapping, we may as well take \check{S} to be Alice's ancilla. Then, let $A \equiv S\check{S}$ be the augmented channel input. We are effectively coding over the channel $\tilde{\mathcal{N}}_{A \rightarrow B}$, which is defined by

$$\tilde{\mathcal{N}}_{A \rightarrow B}(\rho_{S\check{S}}) \equiv \mathcal{N}_{S \rightarrow B}(\text{Tr}_{\check{S}}(\rho_{S\check{S}})), \quad (63)$$

using the isometric map $F_{A_0 \rightarrow A}^{(x)}$.

From this point, we will focus on the quantum channel $\tilde{\mathcal{N}}_{A \rightarrow B}$ and use the encoding isometry $F_{A_0 \rightarrow A}^{(x)}$. Define

$$|\psi_{AG_2}^x\rangle = (F^{(x)} \otimes \mathbb{1})|\phi_{G_1 G_2}\rangle, \quad (64)$$

$$\omega_{BG_2}^x = (\tilde{\mathcal{N}} \otimes \text{id})(\psi_{AG_2}^x). \quad (65)$$

We will often use the notation $|\psi^{x^n}\rangle \equiv \bigotimes_{i=1}^n |\psi^{x_i}\rangle$. The code construction, encoding and decoding procedures are described below.

C.1.1 Code Construction

First, consider a classical codebook. Let $\{x^n(m)\}_{m \in [1:2^{nR}]}$ be a set of 2^{nR} classical codewords that will be chosen later, in Subsection C.1.5 below. We define the encoding operators in terms of this classical codebook. Denote the Heisenberg-Weyl operators of dimension D by $\{\Sigma(a, b) = \Sigma_X^a \Sigma_Z^b\}$, where $\Sigma_X = \sum_{j=0}^{D-1} |j \oplus 1\rangle\langle j|$ and $\Sigma_Z = \sum_{j=0}^{D-1} e^{2\pi i j/D} |j\rangle\langle j|$, for $a, b \in \{0, 1, \dots, D-1\}$, with $j \oplus k = (j + k) \bmod D$ and $i = \sqrt{-1}$.

Consider a Schmidt decomposition of the pure state in (64),

$$|\psi_{AG_2}^x\rangle = \sum_{z \in \mathcal{Z}} \sqrt{p_{Z|X}(z|x)} |\xi_{z,x}\rangle \otimes |\xi'_{z,x}\rangle, \quad (66)$$

where $p_{Z|X}$ is a conditional probability distribution, while $\{|\xi_{z,x}\rangle\}$ and $\{|\xi'_{z,x}\rangle\}$ are orthonormal sets. For every $x^n \in \mathcal{X}^n$ and every conditional type class $\mathcal{T}_n(t|x^n)$ in \mathcal{Z}^n , define the operators

$$\begin{aligned} V_t(a_t, b_t, c_t) &= (-1)^{c_t} \Sigma(a_t, b_t), \\ a_t, b_t &\in \{0, 1, \dots, D_t - 1\}, \quad c_t \in \{0, 1\}, \end{aligned} \quad (67)$$

where $D_t = |\mathcal{T}_n(t|x^n)|$ is the size of type class associated with the conditional type t . Then, define the operator

$$U(\gamma) = \bigoplus_t V_t(a_t, b_t, c_t) \quad (68)$$

with $\gamma = ((a_t, b_t, c_t)_t)$. Let Γ_{x^n} denote the set of all possible vectors γ .

For every $m \in [1 : 2^{nR}]$, choose $2^{nR'}$ vectors $\gamma(m'|x^n(m))$, $m' \in [1 : 2^{nR'}]$, uniformly at random from $\Gamma_{x^n(m)}$. The mappings are revealed to both Alice and Bob.

C.1.2 Encoder

To send the messages $(m, m') \in [1 : 2^{nR}] \times [1 : 2^{nR'}]$, apply the operators $F^{(x_i(m))}$ and $U(\gamma(m'|x^n(m)))$. This yields the input state

$$\left| \chi_{A^n G_2^n}^{\gamma, x^n} \right\rangle \equiv (U(\gamma) F^{(x^n)} \otimes \mathbb{1}) |\phi_{G_1 G_2}\rangle^{\otimes n}, \quad (69)$$

for $x^n = x^n(m)$ and $\gamma = \gamma(m'|x^n)$, where $F^{(x^n)} \equiv \bigotimes_{i=1}^n F^{(x_i)}$. Then, transmit A^n through the channel.

C.1.3 Decoder

Bob receives the systems B^n in a state $\rho_{B^n G_2^n}^{\gamma, x^n}$, and decodes as follows.

- (i) Measure B^n using a POVM $\{\Lambda_m\}_{m \in [1:2^{nR}]}$. Denote the measurement outcome by \hat{m} .
- (ii) If there is no entanglement assistance, declare \hat{m} as the message estimate.
- (iii) If entanglement assistance is present, measure $B^n G_2^n$ jointly using a second POVM $\{\Upsilon_{m'|x^n(\hat{m})}\}_{m' \in [1:2^{nR}]}$. Let \hat{m}' be the outcome of this measurement. Then, declare (\hat{m}, \hat{m}') as the estimated message pair.

The POVMs $\{\Lambda_m\}$ and $\{\Upsilon_{m'|x^n(\hat{m})}\}$ will be chosen later in Subsections C.1.5 and C.1.6, respectively.

C.1.4 Code Properties

Before we go into the error analysis, we show that Alice's operations for encoding the second message m' can be effectively reflected to Bob's side. To this end, we will apply the "ricochet property"⁶⁸ Eq. (17),

$$(U \otimes \mathbb{1}) |\Phi_{AB}\rangle = (\mathbb{1} \otimes U^T) |\Phi_{AB}\rangle . \quad (70)$$

Now, for every $x^n \in \mathcal{X}^n$,

$$\left| \psi_{A^n G_2^n}^{x^n} \right\rangle = \sum_{z^n \in \mathcal{Z}^n} \sqrt{p_{Z^n|X^n}(z^n|x^n)} |\xi_{x^n, z^n}\rangle \otimes |\xi'_{x^n, z^n}\rangle , \quad (71)$$

where $p_{Z^n|X^n}(z^n|x^n) = \prod_{i=1}^n p_{Z|X}(z_i|x_i)$. As the space \mathcal{Z}^n can be partitioned into conditional type classes given x^n , we may write

$$\begin{aligned} \left| \psi_{A^n G_2^n}^{x^n} \right\rangle &= \sum_{t \in \mathcal{P}_n(\mathcal{Z})} \sum_{z^n \in \mathcal{T}_n(t|x^n)} \sqrt{p_{Z^n|X^n}(z^n|x^n)} |\xi_{x^n, z^n}\rangle \otimes |\xi'_{x^n, z^n}\rangle \\ &= \sum_{t \in \mathcal{P}_n(\mathcal{Z})} \sqrt{p_{Z^n|X^n}(z_t^n|x^n)} \sum_{z^n \in \mathcal{T}_n(t|x^n)} |\xi_{x^n, z^n}\rangle \otimes |\xi'_{x^n, z^n}\rangle , \end{aligned} \quad (72)$$

where z_t^n is any sequence in the conditional type class $\mathcal{T}_n(t|x^n)$. Therefore,

$$\left| \psi_{A^n G_2^n}^{x^n} \right\rangle = \sum_{t \in \mathcal{P}_n(\mathcal{Z})} \sqrt{P(t|x^n)} |\Phi_t\rangle , \quad (73)$$

where $P(t|x^n) = P_{Z^n|X^n}(z_t^n|x^n) |\mathcal{T}_n(t|x^n)|$ is the conditional probability of the type class $\mathcal{T}_n(t|x^n)$, and

$$|\Phi_t\rangle = \frac{1}{\sqrt{|\mathcal{T}_n(t|x^n)|}} \sum_{z^n \in \mathcal{T}_n(t|x^n)} |\xi_{x^n, z^n}\rangle \otimes |\xi'_{x^n, z^n}\rangle . \quad (74)$$

Alice applies the operator $U(\gamma(m'|x^n(m)))$ to the entangled states. Since the state $|\Phi_t\rangle$ is maximally entangled, we have by (70),

$$\begin{aligned} \left| \chi_{A^n G_2^n}^{\gamma, x^n} \right\rangle &\equiv (U(\gamma(m, m')) \otimes \mathbb{1}) \left| \psi_{A^n G_2^n}^{x^n} \right\rangle \\ &= (\mathbb{1} \otimes U^T(\gamma(m, m'))) \left| \psi_{A^n G_2^n}^{x^n} \right\rangle , \end{aligned} \quad (75)$$

where $\left| \psi_{A^n G_2^n}^{x^n} \right\rangle \equiv \bigotimes_{i=1}^n \left| \psi_{AG_2}^{x_i} \right\rangle$ (see (64)). By the same considerations,

$$\begin{aligned} \left| \psi_{A^n G_2^n}^{x^n} \right\rangle &= (F^{(x^n)} \otimes \mathbb{1}) \left| \phi_{G_1 G_2} \right\rangle^{\otimes n} \\ &= (\mathbb{1} \otimes (F^{(x^n)})^T) \left| \phi_{AG_2'} \right\rangle^{\otimes n} . \end{aligned} \quad (76)$$

That is, Alice's unitary operations can be reflected and treated as if performed by Bob.

Bob then receives the systems B^n in the state

$$\rho_{B^n G_2^n}^{\gamma, x^n} = (\tilde{\mathcal{N}}^{\otimes n} \otimes \text{id}) \left(\chi_{A^n G_2^n}^{\gamma, x^n} \right) \quad (77)$$

$$= (\tilde{\mathcal{N}}^{\otimes n} \otimes \text{id}) \left((\mathbb{1} \otimes U^T(\gamma)) \psi_{A^n G_2^n}^{x^n} (\mathbb{1} \otimes U^*(\gamma)) \right) , \quad (78)$$

where $\tilde{\mathcal{N}}$ is as in (63), and the last line is due to (75). Since a quantum channel is a linear map, the above can be written as

$$\begin{aligned}\rho_{B^n G_2^n}^{\gamma, x^n} &= (\mathbb{1} \otimes U^T(\gamma))(\tilde{\mathcal{N}} \otimes \text{id})(\psi_{A^n G_2^n}^{x^n})(\mathbb{1} \otimes U^*(\gamma)) \\ &= (\mathbb{1} \otimes U^T(\gamma))\omega_{B^n G_2^n}^{x^n}(\mathbb{1} \otimes U^*(\gamma)).\end{aligned}\quad (79)$$

C.1.5 Error Analysis Without Assistance

Recall that if entanglement assistance is absent, then Bob does not decode m' . Furthermore, since the decoder cannot measure G_2^n in this case, we need to consider the reduced state $\rho_{B^n}^{\gamma, x^n}$ of the joint output state $\rho_{B^n G_2^n}^{\gamma, x^n}$. Observe that by (79), the reduced output state is

$$\rho_{B^n}^{\gamma, x^n(m)} = \omega_{B^n}^{x^n(m)}. \quad (80)$$

Thereby, the reduced output is not affected by the encoding of the message m' using $\gamma(m'|x^n(m))$, and we can use the standard results on classical communication over a quantum channel without assistance.

Fix $\delta > 0$. Based on the HSW Theorem^{15;16}, there exists a codebook $\{x^n(m)\}$ and a POVM $\{\Lambda_m\}$ such that

$$\begin{aligned}P_{e|m, m'}^{*(n)}(\mathcal{F}, \phi_{G_1 G_2}^{\otimes n}, \Lambda) &= 1 - \text{Tr}(\Lambda_m \rho_{B^n}^{\gamma(m'|x^n(m)), x^n(m)}) \\ &= 1 - \text{Tr}(\Lambda_m \omega_{B^n}^{x^n(m)}) \\ &\leq 2^{-n(I(X; B)_\omega - R - \varepsilon_1(\delta))},\end{aligned}\quad (81)$$

where $x^n(m) \in \mathcal{A}^\delta(p_X)$ for all $m \in [1 : 2^{nR}]$ (see⁵⁵ Section 20.3.1). We use the notation $\varepsilon_j(\delta)$ for terms that tend to zero as $\delta \rightarrow 0$. Thus, in the absence of entanglement assistance, the probability of error tends to zero as $n \rightarrow \infty$, provided that

$$R < I(X; B)_\omega - \varepsilon_1(\delta). \quad (82)$$

C.1.6 Packing Lemma Requirements

In the error analysis with entanglement assistance, we will use the quantum packing lemma. Fix a sequence $x^n \in \mathcal{A}^\delta(p_X)$. Consider the ensemble $\{p(\gamma) = \frac{1}{|\Gamma_{x^n}|}, \rho_{B^n G_2^n}^{\gamma, x^n}\}$, for which the expected density operator is

$$\bar{\rho}_{B^n G_2^n}^{x^n} = \frac{1}{|\Gamma_{x^n}|} \sum_{\gamma \in \Gamma_{x^n}} \rho_{B^n G_2^n}^{\gamma, x^n}. \quad (83)$$

Define the code projector and the codeword projectors by

$$\Pi \equiv \Pi^\delta(\omega_B | x^n) \otimes \Pi^\delta(\omega_{G_2} | x^n) \quad (84)$$

$$\Pi_\gamma \equiv (\mathbb{1} \otimes U^T(\gamma))\Pi^\delta(\omega_{B G_2} | x^n)(\mathbb{1} \otimes U^*(\gamma)), \text{ for } \gamma \in \Gamma_{x^n}, \quad (85)$$

where $\Pi^\delta(\omega_{B G_2} | x^n)$, $\Pi^\delta(\omega_B | x^n)$ and $\Pi^\delta(\omega_{G_2} | x^n)$ are the projectors onto the conditional δ -typical subspaces associated with the states $\omega_{B G_2}^x$, $\omega_B^x = \text{Tr}_{G_2}(\omega_{B G_2}^x)$ and $\omega_{G_2}^x = \text{Tr}_B(\omega_{B G_2}^x)$, respectively (see (65)).

Applying the bounds in ⁶⁸ Appendix II to the operators above, we obtain

$$\text{Tr}(\Pi \rho_{B^n G_2^n}^{\gamma, x^n}) \geq 1 - 2\varepsilon_2(\delta), \quad (86)$$

$$\text{Tr}(\Pi_\gamma \rho_{B^n G_2^n}^{\gamma, x^n}) \geq 1 - \varepsilon_3(\delta), \quad (87)$$

$$\text{Tr}(\Pi_\gamma) \leq 2^{n(H(BG_2|X)_\omega + \varepsilon_4(\delta))}, \quad (88)$$

$$\Pi \sigma_{B^n G_2^n}^{x^n} \Pi \leq 2^{-n(H(B|X)_\omega + H(G_2|X)_\omega + \varepsilon_5(\delta))} \Pi, \quad (89)$$

where $\varepsilon_j(\delta)$ tend to zero as $\delta \rightarrow 0$. Hence, the requirements of the packing lemma are satisfied. Then, by Lemma 8, there exist deterministic vectors $\gamma(m'|x^n)$, $m' \in [1 : 2^{nR'}]$, and a POVM $\{\Upsilon_{m'|x^n}\}_{m' \in [1:2^{nR}]}$, such that

$$\text{Tr}\left(\Upsilon_{m'|x^n} \rho_{B^n G_2^n}^{\gamma(m'|x^n), x^n}\right) \geq 1 - 2^{-n[I(B;G_2|X)_\omega - R' - \varepsilon_6(\delta)]} \quad (90)$$

for all $m' \in [1 : 2^{nR'}]$.

C.1.7 Error Analysis with Entanglement Assistance

Suppose that entanglement assistance is present, in which case Bob estimates both m and m' . Hence, the error event is bounded by the union of the following events,

$$\mathcal{E}_1(m) = \{\hat{m} \neq m\}, \quad (91)$$

$$\mathcal{E}_2(m') = \{\hat{m}' \neq m'\}. \quad (92)$$

Then, by the union of events bound,

$$P_{e|m, m'}^{(n)}(\mathcal{F}, \phi_{G_1 G_2}^{\otimes n}, \Upsilon \circ \Lambda) \leq \Pr(\mathcal{E}_1(m)) + \Pr(\mathcal{E}_2(m') | \mathcal{E}_1^c(m)). \quad (93)$$

The first term corresponds to the measurement of $\{\Lambda_m\}$ above. Based on our previous analysis (see (81)),

$$\Pr(\mathcal{E}_1(m)) \leq 2^{-n(I(X;B)_\omega - R - \varepsilon_1(\delta))}, \quad (94)$$

which tends to zero for a rate R as in (82).

Given \mathcal{E}_1^c , Bob has recovered the correct m in step (i) of the decoding procedure. Denote the joint state of the systems $B^n G_2^n$ after this measurement by $\tilde{\rho}_{B^n G_2^n}^{\gamma, x^n(m)}$. As previously observed ^{72;73}, by the gentle measurement lemma ^{74;75} and (94), the post-measurement state is close to the original state in the sense that

$$\begin{aligned} & \frac{1}{2} \left\| \tilde{\rho}_{B^n G_2^n}^{\gamma, x^n(m)} - \rho_{B^n G_2^n}^{\gamma, x^n(m)} \right\|_1 \\ & \leq 2^{-n \frac{1}{2} (I(X;B)_\omega - R - \varepsilon_1(\delta))} \\ & \leq \varepsilon_7(\delta) \end{aligned} \quad (95)$$

for sufficiently large n and R as in (82). Therefore, the distribution of measurement outcomes, when $\tilde{\rho}_{B^n G_2^n}^{\gamma, x^n}$ is measured, is roughly the same as if the POVM Λ_m was never performed. To be precise, the difference between the probability of a measurement outcome \hat{m}' when $\tilde{\rho}_{B^n G_2^n}^{\gamma, x^n}$ is measured and the probability when $\rho_{B^n G_2^n}^{\gamma, x^n}$ is measured is bounded by $\varepsilon_7(\delta)$ in absolute value (see ⁵⁵

Lemma 9.11). Therefore, by (90), the POVM $\Upsilon_{m'|x^n(m)}$ satisfies $\Pr(\mathcal{E}_2 | \mathcal{E}_1^c) \leq 2^{-n(I(G_2; B|X)_\rho - R' - \varepsilon_8(\delta))}$, which tends to zero as $n \rightarrow \infty$, if

$$R' < I(G_2; B|X)_\omega - \varepsilon_8(\delta). \quad (96)$$

Finally, we let A_0, A_1 replace G_1, G_2 , respectively. Thus, the probability of error tends to zero as $n \rightarrow \infty$ provided that $R < I(X; B)_\omega - \varepsilon_1(\delta)$ and $R' < I(A_1; B|X)_\omega - \varepsilon_8(\delta)$. This completes the proof of the direct part.

C.2 Converse Proof

Suppose that Alice and Bob are trying to distribute randomness. An upper bound on the rate at which Alice can distribute randomness to Bob also serves as an upper bound on the rate at which they can communicate. In this task, Alice and Bob share an unreliable entangled resource $\Psi_{G_A G_B}$. Alice first prepares maximally correlated states,

$$\begin{aligned} \pi_{KMK'M'} \equiv & \left(\frac{1}{2^{nR}} \sum_{m=1}^{2^{nR}} |m\rangle\langle m| \otimes |m\rangle\langle m| \right) \\ & \otimes \left(\frac{1}{2^{nR'}} \sum_{m'=1}^{2^{nR'}} |m'\rangle\langle m'| \otimes |m'\rangle\langle m'| \right) \end{aligned} \quad (97)$$

locally. That is, K, M, K' , and M' are classical registers that store uniformly-distributed indices m and m' . Then, Alice applies an encoding channel to the classical system MM' and her share G_A of the entangled state $\Psi_{G_A G_B}$. As Alice applies $\mathcal{F}_{MM'G_A \rightarrow A^n}$, the resulting state is

$$\sigma_{KK'A^n G_B} \equiv (\text{id} \otimes \mathcal{F} \otimes \text{id})(\pi_{KMK'M'} \otimes \Psi_{G_A G_B}). \quad (98)$$

After Alice sends the system A^n through the channel, Bob receives the system B^n in the state

$$\omega_{KK'G_B B^n} \equiv (\text{id} \otimes \mathcal{N}^{\otimes n})(\sigma_{KK'A^n G_B}). \quad (99)$$

In the presence of entanglement assistance, Bob performs a decoding channel $\mathcal{D}_{B^n G_B \rightarrow \hat{M}\hat{M}'}$, which yields

$$\rho_{KK'\hat{M}\hat{M}'} \equiv (\text{id} \otimes \mathcal{D})(\omega_{KK'G_B B^n}). \quad (100)$$

If the entanglement assistance is not available, Bob performs $\mathcal{D}_{B^n \rightarrow \tilde{M}}^*$, producing

$$\rho_{KK'\tilde{M}G_B}^* \equiv (\text{id} \otimes \mathcal{D}^* \otimes \text{id})(\omega_{KK'G_B B^n}). \quad (101)$$

Consider a sequence of codes $(\mathcal{E}_n, \Psi_n, \mathcal{D}_n, \mathcal{D}_n^*)$ of randomness distribution with unreliable entanglement assistance, such that

$$\frac{1}{2} \left\| \rho_{K\hat{M}K'\hat{M}'} - \pi_{KMK'M'} \right\|_1 \leq \alpha_n, \quad (102)$$

$$\frac{1}{2} \left\| \rho_{K\tilde{M}}^* - \pi_{KM} \right\|_1 \leq \alpha_n^*, \quad (103)$$

where $\rho_{K\tilde{M}}^*$ is the reduced density operator of $\rho_{KK'\tilde{M}G_B}^*$, while α_n, α_n^* tend to zero as $n \rightarrow \infty$. By the Alicki-Fannes-Winter inequality^{76;77,55} Theorem 11.10.3, this implies

$$\left| H(K'| \hat{M}'K)_\rho - H(K'| M'K)_\pi \right| \leq n\varepsilon_n, \quad (104)$$

$$\left| H(K| \tilde{M})_{\rho^*} - H(K| M)_\pi \right| \leq n\varepsilon_n^*, \quad (105)$$

where $\varepsilon_n, \varepsilon_n^*$ tends to zero as $n \rightarrow \infty$.

Now, suppose that entanglement assistance is absent. Observe that $H(K)_{\rho^*} = H(K)_\pi = nR$ implies $I(K; M)_\pi - I(K; \hat{M})_{\rho^*} = H(K| \hat{M})_{\rho^*} - H(K| M)_\pi$. Therefore, by (105),

$$\begin{aligned} nR &= I(K; M)_\pi \\ &\leq I(K; \hat{M})_{\rho^*} + n\varepsilon_n^* \\ &\leq I(K; B^n)_\omega + n\varepsilon_n^*, \end{aligned} \quad (106)$$

where the last line follows from (101) and the quantum data processing inequality⁶⁷ Theorem 11.5. Here, the system G_B need not be included since the decoding measurement \mathcal{D}^* is only applied to B^n .

We move to the case where entanglement assistance is present. Similarly, $I(K'; M'| K)_\pi - I(K'; \hat{M}'| K)_\rho = H(K'| \hat{M}'K)_\rho - H(K'| M'K)_\pi$. Therefore, by (104),

$$\begin{aligned} nR' &= I(K'; M'| K)_\pi \\ &\leq I(K'; \hat{M}'| K)_\rho + n\varepsilon_n \\ &\leq I(K'; G_B B^n | K)_\omega + n\varepsilon_n \end{aligned} \quad (107)$$

by (100) and the quantum data processing inequality. We must include the entanglement resource system G_B , since the decoder measures $G_B B^n$. By the chain rule, the last bound can also be written as

$$\begin{aligned} nR' &\leq I(K' G_B; B^n | K)_\rho - I(G_B; B^n | K)_\rho \\ &\quad + I(K'; G_B | K)_\rho + n\varepsilon_n \\ &\leq I(K' G_B; B^n | K)_\rho + I(K'; G_B | K)_\omega + n\varepsilon_n \\ &= I(K' G_B; B^n | K)_\omega + n\varepsilon_n, \end{aligned} \quad (108)$$

where the equality holds since G_B and (K, K') are in a product state. To complete the regularized converse proof, set $X^n = f(K)$ and $A_1^n \equiv (K', G_B)$, where f is an arbitrary one-to-one function from $[1 : 2^{nR}]$ to \mathcal{X}^n . This concludes the proof of Theorem 5. \square

D Proof of Theorem 7

Consider quantum communication over $\mathcal{N}_{A \rightarrow B}$ with unreliable entanglement assistance.

D.1 Achievability Proof

In the proof we follow Dupuis' methods⁶⁶, originally applied to the quantum broadcast channel.

At first we restrict the entanglement resources to a given rate R_e . That is, we assume $|\mathcal{H}_{G_A}| = |\mathcal{H}_{G_B}| \leq 2^{nR_e}$. We are going to show that any rate pair (Q, Q') is achievable with unreliable entanglement assistance if

$$0 \leq Q < H(A_1|A_2)_\omega \quad (109a)$$

$$Q < I(A_1)B)_\omega \quad (109b)$$

$$Q + Q' + R_e < H(A_2)_\omega \quad (109c)$$

$$Q + Q' - R_e < I(A_2)B)_\omega \quad (109d)$$

for some $\varphi_{A_1A_2A}$, where A_1, A_2 are arbitrary systems, and $\omega_{A_1A_2B} = \mathcal{N}_{A \rightarrow B}(\varphi_{A_1A_2A})$.

Let $|\phi_{A_1A_2AJ}\rangle$ be a purification of $\varphi_{A_1A_2A}$. Then, the corresponding channel output is

$$|\omega_{A_1A_2BEJ}\rangle = U_{A \rightarrow BE}^{\mathcal{N}} |\phi_{A_1A_2AJ}\rangle, \quad (110)$$

where $U_{A \rightarrow BE}^{\mathcal{N}}$ is a Stinespring dilation such that $U_{A \rightarrow BE}^{\mathcal{N}}(\rho_A) = U_{A \rightarrow BE}^{\mathcal{N}}\rho_A(U_{A \rightarrow BE}^{\mathcal{N}})^\dagger$.

Given a quantum message state $\theta_M \otimes \xi_{\bar{M}}$, let K and \bar{K} be reference systems that purify the message systems M and \bar{M} , respectively, *i.e.* such that the systems M, \bar{M}, K , and \bar{K} have a pure joint state $|\theta_{MK}\rangle \otimes |\xi_{\bar{M}\bar{K}}\rangle$, with $|\mathcal{H}_K| = |\mathcal{H}_M| = 2^{nQ}$ and $|\mathcal{H}_{\bar{K}}| = |\mathcal{H}_{\bar{M}}| = 2^{n(Q+Q')}$. Suppose that given reliable entanglement assistance, Alice and Bob share an entangled state $|\Phi_{G_A G_B}\rangle$ of dimension $|\mathcal{H}_{G_A}| = |\mathcal{H}_{G_B}| = 2^{nR_e}$.

Let $V_{M \rightarrow A_1}^{(1)}$ and $V_{\bar{M}G_A \rightarrow A_2}^{(2)}$ be arbitrary full-rank partial isometries. That is, each operator has 0-1 singular values with a rank of 2^{nQ} and $2^{n(Q+Q')}$, respectively. Denote

$$|\psi_{A_1^n K}^{(1)}\rangle = V_{M \rightarrow A_1}^{(1)} |\theta_{MK}\rangle, \quad (111)$$

$$|\psi_{A_2^n G_B \bar{K}}^{(2)}\rangle = V_{\bar{M}G_A \rightarrow A_2}^{(2)} (|\xi_{\bar{K}\bar{M}}\rangle \otimes |\Phi_{G_A, G_B}\rangle). \quad (112)$$

D.1.1 Decoupling Inequalities

First, we establish decoupling inequalities. We introduce the following notation of operators and channels. For every pair of Hilbert spaces \mathcal{H}_A and \mathcal{H}_B with orthonormal bases $\{|i_A\rangle\}$ and $\{|j_B\rangle\}$, respectively, define the operator $\text{op}_{A \rightarrow B}(|\psi_{AB}\rangle)$ by

$$\text{op}_{A \rightarrow B}(|i_A\rangle \otimes |j_B\rangle) \equiv |j_B\rangle\langle i_A|. \quad (113)$$

While the operation above depends on the choice of bases, we will not specify these since it is not important for our purposes. To generalize this definition to any state $|\psi_{AB}\rangle$, consider its decomposition $|\psi_{AB}\rangle = \sum_{i,j} a_{i,j} |i_A\rangle \otimes |j_B\rangle$, and define $\text{op}_{A \rightarrow B}(|\psi_{AB}\rangle) = \sum_{i,j} a_{i,j} \text{op}_{A \rightarrow B}(|i_A\rangle \otimes |j_B\rangle)$.

Consider the operators

$$\Pi_{A_2 \rightarrow A_1 A J} = \sqrt{|\mathcal{H}_{A_2}|} \text{op}_{A_2 \rightarrow A_1 A J}(\phi_{A_1 A_2 A J}), \quad (114)$$

$$\Pi_{A_1 \rightarrow A_2 A J} = \sqrt{|\mathcal{H}_{A_1}|} \text{op}_{A_1 \rightarrow A_2 A J}(\phi_{A_1 A_2 A J}). \quad (115)$$

Given a pair of unitaries, $U_{A_1^n}^{(1)}$ and $U_{A_2^n}^{(2)}$, define the following quantum states,

$$\left| \omega_{A_1^n A^n J^n \bar{K} G_B}^{U^{(2)}} \right\rangle = \Pi_{A_2 \rightarrow A_1 A J}^{\otimes n} U_{A_2^n}^{(2)} \left| \psi_{A_2^n G_B \bar{K}}^{(2)} \right\rangle, \quad (116)$$

$$\left| \omega_{A_2^n A^n J^n K}^{U^{(1)}} \right\rangle = \Pi_{A_1 \rightarrow A_2 A J}^{\otimes n} U_{A_1^n}^{(1)} \left| \psi_{A_1^n K}^{(1)} \right\rangle. \quad (117)$$

The corresponding channel outputs are then

$$\left| \omega_{A_1^n B^n E^n J^n \bar{K} G_B}^{U^{(2)}} \right\rangle = (U_{A \rightarrow B E}^{\mathcal{N}})^{\otimes n} \left| \omega_{A_1^n A^n J^n \bar{K} G_B}^{U^{(2)}} \right\rangle, \quad (118)$$

$$\left| \omega_{A_2^n B^n E^n J^n K}^{U^{(1)}} \right\rangle = (U_{A \rightarrow B E}^{\mathcal{N}})^{\otimes n} \left| \omega_{A_2^n A^n J^n K}^{U^{(1)}} \right\rangle. \quad (119)$$

Now, consider the operators

$$\Pi_{A_1^n \rightarrow A^n J^n \bar{K} G_B}^{U^{(2)}} = \sqrt{|\mathcal{H}_{A_1}|^n} \text{op}_{A_1^n \rightarrow A J \bar{K} G_B}(\omega_{A_1^n A^n J^n \bar{K} G_B}^{U^{(2)}}), \quad (120)$$

$$\Pi_{A_2^n \rightarrow A^n J^n K}^{U^{(1)}} = \sqrt{|\mathcal{H}_{A_2}|^n} \text{op}_{A_2^n \rightarrow A^n J^n K}(\omega_{A_2^n A^n J^n K}^{U^{(1)}}), \quad (121)$$

$$\Pi_{A_1 A_2 \rightarrow A J} = \sqrt{|\mathcal{H}_{A_1}| |\mathcal{H}_{A_2}|} \text{op}_{A_1 A_2 \rightarrow A J}(\phi_{A_1 A_2 A J}), \quad (122)$$

and define the quantum channels $\mathcal{T}_{A_1^n \rightarrow E^n J^n \bar{K} G_B}^{U^{(2)}}$, $\mathcal{T}_{A_2^n \rightarrow E^n J^n K}^{U^{(1)}}$, and $\mathcal{T}_{A_1 A_2 \rightarrow E J}$, by

$$\mathcal{T}_{A_1^n \rightarrow E^n J^n \bar{K} G_B}^{U^{(2)}}(\rho_{A_1^n}) = \text{Tr}_{B^n} \left[\mathcal{U}_{A \rightarrow B E}^{\mathcal{N}}(\Pi_{A_1^n \rightarrow A^n J^n \bar{K} G_B}^{U^{(2)}}(\rho_{A_1^n})) \right], \quad (123)$$

$$\mathcal{T}_{A_2^n \rightarrow E^n J^n K}^{U^{(1)}}(\rho_{A_2^n}) = \text{Tr}_{B^n} \left[\mathcal{U}_{A \rightarrow B E}^{\mathcal{N}}(\Pi_{A_2^n \rightarrow A^n J^n K}^{U^{(1)}}(\rho_{A_2^n})) \right], \quad (124)$$

$$\mathcal{T}_{A_1 A_2 \rightarrow E J}(\rho_{A_1 A_2}) = \text{Tr}_B \left[\mathcal{U}_{A \rightarrow B E}^{\mathcal{N}}(\Pi_{A_1 A_2 \rightarrow A J}(\rho_{A_1 A_2})) \right]. \quad (125)$$

According to⁶⁶ Lemma 2.7, $\text{op}_{A \rightarrow B}(\psi_{AB}) |\phi_{AC}\rangle = \text{op}_{A \rightarrow C}(\phi_{AC}) |\psi_{AB}\rangle$, hence

$$\begin{aligned} \mathcal{T}_{A_1^n \rightarrow E^n J^n \bar{K} G_B}^{U^{(2)}}(U_{A_1^n}^{(1)} \psi_{A_1^n K}^{(1)}) &= \mathcal{T}_{A_2^n \rightarrow E^n J^n K}^{U^{(1)}}(U_{A_2^n}^{(2)} \psi_{A_2^n \bar{K} G_B}^{(2)}) \\ &= \mathcal{T}_{A_1 A_2 \rightarrow E J}^{\otimes n}(U_{A_1^n}^{(1)} \psi_{A_1^n K}^{(1)} \otimes U_{A_2^n}^{(2)} \psi_{A_2^n \bar{K} G_B}^{(2)}). \end{aligned} \quad (126)$$

Applying the decoupling theorem, Theorem 9, to the channels in (123)-(124), we obtain

$$\begin{aligned} &\int_{\mathbb{U}_{A_1^n}} \left\| \mathcal{T}_{A_1^n \rightarrow E^n J^n \bar{K} G_B}^{U^{(2)}}(U_{A_1^n}^{(1)} \psi_{A_1^n K}^{(1)}) - \theta_K \otimes \omega_{E^n J^n \bar{K} G_B}^{U^{(2)}} \right\|_1 dU_{A_1^n}^{(1)} \\ &\leq 2^{-\frac{1}{2}} \left[H_{\min}^\varepsilon(A_1^n | E^n J^n \bar{K} G_B)_{\omega^{U^{(2)}}} - nQ \right] + 8\varepsilon, \end{aligned} \quad (127)$$

$$\begin{aligned} &\int_{\mathbb{U}_{A_2^n}} \left\| \mathcal{T}_{A_2^n \rightarrow E^n J^n K}^{U^{(1)}}(U_{A_2^n}^{(2)} \psi_{A_2^n \bar{K} G_B}^{(2)}) - \xi_{\bar{K}} \otimes \omega_{E^n J^n K}^{U^{(1)}} \right\|_1 dU_{A_2^n}^{(2)} \\ &\leq 2^{-\frac{1}{2}} \left[H_{\min}^\varepsilon(A_2^n | E^n J^n K)_{\omega^{U^{(1)}}} - n(Q+Q' - R_e) \right] + 8\varepsilon. \end{aligned} \quad (128)$$

Using (126), we can rewrite those decoupling inequalities as

$$\begin{aligned} & \int_{\mathbb{U}_{A_1^n}} \left\| \mathcal{T}_{A_1 A_2 \rightarrow ED}^{\otimes n} (U_{A_1^n}^{(1)} \psi_{A_1^n K}^{(1)} \otimes U_{A_2^n}^{(2)} \psi_{A_2^n \bar{K} G_B}^{(2)}) - \theta_K \otimes \omega_{E^n J^n \bar{K} G_B}^{U^{(2)}} \right\|_1 dU_{A_1^n}^{(1)} \\ & \leq 2^{-\frac{1}{2}} \left[H_{\min}^\varepsilon(A_1^n | E^n J^n \bar{K} G_B)_{\omega^{U^{(2)}}} - n(Q - \alpha_{1n}) \right], \end{aligned} \quad (129)$$

$$\begin{aligned} & \int_{\mathbb{U}_{A_2^n}} \left\| \mathcal{T}_{A_1 A_2 \rightarrow EJ}^{\otimes n} (U_{A_1^n}^{(1)} \psi_{A_1^n K}^{(1)} \otimes U_{A_2^n}^{(2)} \psi_{A_2^n \bar{K} G_B}^{(2)}) - \xi_{\bar{K}} \otimes \omega_{E^n J^n K}^{U^{(1)}} \right\|_1 dU_{A_2^n}^{(2)} \\ & \leq 2^{-\frac{1}{2}} \left[H_{\min}^\varepsilon(A_2^n | E^n J^n K)_{\omega^{U^{(1)}}} - n(Q + Q' - R_e + \alpha_{2n}) \right], \end{aligned} \quad (130)$$

where $\alpha_{jn} \rightarrow 0$ as $n \rightarrow \infty$. The last bounds tend to zero provided that

$$Q < \frac{1}{n} H_{\min}^\varepsilon(A_1^n | E^n J^n \bar{K} G_B)_{\omega^{U^{(2)}}} - \alpha_{1n}, \quad (131)$$

$$Q + Q' - R_e < \frac{1}{n} H_{\min}^\varepsilon(A_2^n | E^n J^n K)_{\omega^{U^{(1)}}} - \alpha_{2n}. \quad (132)$$

This is close to what we would like to show. However, we need the encoder to be an isometry, and we need to replace $\omega^{U^{(1)}}$, $\omega^{U^{(2)}}$ in the inequalities above by ω . Applying the decoupling theorem, with $\bar{\mathcal{T}}_{A_1^n \rightarrow \bar{K} G_B}^{U^{(2)}}(\rho_{A_1^n}) = \text{Tr}_{A^n J^n} [\Pi_{A_1^n \rightarrow A^n J^n \bar{K} G_B}^{U^{(2)}}(\rho_{A_1^n})]$ and $\bar{\mathcal{T}}_{A_2^n \rightarrow C}(\rho_{A_2^n}) = \text{Tr}[\Pi_{A_2^n \rightarrow A_1^n A_2^n J^n}(\rho_{A_2^n})]$, we obtain

$$\begin{aligned} & \int_{\mathbb{U}_{A_1^n}} \left\| \text{Tr}_{A^n J^n} [\Pi_{A_1^n \rightarrow A^n J^n \bar{K} G_B}^{U^{(2)}} U_{A_1^n}^{(1)} \psi_{A_1^n K}^{(1)}] - \theta_K \otimes \omega_{\bar{K} G_B}^{U^{(2)}} \right\|_1 dU_{A_1^n}^{(1)} \\ & \leq 2^{-\frac{1}{2}} \left[H_{\min}^\varepsilon(A_1^n | \bar{K} G_B)_{\omega^{U^{(2)}}} - n(Q + \alpha_{3n}) \right], \end{aligned} \quad (133)$$

$$\begin{aligned} & \int_{\mathbb{U}_{A_2^n}} \left\| \omega_{\bar{K} G_B}^{U^{(2)}} - \xi_{\bar{K}} \otimes \Phi_{G_B} \right\|_1 dU_{A_2^n}^{(2)} \\ & = \int_{\mathbb{U}_{A_2^n}} \left\| \bar{\mathcal{T}}_{A_2^n \rightarrow C}^{U^{(2)}}(U_{A_2^n}^{(2)} \psi_{A_2^n \bar{K} G_B}^{(2)}) - \xi_{\bar{K}} \otimes \Phi_{G_B} \right\|_1 dU_{A_2^n}^{(2)} \\ & \leq 2^{-\frac{1}{2}} n [H(A_2)_\phi - (Q + Q' + R_e + \alpha_{4n})], \end{aligned} \quad (134)$$

which tend to zero for

$$Q < \frac{1}{n} H_{\min}^\varepsilon(A_1^n | \bar{K} G_B)_{\omega^{U^{(2)}}} - \alpha_{3n}, \quad (135)$$

$$Q + Q' + R_e < H(A_2)_\phi - \alpha_{4n}. \quad (136)$$

We will use these decoupling properties in order to obtain the encoding map, by applying Uhlmann's theorem (see Theorem 10). However, before that, we give the bounds on the smoothed min-entropies.

D.1.2 Entropy Bounds

We would like to bound the min-entropies in (131)-(132) and (135). We begin with the min-entropy $H_{\min}^\varepsilon(A_1^n | \bar{K} G_B)_{\omega^{U^{(2)}}}$. Suppose that $\tilde{\phi}_{A_1^n A_2^n A^n J^n}$ is a state such that

$$\left\| \tilde{\phi}_{A_1^n A_2^n A^n J^n} - \phi_{A_1 A_2 A J}^{\otimes n} \right\|_1 \leq 2\varepsilon_0 \quad (137)$$

and

$$H_{\min}(A_1^n|A_2^n)_{\tilde{\phi}} = H_{\min}(A_1^n|A_2^n)_{\phi}. \quad (138)$$

Define

$$\tilde{\Pi}_{A_2^n \rightarrow \bar{K}G_B}^{U(2)} = \sqrt{|\mathcal{H}_{A_2^n}|} \text{op}_{A_2^n \rightarrow \bar{K}G_B}(U_{A_2^n}^{(2)} W_{\bar{M}G_A \rightarrow A_2^n}^{(2)} |\psi_{\bar{M}G_A G_B \bar{K}}^{(2)}\rangle), \quad (139)$$

hence

$$\left| \omega_{A_1^n A^n J^n \bar{K}G_B}^{U(2)} \right\rangle = \tilde{\Pi}_{A_2^n \rightarrow \bar{K}G_B}^{U(2)} \left| \phi_{A_1 A_2 A J}^{\otimes n} \right\rangle. \quad (140)$$

Consider a decomposition of the operator $(\tilde{\phi} - \phi^{\otimes n})$ into its positive and negative parts,

$$\tilde{\phi}_{A_1^n A_2^n A^n J^n} - \phi_{A_1 A_2 A J}^{\otimes n} = \Delta_+ - \Delta_-, \quad (141)$$

where $\Delta_+, \Delta_- \succeq 0$ have a disjoint support. Hence, by (137), $\text{Tr}(\Delta_{\pm}) \leq 2\varepsilon_0$. We note that

$$\begin{aligned} & \int_{\mathbb{U}_{A_2^n}} \tilde{\Pi}_{A_2^n \rightarrow \bar{K}G_B}^{U(2)}(P_{A_2^n}) dU_{A_2^n}^{(2)} \\ &= \text{Tr}(P_{A_2^n}) \cdot \frac{1}{|\mathcal{H}_{A_2^n}|^n} \tilde{\Pi}_{A_2^n \rightarrow \bar{K}G_B}^{U(2)} \tilde{\Pi}_{A_2^n \rightarrow \bar{K}G_B}^{U(2)\dagger}. \end{aligned} \quad (142)$$

Thus,

$$\begin{aligned} & \int_{\mathbb{U}_{A_2^n}} \left\| \tilde{\Pi}_{A_2^n \rightarrow \bar{K}G_B}^{U(2)}(\tilde{\phi}_{A_1^n A_2^n A^n J^n}) - \tilde{\Pi}_{A_2^n \rightarrow \bar{K}G_B}^{U(2)}(\phi_{A_1 A_2 A J}^{\otimes n}) \right\|_1 dU_{A_2^n}^{(2)} \\ &= \int_{\mathbb{U}_{A_2^n}} \left\| \tilde{\Pi}_{A_2^n \rightarrow \bar{K}G_B}^{U(2)}(\Delta_+ - \Delta_-) \right\|_1 dU_{A_2^n}^{(2)} \\ &\leq \text{Tr}\left(\tilde{\Pi}_{A_2^n \rightarrow \bar{K}G_B}^{U(2)}(\Delta_+)\right) + \text{Tr}\left(\tilde{\Pi}_{A_2^n \rightarrow \bar{K}G_B}^{U(2)}(\Delta_-)\right) \\ &\leq 4\varepsilon_0, \end{aligned} \quad (143)$$

which, in turn, implies

$$\int_{\mathbb{U}_{A_2^n}} d_F\left(\tilde{\Pi}_{A_2^n \rightarrow \bar{K}G_B}^{U(2)}(\tilde{\phi}_{A_1^n A_2^n A^n J^n}), \tilde{\Pi}_{A_2^n \rightarrow \bar{K}G_B}^{U(2)}(\phi_{A_1 A_2 A J}^{\otimes n})\right) dU_{A_2^n}^{(2)} \leq 2\sqrt{\varepsilon_0}, \quad (144)$$

based on the relation between the fidelity and trace distance⁵⁵ Corollary 9.3.1. We deduce that

$$\int_{\mathbb{U}_{A_2^n}} H_{\min}^{2\sqrt{\varepsilon_0}}(A_1^n|\bar{K}G_B)_{\omega_{U(2)}} dU_{A_2^n}^{(2)} \geq H_{\min}^{\varepsilon_0}(A_1^n|A_2^n)_{\phi}. \quad (145)$$

For $\varepsilon_0 = \frac{\varepsilon^2}{4}$, we obtain

$$\int_{\mathbb{U}_{A_2^n}} \frac{1}{n} H_{\min}^{\varepsilon}(A_1^n|\bar{K}G_B)_{\omega_{U(2)}} dU_{A_2^n}^{(2)} \geq H(A_1|A_2)_{\phi} - \alpha_{5n}. \quad (146)$$

By the same considerations,

$$\begin{aligned}
\int_{\mathbb{U}_{A_1^n}} \frac{1}{n} H_{\min}^\varepsilon(A_2^n | E^n J^n K)_{\omega^{U(1)}} dU_{A_1^n}^{(1)} &\geq H(A_2 | EDA_1)_\omega - \alpha_{6n} \\
&= -H(A_2 | B)_\omega - \alpha_{6n} \\
&= I(A_2 | B)_\omega - \alpha_{6n}, \tag{147}
\end{aligned}$$

and

$$\begin{aligned}
\int_{\mathbb{U}_{A_2^n}} \frac{1}{n} H_{\min}^\varepsilon(A_1^n | E^n J^n \bar{K} G_B)_{\omega^{U(2)}} dU_{A_2^n}^{(2)} &\geq H(A_1 | EDA_2)_\omega - \alpha_{7n} \\
&= I(A_1 | B)_\omega - \alpha_{7n}. \tag{148}
\end{aligned}$$

Therefore, there exist unitaries $U_{A_1^n}^{(1)}$ and $U_{A_2^n}^{(2)}$ that satisfy the following inequalities,

$$\begin{aligned}
&\left\| \text{Tr}_{A^n J^n} \left[\Pi_{A_1^n \rightarrow A^n J^n \bar{K} G_B}^{U^{(2)}} U_{A_1^n}^{(1)} \psi_{A_1^n K}^{(1)} \right] - \theta_K \otimes \omega_{\bar{K} G_B}^{U^{(2)}} \right\|_1 \\
&\leq 2^{-\frac{1}{2}n[H(A_1 | A_2)_\phi - Q - \beta_n]}, \tag{149}
\end{aligned}$$

$$\begin{aligned}
&\left\| \mathcal{T}_{A_1 A_2 \rightarrow E J}^{\otimes n} (U_{A_1^n}^{(1)} \psi_{A_1^n K}^{(1)} \otimes U_{A_2^n}^{(2)} \psi_{A_2^n \bar{K} G_B}^{(2)}) - \theta_K \otimes \omega_{E^n J^n \bar{K} G_B}^{U^{(2)}} \right\|_1 \\
&\leq 2^{-\frac{1}{2}n[I(A_1 | B)_\omega - Q - \beta_n]}, \tag{150}
\end{aligned}$$

$$\begin{aligned}
&\left\| \mathcal{T}_{A_1 A_2 \rightarrow E J}^{\otimes n} (U_{A_1^n}^{(1)} \psi_{A_1^n K}^{(1)} \otimes U_{A_2^n}^{(2)} \psi_{A_2^n \bar{K}}^{(2)}) - \xi_{\bar{K}} \otimes \omega_{E^n J^n K}^{U^{(1)}} \right\|_1 \\
&\leq 2^{-\frac{1}{2}n[I(A_2 | B)_\omega - (Q + Q' - R_e) - \beta_n]}, \tag{151}
\end{aligned}$$

$$\begin{aligned}
&\left\| \omega_{\bar{K} G_B}^{U^{(2)}} - \xi_{\bar{K}} \otimes \Phi_{G_B} \right\|_1 = \left\| \bar{\mathcal{T}}_{A_2 \rightarrow C}^{\otimes n} (U_{A_2^n}^{(2)} \psi_{A_2^n \bar{K} G_B}^{(2)}) - \xi_{\bar{K}} \otimes \Phi_{G_B} \right\|_1 \\
&\leq 2^{-\frac{1}{2}n[H(A_2)_\phi - (Q + Q' + R_e) - \beta_n]}, \tag{152}
\end{aligned}$$

for some β_n that tends to zero as $n \rightarrow \infty$, as the first inequality follows from (133) and (146), the second from (129) and (148), the third is due to (130) and (147), and the last holds by (134).

D.1.3 Encoding

By the triangle inequality, (149) and (152) yield

$$\left\| \text{Tr}_{A^n J^n} \left[\Pi_{A_1^n \rightarrow A^n J^n \bar{K} G_B}^{U^{(2)}} U_{A_1^n}^{(1)} \psi_{A_1^n K}^{(1)} \right] - \theta_K \otimes \xi_{\bar{K}} \otimes \Phi_{G_B} \right\|_1 \leq \delta_{\text{enc}}(n), \tag{153}$$

where

$$\delta_{\text{enc}}(n) \equiv 2^{-\frac{1}{2}n[H(A_1 | A_2)_\phi - Q - \beta]} + 2^{-\frac{1}{2}n[H(A_2)_\phi - (Q + Q' + R_e) - \beta]}. \tag{154}$$

Based on Uhlmann's theorem, it follows that there exists an isometry $F_{M \bar{M} G_A \rightarrow A^n J^n}$ such that

$$\begin{aligned}
&\left\| \Pi_{A_1^n \rightarrow A^n J^n \bar{K} G_B}^{U^{(2)}} U_{A_1^n}^{(1)} \psi_{A_1^n K}^{(1)} - F_{M \bar{M} G_A \rightarrow A^n J^n} (\theta_{MK} \otimes \xi_{\bar{M} \bar{K}} \otimes \Phi_{G_A G_B}) \right\|_1 \\
&\leq 2\sqrt{\delta_{\text{enc}}(n)}. \tag{155}
\end{aligned}$$

D.1.4 Decoding without Assistance

By applying the isometric extension of the channel to the states on the RHS of (155) and using the triangle inequality and the monotonicity of the trace distance under quantum channels, we obtain

$$\begin{aligned} & \left\| \mathcal{T}_{A_1^n \rightarrow E^n J^n \bar{K} G_B}^{U^{(2)}} (U_{A_1^n}^{(1)} \psi_{A_1^n K}^{(1)}) \right. \\ & \quad \left. - \text{Tr}_{B^n} [(U_{A \rightarrow BE}^{\mathcal{N}})^{\otimes n} F_{M\bar{M}G_A \rightarrow A^n J^n} (\theta_{MK} \otimes \xi_{\bar{M}\bar{K}} \otimes \Phi_{G_A G_B})] \right\|_1 \\ & \leq 2\sqrt{\delta_{\text{enc}}(n)}. \end{aligned} \quad (156)$$

By (126), the inequality above can also be written as

$$\begin{aligned} & \left\| \mathcal{T}_{A_1 A_2 \rightarrow EJ}^{\otimes n} (U_{A_1^n}^{(1)} \psi_{A_1^n K}^{(1)} \otimes U_{A_2^n}^{(2)} \psi_{A_2^n \bar{K} G_B}^{(2)}) \right. \\ & \quad \left. - \text{Tr}_{B^n} [(U_{A \rightarrow BE}^{\mathcal{N}})^{\otimes n} F_{M\bar{M}G_A \rightarrow A^n J^n} (\theta_{MK} \otimes \xi_{\bar{M}\bar{K}} \otimes \Phi_{G_A G_B})] \right\|_1 \\ & \leq 2\sqrt{\delta_{\text{enc}}(n)}. \end{aligned} \quad (157)$$

Together with (150), this implies

$$\begin{aligned} & \left\| \text{Tr}_{B^n} [(U_{A \rightarrow BE}^{\mathcal{N}})^{\otimes n} F_{M\bar{M}G_A \rightarrow A^n J^n} (\theta_{MK} \otimes \xi_{\bar{M}\bar{K}} \otimes \Phi_{G_A G_B})] \right. \\ & \quad \left. - \theta_K \otimes \omega_{E^n J^n \bar{K} G_B}^{U^{(2)}} \right\|_1 \\ & \leq 2\sqrt{\delta_{\text{enc}}(n)} + \delta_1(n), \end{aligned} \quad (158)$$

where $\delta_1(n) \equiv 2^{-\frac{1}{2}n[I(A_1)B]_{\omega} - Q - \beta}$.

Thus, by Uhlmann's theorem, there exists an isometry $D_{B^n \rightarrow MJ_1}^*$, such that

$$\begin{aligned} & \left\| D_{B^n \rightarrow MJ_1}^* (U_{A \rightarrow BE}^{\mathcal{N}})^{\otimes n} F_{M\bar{M}G_A \rightarrow A^n J^n} (\theta_{MK} \otimes \xi_{\bar{M}\bar{K}} \otimes \Phi_{G_A G_B}) \right. \\ & \quad \left. - \theta_{MK} \otimes \hat{\omega}_{E^n J^n \bar{K} G_B J_1} \right\|_1 \leq 2\sqrt{2\sqrt{\delta_{\text{enc}}(n)} + \delta_1(n)}, \end{aligned} \quad (159)$$

where $\hat{\omega}_{E^n J^n \bar{K} G_B J_1}$ is an arbitrary purification of $\omega_{E^n J^n \bar{K} G_B}^{U^{(2)}}$. By tracing over $E^n J^n \bar{K} G_B J_1$, we deduce that there exist an encoding map $\mathcal{F}_{M\bar{M}G_A \rightarrow A^n}$ and a decoding map $\mathcal{D}_{B^n \rightarrow M}^*$, such that

$$\begin{aligned} & \left\| (\mathcal{D}_{B^n \rightarrow M}^* \circ \mathcal{N}_{A \rightarrow B}^{\otimes n} \circ \mathcal{F}_{M\bar{M}G_A \rightarrow A^n}) (\theta_{MK} \otimes \xi_{\bar{M}} \otimes \Phi_{G_A}) - \theta_{MK} \right\|_1 \\ & \leq 2\sqrt{2\sqrt{\delta_{\text{enc}}(n)} + \delta_1(n)}. \end{aligned} \quad (160)$$

D.1.5 Decoding with Entanglement Assistance

The bound in (157), together with (151), implies

$$\begin{aligned} & \left\| \text{Tr}_{B^n G_B} [(U_{A \rightarrow BE}^{\mathcal{N}})^{\otimes n} F_{M\bar{M}G_A \rightarrow A^n J^n} (\theta_{MK} \otimes \xi_{\bar{M}\bar{K}} \otimes \Phi_{G_A G_B})] \right. \\ & \quad \left. - \xi_{\bar{K}} \otimes \omega_{E^n J^n K}^{U^{(1)}} \right\|_1 \leq 2\sqrt{\delta_{\text{enc}}(n)} + \delta_2(n), \end{aligned} \quad (161)$$

where $\delta_2(n) \equiv 2^{-\frac{1}{2}n[I(A_2|B)_\omega - (Q+Q'-R_e) - \beta]}$. Thus, by Uhlmann's theorem, there exists an isometry $D_{B^n G_B \rightarrow \bar{M} G'_A G'_B J_2}$, such that

$$\left\| D_{B^n G_B \rightarrow \bar{M} G'_A G'_B J_2} (U_{A \rightarrow BE}^{\mathcal{N}})^{\otimes n} F_{M\bar{M}G_A \rightarrow A^n J^n} (\theta_{MK} \otimes \xi_{\bar{M}\bar{K}} \otimes \Phi_{G_A G_B}) - \xi_{\bar{M}\bar{K}} \otimes \Phi_{G_A G_B} \otimes \hat{\omega}_{E^n J^n K J_2} \right\|_1 \leq 2\sqrt{2\sqrt{\delta_{\text{enc}}(n)} + \delta_2(n)}. \quad (162)$$

By tracing over $E^n J^n K G'_A G'_B J_2$, we deduce that $\mathcal{F}_{M\bar{M}G_A \rightarrow A^n}$ and $\mathcal{D}_{B G_B \rightarrow \bar{M}}$ satisfy

$$\left\| \mathcal{D}_{B^n G_B \rightarrow \bar{M}} \circ \mathcal{N}_{A \rightarrow B}^{\otimes n} \circ \mathcal{F}_{M\bar{M}G_A \rightarrow A^n} (\theta_M \otimes \xi_{\bar{M}\bar{K}} \otimes \Phi_{G_A G_B}) - \xi_{\bar{M}\bar{K}} \right\|_1 \leq 2\sqrt{2\sqrt{\delta_{\text{enc}}(n)} + \delta_2(n)}. \quad (163)$$

As $\delta_{\text{enc}}(n)$, $\delta_1(n)$, and $\delta_2(n)$ tend to zero as $n \rightarrow \infty$ for rates as in (109), we deduce that the errors tend to zero as well.

Choosing the entanglement rate $R_e = \frac{1}{2}[H(A_2)_\omega + H(A_2|B)_\omega]$, it follows that $\mathcal{L}_{\text{EA}^*}(\mathcal{N})$ is an achievable rate region (cf. (28) and (109)). To show that rate pairs in $\frac{1}{k}\mathcal{L}_{\text{EA}^*}(\mathcal{N}^{\otimes k})$ are achievable as well, we employ the coding scheme above for the product channel $\mathcal{N}^{\otimes k}$, where k is arbitrarily large. This completes the achievability proof.

D.2 Converse Proof

Consider the converse part. Suppose that Alice and Bob are trying to generate entanglement between them. An upper bound on the rate at which Alice and Bob can generate entanglement also serves as an upper bound on the quantum rate at which they can communicate qubits, since a noiseless quantum channel can be used to generate entanglement by sending one part of an entangled pair. In this task, Alice locally prepares two maximally entangled pairs,

$$\begin{aligned} |\Phi_{MK}\rangle \otimes |\Phi_{\bar{M}\bar{K}}\rangle &= \left[\frac{1}{\sqrt{2^{nQ}}} \sum_{m=1}^{2^{nQ}} |m\rangle_M \otimes |m\rangle_K \right] \\ &\otimes \left[\frac{1}{\sqrt{2^{n(Q+Q')}}} \sum_{\bar{m}=1}^{2^{n(Q+Q')}} |\bar{m}\rangle_{\bar{M}} \otimes |\bar{m}\rangle_{\bar{K}} \right]. \end{aligned} \quad (164)$$

If the entanglement assistance is reliable, then Alice and Bob share the quantum state $|\Phi_{G_A G_B}\rangle$, where G_A and G_B represent the entanglement resources that Alice and Bob share, respectively. Then Alice applies an encoding channel $\mathcal{F}_{M\bar{M}G_A \rightarrow A^n}$ to the quantum message systems $M\bar{M}$ and her share G_A of the entanglement resources. The resulting state is

$$\omega_{K\bar{K}G_B A^n} \equiv \mathcal{F}_{M\bar{M}G_A \rightarrow A^n} (\Phi_{MK} \otimes \Phi_{\bar{M}\bar{K}} \otimes \Phi_{G_A G_B}). \quad (165)$$

As Alice sends the systems A^n through the channel, the output state is

$$\omega_{K\bar{K}G_B B^n} \equiv \mathcal{N}_{A \rightarrow B}^{\otimes n} (\omega_{K\bar{K}G_B A^n}). \quad (166)$$

If the entanglement assistance is present, then Bob can access G_B . In this case, Bob performs a decoding channel $\mathcal{D}_{G_B B^n \rightarrow \check{M}}$, hence

$$\rho_{K\bar{K}\check{M}} \equiv \mathcal{D}_{G_B B^n \rightarrow \check{M}}(\rho_{K\bar{K}G_B B^n}). \quad (167)$$

On the other hand, without assistance, Bob performs $\mathcal{D}_{B^n \rightarrow \hat{M}}^*$, producing

$$\rho_{K\bar{K}\hat{M}G_B}^* \equiv \mathcal{D}_{B^n \rightarrow \hat{M}}^*(\rho_{K\bar{K}G_B B^n}). \quad (168)$$

Since Bob has not received the entanglement resources, the system G_B is not affected by itself.

Consider a sequence of codes $(\mathcal{F}_n, \mathcal{D}_n, \mathcal{D}_n^*)$ for entanglement generation given unreliable assistance, such that

$$\frac{1}{2} \|\rho_{\check{M}\bar{K}} - \Phi_{\bar{M}\bar{K}}\|_1 \leq \alpha_n, \quad (169)$$

$$\frac{1}{2} \|\rho_{\hat{M}K}^* - \Phi_{MK}\|_1 \leq \alpha_n^*, \quad (170)$$

where α_n, α_n^* tend to zero as $n \rightarrow \infty$.

By the Alicki-Fannes-Winter inequality^{76;77 55} Theorem 11.10.3, (170) implies $|H(K|\hat{M})_{\rho^*} - H(K|M)_{\Phi}| \leq n\varepsilon_n$, or equivalently,

$$|I(K)\hat{M}_{\rho^*} - I(K)M_{\Phi}| \leq n\varepsilon_n, \quad (171)$$

where ε_n tends to zero as $n \rightarrow \infty$. Observe that $I(K)M_{\Phi} = H(M)_{\Phi} - H(KM)_{\Phi} = nQ - 0 = nQ$. Thus,

$$\begin{aligned} nQ &= I(K)M_{\Phi} \\ &\leq I(K)\hat{M}_{\rho^*} + n\varepsilon_n \\ &\leq I(K)B^n_{\omega} + n\varepsilon_n, \end{aligned} \quad (172)$$

where the last line follows from (168) and the data processing inequality for the coherent information⁵⁵ Theorem 11.9.3. In addition,

$$\begin{aligned} nQ &= H(K)_{\Phi} \\ &= H(K|\bar{K}G_B)_{\Phi \otimes \Phi} \\ &= H(K|\bar{K}G_B)_{\omega}, \end{aligned} \quad (173)$$

where the second line follows since K and \bar{K} are in a product state.

As for decoding with entanglement assistance, (169) implies $|I(\bar{K}; \bar{M})_{\Phi} - I(\bar{K}; \check{M})_{\rho}| \leq n\bar{\varepsilon}_n$, by the Alicki-Fannes-Winter inequality, where $\bar{\varepsilon}_n$ tends to zero as $n \rightarrow \infty$. Therefore,

$$\begin{aligned} n(Q + Q') &= \frac{1}{2} I(\bar{K}; \bar{M})_{\Phi} \\ &\leq \frac{1}{2} I(\bar{K}; \check{M})_{\rho} + n\bar{\varepsilon}_n \\ &\leq \frac{1}{2} I(\bar{K}; G_B B^n)_{\omega} + n\bar{\varepsilon}_n \end{aligned} \quad (174)$$

by the data processing inequality for the quantum mutual information. By the chain rule, the mutual information above satisfies

$$\begin{aligned} I(\bar{K}; G_B B^n)_\omega &= I(\bar{K}; B^n | G_B)_\omega + I(\bar{K}; G_B)_{\Phi \otimes \Phi} \\ &= I(\bar{K}; B^n | G_B)_\omega \\ &\leq I(\bar{K} G_B; B^n)_\omega. \end{aligned} \quad (175)$$

The regularized converse follows from (172), (173), and (174)-(175), as we let A_1^n and A_2^n be quantum systems such that for some isometries $W_{K \rightarrow A_1^n}^{(1)}$ and $W_{\bar{K} G_B \rightarrow A_2^n}^{(2)}$,

$$\varphi_{A_1^n A_2^n A^n} = \left(W_{K \rightarrow A_1^n}^{(1)} \otimes W_{\bar{K} G_B \rightarrow A_2^n}^{(2)} \right) \varphi_{K \bar{K} G_B A^n} \left(W_{K \rightarrow A_1^n}^{(1)} \otimes W_{\bar{K} \rightarrow A_2^n}^{(2)} \right)^\dagger. \quad (176)$$

This completes the proof of Theorem 7. □

References

- [1] J. Yin, Y. H. Li, S. K. Liao, M. Yang, Y. Cao, L. Zhang, J. G. Ren, W. Q. Cai, W. Y. Liu, and S. L. Li, “Entanglement-based secure quantum cryptography over 1,120 kilometres,” *Nature*, vol. 582, no. 7813, pp. 501–505, 2020.
- [2] E. T. Khabiboulline, J. Borregaard, K. De Greve, and M. D. Lukin, “Optical interferometry with quantum networks,” *Phys. Rev. Lett.*, vol. 123, no. 7, p. 070504, 2019.
- [3] Q. Zhuang and Z. Zhang, “Physical-layer supervised learning assisted by an entangled sensor network,” *Phys. Rev. X*, vol. 9, no. 4, p. 041023, 2019.
- [4] Y. Xia, W. Li, Q. Zhuang, and Z. Zhang, “Quantum-enhanced data classification with a variational entangled sensor network,” *Phys. Rev. X*, vol. 11, no. 2, p. 021047, 2021.
- [5] S. Adhikary, “Entanglement assisted training algorithm for supervised quantum classifiers,” *Quantum Info. Proc.*, vol. 20, no. 8, pp. 1–12, 2021.
- [6] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, “Entanglement-assisted classical capacity of noisy quantum channels,” *Phys. Rev. Lett.*, vol. 83, no. 15, p. 3081, Oct 1999.
- [7] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, “Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem,” *IEEE Trans. Inf. Theory*, vol. 48, no. 10, pp. 2637–2655, Oct 2002.
- [8] S. Hao, H. Shi, W. Li, J. H. Shapiro, Q. Zhuang, and Z. Zhang, “Entanglement-assisted communication surpassing the ultimate classical capacity,” *Phys. Rev. Lett.*, vol. 126, no. 25, p. 250501, 2021.

- [9] G. S. Jaeger and V. Sergienko, “Entanglement sudden death: a threat to advanced quantum key distribution?” *Natural Computing*, vol. 13, no. 4, pp. 459–467, 2014.
- [10] J. Yin, Y. Cao, Y. H. Li, J. G. Ren, S. K. Liao, L. Zhang, W. Q. Cai, W. Y. Liu, B. Li, and H. Dai, “Satellite-to-ground entanglement-based quantum key distribution,” *Phys. Rev. Lett.*, vol. 119, no. 20, p. 200501, 2017.
- [11] G. Fettweis, H. Boche, T. Wiegand, E. Zielinski, H. Schotten, P. Merz, S. Hirche, A. Festag, W. Häffner, M. Meyer, and E. Steinbach, “The Tactile Internet-ITU-T Technology Watch Report,” *Int. Telecom. Union (ITU), Geneva*, 2014.
- [12] G. Fettweis and H. Boche, “6G: The personal tactile internet - and open questions for information theory,” *IEEE BITS the Information Theory Magazine*, Oct 2021.
- [13] —, “On 6G and trustworthiness,” *Proc. ACM, invited, to be published*, 2022.
- [14] H. Boche, R. Schaefer, and H. Poor, “On the algorithmic solvability of channel dependent classification problems in communication systems,” *IEEE/ACM Transactions on Networking*, vol. 29, no. 3, pp. 1155–1168, Jun 2021.
- [15] A. S. Holevo, “The capacity of the quantum channel with general signal states,” *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 269–273, Jan 1998.
- [16] B. Schumacher and M. D. Westmoreland, “Sending classical information via noisy quantum channels,” *Phys. Rev. A*, vol. 56, no. 1, p. 131, July 1997.
- [17] A. S. Holevo, *Quantum systems, channels, information: a mathematical introduction*. Walter de Gruyter, 2012, vol. 16.
- [18] I. Devetak, “The private classical capacity and quantum capacity of a quantum channel,” *IEEE Trans. Inf. Theory*, vol. 51, no. 1, pp. 44–55, 2005.
- [19] C. Shannon, “A mathematical theory of communication,” *Bell Syst. Tech. J*, vol. 27, pp. 379–423, 623–656, Jul 1948.
- [20] P. W. Shor, “The classical capacity achievable by a quantum channel assisted by a limited entanglement,” *Quantum Inf. Comp.*, vol. 4, no. 6, pp. 537–545, Dec 2004.
- [21] I. Devetak, A. W. Harrow, and A. J. Winter, “A resource framework for quantum Shannon theory,” *IEEE Trans. Inf. Theory*, vol. 54, no. 10, pp. 4587–4618, Oct 2008.
- [22] M. Hsieh and M. M. Wilde, “Entanglement-assisted communication of classical and quantum information,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4682–4704, Sep. 2010.

- [23] —, “Trading classical communication, quantum communication, and entanglement in quantum Shannon theory,” *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4705–4730, Sep 2010.
- [24] M. M. Wilde and M. H. Hsieh, “The quantum dynamic capacity formula of a quantum channel,” *Quantum Inf. Proc.*, vol. 11, no. 6, pp. 1431–1463, Sep 2012.
- [25] K. Wang and M. Hayashi, “Permutation enhances classical communication assisted by entangled states,” in *2020 IEEE International Symposium on Information Theory (ISIT)*, Los Angeles, CA, USA, 2020, pp. 1840–1845.
- [26] Q. Zhuang, E. Y. Zhu, and P. W. Shor, “Additive classical capacity of quantum channels assisted by noisy entanglement,” *Phys. Rev. Lett.*, vol. 118, no. 20, p. 200503, 2017.
- [27] J. Nötzel and S. DiAdamo, “Entanglement-assisted data transmission as an enabling technology: A link-layer perspective,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT’2020)*, Los Angeles, CA, USA, 2020, pp. 1955–1960.
- [28] U. Pereg, C. Deppe, and H. Boche, “Quantum channel state masking,” *IEEE Trans. Inf. Theory*, vol. 67, no. 4, pp. 2245–2268, 2021.
- [29] Y. Steinberg, “Channels with cooperation links that may be absent,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT’2014)*, 2014, pp. 1947–1951.
- [30] W. Huleihel and Y. Steinberg, “Channels with cooperation links that may be absent,” *IEEE Trans. Inf. Theory*, vol. 63, no. 9, pp. 5886–5906, 2017.
- [31] —, “Multiple access channel with unreliable cribbing,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT’2016)*, 2016, pp. 1491–1495.
- [32] D. Itzhak and Y. Steinberg, “The broadcast channel with degraded message sets and unreliable conference,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT’2017)*, 2017, pp. 1043–1047.
- [33] —, “The broadcast channel with degraded message sets and unreliable conference,” *IEEE Trans. Inf. Theory*, vol. 67, no. 9, pp. 5623–5650, 2021.
- [34] U. Pereg and Y. Steinberg, “Arbitrarily varying broadcast channel with uncertain cooperation,” in *Proc. Int’l Zurich Semin. Inf. Commun. (IZS’2020)*. ETH Zurich, 2020, pp. 63–67.
- [35] L. H. Ozarow, S. Shamai, and A. D. Wyner, “Information theoretic considerations for cellular mobile radio,” *IEEE Trans. Vehicular Tech.*, vol. 43, no. 2, pp. 359–378, 1994.
- [36] R. Karasik, O. Simeone, and S. Shamai, “Robust uplink communications over fading channels with variable backhaul connectivity,” *IEEE Trans. Inf. Theory*, vol. 12, no. 11, pp. 5788–5799, 2013.
- [37] G. Caire and D. Tuninetti, “The throughput of hybrid-ARQ protocols for the Gaussian collision channel,” *IEEE Trans. Inf. Theory*, vol. 47, no. 5, pp. 1971–1988, 2001.

- [38] A. Steiner and S. Shamai, “Multi-layer broadcasting hybrid-ARQ strategies for block fading channels,” *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2640–2650, 2008.
- [39] A. Goldsmith, S. A. Jafar, I. Maric and S. Srinivasa, “Multi-layer broadcasting hybrid-ARQ strategies for block fading channels,” *Proceedings of the IEEE*, vol. 97, no. 5, pp. 894–914, 2009.
- [40] C. H. Bennett, D. P. DiVincenzo, P. W. Shor, J. A. Smolin, B. M. Terhal, and W. K. Wootters, “Remote state preparation,” *Phys. Rev. Lett.*, vol. 87, no. 7, p. 077902, 2001.
- [41] H. Barnum, M. A. Nielsen, and B. Schumacher, “Information transmission through a noisy quantum channel,” *Phys. Rev. A*, vol. 57, no. 6, p. 4153, June 1998.
- [42] S. Lloyd, “Capacity of the noisy quantum channel,” *Phys. Rev. A*, vol. 55, no. 3, p. 1613, March 1997.
- [43] P. W. Shor, “The quantum channel capacity and coherent information,” in *Lecture notes, MSRI Workshop Quant. Comput.*, 2002.
- [44] C. H. Bennett and S. J. Wiesner, “Communication via one-and two-particle operators on Einstein-Podolsky-Rosen states,” *Phys. Rev. Lett.*, vol. 69, no. 20, p. 2881, Nov 1992.
- [45] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels,” *Physical review letters*, vol. 70, no. 13, p. 1895, 1993.
- [46] H. G. Eggleston, “Convexity,” *J. London Math. Society*, vol. 1, no. 1, pp. 183–186, 1966.
- [47] J. Yard, P. Hayden, and I. Devetak, “Capacity theorems for quantum multiple-access channels: classical-quantum and quantum-quantum capacity regions,” *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3091–3113, July 2008.
- [48] C. King, “The capacity of the quantum depolarizing channel,” *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 221–229, 2003.
- [49] K. Arora, J. Singh, and Y. S. Randhawa, “A survey on channel coding techniques for 5g wireless networks,” *Telecommun. Syst.*, pp. 1–27, 2019.
- [50] D. J. Costello and G. D. Forney, “Channel coding: The road to channel capacity,” *Proc. IEEE*, vol. 95, no. 6, pp. 1150–1177, 2007.
- [51] E. Nisioti and N. Thomos, “Design of capacity-approaching low-density parity-check codes using recurrent neural networks,” [arXiv:2001.01249](https://arxiv.org/abs/2001.01249), 2020.
- [52] T. Richardson and S. Kudekar, “Design of low-density parity check codes for 5g new radio,” *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 28–34, 2018.

- [53] J. Körner, “The concept of single-letterization in information theory,” in *Open Prob. Commun. Comp.* Springer, 1987, pp. 35–36.
- [54] U. Pereg, “Communication over quantum channels with parameter estimation,” *IEEE Trans. Inf. Theory*, 2021.
- [55] M. M. Wilde, *Quantum information theory*, 2nd ed. Cambridge University Press, 2017.
- [56] R. Stassi, M. Cirio, and F. Nori, “Scalable quantum computer with superconducting circuits in the ultrastrong coupling regime,” *npj Quantum Information*, vol. 6, no. 1, pp. 1–6, 2020.
- [57] N. M. Linke, D. Maslov, M. Roetteler, S. Debnath, C. Figgatt, K. A. Landsman, K. Wright, and C. Monroe, “Experimental comparison of two quantum computing architectures,” *Proc. Nation. Acad. Scien.*, vol. 114, no. 13, pp. 3305–3310, 2017.
- [58] F. Dupuis, P. Hayden, and K. Li, “A father protocol for quantum broadcast channels,” *IEEE Trans. Inf. Theory*, vol. 56, no. 6, pp. 2946–2956, June 2010.
- [59] H. Qi, K. Sharma, and M. M. Wilde, “Entanglement-assisted private communication over quantum broadcast channels,” *J. Phys. A: Math. and Theo.*, vol. 51, no. 37, p. 374001, 2018.
- [60] K. Li and A. Winter, “Relative entropy and squashed entanglement,” *Commun. Math. Phys.*, vol. 326, no. 1, pp. 63–80, Jan 2014.
- [61] F. Dupuis, “The capacity of quantum channels with side information at the transmitter,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT’2009)*, June 2009, pp. 948–952.
- [62] J. Yard, P. Hayden, and I. Devetak, “Quantum broadcast channels,” *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 7147–7162, Oct 2011.
- [63] U. Pereg, “Entanglement-assisted capacity of quantum channels with side information,” [arXiv:1909.09992](https://arxiv.org/pdf/1909.09992), Sep 2019. [Online]. Available: <https://arxiv.org/pdf/1909.09992.pdf>
- [64] F. Dupuis, “Coding for quantum channels with side information at the transmitter,” *arXiv preprint arXiv:0805.3352*, 2008.
- [65] U. Pereg, C. Deppe, and H. Boche, “Quantum broadcast channels with cooperating decoders: An information-theoretic perspective on quantum repeaters,” *J. Math. Phys.*, vol. 62, no. 6, p. 062204, 2021.
- [66] F. Dupuis, “The decoupling approach to quantum information theory,” Ph.D. dissertation, Université de Montréal, 2010.
- [67] M. A. Nielsen and I. Chuang, “Quantum computation and quantum information,” 2002.
- [68] M. Hsieh, I. Devetak, and A. Winter, “Entanglement-assisted capacity of quantum multiple-access channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3078–3090, July 2008.

- [69] R. Renner, “Security of quantum key distribution,” *Int’l J. Quantum Info.*, vol. 6, no. 01, pp. 1–127, 2008.
- [70] A. Uhlmann, “The “transition probability” in the state space of a*-algebra,” *Reports Math. Phys.*, vol. 9, no. 2, pp. 273–279, 1976.
- [71] U. Pereg, “Entanglement-assisted capacity of quantum channels with side information,” in *Int. Zürich Seminar Inf. Commun. (IZS’2020)*, Zürich, Switzerland, Feb 2020, pp. 106–110.
- [72] —, “Communication over quantum channels with parameter estimation,” [arXiv:2001.00836](https://arxiv.org/pdf/2001.00836), Jan 2020. [Online]. Available: <https://arxiv.org/pdf/2001.00836.pdf>
- [73] —, “Communication over quantum channels with parameter estimation,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT’2020)*, June 2020.
- [74] A. Winter, “Coding theorem and strong converse for quantum channels,” *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2481–2485, Nov 1999.
- [75] T. Ogawa and H. Nagaoka, “Making good codes for classical-quantum channel coding via quantum hypothesis testing,” *IEEE Trans. Inf. Theory*, vol. 53, no. 6, pp. 2261–2266, June 2007.
- [76] R. Alicki and M. Fannes, “Continuity of quantum conditional information,” *J. Phys. A: Math. General*, vol. 37, no. 5, pp. L55–L57, Jan 2004.
- [77] A. Winter, “Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints,” *Commun. in Math. Phys.*, vol. 347, no. 1, pp. 291–313, 2016.