Amortized entanglement of a quantum channel and approximately teleportation-simulable channels

Eneet Kaur1 and Mark M Wilde1,2

1 Department of Physics and Astronomy, Louisiana State University, Baton Rouge, LA 70803, United States of America
2 Center for Computation and Technology, Louisiana State University, Baton Rouge, LA 70803, United States of America

E-mail: ekaur1@lsu.edu and mwilde@lsu.edu

Received 2 September 2017, revised 6 November 2017
Accepted for publication 28 November 2017
Published 15 December 2017

Abstract
This paper defines the amortized entanglement of a quantum channel as the largest difference in entanglement between the output and the input of the channel, where entanglement is quantified by an arbitrary entanglement measure. We prove that the amortized entanglement of a channel obeys several desirable properties, and we also consider special cases such as the amortized relative entropy of entanglement and the amortized Rains relative entropy. These latter quantities are shown to be single-letter upper bounds on the secret-key-agreement and PPT-assisted quantum capacities of a quantum channel, respectively. Of especial interest is a uniform continuity bound for these latter two special cases of amortized entanglement, in which the deviation between the amortized entanglement of two channels is bounded from above by a simple function of the diamond norm of their difference and the output dimension of the channels. We then define approximately teleportation- and positive-partial-transpose-simulable (PPT-simulable) channels as those that are close in diamond norm to a channel which is either exactly teleportation- or PPT-simulable, respectively. These results then lead to single-letter upper bounds on the secret-key-agreement and PPT-assisted quantum capacities of channels that are approximately teleportation- or PPT-simulable, respectively. Finally, we generalize many of the concepts in the paper to the setting of general resource theories, defining the amortized resourcefulness of a channel and the notion of $\nu$-freely-simulable channels, connecting these concepts in an operational way as well.
1. Introduction

Evaluating or determining bounds on the various communication capacities of a quantum channel is one of the main concerns of quantum information theory [Hol12, Wil16a]. One can consider supplementing a channel with an additional resource such as free entanglement [BSST99, BSST02] or classical communication [BBP’96, BDSW96], and such a consideration leads to different kinds of capacities. Supplementing a channel with free classical communication, with the goal being to communicate quantum information or private classical information reliably, is of particular relevance due to its connection with the operational setting of quantum key distribution [BB84, Eke91]. The former is called the local operations and classical communication (LOCC) assisted quantum capacity, while the latter is called the secret-key-agreement capacity.

The relevance of these latter capacities is that an upper bound on them can serve as a benchmark to determine whether one has experimentally implemented a working quantum repeater [LG15], which is a device needed for the practical implementation of quantum key distribution. A first result in this direction, building on earlier developments in [CW04, Chr06, HHHO05b, HHHO09], is due to [TGW14b, TGW14a] (see also [Wil16b]), in which it was shown that the squashed entanglement of a quantum channel is an upper bound on both its LOCC-assisted quantum capacity and its secret-key-agreement capacity. Some follow-up works [PLOB16, WTB17] then considered other entanglement measures such as relative entropy of entanglement and established their relevance as bounds on these capacities in certain cases. There has been an increasing interest in this topic in recent years, with a series of papers developing it further [TGW14b, TGW14a, STW16, PLOB16, GEW16, TSW16, AML16, WTB17, CMH17, Wil16b, BA17, RGR’17, KW17, TSW17, RKB’17].

In this paper, we develop this topic even further, in the following ways:

1. First, we define the amortized entanglement of a quantum channel as the largest difference in the entanglement between the output and the input of the channel, with entanglement quantified by some entanglement measure [HHHH09]. We note that amortized entanglement is closely related to ideas put forth in [BHLS03, LHL03, CMH17, BDGDMW17], which were used therein to give bounds on the performance of adaptive protocols (see also the very recent paper RKB’17 for related ideas).

2. We then prove several properties of the amortized entanglement, while considering special cases in which the entanglement measure is set to the relative entropy of entanglement [VP98] or the Rains relative entropy [Rai99, Rai01, ADMVW02]. These latter quantities are shown to be single-letter upper bounds on the secret-key-agreement and PPT-assisted quantum capacities of a quantum channel, respectively. Another important property that we establish in these special cases is that the amortized entanglement obeys a uniform continuity bound of the flavor in [Win16, Shi16], with a dependence on the output dimension of the two channels under consideration and the diamond norm of their difference [Kit97].

3. These latter results lead to upper bounds on the secret-key-agreement capacity of approximately teleportation-simulable channels (channels that are close in diamond
norm to a teleportation-simulable channel [BDSW96, HHH99, CDP09]). Similarly, we find upper bounds on the positive-partial-transpose (PPT) assisted quantum capacity for approximately PPT-simulable channels (defined later). The main idea behind obtaining these bounds is broadly similar to the approach of approximately degradable channels put forth in [SSWR14].

4. We next showcase the aforementioned bounds for a simple qubit channel, which is a convex combination of an amplitude damping channel and a depolarizing channel (note that this channel is considered in the concurrent work [LKDW17] as well). The main finding here is that the upper bounds from approximate simulation are reasonably close to lower bounds on the capacities whenever the noise in the channel is low, and this result is consistent with that which was found in earlier work [SSWR14, LLS17].

5. Finally, we discuss how many of the concepts developed in our paper can be extended to general resource theories [BG15, Fri17, dRKR15, KdR16]. In particular, we discuss the amortized resourcefulness of a quantum channel and prove how it leads to an upper bound on the amount of resourcefulness that can be extracted from multiple calls to a quantum channel by interleaving calls to it with free channels. We also introduce the notion of a \( \nu \)-freely-simulable channel as a generalization of the concept of a teleportation-simulable channel.

At the end of the paper, we conclude with a summary and open questions. The rest of our paper proceeds in the order given above, appendix A provides some supplementary lemmas that are needed to establish the uniform continuity bound mentioned above, and appendix B discusses the relation between approximate covariance [LKDW17] and approximately teleportation-simulable channels, as well as showing how to simulate the twirling of a channel [BDSW96] via a generalized teleportation protocol. Throughout our paper, we use notation and concepts that are by now standard in quantum information theory, and we point the reader to [Wil16a] for background.

2. Amortized entanglement of a quantum channel

We begin by defining the amortized entanglement of a quantum channel as the largest difference that can be achieved between the entanglement of an output and input state of a quantum channel (see figure 1 for a visual illustration of the scenario to which amortized entanglement corresponds). Definition 1 below applies to any entanglement measure, which, as in [HHHH99], we define to be any function of a bipartite quantum state that is monotone with respect to an LOCC channel, i.e. a quantum channel that can be implemented by local operations and classical communication (LOCC). As a minimal requirement, we also take an entanglement measure to be equal to zero when evaluated on a product state and non-negative in general.

**Definition 1 (Amortized entanglement of a quantum channel).** For a quantum channel \( \mathcal{N}_{A \rightarrow B} \) and an entanglement measure \( E \), we define the channel’s amortized entanglement as follows:

\[
E_A(\mathcal{N}) \equiv \sup_{\rho_{A'AB'}} E(A'; BB')_\theta - E(A'A; B')_\rho,
\]

where \( \theta_{A'BB'} \equiv \mathcal{N}_{A \rightarrow B}(\rho_{A'AB'}) \).

As we stressed in the introduction, the quantity \( E_A(\mathcal{N}) \) is closely related to ideas from prior work [BHLS03, LHL03, CMH17, BDGDMW17], as well as the very recent RKB+17.
Intuitively, the amortized entanglement of a channel captures the largest difference in entanglement that can be generated between the output state on systems $A':BB'$ and the input state on systems $A':B'$, the former of which is generated by the quantum channel $\mathcal{N}_{A\rightarrow B}$.

Recall that the quantum relative entropy

$$D(\varsigma \parallel \xi) \equiv \text{Tr} \{ \varsigma \log_2 \varsigma - \log_2 \xi \}, \quad (2.2)$$

whenever $\text{supp}(\varsigma) \subseteq \text{supp}(\xi)$ and it is equal to $+\infty$ otherwise. We obtain two special cases of amortized entanglement by considering the relative entropy of entanglement [VP98] and the Rains relative entropy [Rai99, Rai01] as the underlying entanglement measures. The former entanglement measure is relevant in the context of secret-key distillation [HHHO05b, HHH09] and the latter in the context of entanglement distillation [Rai99, Rai01], both tasks performed with respect to a bipartite state. Sections 3 and 4 show how the amortized measures given below are relevant in the context of secret-key-agreement and quantum communication assisted by classical communication, respectively, both tasks performed with respect to a quantum channel.

**Definition 2 (Amortized relative entropy of entanglement).** For a quantum channel $\mathcal{N}_{A\rightarrow B}$, its amortized relative entropy of entanglement is defined as follows:

$$E_{AR}(\mathcal{N}) \equiv \sup_{\rho_{A'AB'}} E_R(A';BB')_\theta - E_R(A';B')_{\rho'}, \quad (2.3)$$

where $\theta_{A';BB'} \equiv \mathcal{N}_{A\rightarrow B}(\rho_{A'AB'})$ and the relative entropy of entanglement $E_R(C;D)_\tau$ of a bipartite state $\tau_{CD}$ is defined as [VP98]

$$E_R(C;D)_\tau \equiv \inf_{\sigma_{CD} \in \text{SEP}(C,D)} D(\tau_{CD} \parallel \sigma_{CD}), \quad (2.4)$$

with SEP denoting the set of separable states [Wer89].

**Definition 3 (Amortized Rains relative entropy).** For a quantum channel $\mathcal{N}_{A\rightarrow B}$, its amortized Rains relative entropy is defined as follows:

$$R_A(\mathcal{N}) \equiv \sup_{\rho_{A'AB'}} R(A';BB')_\theta - R(A';B')_{\rho'}, \quad (2.5)$$
where $\theta_{A'B'} \equiv N_{A \to B} (\rho_{A'B'})$ and the Rains relative entropy $R(C; D)_{\tau}$ of a bipartite state $\tau_{CD}$ is defined as [Rai99, Rai01]

$$R(C; D)_{\tau} \equiv \inf_{\sigma_{CD} \in \text{PPT}'(C; D)} D(\tau_{CD} \| \sigma_{CD}),$$

(2.6)

with $\text{PPT}'(C; D)$ denoting the Rains set [ADMVW02]:

$$\text{PPT}'(C; D) = \{ \sigma_{CD} : \sigma_{CD} \geq 0 \land \| T_D(\sigma_{CD}) \|_1 \leq 1 \},$$

(2.7)

and $T_D$ denotes the partial transpose of system $D$.

Observe that $\text{SEP} \subset \text{PPT}'$. Also, note that the quantities $E_{AB}(N)$ and $R_A(N)$ involve an optimization over mixed states on systems $A'AB'$, and we do not have an upper bound on the dimension of the $A'$ or $B'$ systems. So these quantities could be difficult to calculate in general. One of the main contributions of our paper (see section 5) is to show how this quantity can be approximated well in certain cases.

### 2.1. Amortized entanglement versus the entanglement of a channel

For any entanglement measure $E$, the entanglement of the channel is defined as [TGW14b, TGW14a, TWW17, PLOB16, RKB17]

$$E(N) \equiv \sup_{\psi_{A'A}} E(A'; B)_{\theta},$$

(2.8)

where

$$\theta_{A'B} \equiv N_{A \to B}(\psi_{A'A}),$$

(2.9)

and $\psi_{A'A}$ is an arbitrary pure bipartite state with system $A'$ isomorphic to the channel input system $A$. It suffices to optimize over pure states of the above form instead of general mixed states, due to purification, Schmidt decomposition, and monotonicity of the entanglement measure $E$ with respect to local operations (one of which is partial trace). Particular measures of interest are a channel’s relative entropy of entanglement and the Rains relative entropy:

$$E_R(N) = \sup_{\psi_{A'A}} E_R(A'; B)_{\theta},$$

(2.10)

$$R(N) = \sup_{\psi_{A'A}} R(A'; B)_{\theta}.$$  

(2.11)

The amortized entanglement of a channel is never smaller than that channel’s entanglement. That is, we always have the following inequality:

$$E_A(N) \geq E(N),$$

(2.12)

by taking $B'$ to be a trivial system in definition 1.

The squashed entanglement $E_{sq}$ is a special entanglement measure that obeys many desirable properties [CW04, KW04, Chr06, BCY11, LW14] (see also the various discussions in [Tuc99, Tuc02]). One can also define the dynamic version of this entanglement measure as the squashed entanglement of a channel [TGW14b], denoted as $E_{sq}(N)$. A particular property of squashed entanglement was established as [TGW14b, theorem 7]. We remark here (briefly) that [76, theorem 7] implies the following inequality for the amortized version of squashed entanglement

$$E_{A, sq}(N) \leq E_{sq}(N),$$

(2.13)
which by (2.12), implies the following equality for squashed entanglement:

$$E_{A_{sq}}(\mathcal{N}) = E_{sq}(\mathcal{N}).$$

(2.14)

Thus, the squashed entanglement is rather special, in the sense that amortization does not enhance its value.

2.2. Convexity of a channel’s amortized entanglement

An entanglement measure $E$ is convex with respect to states $[HHHH09]$ if for all bipartite states $\rho_{CD}^0$ and $\rho_{CD}^1$ and $\lambda \in [0,1]$, the following equality holds:

$$E(C:D)_{\rho^\lambda} \leq \lambda E(C:D)_{\rho^0} + (1 - \lambda) E(C:D)_{\rho^1},$$

(2.15)

where $\rho_{CD}^\lambda = \lambda \rho_{CD}^0 + (1 - \lambda) \rho_{CD}^1$. As the following proposition states, this property extends to amortized entanglement:

**Proposition 4 (Convexity).** Let $E$ be an entanglement measure that is convex with respect to states. Then the amortized entanglement $E_A$ of a channel is convex with respect to channels, in the sense that the following inequality holds for all quantum channels $\mathcal{N}^0$ and $\mathcal{N}^1$ and $\lambda \in [0,1]$:

$$E_A(\mathcal{N}^\lambda) \leq \lambda E_A(\mathcal{N}^0) + (1 - \lambda) E_A(\mathcal{N}^1),$$

(2.16)

where $\mathcal{N}^\lambda = \lambda \mathcal{N}^0 + (1 - \lambda) \mathcal{N}^1$.

**Proof.** Let $\rho_{A'AB'}$ be a state and set $\tau_{A'B'B'}^\lambda = \lambda \mathcal{N}^\lambda_{A'\rightarrow A}(\rho_{A'AB'}) + (1 - \lambda) \mathcal{N}^1(\rho_{A'AB'})$. Then consider that

$$E(\lambda A'; A'B')_{\tau} - E(\lambda A'; A'B')_{\rho} = E(\lambda A'; A'B')_{\tau} - \lambda E(A'A; B')_{\rho} - (1 - \lambda) E(A'A; B')_{\rho}$$

(2.17)

$$\leq \lambda E(\lambda A'; A'B')_{\mathcal{N}^\lambda} + (1 - \lambda) E(\lambda A'; A'B')_{\mathcal{N}^1} - \lambda E(A'A; B')_{\rho} - (1 - \lambda) E(A'A; B')_{\rho}$$

(2.18)

$$= (\lambda E(A'; B')_{\mathcal{N}^\lambda})_{(\rho)} + (1 - \lambda) E(A'; B')_{\mathcal{N}^1} - E(A'A; B')_{\rho} - (1 - \lambda) E(A'A; B')_{\rho}$$

(2.19)

$$\leq \lambda E_A(\mathcal{N}^0) + (1 - \lambda) E_A(\mathcal{N}^1).$$

(2.20)

The first equality follows from expanding the second term. The first inequality follows from the convexity of the entanglement measure $E$. The second equality from rearrangement of the terms. The second inequality follows from taking the supremum over all states $\rho_{A'AB'}$. Since the inequality in (2.20) holds for all states $\rho_{A'AB'}$, the proof is complete.

2.3. Faithfulness of a channel’s amortized entanglement

An entanglement measure $E$ is faithful if it is equal to zero if and only if the state on which it is evaluated is a separable state. A quantum channel $\mathcal{N}$ is entanglement-breaking $[HSR03]$ if for all input states $\rho_A$, the output state $(\text{id}_R \otimes \mathcal{N}_{A\rightarrow B})(\rho_A)$ is a separable state. The following proposition extends the faithfulness property of entanglement measures to amortized entanglement and entanglement-breaking channels:
Proposition 5. (Faithfulness) Let $E$ be an entanglement measure that is equal to zero for all separable states. If a channel $\mathcal{N}$ is entanglement-breaking, then its amortized entanglement $E_A(\mathcal{N})$ is equal to zero. If the entanglement measure $E$ is faithful and the amortized entanglement $E_A(\mathcal{N})$ of a channel $\mathcal{N}$ is equal to zero, then the channel $\mathcal{N}$ is entanglement-breaking.

Proof. We begin by proving the first statement above: for an arbitrary entanglement measure $E$, if a channel $\mathcal{N}$ is entanglement-breaking, then its amortized entanglement is equal to zero. Let $\rho_{A'AB'}$ be an arbitrary input state to the channel, and let $\sigma_{A'BB'} = N(\rho_{A'AB'})$ denote the output of the channel. Recall that any entanglement-breaking channel can be represented as a measurement of the input system, followed by the preparation of a state on the output system, conditioned on the outcome of the measurement [HSR03]. As such, the channel itself can be implemented by LOCC from the sender to the receiver. Then consider that the respective input and output quantum systems for quantum channel $\mathcal{N}$, and let $A_1$ and $B_1$ denote the respective input and output systems for quantum channel $\mathcal{M}$. Let $\rho_{A'1A_2B'}$ denote a state to consider at the input of $\mathcal{N} \otimes \mathcal{M}$ when optimizing the amortized entanglement. Let $\theta_{A'1A_2B'} = (\mathcal{N}_{A_1 \rightarrow B_1} \otimes \mathcal{M}_{A_2 \rightarrow B_2})(\rho_{A'1A_2B'})$, which is the state at the output of the channel $\mathcal{N} \otimes \mathcal{M}$ when inputting $\rho_{A'1A_2B'}$. Define the intermediary state $\tau_{A'A_1A_2B'2} = \mathcal{M}_{A_2 \rightarrow B_2}(\rho_{A'A_1A_2B'}).$ Then consider that

$$E(\rho_{A'1A_2B'}; A'B') - E(\rho_{A'A_1A_2B'}; B') \leq E(\rho_{A'A_1A_2B'}; B') - E(\rho_{A'A_1A_2B'}; B') = E(\rho_{A'1A_2B'}; A'B') - E(\rho_{A'A_1A_2B'}; B') = E(\rho_{A'A_1A_2B'}; B').$$

By Proposition 6 (Subadditivity). For any entanglement measurement $E$, the amortized entanglement $E_A$ of a channel is a subadditive function of quantum channels, in the sense that the following inequality holds for quantum channels $\mathcal{N}$ and $\mathcal{M}$:

$$E_A(\mathcal{N} \otimes \mathcal{M}) \leq E_A(\mathcal{N}) + E_A(\mathcal{M}).$$

2.4. (Sub)additivity of a channel’s amortized entanglement

Proof. Let $A_1$ and $B_1$ denote the respective input and output systems for quantum channel $\mathcal{N}$, and let $A_2$ and $B_2$ denote the respective input and output quantum systems for quantum channel $\mathcal{M}$. Let $\rho_{A'1A_2B'}$ denote a state to consider at the input of $\mathcal{N} \otimes \mathcal{M}$ when optimizing the amortized entanglement. Let $\theta_{A'1A_2B'} = (\mathcal{N}_{A_1 \rightarrow B_1} \otimes \mathcal{M}_{A_2 \rightarrow B_2})(\rho_{A'1A_2B'})$, which is the state at the output of the channel $\mathcal{N} \otimes \mathcal{M}$ when inputting $\rho_{A'1A_2B'}$. Define the intermediary state $\tau_{A'A_1A_2B'} = \mathcal{M}_{A_2 \rightarrow B_2}(\rho_{A'A_1A_2B'})$. Then consider that

$$E(\rho_{A'1A_2B'}; A'B') - E(\rho_{A'A_1A_2B'}; B') \leq E(\rho_{A'A_1A_2B'}; B') - E(\rho_{A'A_1A_2B'}; B') = E(\rho_{A'A_1A_2B'}; B') - E(\rho_{A'A_1A_2B'}; B') = E(\rho_{A'A_1A_2B'}; B').$$

By Proposition 6 (Subadditivity). For any entanglement measurement $E$, the amortized entanglement $E_A$ of a channel is a subadditive function of quantum channels, in the sense that the following inequality holds for quantum channels $\mathcal{N}$ and $\mathcal{M}$:

$$E_A(\mathcal{N} \otimes \mathcal{M}) \leq E_A(\mathcal{N}) + E_A(\mathcal{M}).$$

Proof. Let $A_1$ and $B_1$ denote the respective input and output systems for quantum channel $\mathcal{N}$, and let $A_2$ and $B_2$ denote the respective input and output quantum systems for quantum channel $\mathcal{M}$. Let $\rho_{A'1A_2B'}$ denote a state to consider at the input of $\mathcal{N} \otimes \mathcal{M}$ when optimizing the amortized entanglement. Let $\theta_{A'1A_2B'} = (\mathcal{N}_{A_1 \rightarrow B_1} \otimes \mathcal{M}_{A_2 \rightarrow B_2})(\rho_{A'1A_2B'})$, which is the state at the output of the channel $\mathcal{N} \otimes \mathcal{M}$ when inputting $\rho_{A'1A_2B'}$. Define the intermediary state $\tau_{A'A_1A_2B'} = \mathcal{M}_{A_2 \rightarrow B_2}(\rho_{A'A_1A_2B'})$. Then consider that

$$E(\rho_{A'1A_2B'}; A'B') - E(\rho_{A'A_1A_2B'}; B') \leq E(\rho_{A'A_1A_2B'}; B') - E(\rho_{A'A_1A_2B'}; B') = E(\rho_{A'A_1A_2B'}; B') - E(\rho_{A'A_1A_2B'}; B') = E(\rho_{A'A_1A_2B'}; B').$$

By Proposition 6 (Subadditivity). For any entanglement measurement $E$, the amortized entanglement $E_A$ of a channel is a subadditive function of quantum channels, in the sense that the following inequality holds for quantum channels $\mathcal{N}$ and $\mathcal{M}$:

$$E_A(\mathcal{N} \otimes \mathcal{M}) \leq E_A(\mathcal{N}) + E_A(\mathcal{M}).$$
The first equality follows by adding and subtracting $E(A'B_1;B_2B'')_\tau$. The second inequality follows because the states $\tau_{A'1;B_1B''}$ and $\theta_{A1;B_1B''}$ are particular states to consider at the respective input and output for the amortized entanglement of the channel $\mathcal{N}$, by making the identifications $A' \leftrightarrow A'$, $B' \leftrightarrow B_1B_2$, $B \leftrightarrow B_1$, and $A \leftrightarrow A_1$, while the states $\rho_{A'A1;B'B_2}$ and $\tau_{A'A1;B'B_2}$ are particular states to consider at the respective input and output for the amortized entanglement of the channel $\mathcal{M}$, by making the identifications $A' \leftrightarrow A'$, $B' \leftrightarrow B_1B_2$, $B \leftrightarrow B_2$, and $A \leftrightarrow A_2$. Since the inequality in (2.24) holds for all states $\rho_{A'A1;B'B_2}$, we can conclude the inequality in (2.22).

An immediate consequence of proposition 6 is the following inequality:

$$\sup_\mathcal{M} [E_A(\mathcal{N} \otimes \mathcal{M}) - E_A(\mathcal{M})] \leq E_A(\mathcal{N}),$$

(2.25)

where the supremum is with respect to a quantum channel $\mathcal{M}$. This inequality demonstrates that no other channel can help to enhance the amortized entanglement of a quantum channel. See [SSW08, WY16] for related notions, i.e. potential capacity.

An entanglement measure $E$ is additive with respect to states [HHHH09] if the following equality holds

$$E(\tau_{\mathcal{C};\mathcal{D};\mathcal{D}}) = E(\tau_{\mathcal{C};\mathcal{D}}) + E(\tau_{\mathcal{C};\mathcal{D}}),$$

(2.26)

where $\tau_{\mathcal{C};\mathcal{D};\mathcal{D}} = \xi_{\mathcal{C};\mathcal{D}} \otimes \zeta_{\mathcal{C};\mathcal{D}}$ and $\xi_{\mathcal{C};\mathcal{D}}$ and $\zeta_{\mathcal{C};\mathcal{D}}$ are bipartite states. It is subadditive if

$$E(\tau_{\mathcal{C};\mathcal{D};\mathcal{D}}) \leq E(\tau_{\mathcal{C};\mathcal{D}}) + E(\tau_{\mathcal{C};\mathcal{D}}),$$

(2.27)

and this latter property holds for both the relative entropy of entanglement and the Rains relative entropy [HHHH09]. The following proposition states that amortized entanglement is additive if the underlying entanglement measure is additive:

**Proposition 7. (Additivity)** For any entanglement measurement $E$ that is additive with respect to states, the amortized entanglement $E_A$ of a channel is an additive function of quantum channels, in the sense that the following equality holds for quantum channels $\mathcal{N}$ and $\mathcal{M}$:

$$E_A(\mathcal{N} \otimes \mathcal{M}) = E_A(\mathcal{N}) + E_A(\mathcal{M}).$$

(2.28)

**Proof.** The inequality $\leq$ holds for all channels as shown in proposition 6. To see the other inequality, let $\rho_{A1;B1} \otimes \kappa_{A1;B1}$ be an arbitrary state to consider for $E_A(\mathcal{N} \otimes \mathcal{M})$, and let

$$\theta_{A1;B1} = \mathcal{N} \rightarrow B_1(\rho_{A1;B1} \otimes \mathcal{M} \rightarrow B_1(\kappa_{A1;B1}).$$

(2.29)

Then

$$E_A(\mathcal{N} \otimes \mathcal{M}) \geq E(A_1',A_2';B_1B_2B_2')_\theta - E(A_1,A_2;B_1B_2B_2')_{\rho \otimes \kappa}$$

(2.30)

$$= E(A_1';B_1B_2')_\theta - E(A_1';B_1')_{\rho} + E(A_2';B_2B_2')_\theta - E(A_2'A_2';B_2')_{\kappa}.$$

(2.31)

The equality follows from the assumption that the underlying entanglement measure is additive with respect to states. Since the above inequality holds for all input states $\rho_{A1;B1}$ and $\kappa_{A1;B1}$, we can conclude (2.28) after applying definition 1.

### 2.5. Amortized entanglement and teleportation simulation

Teleportation simulation of a quantum channel is one of the earliest and most central insights in quantum information theory [BDSW96], and it is a key tool used to establish upper bounds
on capacities of quantum channels assisted by local operations and classical communication (LOCC) [BDSW96, WPGG07, NFC09, MH12]. The basic idea behind this tool is that a quantum channel can be simulated by the action of a teleportation protocol [BBC'93, BK98, Wer01] on a resource state $\omega_{RB}$ shared between the sender $A$ and receiver $B$. More generally, a channel $\mathcal{N}_{A\rightarrow B}$ with input system $A$ and output system $B$ is defined to be teleportation-simulable with associated resource state $\omega_{RB}$ if the following equality holds for all input states $\rho_A$ [HHH99, equation (11)]:

$$\mathcal{N}_{A\rightarrow B}(\rho_A) = L_{ARB\rightarrow B}(\rho_A \otimes \omega_{RB}),$$

(2.32)

where $L_{ARB\rightarrow B}$ is a quantum channel consisting of LOCC between the sender, who has systems $A$ and $R$, and the receiver, who has system $B$ ($L_{ARB\rightarrow B}$ can also be considered a generalized teleportation protocol, as in [Wer01]).

Whenever the underlying entanglement measure is subadditive with respect to quantum states, then one can easily bound the amortized entanglement $E_A(\mathcal{N})$ from above for channels that are teleportation-simulable:

**Proposition 8.** Let $E_S$ be an entanglement measure that is subadditive with respect to states, and let $E_{AS}$ denote its amortized version. If a channel $\mathcal{N}_{A\rightarrow B}$ is teleportation-simulable with associated state $\omega_{RB}$, then the following bound holds

$$E_{AS}(\mathcal{N}) \leq E_S(R;B)_{\omega},$$

(2.33)

where $E_{AS}(\mathcal{N})$ denotes the amortized entanglement defined through $E_S$ and definition 1.

**Proof.** By the definition of a teleportation-simulable channel, we have that

$$\mathcal{N}_{A\rightarrow B}(\rho_A) = L_{ARB\rightarrow B}(\rho_A \otimes \omega_{RB}),$$

(2.34)

where $L_{ARB\rightarrow B}$ is an LOCC channel. Then for any input state $\rho_{A'B'A}$, we have that

$$E_S(A';BB')_{L(\rho \otimes \omega)} - E_S(A'A;B')_{\rho} \leq E_S(A'AR;B'B)_{\rho \otimes \omega} - E_S(A'A;B')_{\rho} \leq E_S(A'A;B')_{\rho} + E_S(R;B)_{\omega} - E_S(A'A;B')_{\rho} \leq E_S(R;B)_{\omega} \leq E_S(R;B)_{\omega}.$$

(2.35)

The first inequality follows from monotonicity of $E_S$ with respect to LOCC channels (the fact that $E_S$ is an entanglement measure). The second inequality follows from the assumption that $E_S$ is subadditive.

Proposition 8 implies that the amortized entanglement of a channel never exceeds the entanglement of the maximally entangled state, whenever the underlying entanglement measure is subadditive. This follows because any channel can be simulated by teleportation using the maximally entangled state as the resource state, along with local processing. In particular, Alice could apply the channel locally to her system and then teleport it to Bob; also, she could first teleport to Bob and then he could perform the local processing. So this leads to the following upper bound on amortized entanglement in this case:

**Proposition 9 (Dimension bound).** Let $E_S$ be an entanglement measure that is subadditive with respect to states, and let $E_{AS}$ denote its amortized version. Let $\mathcal{N}_{A\rightarrow B}$ be a quantum channel. The following bound holds
\[ E_{AS}(\mathcal{N}) \leq \min \{ E_S(A; \bar{A})_\Phi, E_S(B; \bar{B})_\Phi \}, \]  
\tag{2.38}

where \( E_{AS}(\mathcal{N}) \) denotes the amortized entanglement defined through \( E_S \) and definition 1, \( \bar{A} \) is a system isomorphic to the channel input system \( A \), \( \bar{B} \) is a system isomorphic to the channel output system \( B \), and \( \Phi \) denotes the maximally entangled state. For the amortized relative entropy of entanglement and the amortized Rains relative entropy, the above implies that
\[ E_{AR}(\mathcal{N}), R_A(\mathcal{N}) \leq \log_2 \min \{ |A|, |B| \}, \]  
\tag{2.39}

because these underlying entanglement measures are equal to \( \log_2 d \) when evaluated on a maximally entangled state of Schmidt rank \( d \) [HHHH09].

In certain cases, the inequality in proposition 8 is actually an equality:

**Proposition 10.** Let \( E_S \) be an entanglement measure that is subadditive with respect to states, and let \( E_{AS} \) denote its amortized version. If a channel \( \mathcal{N}_{A \rightarrow B} \) is teleportation-simulable with associated state \( \omega_{RB} = \mathcal{N}_{A \rightarrow B}(\rho_{RA}) \) for some input state \( \rho_{RA} \), then the following equality holds
\[ E_{AS}(\mathcal{N}) = E_S(R; B)_\omega. \]  
\tag{2.40}

**Proof.** From proposition 8, we have that \( E_{AS}(\mathcal{N}) \leq E_S(R; B)_\omega \). The other inequality follows by picking \( \rho_{A'B'} = \rho_{RA} \), with the identification \( A' \leftrightarrow R \) and \( B' \leftrightarrow \emptyset \) (i.e. \( B' \) is a trivial system), and then we find that
\[ E_{AS}(\mathcal{N}) = \sup_{\rho_{A'B'}} E_S(A'; B')_\emptyset - E_S(A'A; B')_\rho \geq E_S(R; B)_\omega. \]  
\tag{2.41}

This concludes the proof. \( \blacksquare \)

**Remark 11.** For several channels with sufficient symmetry, such as covariant channels, one can pick the input state \( \rho_{RA} \) in proposition 10 to be the maximally entangled state \( \Phi_{RA} \) [CDP09, section 7].

### 2.6. Uniform continuity of amortized relative entropy of entanglement and amortized Rains relative entropy

The following theorem establishes that both the amortized relative entropy of entanglement and the amortized Rains relative entropy obey a uniform continuity bound. This bound will play a central role in bounding the respective secret-key-agreement and LOCC-assisted quantum capacities of approximately teleportation-simulable channels (see sections 3 and 4).

Before we state the theorem, we recall that the diamond norm of the difference of two quantum channels \( \mathcal{N}_{A \rightarrow B} \) and \( \mathcal{M}_{A \rightarrow B} \) is defined as [Kit97]
\[ \| \mathcal{N}_{A \rightarrow B} - \mathcal{M}_{A \rightarrow B} \|_\diamond = \sup_{\rho_{RA}} \| [\text{id}_R \otimes (\mathcal{N}_{A \rightarrow B} - \mathcal{M}_{A \rightarrow B})](\rho_{RA}) \|_1, \]  
\tag{2.42}

\[ = \max_{\psi_{RA}} \| [\text{id}_R \otimes (\mathcal{N}_{A \rightarrow B} - \mathcal{M}_{A \rightarrow B})](\psi_{RA}) \|_1, \]  
\tag{2.43}

with \( \| X \|_1 = \text{Tr}\{ \sqrt{X^\dagger X} \} \) and the second equality, with an optimization restricted to pure states \( \psi_{RA} \) with \( |R| = |A| \), follows from the convexity of the trace norm and the Schmidt
decomposition. The diamond norm is a well established and operationally meaningful measure of the distinguishability of two quantum channels.

**Theorem 12.** Let \( \varepsilon \in [0, 1] \). Let \( E \) refer to either the relative entropy of entanglement or the Rains relative entropy, and let \( E_A \) refer to their amortized versions. For channels \( \mathcal{N}_{A \to B} \) and \( \mathcal{M}_{A \to B} \) such that

\[
\frac{1}{2} \| \mathcal{N}_{A \to B} - \mathcal{M}_{A \to B} \|_\diamond \leq \varepsilon, \tag{2.44}
\]

the following bound holds

\[
|E_A(N) - E_A(M)| \leq 2\varepsilon \log_2 |B| + g(\varepsilon), \tag{2.45}
\]

where \(|B|\) is the dimension of the channel output system B and \( g(\varepsilon) \equiv (\varepsilon + 1) \log_2 (\varepsilon + 1) - \varepsilon \log_2 \varepsilon \).

**Proof.** Our proof follows the general approach from [Win16], but it has some additional observations needed for our context. For a state \( \rho_{A'AB'} \), let us define

\[
E_A(\rho, N) \equiv E(A'; BB')_{B'} - E(A'; B')_\rho,
\]

where \( \theta_{A'AB'}^N \equiv \mathcal{N}_{A \to B}(\rho_{A'AB'}) \). Then consider that

\[
|E_A(\rho, N) - E_A(\rho, M)| = |E(A'; BB')_{B'} - E(A'; BB')_{B})|,
\]

where \( \theta_{A'AB'}^M \equiv \mathcal{M}_{A \to B}(\rho_{A'AB'}) \). Our intent now is to prove that the following bound holds for all states \( \rho_{A'AB'} \)

\[
|E_A(\rho, N) - E_A(\rho, M)| \leq 2\varepsilon \log_2 |B| + g(\varepsilon). \tag{2.48}
\]

Since the bound in (2.44) holds, we can conclude that

\[
\frac{1}{2} \| \theta_{A'BB'}^N - \theta_{A'BB'}^M \|_1 \equiv \varepsilon_0 \leq \varepsilon. \tag{2.49}
\]

Let us suppose that \( \varepsilon_0 > 0 \). Otherwise, the bound in (2.48) trivially holds. Let us define the states \( \Omega_{A'BB'} \) as

\[
\Omega_{A'BB'} = \frac{[\theta_{A'BB'}^N - \theta_{A'BB'}^M]_+}{\text{Tr}([\theta_{A'BB'}^N - \theta_{A'BB'}^M]_+)} = \frac{1}{\varepsilon_0} [\theta_{A'BB'}^N - \theta_{A'BB'}^M]_+,
\]

where \([ \cdot ]_+\) denotes the positive part of an operator. Note that the equality \( \text{Tr}([\theta_{A'BB'}^N - \theta_{A'BB'}^M]_+) = \varepsilon_0 \) follows from the fact that \( \theta_{A'BB'}^N \) and \( \theta_{A'BB'}^M \) are states (see [Wil16a] for more details). Since

\[
\theta_{A'BB'}^N = \theta_{A'BB'}^N - \theta_{A'BB'}^M + \theta_{A'BB'}^M
\]

\[
\leq [\theta_{A'BB'}^N - \theta_{A'BB'}^M]_+ + \theta_{A'BB'}^M
\]

\[
= (1 + \varepsilon_0) \left( \frac{1}{1 + \varepsilon_0} [\theta_{A'BB'}^N - \theta_{A'BB'}^M]_+ + \frac{1}{1 + \varepsilon_0} \theta_{A'BB'}^M \right)
\]

(2.53)
\[ (1 + \varepsilon_0) \left( \frac{\varepsilon_0}{1 + \varepsilon_0} \Omega_{A'B'} + \frac{1}{1 + \varepsilon_0} \theta_{A'B'}^N \right), \quad (2.54) \]

we can define
\[ \xi_{A'B'} \equiv \frac{\varepsilon_0}{1 + \varepsilon_0} \Omega_{A'B'} + \frac{1}{1 + \varepsilon_0} \theta_{A'B'}^N, \quad (2.55) \]

and it follows that
\[ \xi_{A'B'} = \frac{\varepsilon_0}{1 + \varepsilon_0} \Omega_{A'B'} + \frac{1}{1 + \varepsilon_0} \theta_{A'B'}^N \quad (2.56) \]

where the state \( \Omega_{A'B'}' \) is defined as
\[ \Omega_{A'B'}' \equiv \frac{1}{\varepsilon_0} \left( (1 + \varepsilon_0) \xi_{A'B'} - \theta_{A'B'}^N \right). \quad (2.57) \]

Consider that
\[ \Omega_{A'B'} = \Omega_{A'B'}' \quad (2.58) \]

because
\[ \text{Tr}_B \left\{ \frac{\varepsilon_0}{1 + \varepsilon_0} \Omega_{A'B'} + \frac{1}{1 + \varepsilon_0} \theta_{A'B'}^M \right\} = \frac{\varepsilon_0}{1 + \varepsilon_0} \Omega_{A'B'} + \frac{1}{1 + \varepsilon_0} \theta_{A'B'}^M \quad (2.59) \]
\[ = \frac{\varepsilon_0}{1 + \varepsilon_0} \Omega_{A'B'} + \frac{1}{1 + \varepsilon_0} \rho_{A'B'}, \quad (2.60) \]
\[ \text{Tr}_B \left\{ \frac{\varepsilon_0}{1 + \varepsilon_0} \Omega_{A'B'}' + \frac{1}{1 + \varepsilon_0} \theta_{A'B'}^N \right\} = \frac{\varepsilon_0}{1 + \varepsilon_0} \Omega_{A'B'}' + \frac{1}{1 + \varepsilon_0} \theta_{A'B'}^N \quad (2.61) \]
\[ = \frac{\varepsilon_0}{1 + \varepsilon_0} \Omega_{A'B'}' + \frac{1}{1 + \varepsilon_0} \rho_{A'B'}, \quad (2.62) \]

and so
\[ \frac{\varepsilon_0}{1 + \varepsilon_0} \Omega_{A'B'} + \frac{1}{1 + \varepsilon_0} \rho_{A'B'} = \frac{\varepsilon_0}{1 + \varepsilon_0} \Omega_{A'B'}' + \frac{1}{1 + \varepsilon_0} \rho_{A'B'}. \quad (2.63) \]

from which we can conclude (2.58) since \( \varepsilon_0 > 0 \). By convexity of relative entropy of entanglement and the Rains relative entropy [HHHH09], we have that
\[ E(A'; BB')_\xi \leq \frac{1}{1 + \varepsilon_0} E(A'; BB')_\theta^M + \frac{\varepsilon_0}{1 + \varepsilon_0} E(A'; BB')_\Omega, \quad (2.64) \]

and from lemma A.3, we have that
\[ \frac{1}{1 + \varepsilon_0} E(A'; BB')_\theta^N + \frac{\varepsilon_0}{1 + \varepsilon_0} E(A'; BB')_\Omega^N \leq E(A'; BB')_\xi + \chi_2 \left( \frac{\varepsilon_0}{1 + \varepsilon_0} \right). \quad (2.65) \]
So this means that

\[ E(A'; BB')_{\theta_N} \leq (1 + \varepsilon_0) E(A'; BB')_\xi + (1 + \varepsilon_0) h_2 \left( \frac{\varepsilon_0}{1 + \varepsilon_0} \right) - \varepsilon_0 E(A'; BB')_{\Omega} \]  

(2.66)

\[ \leq E(A'; BB')_{\theta_M} + \varepsilon_0 E(A'; BB')_{\Omega} + g(\varepsilon_0) - \varepsilon_0 E(A'; BB')_{\Omega} \]  

(2.67)

\[ = E(A'; BB')_{\theta_M} + g(\varepsilon_0) + \varepsilon_0 [E(A'; BB')_{\Omega} - E(A'; BB')_{\Omega'}] . \]  

(2.68)

where we used that \((1 + \varepsilon_0) h_2 \left( \frac{\varepsilon_0}{1 + \varepsilon_0} \right) = g(\varepsilon_0)\). Finally, consider that

\[ E(A'; BB')_{\Omega} - E(A'; BB')_{\Omega'} \leq 2 \log_2 |B| + E(A'; B')_{\Omega} - E(A'; B')_{\Omega'} \]  

(2.69)

\[ = 2 \log_2 |B| . \]  

(2.70)

The first inequality follows from lemma A.1, the LOCC monotonicity of relative entropy of entanglement and the Rains relative entropy, and (2.58). So this implies that

\[ E(A'; BB')_{\theta_N} - E(A'; BB')_{\theta_M} \leq g(\varepsilon_0) + 2\varepsilon_0 \log_2 |B| \]  

(2.71)

\[ \leq g(\varepsilon) + 2\varepsilon \log_2 |B| , \]  

(2.72)

the latter inequality holding because \(g(\cdot)\) is a monotone increasing function. The other inequality

\[ E(A'; BB')_{\theta_M} - E(A'; BB')_{\theta_N} \leq g(\varepsilon) + 2\varepsilon \log_2 |B| \]  

(2.73)

follows immediately using similar steps, and this now establishes (2.48). Then we have that the following bound holds for all input states \(\rho_{AB'BA'}\):

\[ E_A(\rho_N) \leq \sup_{\rho} E_A(\rho), M) + 2\varepsilon \log_2 |B| + g(\varepsilon) \]  

(2.74)

\[ = E_A(M) + 2\varepsilon \log_2 |B| + g(\varepsilon) . \]  

(2.75)

Since the bound holds for all input states \(\rho_{AB'BA'}\), we can conclude that

\[ E_A(\mathcal{N}) \leq E_A(M) + 2\varepsilon \log_2 |B| + g(\varepsilon) . \]  

(2.76)

In a similar way, we obtain the opposite inequality

\[ E_A(M) \leq E_A(\mathcal{N}) + 2\varepsilon \log_2 |B| + g(\varepsilon) . \]  

(2.77)

and this completes the proof. ■

3. Amortized relative entropy of entanglement and secret key agreement

In this section, we prove that the amortized relative entropy of entanglement is an upper bound on the secret-key-agreement capacity of a quantum channel. We begin by reviewing the structure of a secret-key-agreement protocol [TGW14b, TGW14a], how such a protocol can be purified along the lines observed in [HHHO03b, HHHO09], the critical performance
parameters for such a protocol, and then we finally give a proof for the aforementioned claim. Note that the proof bears some similarities with proofs in prior works [WTB17, CMH17, BDGDMW17], as well as an argument that appeared recently in [DW17] in a different context.

3.1. Protocol for secret key agreement

Here we review the structure of a secret-key-agreement protocol, along the lines discussed in [TGW14b, TGW14a]:

A sender Alice and a receiver Bob are spatially separated and are connected by a quantum channel $\mathcal{N}_{A\rightarrow B}$. They begin by performing an LOCC channel $\mathcal{E}_{B\rightarrow A}^{(1)}$ which leads to a separable state $\rho_{A_1'B_1'}^{(1)}$ where $A_1'$ and $B_1'$ are systems that are finite-dimensional but arbitrarily large and $A_1$ is a system that can be fed into the first channel use. Alice transmits system $A_1$ into the first channel, leading to a state $\sigma_{A_2'B_2'}^{(1)} \equiv \mathcal{N}_{A_1\rightarrow B_1}(\rho_{A_1'B_1'}^{(1)})$. They then perform the LOCC channel $\mathcal{E}_{A_2'B_2'\rightarrow A_2'A_2''B_2''}^{(2)}$ which leads to the state

$$\rho_{A_2'A_2''B_2''}^{(2)} \equiv \mathcal{E}_{A_1B_1\rightarrow A_2'A_2''B_2''}(\sigma_{A_2'B_2'}^{(1)}).$$

(3.1)

Alice feeds in the system $A_2$ to the second channel use $\mathcal{N}_{A_2\rightarrow B_2}$, leading to the state $\rho_{A_2'B_2'}^{(2)} \equiv \mathcal{N}_{A_2\rightarrow B_2}(\rho_{A_2'A_2''B_2''}^{(2)})$. This process continues: the protocol uses the channel $n$ times. In general, we have the following states for all $i \in \{2, \ldots, n\}$:

$$\rho_{A_i'A_i'B_i'}^{(i)} \equiv \mathcal{E}_{K_{i-1}B_{i-1}\rightarrow A_i'A_i'B_i'}^{(i)}(\sigma_{A_{i-1}'B_{i-1}'}^{(i-1)}),$$

(3.2)

$$\sigma_{A_i'B_i'}^{(i)} \equiv \mathcal{N}_{A_i\rightarrow B_i}(\rho_{A_i'A_i'B_i'}^{(i)}).$$

(3.3)

where $\mathcal{E}_{K_{i-1}B_{i-1}\rightarrow A_i'A_i'B_i'}^{(i)}$ is an LOCC channel. The final step of the protocol consists of an LOCC channel $\mathcal{E}_{A_n'B_n'\rightarrow K_fK_k}$, which produces the key systems $K_A$ and $K_B$ for Alice and Bob, respectively. The final state of the protocol is then as follows:

$$\omega_{K_AK_B} \equiv \mathcal{E}_{A_n'B_n'\rightarrow K_fK_k}(\sigma_{A_n'B_n'}^{(n)}).$$

(3.4)

The goal of the protocol is that the final state $\omega_{K_AK_B}$ is close to a secret-key state. Figure 2 depicts such a protocol. It may not yet be clear exactly what we mean by “close to a secret-key state,” but our approach is standard and we clarify this point in the following two sections.

3.2. Purifying a secret-key-agreement protocol

Related to the observations in [HHHO05b, HHHO09], any protocol of the above form can be purified in the following sense. The initial state $\rho_{A_1'A_1'B_1'}^{(1)}$ is a separable state of the following form:

$$\rho_{A_1'A_1'B_1'}^{(1)} \equiv \sum_{y_1} p_{Y_1}(y_1) \tau_{A_1'A_1'}^{y_1} \otimes \zeta_{B_1'B_1'}^{y_1}.$$

(3.5)

The classical random variable $Y_1$ corresponds to a message exchanged between Alice and Bob to establish this state. It can be purified in the following way:

$$|\psi(1)\rangle_{A_1S_1S_1'}Y_1 \equiv \sum_{y_1} \sqrt{p_{Y_1}(y_1)} |\psi(1)\rangle_{A_1A_1'S_1} \otimes |\zeta^{y_1}\rangle_{B_1'B_1'} \otimes |y_1\rangle_{Y_1},$$

(3.6)
where $S_A$ and $S_B$ are local “shield” systems that in principle could be held by Alice and Bob, respectively, $|\gamma_{\ell}^{\Lambda(A)}\rangle_{\Lambda(A)}$ and $|\zeta_{\ell}^{\Xi(B)}\rangle_{\Xi(B)}$ purify $\tau_{\Lambda(A)}^{\Lambda(A)}$ and $\tau_{\Xi(B)}^{\Xi(B)}$, respectively, and Eve possesses system $Y_1$, which contains a coherent classical copy of the classical data exchanged.

Each LOCC channel $E^{(i)}_{A_0',B_0',\ldots,B_0'-1\rightarrow A_0',B_0'}$ can be written in the following form [Wat15], for all $i \in \{2, \ldots, n\}$:

$$L^{(i)}_{A_0',B_0',\ldots,B_0'-1\rightarrow A_0',B_0'} \equiv \sum_{y_i} E^{y_i}_{A_0',B_0',\ldots,B_0'-1\rightarrow A_0',B_0'} \otimes F^{y_i}_{B_0',\ldots,B_0'-1\rightarrow B_0'},$$  \quad (3.7)

where $\{E^{y_i}_{A_0',B_0',\ldots,B_0'-1\rightarrow A_0',B_0'}\}_{y_i}$ and $\{F^{y_i}_{B_0',\ldots,B_0'-1\rightarrow B_0'}\}_{y_i}$ are collections of completely positive, trace non-increasing maps such that the map in (3.7) is trace preserving. Such an LOCC channel can be purified to an isometry in the following way:

$$U^{(i)}_{A_0',B_0',\ldots,B_0'-1\rightarrow A_0',B_0'} \equiv \sum_{y_i} U_{A_0',B_0',\ldots,B_0'-1\rightarrow A_0',B_0'}^{y_i} \otimes U_{B_0',\ldots,B_0'-1\rightarrow B_0'}^{y_i} \otimes |y_i\rangle \langle y_i|,$$  \quad (3.8)

where $\{U_{A_0',B_0',\ldots,B_0'-1\rightarrow A_0',B_0'}^{y_i}\}_{y_i}$ and $\{U_{B_0',\ldots,B_0'-1\rightarrow B_0'}^{y_i}\}_{y_i}$ are collections of linear operators (each of which is a contraction, i.e. $||U_{A_0',B_0',\ldots,B_0'-1\rightarrow A_0',B_0'}^{y_i}||_\infty \leq 1$) such that the linear operator in (3.8) is an isometry, and $Y_i$ is a system containing a coherent classical copy of the classical data exchanged in this round, the system $Y_i$ being held by Eve. The final LOCC channel can be written similarly as

$$L^{(n+1)}_{A_0\rightarrow K_0} \equiv \sum_{y_{n+1}} E^{y_{n+1}}_{A_0',K_0} \otimes F^{y_{n+1}}_{B_0',K_0},$$  \quad (3.9)

and it can be purified to an isometry similarly as

$$U^{(n+1)}_{A_0\rightarrow K_0} \equiv \sum_{y_{n+1}} U^{y_{n+1}}_{A_0',K_0} \otimes U^{y_{n+1}}_{B_0',K_0} \otimes |y_{n+1}\rangle \langle y_{n+1}|,$$  \quad (3.10)

Furthermore, each channel use $N_{A_0\rightarrow B_0}$ for all $i \in \{1, \ldots, n\}$ is purified by an isometry $U^{N}_{A_0\rightarrow B_0}$, such that Eve possesses the environment system $E_i$.

### 3.3. Performance of a secret-key-agreement protocol

At the end of the purified protocol, Alice possesses the key system $K_1$ and the shield systems $S_A \equiv S_{A_1} \cdots S_{A_{n+1}}$, Bob possesses the key system $K_B$ and the shield systems $S_B \equiv S_{B_1} \cdots S_{B_{n+1}}$, and Eve possesses the environment systems $E^n \equiv E_1 \cdots E_n$ as well as the coherent copies $Y^{n+1} \equiv Y_1 \cdots Y_{n+1}$ of the classical data exchanged. The state at the end of the purified protocol is a pure state $|\omega\rangle_{K_0S_AK_0S_BY^{n+1}}$. Fix $n, K \in \mathbb{N}$ and $\varepsilon \in [0, 1]$. The original protocol is an $(n, K, \varepsilon)$ protocol if
where the fidelity 
\[ F(\tau, \kappa) \equiv \| \sqrt{\tau} \sqrt{\kappa} \|_1 \] [Uhl76], the maximally correlated state \( \Phi_{KAKB} \otimes \xi_E \) is defined as
\[ \Phi_{KAKB} \equiv \sum_{k=1}^{K} |k\rangle_{kA} \otimes |k\rangle_{kB}, \] (3.12)
and \( \xi_E \) is an arbitrary state.

By the observations of [HHHO05b, HHHO09] (understood as a clever application of Uhlmann’s theorem for fidelity [Uhl76]), rather than focusing on the tripartite scenario, one can focus on the bipartite scenario, in which the goal is to produce an approximate private state of Alice and Bob’s systems. The criterion in (3.11) is fully equivalent to
\[ F(\omega_{KSAKBSB}^{\otimes n}, \gamma_{KSAKBSB}) \geq 1 - \varepsilon, \] (3.13)
where \( \gamma_{KSAKBSB} \) is a private state [HHHO05b, HHHO09] of the following form:
\[ U_{KSAKBSB}(\Phi_{KAKB} \otimes \theta_{SASB}) U_{KSAKBSB}^\dagger, \] (3.14)
with \( U_{KSAKBSB} \) a twisting unitary of the form \( U_{KSAKBSB} = \sum_{i,j=1}^{K} |i\rangle_{iA} \otimes |j\rangle_{jB} \otimes U_{SASB}^{ij} \), \( \Phi_{KAKB} \) is a maximally entangled state of the form
\[ \Phi_{KAKB} \equiv \sum_{i,j=1}^{K} |i\rangle_{iA} \otimes |j\rangle_{jB}, \] (3.15)
and \( \theta_{SASB} \) is an arbitrary state of the shield systems. The main idea in this latter picture is that we can use the techniques of entanglement theory to understand private communication protocols [HHHO05b, HHHO09].

A rate \( R \) is achievable for secret key agreement if for all \( \varepsilon \in (0, 1) \), \( \delta > 0 \), and sufficiently large \( n \), there exists an \( (n, 2^{n(k-\delta)}, \varepsilon) \) protocol. The secret-key-agreement capacity of \( N_A \rightarrow B \), denoted as \( P_{SAKBSB}^{\otimes n} \), is equal to the supremum of all achievable rates.

3.4. Teleportation-simulable channels and reduction by teleportation

An implication of channel simulation via teleportation, as discussed in section 2.5, is that the performance of a general protocol that uses the channel \( n \) times, with each use interleaved by local operations and classical communication (LOCC), can be bounded from above by the performance of a protocol with a much simpler form: the simplified protocol consists of a single round of LOCC acting on \( n \) copies of the resource state \( \omega_{RB} \) [BDSW96, NFC09, MH12]. This is called reduction by teleportation. Note that reduction by teleportation is a very general procedure and clearly can be used more generally in any LOCC-assisted protocol trying to accomplish an arbitrary information-processing task. Of course, a secret-key-agreement protocol is one particular kind of protocol of the above form, as considered in the follow-up works [PLOB16, WTB17], and so the general reduction method of [BDSW96, NFC09, MH12] applies to this particular case.

3.5. Amortized relative entropy of entanglement as a bound for secret-key-agreement protocols

The main goal of this section is to show that the amortized relative entropy of entanglement is an upper bound on the rate of secret key that can be extracted by a secret-key-agreement protocol. We begin by establishing the following theorem:
Proposition 13. The following weak-converse bound holds for an \((n, K, \varepsilon)\) secret-key-agreement protocol conducted over a quantum channel \(\mathcal{N}\):
\[
(1 - \varepsilon) \log_2 K \leq E_{AR}(\mathcal{N}) + \frac{1}{n} h_2(\varepsilon),
\]
(3.16)
where \(E_{AR}(\mathcal{N})\) is the amortized relative entropy of entanglement and \(h_2(\varepsilon) \equiv -\varepsilon \log_2 \varepsilon - (1 - \varepsilon) \log_2(1 - \varepsilon)\) denotes the binary entropy.

Proof. To see how the amortized relative entropy of entanglement gives an upper bound on the performance of a secret-key-agreement protocol, consider the following steps. We suppose that we are dealing with an \((n, K, \varepsilon)\) secret-key-agreement protocol as described previously. First, at the end of the protocol one can perform a privacy test [WTB17] (see also [HHHO09, HHH’08a34, HHH’08b35]), which untwists the twisting unitary of the ideal target private state and projects onto the maximally entangled state of the key systems (see section 3.3). Let \(F^*\) denote the probability of the actual state \(\omega_{K_3S_3K_3S_4}\) at the end of the protocol passing this test. By [WTB17, lemma 9], this probability is larger than \(1 - \varepsilon\). Let \(p_{SEP}\) denote the probability that a given separable state \(\sigma_{K_3S_3K_3S_4}\) of systems \(K_3S_3K_3S_4\) passes the test. This probability is no larger than \(1/K\), following from results of [HHHO09] (reviewed as [WTB17, lemma 10]). Then we find that
\[
-h_2(\varepsilon) + (1 - \varepsilon) \log_2 K \leq D(\{1 - \varepsilon, \varepsilon\}||\{1/K, 1 - 1/K\})
\]
(3.17)
\[
\leq D(\{F^*, 1 - F^*\}||\{p_{SEP}, 1 - p_{SEP}\})
\]
(3.18)
\[
\leq D(\omega_{K_3S_3K_3S_4}||\sigma_{K_3S_3K_3S_4}).
\]
(3.19)

The first inequality follows because
\[
D(\{1 - \varepsilon, \varepsilon\}||\{1/K, 1 - 1/K\}) = (1 - \varepsilon) \log_2 \left(\frac{1 - \varepsilon}{1/K}\right) + \varepsilon \log_2 \left(\frac{\varepsilon}{1 - 1/K}\right)
\]
(3.20)
\[
= -h_2(\varepsilon) + (1 - \varepsilon) \log_2 K + \varepsilon \log_2 \left(\frac{K}{K - 1}\right)
\]
(3.21)
\[
\geq -h_2(\varepsilon) + (1 - \varepsilon) \log_2 K.
\]
(3.22)

with the last inequality above following because \(K \geq 1\) (note that the singular case of \(K = 1\) is not particularly interesting because the rate is zero and the protocol is thus trivial). The second inequality follows because the distributions \(\{F^*, 1 - F^*\}\) and \(\{p_{SEP}, 1 - p_{SEP}\}\) are more distinguishable than the distributions \(\{1 - \varepsilon, \varepsilon\}\) and \(\{1/K, 1 - 1/K\}\), due to the conditions \(F^* \geq 1 - \varepsilon\) and \(p_{SEP} \leq 1/K\) (we are assuming without loss of generality that \(1 - \varepsilon \geq 1/K\) for this statement; if it is not the case, then the code is in a rather sad state of affairs with poor performance and there is no need to give a converse bound in this case—the bound would simply be \(\log_2 K < -\log_2(1 - \varepsilon)\)). The final inequality follows from monotonicity of quantum relative entropy with respect to the privacy test (understood as a measurement channel). Since the above chain of inequalities holds for all separable states \(\sigma_{K_3S_3K_3S_4}\), we find that
\[
-h_2(\varepsilon) + (1 - \varepsilon) \log_2 K \leq E_{AR}(K_3S_3K_3S_4)_{\omega}.
\]
(3.23)
which can be rewritten as\(^3\)

\[
(1 - \varepsilon) \log_2 K \leq E_R(K_A S_A; K_B S_B) \omega + h_2(\varepsilon). \tag{3.24}
\]

From the monotonicity of the relative entropy of entanglement with respect to LOCC [VP98], we find that

\[
E_R(K_A S_A; K_B S_B) \omega \leq E_R(A'_n; B'_n)_{\sigma(\omega)} \tag{3.25}
\]

\[
= E_R(A'_n; B'_n)_{\sigma(\omega)} - E_R(A'_1 A'_1; B'_1)_{\rho(1)} \tag{3.26}
\]

\[
= E_R(A'_n; B'_n)_{\sigma(\omega)} + \left[ \sum_{i=2}^{n} E_R(A'_i A'_i; B'_i)_{\rho(i)} - E_R(A'_i A'_i; B'_i)_{\rho(1)} \right] \tag{3.27}
\]

\[
\leq \sum_{i=1}^{n} E_R(A'_i A'_i; B'_i)_{\rho(i)} - E_R(A'_1 A'_1; B'_1)_{\rho(1)} \tag{3.28}
\]

\[
\leq n E_{AR}(\mathcal{N}). \tag{3.29}
\]

The first equality follows because the state \(\rho^{(1)}_{A'_1 A'_1 B'_1}\) is a separable state with vanishing relative entropy of entanglement. The second equality follows by adding and subtracting terms. The second inequality follows because \(E_R(A'_i A'_i; B'_i)_{\rho(i)} \leq E_R(A'_i A'; B'_i)_{\rho(i)}\) for all \(i \in \{2, \ldots, n\}\), due to monotonicity of the relative entropy of entanglement with respect to LOCC. The final inequality follows because each term \(E_R(A'_i A'_i; B'_i)_{\rho(i)} - E_R(A'_i A'; B'_i)_{\rho(i)}\) is of the form in the amortized relative entropy of entanglement, so that optimizing over all inputs of the form \(\rho^{(i)}\) cannot exceed \(E_{AR}(\mathcal{N})\). Combining (3.24) and (3.29), we arrive at the inequality in (3.16).

Taking the limit in proposition 13 as \(n \to \infty\) and then as \(\varepsilon \to 0\) leads to the following asymptotic statement:

**Theorem 14.** The secret-key-agreement capacity \(P^{\ast\ast}(\mathcal{N}_{A \to B})\) of a quantum channel \(\mathcal{N}_{A \to B}\) cannot exceed its amortized relative entropy of entanglement:

\[
P^{\ast\ast}(\mathcal{N}) \leq E_{AR}(\mathcal{N}). \tag{3.30}
\]

**Remark 15.** Interestingly, a similar approach using the sandwiched Rényi relative entropy [MLDS+13, WWY14] gives the following upper bound for all \(\alpha > 1\)

\[
\frac{\alpha}{\alpha - 1} \log_2 (1 - \varepsilon) \leq n \tilde{E}_{AR}^{\alpha}(\mathcal{N}) - \log_2 K, \tag{3.31}
\]

where

\[
\tilde{E}_{AR}^{\alpha}(\mathcal{N}) = \sup_{\rho^{(\alpha)}, \lambda^{(\alpha)}} \tilde{E}_{R}^{\alpha}(A'; B') \omega - \tilde{E}_{R}^{\alpha}(A' A'; B' B'), \tag{3.32}
\]

\(^3\)Alternatively, the bound in (3.24) can be established for all \(\varepsilon \in (0, 1)\) and \(K \geq 1\) by using several methods from [WR12, MW14, WTB17, KW17]. In more detail, we could make use of the \(\varepsilon\)-relative entropy of entanglement [BD11] as an intermediary step to get that \(\log_2 K \leq E_R(K_A S_A; K_B S_B) \omega + h_2(\varepsilon)\), with the first bound following from [WTB17, theorem 11] and the second from [WR12, MW14, KW17].
and \( \tilde{E}_R^{\alpha} \) denotes the sandwiched Rényi relative entropy of entanglement [WTB17], defined from the sandwiched Rényi relative entropy [MLDS13, WWY14]. One of the main results of [CMH17] is the bound \( \tilde{E}_R^{\alpha}(\mathcal{N}) \leq E_{\text{max}}(\mathcal{N}) \), where \( E_{\text{max}}(\mathcal{N}) \) denotes the channel’s max-relative entropy of entanglement (see [Dat09]). The authors of [CMH17] observed that this latter bound in turn implies the following bound for all \( \alpha > 1 \):

\[
\frac{\alpha}{\alpha - 1} \log_2(1 - \epsilon) \leq nE_{\text{max}}(\mathcal{N}) - \log_2 K.
\]  

(3.33)

4. Amortized Rains relative entropy and PPT-assisted quantum communication

The main goal of this section is to prove that the amortized Rains relative entropy from definition 3 is an upper bound on a channel’s PPT-assisted quantum capacity. By this, we mean that a sender and receiver are allowed to use a channel many times, and between every channel use, they are allowed free usage of channels that are positive-partial-transpose (PPT) preserving. In what follows, we detail these concepts, and then we state the main theorem (theorem 18).

4.1. Positive-partial-transpose preserving quantum channels

A quantum channel \( \mathcal{P} \) is a positive-partial-transpose (PPT) preserving channel from systems \( A:B \) to systems \( A':B' \) if the map \( T_{B'} \circ N_{AB} \rightarrow A'B' \circ T_B \) is completely positive and trace preserving [Rai01], where \( T_B \) and \( T_{B'} \) denote the partial transpose map. For a given basis \( \{|i\rangle\}_i \), the transpose map is a positive map, specified by \( \rho \rightarrow \sum_{i,j} |i\rangle \langle j| \rho |j\rangle \langle i| \). In what follows, we call PPT-preserving channels “PPT channels” as an abbreviation. It has been known for a long time that PPT channels contain the set of LOCC channels [Rai01], and so an immediate operational consequence of this containment is that any general upper bound on the performance of a PPT-assisted protocol serves as an upper bound on the performance of an LOCC-assisted protocol [Rai01]. This fact and the fact that PPT channels are simpler to analyze mathematically than LOCC were some of the main motivations for introducing this class of channels [Rai01].

PPT channels preserve the set \( \mathbb{P}_{\text{PT}}' \) discussed in definition 3 [Rai01, ADMVW02]. For this reason and since the relative entropy is monotone with respect to quantum channels [Lin75], it follows that the Rains relative entropy is monotone with respect to PPT channels [Rai01, ADMVW02], in the sense that

\[
R(A;B)_{\rho} \geq R(A';B')_{\mathcal{P}(\rho)},
\]  

(4.1)

where \( \rho_{AB} \) is a bipartite state and \( \mathcal{P}_{AB \rightarrow A'B'} \) is a PPT channel.

The notion of PPT channels then leads to a more general notion of the teleportation simulation of a quantum channel:

**Definition 16 (\( \omega \)-PPT-simulable channel).** A channel \( \mathcal{N}_{A \rightarrow B} \) with input system \( A \) and output system \( B \) is defined to be PPT-simulable with associated resource state \( \omega_{RB} \) (\( \omega \)-PPT-simulable for short) if the following equality holds for all input states \( \rho_A \):

\[
\mathcal{N}_{A \rightarrow B}(\rho_A) = \mathcal{P}_{ARB \rightarrow B}(\rho_A \otimes \omega_{RB}),
\]  

(4.2)
where $\mathcal{P}_{ARB\rightarrow B}$ is a PPT quantum channel with respect to the bipartite cut $AR|B$ at the input. Note that every teleportation-simulable channel with associated resource state $\omega_{RB}$ is PPT-simulable with associated resource state $\omega_{RB}$.

4.2. Protocols for PPT-assisted quantum communication and their performance

The structure of an $(n, M, \varepsilon)$ protocol for PPT-assisted quantum communication is quite similar to that for an $(n, K, \varepsilon)$ protocol for secret key agreement, which we discussed previously in section 3.1. In fact, such a PPT-assisted protocol is exactly as outlined in section 3.1 and figure 2, but each LOCC channel is replaced with a PPT channel. Let us denote the final state of the protocol by $\omega_{MAMB}$ instead of $\omega_{KAKB}$. Fixing $n, M \in \mathbb{N}$ and $\varepsilon \in [0, 1]$, the protocol is an $(n, M, \varepsilon)$ PPT-assisted quantum communication protocol if

$$F(\omega_{MAMB}, \Phi_{MAMB}) \geq 1 - \varepsilon, \quad (4.3)$$

where the maximally entangled state $\Phi_{MAMB}$ is defined in (3.15).

A rate $R$ is achievable for PPT-assisted quantum communication if for all $\varepsilon \in (0, 1), \delta > 0$, and sufficiently large $n$, there exists an $(n, 2n(R-\delta), \varepsilon)$ protocol. The PPT-assisted quantum capacity of $\mathcal{N}_{A\rightarrow B}$, denoted as $Q^{PPT\rightarrow\ast}(\mathcal{N}_{A\rightarrow B})$, is equal to the supremum of all achievable rates.

We can also consider the whole development above when we only allow the assistance of LOCC channels instead of PPT channels. In this case, we have similar notions as above, and then we arrive at the LOCC-assisted quantum capacity $Q^{\rightarrow\ast}(\mathcal{N}_{A\rightarrow B})$. It then immediately follows that

$$Q^{\rightarrow\ast}(\mathcal{N}_{A\rightarrow B}) \leq Q^{PPT\rightarrow\ast}(\mathcal{N}_{A\rightarrow B}), \quad (4.4)$$

because every LOCC channel is a PPT channel. We also have the following bound

$$Q^{\ast\rightarrow}(\mathcal{N}_{A\rightarrow B}) \leq P^{\ast\rightarrow}(\mathcal{N}_{A\rightarrow B}), \quad (4.5)$$

as observed in [TWW17], because a maximally entangled state, the target state of an LOCC-assisted quantum communication protocol, is a particular kind of private state.

For channels that are $\omega$-PPT-simulable, as in definition 16, PPT-assisted protocols simplify immensely, just as was the case for teleportation-simulable channels. Indeed, in this case, PPT-assisted protocols can be reduced to the action of a single PPT channel on $n$ copies of the resource state $\omega_{RB}$, and this reduction is helpful in bounding the performance of PPT-assisted protocols conducted over such channels.

4.3. Amortized Rains relative entropy as a bound for PPT-assisted quantum communication protocols

We can employ an argument nearly identical to that given in the proof of proposition 13 in order to establish that the amortized Rains relative entropy is an upper bound on the rate at which maximal entanglement can be extracted by a PPT-assisted quantum communication protocol. Indeed, we simply replace the privacy test therein by a maximal entanglement test (i.e. a measurement specified by a projection onto the maximally entangled state or its complement). By the definition of an $(n, M, \varepsilon)$ protocol and the fidelity, the probability for the final state $\omega_{MAMB}$ of the protocol to pass this test is larger than $1 - \varepsilon$. Furthermore, due to [Rai99, lemma 2], the bound $\text{Tr}(\Phi_{MAMB} \sigma_{MAMB}) \leq 1/M$ holds for all states $\sigma_{MAMB} \in \text{PPT}(M_A; M_B)$. These bounds and the same reasoning employed in the proof of proposition 13 allow us to
conclude the following weak-converse bound for any PPT-assisted quantum communication protocol:

**Proposition 17.** The following weak-converse bound holds for an \((n, M, \epsilon)\) PPT-assisted quantum communication protocol conducted over a quantum channel \(N\):

\[
(1 - \epsilon) \frac{\log_2 M}{n} \leq R_A(N) + \frac{1}{n} h_2(\epsilon),
\]

(4.6)

where \(R_A(N)\) denotes the amortized Rains relative entropy from definition 3.

Taking the limit in proposition 17 as \(n \to \infty\) and then as \(\epsilon \to 0\) leads to the following asymptotic statement:

**Theorem 18.** The PPT-assisted quantum capacity \(Q^{\text{PPT}}(N_{A \to B})\) of a quantum channel \(N_{A \to B}\) cannot exceed its amortized Rains relative entropy:

\[
Q^{\text{PPT}}(N) \leq R_A(N).
\]

(4.7)

Furthermore, we obtain a bound for PPT-assisted quantum communication similar to that stated in (3.31)–(3.32) by employing similar reasoning.

5. Approximately teleportation- and PPT-simulable channels

We now define approximately teleportation- and PPT-simulable channels:

**Definition 19 (Approximately teleportation- and PPT-simulable channels).** A quantum channel \(N_{A \to B}\) is \(\epsilon\)-approximately teleportation-simulable with associated resource state \(\omega_{RB}\) if there exists a channel \(M_{A \to B}\) that is exactly teleportation-simulable with associated resource state \(\omega_{RB}\) such that

\[
\frac{1}{2} \|N_{A \to B} - M_{A \to B}\|_\diamond \leq \epsilon.
\]

(5.1)

For short, we say that \(N_{A \to B}\) is \((\epsilon, \omega_{RB})\)-approximately teleportation-simulable. The same definition applies for an \((\epsilon, \omega_{RB})\)-approximately PPT-simulable channel, but the difference is that \(M_{A \to B}\) is exactly PPT-simulable with associated resource state \(\omega_{RB}\). Also, if a channel is \((\epsilon, \omega_{RB})\)-approximately teleportation-simulable, then it is \((\epsilon, \omega_{RB})\)-approximately PPT-simulable.

In appendix B, we discuss the relation between the notion of approximately teleportation-simulable channels and the recently introduced notion of approximately covariant channels [LKDW17]. Therein, we also discuss channel twirling and how to simulate this procedure via a generalized teleportation protocol.

The following theorem is an immediate consequence of proposition 8, theorems 12 and 14, and it constitutes one of the main results of our paper:

**Theorem 20.** If a channel \(N_{A \to B}\) is \((\epsilon, \omega_{RB})\)-approximately teleportation-simulable, then its secret-key-agreement capacity \(P^{\leftrightarrow}(N_{A \to B})\) is bounded from above as

\[
P^{\leftrightarrow}(N_{A \to B}) \leq E_B(R; B)_\omega + 2\epsilon \log_2 |B| + g(\epsilon).
\]

(5.2)

Similarly, the following theorem is an immediate consequence of proposition 8, theorems 12 and 18:
Theorem 21. If a channel $\mathcal{N}_{A \rightarrow B}$ is $(\epsilon, \omega_{RB})$-approximately PPT-simulable, then its PPT-assisted quantum capacity $Q^{\text{PPT},\leftrightarrow}(\mathcal{N}_{A \rightarrow B})$ is bounded from above as

$$Q^{\text{PPT},\leftrightarrow}(\mathcal{N}_{A \rightarrow B}) \leq R(R; B)_{\omega} + 2\epsilon \log_2 |B| + g(\epsilon). \quad (5.3)$$

In the next section, we apply the bounds from theorems 20 and 21 to an example qubit channel.

6. Bounds on the assisted capacities of a particular qubit channel

In this section, we apply the bounds from theorems 20 and 21 to a particular qubit channel $\mathcal{N}_p$, which we define to be a convex mixture of an amplitude damping channel and a depolarizing channel:

$$\mathcal{N}_p(\rho) = p \mathcal{A}_p(\rho) + (1 - p) \mathcal{D}_p(\rho), \quad (6.1)$$

where $p \in [0, 1]$ and $\rho$ is an input qubit density operator (this is the same channel considered in concurrent work [LKDW17]). The amplitude damping channel $\mathcal{A}_p$ is defined as

$$\mathcal{A}_p(\rho) = K_1 \rho K_1^\dagger + K_2 \rho K_2^\dagger, \quad (6.2)$$

$$K_1 = |0\rangle\langle 0| + \sqrt{1 - p}|1\rangle\langle 1|, \quad (6.3)$$

$$K_2 = \sqrt{p}|0\rangle\langle 1|. \quad (6.4)$$

Also, $\mathcal{D}_p$ denotes the qubit depolarizing channel:

$$\mathcal{D}_p(\rho) = (1 - p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z), \quad (6.5)$$

where $X$, $Y$, and $Z$ are the Pauli operators.

Let $\Phi(\mathcal{M})$ denote the Choi state associated with a channel $\mathcal{M}$, i.e. the state that results from sending one share of a maximally entangled state through the channel. It has been known for many years now [BDSW96, HHH99, CDP09] that the depolarizing channel is teleportation-simulable with associated resource state $\Phi(\mathcal{D}_p)$. Thus, for small values of $p$, we should expect for a convex mixture of the depolarizing channel and the amplitude channel to be approximately teleportation-simulable with associated resource state $\Phi(\mathcal{N}_p)$, given that $\mathcal{N}_p$ is intuitively close to $\mathcal{D}_p$ for small values of $p$. Indeed, it follows from the results of [LKDW17, section 4.2] and the discussion in appendix B that the channel $\mathcal{N}_p$ is $(p^2/2, \Phi(\mathcal{N}_p))$-approximately teleportation-simulable, where $\overline{\mathcal{N}}_p$ denotes the following teleportation-simulable channel:

$$\overline{\mathcal{N}}_p(\rho) = \frac{1}{2} [\mathcal{N}_p(\rho) + X\mathcal{N}_p(X\rho X)X]. \quad (6.6)$$

We can thus apply theorems 20 and 21 to arrive at the following bounds on the secret-key-agreement capacity $P^{\leftrightarrow}(\mathcal{N}_p)$ and the PPT-assisted quantum capacity $Q^{\text{PPT},\leftrightarrow}(\mathcal{N}_p)$:

$$P^{\leftrightarrow}(\mathcal{N}_p) \leq E_k(A; B|\Phi(\overline{\mathcal{N}}_p)) + p^2 + g(p^2/2), \quad (6.7)$$

$$Q^{\text{PPT},\leftrightarrow}(\mathcal{N}_p) \leq R(A; B|\Phi(\overline{\mathcal{N}}_p)) + p^2 + g(p^2/2). \quad (6.8)$$
By noting that the set $\text{PPT}'$ contains the set of PPT states and applying the well known result that PPT states are equal to separable states for $2 \times 2$ systems [Per96, HHH96], we can conclude that

$$P^{\text{PS}}(\rho_p), \quad Q^{\text{PPT},\text{PS}}(\rho_p) \leq E_{\text{PPT}}(A; B)_{\phi(U_{\rho_p})} + p^2 + g(p^2/2), \quad (6.9)$$

where $E_{\text{PPT}}$ denotes the relative entropy to PPT states.

The upper bound in (6.9) is plotted in figure 3. To calculate $E_{\text{PPT}}(A; B)_{\phi(U_{\rho_p})}$ we have made use of the relative entropy optimization techniques put forward recently in [FF17].

We also consider lower bounds on the assisted capacities. Note that both $P^{\text{PS}}(\rho_p)$ and $Q^{\text{PPT},\text{PS}}(\rho_p)$ are bounded from below by the coherent information [SN96] and the negative CB-entropy [DJKR06] of the channel (note that the latter is sometimes called “reverse coherent information”). These lower bounds are a direct consequence of the developments in [DW05]. In figure 3, we also plot the coherent information of the channel, with the input state being the maximally entangled state. For the negative CB-entropy, we optimize over the input states of the channel and can exploit symmetry to simplify this optimization.

Here we elaborate on how to simplify the calculation of the negative CB-entropy for our example. As discussed in [DJKR06], it is possible to write the negative CB-entropy of a channel $N_{A\rightarrow B}$ as the following optimization:

$$-H_{\text{CB}}(N_{A\rightarrow B}) = \sup_{\rho_p} H(B|E)_{U^{N_{A\rightarrow B}}(\rho_p)}, \quad (6.10)$$

where $U^{N_{A\rightarrow B}}$ denotes an isometric channel that extends $N_{A\rightarrow B}$. Due to the concavity of conditional entropy [LR73b, LR73a], it immediately follows that $H(B|E)_{U^{N_{A\rightarrow B}}(\rho_p)}$ is concave with respect to the input density operator $\rho_p$, and thus the calculation of $-H_{\text{CB}}(N_{A\rightarrow B})$ is a concave optimization problem. For our example, we can further simplify the calculation of $-H_{\text{CB}}(N_{A\rightarrow B})$ by exploiting the symmetry of $N_{A\rightarrow B}$. To see this symmetry, consider that both the amplitude damping channel and the depolarizing channel are covariant with respect to $I$ and $Z$, in the sense that

$$A_p(U\rho U^\dagger) = UA_p(\rho)U^\dagger, \quad D_p(U\rho U^\dagger) = UD_p(\rho)U^\dagger, \quad (6.11)$$

where $U$ can be $I$ or $Z$. This observation then implies that $N_{A\rightarrow B}$ is covariant with respect to $I$ and $Z$. By invoking an observation stated in [Hol06], it follows that

$$U^{N_{A\rightarrow B}}(Z\rho Z) = (Z \otimes Z)U^{N_{A\rightarrow B}}(\rho)(Z \otimes Z), \quad (6.12)$$

where $U^{N_{A\rightarrow B}}$ is an isometric channel that extends $N_{A\rightarrow B}$ and $Z$ is a unitary representation of $Z$. We can then exploit the invariance of conditional entropy with respect to local unitaries and its concavity to find that

$$H(B|E)_{U^{N_{A\rightarrow B}}(\rho_p)} = \frac{1}{2} \left[ H(B|E)_{U^{N_{A\rightarrow B}}(\rho_p)} + H(B|E)_{U^{N_{A\rightarrow B}}(\rho_p)(Z \otimes Z)} \right] \quad (6.13)$$

$$= \frac{1}{2} \left[ H(B|E)_{U^{N_{A\rightarrow B}}(\rho_p)} + H(B|E)_{U^{N_{A\rightarrow B}}(Z\rho Z)} \right] \quad (6.14)$$

$$\leq H(B|E)_{U^{N_{A\rightarrow B}}(\frac{1}{2}(\rho + Z\rho Z))}; \quad (6.15)$$

Since $\frac{1}{2}(\rho + Z\rho Z)$ has no off-diagonal elements with respect to the standard basis, the above calculation reduces the optimization of the negative CB-entropy for $N_{A\rightarrow B}$ to an optimization over a single parameter.
The optimized negative CB-entropy is plotted in figure 3. Our findings are consistent with those in earlier works [SSWR14, LLS17]: the upper bound from (6.9) is closer to the lower bounds in the low-noise regime (small values of $p$) than it is in the high-noise regime.

7. Generalizations to other resource theories

In this section, we discuss how to generalize several of the concepts in our paper to general resource theories [BG15, Fri17, dRKR15, KdR16]. This generalization has already been considered in the context of the resource theory of coherence [BDGDMW17], and in fact, we note here that the recent developments in [BDGDMW17] were what served as the inspiration for our present paper. In short, a resource theory consists of a few basic elements. There is a set $F$ of free quantum states, i.e. those that the players involved are allowed to access without any cost. Related to these, there is a set of free channels, and they should have the property that a free state remains free after a free channel acts on it. Once these are defined, it follows that any state that is not free is considered resourceful, i.e. useful in the context of the resource theory. We can also then define a measure $V$ of the resourcefulness of a quantum state, and some fundamental properties that it should satisfy are that

1. it should be monotone non-increasing under the action of a free channel and
2. it should be equal to zero when evaluated on a free state.

A typical choice of a resourcefulness measure of a state $\rho$ satisfying these requirements is the relative entropy of resourcefulness: $\inf_{\sigma \in F} D(\rho || \sigma)$.

With these basic aspects established and given a measure $V$ of the resourcefulness of a quantum state, we might be interested in quantifying how resourceful a channel $\mathcal{N}$ is. One way of doing so is to define the amortized resourcefulness of a quantum channel as follows, generalizing the amortized entanglement from definition 1:

$$V_{\mathcal{A}}(\mathcal{N}) = \sup_{\rho_{RA}} V((\text{id}_R \otimes \mathcal{N}_{A \rightarrow B})(\rho_{RA})) - V(\rho_{RA}).$$  \hfill (7.1)
Suppose now that we have a protocol that accesses the channel \(N\) a total of \(n\) times and between each channel use, we allow for a free channel to be applied. Such protocols generalize those that we considered in sections 3.1 and 4.2. Let \(\omega\) denote the final state generated by the protocol, let \(\rho_{R_iA_i}\) denote the state before the \(i\)th channel use, and let \(\sigma_{R_iB_i}\) denote the state after the \(i\)th channel use. See figure 4 for a depiction of such a protocol. Then by applying the same reasoning in the proofs of propositions 13 and 17 (but now using properties 1 and 2 above), we find the following bound:

\[
V(\omega) \leq V(\sigma_{R_nB_n}) \leq V(\sigma_{R_nB_n}) - V(\rho_{R_1A_1}) + \sum_{i=2}^{n} V(\rho_{R_iA_i}) - V(\rho_{R_iA_i}) \leq V((\text{id}_R \otimes N_{A_i\rightarrow B_i})(\rho_{R_{i-1}A_{i-1}})) - V(\rho_{R_iA_i}) + \sum_{i=2}^{n} V((\text{id}_R \otimes N_{A_{i-1}\rightarrow B_{i-1}})(\rho_{R_{i-2}A_{i-2}})) - V(\rho_{R_iA_i}) \leq nV_A(N),
\]

which serves as a limitation on how much of the resource we can extract by invoking the channel \(n\) times in such a way. If \(V(\omega)\) can be connected to meaningful operational parameters such as the closeness of the final state \(\omega\) to a desired target state and the number of basic units of a resource, as was the case in propositions 13 and 17, then the above bound would be even more interesting in the context of a given resource theory.

We can also define \(\nu\)-freely-simulable channels as a generalization of the teleportation-simulable channels of [BDSW96, HHH99] and the \(\omega\)-PPT-simulable channels introduced in definition 16:

**Definition 22. (\(\nu\)-freely-simulable channel)** A quantum channel \(N\) is \(\nu\)-freely-simulable if there exists a resourceful state \(\nu\) and a free channel \(F\) such that the following equality holds for all input states \(\rho\):

\[
N(\rho) = F(\rho \otimes \nu).
\]
For $\nu$-freely simulable channels, protocols of the form discussed previously simplify significantly, as depicted in figure 5. The reduction depicted in figure 5 generalizes reduction by teleportation [BDSW96, MH12] reviewed in section 3.4 as well as the more general approach of “quantum simulation” put forward in [DDanM14], as the reduction applies in the context of any resource theory. By employing property 1 above and inspecting figure 5, it is immediate that the following bound holds

$$ V(\omega) \leq V(\nu^\otimes n), $$

which is just the statement that the amount of resourcefulness that can be extracted from the channel is limited by the resourcefulness of the underlying state $\nu$. If the resourcefulness measure is subadditive with respect to quantum states, then we arrive at the following bound for any protocol of the above form:

$$ \frac{1}{n}V(\omega) \leq V(\nu). $$

We think that it would be very interesting to work out some applications or consequences of the above observations in the context of several resource theories, such as thermodynamics BaHO$^+$13, asymmetry [MS14], or non-Gaussianity. We could certainly also consider approximately $\nu$-freely-simulable channels in order to find bounds on the extraction rates that are possible from protocols that use resourceful channels that are close to $\nu$-freely-simulable ones.

8. Conclusion

In this paper, we introduced the amortized entanglement of a channel as the largest difference in entanglement between the output and input of a quantum channel. We proved several properties of amortized entanglement and considered special cases of the measures such as amortized relative entropy of entanglement and amortized Rains relative entropy. One property of especial interest is the uniform continuity of the latter two special cases, in which an upper bound on the deviation of the amortized entanglement of two channels is given in terms of the output dimension of the channels and the diamond norm of their difference. This uniform continuity bound and the notion of approximately teleportation- and PPT-simulable channels then immediately leads to an upper bound on the secret-key-agreement and LOCC-assisted quantum capacities of such channels. We applied these notions to an example channel, which consists of a convex mixture of an amplitude damping channel and a depolarizing channel,
and we found that the upper bound is reasonably close to lower bounds on the capacities whenever the noise in the channel is sufficiently low. Finally, we discussed how to generalize many of the notions in the paper to more general resource theories, introducing concepts such as amortized resourcefulness of a channel and $\nu$-freely-simulable channels.

For future work, we think it would be interesting to explore the aforementioned generalization further, in the context of other resource theories such as thermodynamics, asymmetry, or non-Gaussianity.

Acknowledgments

We thank Stefan Bäuml, Siddhartha Das, Nilanjana Datta, Felix Leditzky, Iman Marvian, and Andreas Winter for discussions related to this paper. We also acknowledge support from the Office of Naval Research.

Appendix A. Supplementary lemmas for uniform continuity

The last inequality in the following lemma was established in [HHHO05a] for relative entropy of entanglement, but we give a different proof in what follows:

Lemma A.1. Let $E$ refer to either the relative entropy of entanglement or the Rains relative entropy. For $\rho_{ABC}$ a state, the following inequality holds

\[
E(A; BC)_{\rho} \leq E(A; B)_{\rho} + I(AB; C)_{\rho} \tag{A.1}
\]

\[
\leq E(A; B)_{\rho} + 2 \log_2 |C|. \tag{A.2}
\]

Proof. Let $S$ refer to either SEP or PPT'. Consider that

\[
E(A; BC)_{\rho} = \min_{\sigma_{ABC} \in S(A; BC)} D(\rho_{ABC} \| \sigma_{ABC}) \tag{A.3}
\]

\[
\leq \min_{\sigma_{AB} \in S(A; B)} D(\rho_{ABC} \| \sigma_{AB} \otimes \rho_C) \tag{A.4}
\]

\[
= \min_{\sigma_{AB} \in S(A; B)} \left[ -H(ABC)_{\rho} - \text{Tr}\{\rho_{ABC} \log_2 (\sigma_{AB} \otimes \rho_C)\} \right] \tag{A.5}
\]

\[
= \min_{\sigma_{AB} \in S(A; B)} \left[ -H(AB)_{\rho} - \text{Tr}\{\rho_{ABC} \log_2 (\sigma_{AB})\} - \text{Tr}\{\rho_{ABC} \log_2 (\rho_C)\} \right] \tag{A.6}
\]

\[
= \min_{\sigma_{AB} \in S(A; B)} \left[ -H(AB)_{\rho} - \text{Tr}\{\rho_{AB} \log_2 (\sigma_{AB})\} + H(C)_{\rho} \right] \tag{A.7}
\]

\[
= \min_{\sigma_{AB} \in S(A; B)} \left[ -H(C|AB)_{\rho} - H(AB)_{\rho} - \text{Tr}\{\rho_{AB} \log_2 (\sigma_{AB})\} + H(C)_{\rho} \right] \tag{A.8}
\]

\[
= -H(C|AB)_{\rho} + \min_{\sigma_{AB} \in S(A; B)} \left[ -H(AB)_{\rho} - \text{Tr}\{\rho_{AB} \log_2 (\sigma_{AB})\} \right] + H(C)_{\rho} \tag{A.9}
\]

\[
= -H(C|AB)_{\rho} + E(A; B)_{\rho} + H(C)_{\rho} \tag{A.10}
\]

\[
= E(A; B)_{\rho} + I(AB; C)_{\rho}. \tag{A.11}
\]

This concludes the proof. □
Lemma A.2. Let $E$ refer to either the relative entropy of entanglement or the Rains relative entropy. For a classical–quantum state

$$\rho_{XAB} \equiv \sum_x p_X(x) |x\rangle\langle x| \otimes \rho_{AB}^x.$$  \hfill (A.12)

the following equality holds

$$E(A;BX)_\rho = \sum_x p_X(x)E(A;B)_{\rho^x}. \hfill (A.13)$$

Proof. Let $S$ refer to either SEP or PPT'. Let $\sigma_{A:B}^x$ be the positive semi-definite operator that achieves the minimum for $\rho_{AB}^x$ in $E(A;B)_{\rho^x}$ and define

$$\theta_{XAB} \equiv \sum_x p_X(x) |x\rangle\langle x| \otimes \sigma_{AB}^x.$$  \hfill (A.14)

Then consider that

$$E(A;BX)_\rho = \min_{\sigma_{A:B} \in S(A:BX)} D(\rho_{ABX}||\sigma_{ABX})$$  \hfill (A.15)

$$\leq D(\rho_{ABX}||\theta_{ABX})$$  \hfill (A.16)

$$= \sum_x p_X(x)D(\rho_{AB}^x||\sigma_{AB}^x)$$  \hfill (A.17)

$$= \sum_x p_X(x)E(A;B)_{\rho^x}. \hfill (A.18)$$

To see the other inequality, let $\Sigma_X$ be a completely dephasing channel on system $X$ and consider for any positive semi-definite operator $\xi_{A:BX} \in S$ that

$$D(\rho_{ABX}||\xi_{ABX}) \geq D(\Sigma_X(\rho_{ABX})||\Sigma_X(\xi_{ABX}))$$  \hfill (A.19)

$$= D(\rho_{ABX}||\xi'_{ABX})$$  \hfill (A.20)

$$= \sum_x p_X(x)D(\rho_{AB}^x||\xi_{AB}^x) + D(p_X||q_X)$$  \hfill (A.21)

$$\geq \sum_x p_X(x)E(A;B)_{\rho^x}. \hfill (A.22)$$

where

$$\xi'_{ABX} = \Sigma_X(\xi_{ABX}) = \sum_x q_X(x) |x\rangle\langle x| \otimes \xi_{AB}^x.$$  \hfill (A.23)

In the case that $S =$PPT', the positive semi-definite operators are subnormalized [TWW17], which implies that $q_X(x)$ is a subnormalized probability distribution, and which in turn implies that $D(p_X||q_X) \geq 0$ [Wil16a].
The following lemma, of which the first inequality was proved in [LPSW05] for relative entropy of entanglement, can be understood as a direct consequence of Lemmas A.1 and A.2 and the fact that $I(X;AB)_{\rho} \leq H(X)_{\rho}$ for a classical system $X$:

**Lemma A.3.** Let $E$ refer to either the relative entropy of entanglement or the Rains relative entropy. Let $\{p_{X}(x), \rho_{AB}^{x}\}$ be an ensemble of states and let $\overline{p}_{AB} \equiv \sum_{x} p_{X}(x) \rho_{AB}^{x}$. Then we have that

$$\sum_{x} p_{X}(x) E(A;B)_{\rho} \leq E(A;B)_{\overline{p}} + I(X;AB)_{\rho}$$

(A.24)

$$\leq E(A;B)_{\overline{p}} + H(X),$$

(A.25)

where $H(X)$ is the Shannon entropy of the distribution $p_{X}$.

**Appendix B. Approximately teleportation-simulable channels, approximate covariance, and channel twirling via teleportation**

In this appendix, we discuss how the approximately covariant channels from [LKDW17] are approximately teleportation simulable in the sense of definition 19. We also mention how the well known protocol of channel twirling [BDSW96] can be implemented via teleportation over the Choi state of the channel. This latter result might have applications in other domains, such as randomized benchmarking [KLR*08].

We begin with a brief review of some background material. Let $G$ be a group with unitary representations $g \mapsto U_{A}^{g}$ on $\mathcal{H}_{A}$ and $g \mapsto V_{B}^{g}$ on $\mathcal{H}_{B}$, respectively. A quantum channel $\mathcal{N}_{A \rightarrow B}$ is covariant with respect to $\{(U_{A}^{g}, V_{B}^{g})\}_{g \in G}$ [Hol02], if

$$V_{B}^{g} \mathcal{N}(\cdot) V_{B}^{g\dagger} = \mathcal{N}(U_{A}^{g}(\cdot) U_{A}^{g\dagger})$$

for all $g \in G$.

A group $G$ is said to form a **unitary one-design**, if there is a unitary representation $g \mapsto U_{A}^{g}$ of $G$ on $\mathcal{H}_{A}$ such that

$$\frac{1}{|G|} \sum_{g \in G} U_{A}^{g}\pi_{A}U_{A}^{g\dagger} = \pi_{A}$$

for all states $\rho_{A}$,

where $\pi_{A} = \frac{1}{|H_{A}|} I_{A}$ denotes the maximally mixed state on $\mathcal{H}_{A}$.

For a group $G$ with unitary representations $g \mapsto U_{A}^{g}$ on $\mathcal{H}_{A}$ and $g \mapsto V_{B}^{g}$ on $\mathcal{H}_{B}$, respectively, and an arbitrary quantum channel $\mathcal{N}_{A \rightarrow B}$, the **twirled channel** $\mathcal{N}_{G}$ of $\mathcal{N}$ is defined as

$$\mathcal{N}_{G}(\cdot) \equiv \frac{1}{|G|} \sum_{g \in G} V_{B}^{g\dagger} \mathcal{N}(U_{A}^{g}(\cdot) U_{A}^{g\dagger}) V_{B}^{g}.$$  

This twirled channel $\mathcal{N}_{G}$ is covariant with respect to $\{(U_{A}^{g}, V_{B}^{g})\}_{g \in G}$ by construction.

The typical way of realizing the twirled channel $\mathcal{N}_{G}$ is by means of LOCC. The sender picks $g$ uniformly at random, applies $U_{A}^{g}$ on the input state, sends the state through the channel $\mathcal{N}$, transmits $g$ to the receiver, who then applies $V_{B}^{g}$ at the output.

A different LOCC simulation of the twirled channel $\mathcal{N}_{G}$ is realized by means of a generalized teleportation protocol, as stated in the following proposition:

**Proposition B.1.** The twirled channel $\mathcal{N}_{G}$ can be simulated from $\mathcal{N} : \mathcal{L}(\mathcal{H}_{A}) \rightarrow \mathcal{L}(\mathcal{H}_{B})$ by means of a generalized teleportation protocol with a resource state equal to the Choi state $\omega_{AB} = \mathcal{N}_{A'' \rightarrow B}(\Phi_{AA''})$ where $\mathcal{H}_{A} \simeq \mathcal{H}_{A'}, \mathcal{H}_{A''} \simeq \mathcal{H}_{A'''}$, the POVM elements as
\[
E_{AA}^{g} \equiv \frac{|A|^2}{|G|} (U_{AA}^g)^\dagger \Phi_{AA} U_{AA}^g,
\]
with \(\{U_{AA}^g\}_{g \in G}\) a one-design, and teleportation correction operations given by \(V_B^g\) acting on the \(B\) system. That is, the following equality holds
\[
\sum_g V_B^g \text{Tr}_{AA'} \{E_{AA}^g (\rho_A \otimes \omega_{AB})\} V_B^g = \frac{1}{|G|} \sum_g V_B^g N_{A \rightarrow B} (U_{AA}^g \rho_A U_{AA}^g\dagger) V_B^g.
\]

**Proof.** We follow the proof of [WTB17, appendix A] closely. Let \(N : \mathcal{L}(\mathcal{H}_A) \rightarrow \mathcal{L}(\mathcal{H}_B)\) be a quantum channel, and let \(G\) be a group with unitary representations \(U_A^g\) and \(V_B^g\) for \(g \in G\), such that
\[
\frac{1}{|G|} \sum_g U_A^g X_A (U_A^g)^\dagger = \text{Tr}\{X_A\} \pi_A,
\]
where \(X_A \in \mathcal{L}(\mathcal{H}_A)\) and \(\pi\) denotes the maximally mixed state. (For notational convenience, we are placing the index \(g\) as a superscript.) Consider that
\[
\frac{1}{|G|} \sum_g U_A^g \Phi_{AA'} (U_A^g)^\dagger = \pi_{A'} \otimes \pi_A,
\]
where \(\Phi\) denotes a maximally entangled state and \(A'\) is a system isomorphic to \(A\). Note that in order for \(\{U_A^g\}\) to satisfy (B.3), it is necessary that \(|A|^2 \leq |G|\) [AMTdW00]. Consider the POVM \(\{E_{AA}^g\}_g\), with \(A'\) a system isomorphic to \(A\) and each element \(E_{AA}^g\) defined as
\[
E_{AA}^g \equiv \frac{|A|^2}{|G|} (U_{AA}^g)^\dagger \Phi_{AA} U_{AA}^g.
\]
It follows from the fact that \(|A|^2 \leq |G|\) (B.4), and the group property that \(\{E_{AA'}^g\}_g\) is a valid POVM.

The simulation of the channel \(N_G\) via teleportation begins with a state \(\rho_A\) and a shared resource \(\omega_{AB} \equiv N_{A \rightarrow B} (\Phi_{AA'})\). The desired outcome is for Bob to receive the state \(V_B^\dagger N_{A \rightarrow B} (U_{AA}^g \rho_A U_{AA}^g\dagger) V_B^\dagger\) with probability \(1/|G|\) and for the protocol to work independently of the input state \(\rho_A\). The first step is for Alice to perform the measurement \(\{E_{AA}^g\}_g\) on systems \(A' A\) and then send the outcome \(g\) to Bob. Based on the outcome \(g\), Bob then performs \(V_B^g\). The channel realized by such a generalized teleportation protocol is as follows:
\[
\sum_g V_B^g \text{Tr}_{AA'} \{E_{AA}^g (\rho_A \otimes \omega_{AB})\} V_B^g.
\]

The following analysis demonstrates that this protocol works (i.e. it simulates \(N_G\), by simplifying the form of the post-measurement state:
\[
|G| \text{Tr}_{AA'} \{E_{AA}^g (\rho_A \otimes \omega_{AB})\} = |A|^2 \text{Tr}_{AA'} \{(U_{AA}^g)^\dagger |\Phi_{AA'}\rangle \langle \Phi_{AA'}| A' A \}
\]
\[ |\langle \Phi | A \rho_A \Phi \rangle | = \langle \Phi | A \rho_A (U_A^\dagger \otimes \omega_{AB}) (U_A^\dagger) | \Phi \rangle_{A'A} \quad (B.8) \]

\[ = |A|^2 \langle \Phi | A U_A^\dagger \rho_A (U_A^\dagger) | \Phi \rangle_{A'A} \quad (B.9) \]

\[ = |A|^2 \langle \Phi | A U_A^\dagger \rho_A (U_A^\dagger) | \Phi \rangle_{A'A} \quad (B.10) \]

The first three equalities follow by substitution and some rewriting. The fourth equality follows from the fact that

\[ \langle \Phi | A M A \rangle = \langle \Phi | A M^* A \rangle \quad (B.11) \]

for any operator \(M\) and where \(\ast\) denotes the complex conjugate, taken with respect to the basis in which \(|\Phi\rangle_{A'A}\) is defined. Continuing, we have that

\[ (B.10) = |A| \text{Tr}_A \left\{ \left[ U_A^\rho_A (U_A^\dagger)^\ast \right] N_{A'' \rightarrow B} (\Phi_{AA''}) \right\} \quad (B.12) \]

\[ = |A| \text{Tr}_A \left\{ N_{A'' \rightarrow B} \left[ \left[ U_A^\rho_A (U_A^\dagger)^\ast \right] \Phi_{AA''} \right] \right\} \quad (B.13) \]

\[ = N_{A'' \rightarrow B} \left[ \left[ U_A^\rho_A (U_A^\dagger)^\ast \right] \right] \quad (B.14) \]

\[ = N_{A'' \rightarrow B} \left[ U_A^\rho_A (U_A^\dagger) \right] \quad (B.15) \]

The first equality follows because \(|A| \langle \Phi | A \rho_A \Phi \rangle | \Phi \rangle_{A'A} = \text{Tr}_A \{M_{AB}\}\) for any operator \(M_{AB}\). The second equality follows by applying the conjugate transpose of (B.11). The above development then implies the following equality:

\[ \text{Tr}_{AA'} \left\{ E_{AA'}^A (\rho_A' \otimes \omega_{AB}) \right\} = \frac{1}{|G|} N_{A'' \rightarrow B} \left[ U_A^\rho_A (U_A^\dagger) \right], \quad (B.16) \]

which after insertion into (B.6), establishes the claim in (B.2).

The notion of approximate covariance of a quantum channel from [LKDW17] is based on how close the channel is in diamond norm to its twirled channel:

**Definition B.2 (Approximate covariance [LKDW17]).** Fix a group \(G\) with unitary representations \(g \mapsto U_g^A\) on \(H_A\) and \(g \mapsto V_g^B\) on \(H_B\), respectively. For a given \(\varepsilon \in [0, 1]\), a channel \(N\) \(\varepsilon\)-covariant with respect to \(\{U_g^A\}_{g \in G}\) if

\[ \frac{1}{2} \|N - N_G\|_{\diamond} \leq \varepsilon. \]

It has been known for many years now that a quantum channel covariant with respect to a one-design is teleportation simulable with resource state equal to the Choi state of the channel [CDP09, section 7]. Thus, an immediate consequence of definitions is that a channel is \((\varepsilon, N(\Phi))\)-approximately teleportation-simulable if it is \(\varepsilon\)-covariant, with \(\{U_g^A\}_{g \in G}\) a one-design.
References

[ADMVW02] Audenaert K, De Moor B, Vollbrecht K G H and Werner R F 2002 Asymptotic relative entropy of entanglement for orthogonally invariant states Phys. Rev. A 66 032310

[AML16] Azuma K, Mizutani A and Lo H-K 2016 Fundamental rate-loss trade-off for the quantum internet Nat. Commun. 7 13523

[AMTdW00] Ambainis A, Mosca M, Tapp A and de Wolf R 2000 Private quantum channels IEEE 41st Annual Symp. on Foundations of Computer Science pp 547–53

[BA17] Bäuml S and Azuma K 2017 Fundamental limitation on quantum broadcast networks Quantum Sci. Technol. 2 024004

[BaHO+13] Brandão F G S L, Horodecki M, Oppenheim J, Renes J M and Spekkens R W 2013 Resource theory of quantum states out of thermal equilibrium Phys. Rev. Lett. 111 250404

[BB84] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. of IEEE Int. Conf. on Computers Systems, Signal Processing, (Bangalore and India) pp 175–9

[BBC+93] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels Phys. Rev. Lett. 70 1895–9

[BBP+96] Bennett C H, Brassard G, Popescu S, Schumacher B, Smolin J A and Wootters W K 1996 Purification of noisy entanglement and faithful teleportation via noisy channels Phys. Rev. Lett. 76 722–5

[BCY11] Brandao F G, Christandl M and Yard J 2011 Faithful squashed entanglement Commun. Math. Phys. 306 805–30

[BD11] Brandao F G S L and Datta N 2011 One-shot rates for entanglement manipulation under non-entangling maps IEEE Trans. Inf. Theory 57 1754–60

[BDGDMW17] Ben Dana K, García Diaz M, Mejatty M and Winter A 2017 Resource theory of coherence: beyond states Phys. Rev. A 95 062327

[BDSW96] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 Mixed-state entanglement and quantum error correction Phys. Rev. A 54 3824–51

[BG15] Brandoa F G S L and Gour G 2015 Reversible framework for quantum resource theories Phys. Rev. Lett. 115 070503

[BHLS03] Bennett C H, Harrow A W, Leung D W and Smolin J A 2003 On the capacities of bipartite Hamiltonians and unitary gates IEEE Trans. Inf. Theory 49 1895–911

[BK98] Braunstein S L and Kimble H J 1998 Teleportation of continuous quantum variables Phys. Rev. Lett. 80 689–72

[BSST99] Bennett C H, Shor P W, Smolin J A and Thapliyal A V 1999 Entanglement-assisted classical capacity of noisy quantum channels Phys. Rev. Lett. 83 3081–4

[BSST02] Bennett C H, Shor P W, Smolin J A and Thapliyal A V 2002 Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem IEEE Trans. Inf. Theory 48 2637–55

[CDP09] Chiribella G, D’Ariano G M and Perinotti P 2009 Realization schemes for quantum instruments in finite dimensions J. Math. Phys. 50 042101

[Chr06] Christandl M 2006 The structure of bipartite quantum states: insights from group theory and cryptography PhD Thesis University of Cambridge

[CMH17] Christandl M and Müller-Hermes A 2017 Relative entropy bounds on quantum, private and repeater capacities Commun. Math. Phys. 353 821–52

[CW04] Christandl M and Winter A 2004 Squashed entanglement: an additive entanglement measure J. Math. Phys. 45 829–40

[Dat09] Datta N 2009 Min- and max-relative entropies and a new entanglement monotone IEEE Trans. Inf. Theory 55 2816–26

[DDanM14] Demkowicz-Dobrzański R and Maccone L 2014 Using entanglement against noise in quantum metrology Phys. Rev. Lett. 113 250801
Devetak I, Junge M, King C and Ruskai M B 2006 Multiplicativity of completely bounded p-norms implies a new additivity result Commun. Math. Phys. 266 37–63

Del Rio L, Kraemer L and Renner R 2015 Resource theories of knowledge (arXiv:1511.08818)

Das S and Wilde M M 2017 Quantum reading capacity: general definition and bounds (arXiv:1703.03706)

Ekert A K 1991 Quantum cryptography based on Bell’s theorem Phys. Rev. Lett. 67 661–3

Fawzi H and Fawzi O 2017 Relative entropy optimization in quantum information theory via semidefinite programming approximations (arXiv:1705.06671)

Fritz T 2017 Resource convertibility and ordered commutative monoids Math. Struct. Comput. Sci. 27 189–938

Goodenough K, Elkouss D and Wehner S 2016 Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels New J. Phys. 18 063005

Horodecki M, Horodecki P and Horodecki R 1996 Separability of mixed states: necessary and sufficient conditions Phys. Lett. A 223

Horodecki M, Horodecki P and Horodecki R 1999 General teleportation channel, singlet fraction and quasidistillation Phys. Rev. A 60 1888–98

Horodecki K, Horodecki M, Horodecki P, Leung D and Oppenheim J 2008 Quantum key distribution based on private states: unconditional security over untrusted channels with zero quantum capacity IEEE Trans. Inf. Theory 54 2604–20

Horodecki K, Horodecki M, Horodecki P, Leung D and Oppenheim J 2008 Unconditional privacy over channels which cannot convey quantum information Phys. Rev. Lett. 100 110502

Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Quantum entanglement Rev. Mod. Phys. 81 865–942

Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2005 Locking entanglement with a single qubit Phys. Rev. Lett. 94 200501

Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2005 Secure key from bound entanglement Phys. Rev. Lett. 94 160502

Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2009 General paradigm for distilling classical key from quantum states IEEE Trans. Inf. Theory 55 1898–929

Holevo A S 2002 Remarks on the classical capacity of quantum channel (arXiv:quant-ph/0212025)

Holevo A S 2006 Multiplicativity of p-norms of completely positive maps and the additivity problem in quantum information theory Russ. Math. Surv. 61 301–39

Holevo A S 2012 Quantum Systems, Channels, Information (Studies in Mathematical Physics) vol 16 (Berlin: Walter de Gruyter)

Horodecki M, Shor P W and Ruskai M B 2003 Entanglement breaking channels Rev. Math. Phys. 15 629–41

Kraemer L and del Rio L 2016 Currencies in resource theories (arXiv:1605.01064)

Kitaev A Y 1997 Quantum computations: algorithms and error correction Russ. Math. Surv. 52 1191–249

Knill E, Leibfried D, Reichle R, Britton J, Blakestad R B, Jost D J, Langer C, Ozeri R, Seidelin S and Wineland D J 2008 Randomized benchmarking of quantum gates Phys. Rev. A 77 012307

Koashi M and Winter A 2004 Monogamy of quantum entanglement and other correlations Phys. Rev. A 69 022309

Kaur E and Wilde M M 2017 Upper bounds on secret key agreement over lossy thermal bosonic channels (arXiv:1706.04590)

Lütkenhaus N and Guha S 2015 Quantum repeaters: objectives, definitions and architectures definitions and architectures (available at http://wqrn.pratt.duke.edu/presentations.html)
Leifer M S, Henderson L and Linden N 2003 Optimal entanglement generation from quantum operations *Phys. Rev.* A 67 012306

Lindblad G 1973 Entropy, information and quantum measurements *Commun. Math. Phys.* 33 305–22

Lindblad G 1975 Completely positive maps and entropy inequalities *Commun. Math. Phys.* 40 147–51

Leditzky F, Kaur E, Datta N and Wilde M M 2017 Approaches for approximate additivity of the Holevo information of quantum channels (arXiv:1709.01111)

Leditzky F, Leung D and Smith G 2017 Quantum and private capacities of low-noise channels (arXiv:1705.04335)

Linden N, Popescu S, Schumacher B and Westmoreland M 2005 Reversibility of local transformations of multiparticle entanglement *Quantum Inf. Process.* 4 241–50

Lieb E H and Ruskai M B 1973 A fundamental property of quantum-mechanical entropy *Phys. Rev. Lett.* 30 434–6

Lieb E H and Ruskai M B 1973 Proof of the strong subadditivity of quantum-mechanical entropy *J. Math. Phys.* 14 1938–41

Leditzky F, Leung D and Smith G 2017 Quantum and private capacities of low-noise channels (arXiv:1705.04335)

Lin73

Lin75

Lindblad G 1973 Entropy, information and quantum measurements *Commun. Math. Phys.* 33 305–22

Lindblad G 1975 Completely positive maps and entropy inequalities *Commun. Math. Phys.* 40 147–51

Leditzky F, Kaur E, Datta N and Wilde M M 2017 Approaches for approximate additivity of the Holevo information of quantum channels (arXiv:1709.01111)

Leditzky F, Leung D and Smith G 2017 Quantum and private capacities of low-noise channels (arXiv:1705.04335)

Linden N, Popescu S, Schumacher B and Westmoreland M 2005 Reversibility of local transformations of multiparticle entanglement *Quantum Inf. Process.* 4 241–50

Li 2014

LPSW05

Linden N, Popescu S, Schumacher B and Westmoreland M 2005 Reversibility of local transformations of multiparticle entanglement *Quantum Inf. Process.* 4 241–50

LPSW05

Linden N, Popescu S, Schumacher B and Westmoreland M 2005 Reversibility of local transformations of multiparticle entanglement *Quantum Inf. Process.* 4 241–50

LPSW05

Linden N, Popescu S, Schumacher B and Westmoreland M 2005 Reversibility of local transformations of multiparticle entanglement *Quantum Inf. Process.* 4 241–50

Müller-Hermes A 2012 Transposition in quantum information theory Master’s Thesis Technical University of Munich

Müller-Lennert M, Dupuis F, Szehr O, Fehr S and Tomamichel M 2013 On quantum Rényi entropies: a new definition and some properties *J. Math. Phys.* 54 122203

Marvian I and Spekkens R W 2014 Modes of asymmetry: the application of harmonic analysis to symmetric quantum dynamics and quantum reference frames *Phys. Rev.* A 90 062110

Matthews W and Wehner S 2014 Finite blocklength converse bounds for quantum channels *IEEE Trans. Inf. Theory* 60 7317–29

Niset J, Fiurášek J and Cerf N J 2009 No-go theorem for Gaussian quantum error correction *Phys. Rev. Lett.* 102 120501

Niset J, Fiurášek J and Cerf N J 2009 No-go theorem for Gaussian quantum error correction *Phys. Rev. Lett.* 102 120501

Peres A 1996 Separability criterion for density matrices *Phys. Rev. Lett.* 77 1413–5

Peres A 1996 Separability criterion for density matrices *Phys. Rev. Lett.* 77 1413–5

Pirandola S, Laurenza R, Ottaviani C and Banchi L 2013 On quantum Rényi entropies: a new definition and some properties *J. Math. Phys.* 54 122203

Rains E M 1999 Bound on distillable entanglement *Phys. Rev.* A 60 179–84

Rains E M 2001 A semidefinite program for distillable entanglement *IEEE Trans. Inf. Theory* 47 2921–33

Rozpedek F, Goodenough K, Ribeiro I, Kalb N, Vivoli V C, Reiserer A, Hanson R, Wehner S and Elkouss D 2017 Realistic parameter regimes for a single sequential quantum repeater (arXiv:1705.00043)

Rigovacca L, Kato G, Baemml S, Kim M S, Munro W J and Azuma K 2017 Versatile relative entropy bounds for quantum networks (arXiv:1707.05543)

Shirokov M E 2016 Continuity bounds for information characteristics of quantum channels depending on input dimension and on input energy (arXiv:1610.08870)

Shirokov M E 2016 Continuity bounds for information characteristics of quantum channels depending on input dimension and on input energy (arXiv:1610.08870)

Shuracher B and Nielsen M A 1996 Quantum data processing and error correction *Phys. Rev. A* 54 2629–35

Shuracher B and Nielsen M A 1996 Quantum data processing and error correction *Phys. Rev. A* 54 2629–35

Smith G, Smolin J A and Winter A 2008 The quantum capacity with symmetric side channels *IEEE Trans. Inf. Theory* 54 4208–17

Sutter D, Scholz V B, Winter A and Renner R 2014 Approximate degradable quantum channels (arXiv:1412.0980)

Seshadreesan K P, Takeoka M and Wilde M M 2016 Bounds on entanglement distillation and secret key agreement for quantum broadcast channels *IEEE Trans. Inf. Theory* 62 2849–66

Takeoka M, Guha S and Wilde M M 2014 Fundamental rate-loss tradeoff for optical quantum key distribution *Nat. Commun.* 5 5235

Takeoka M, Guha S and Wilde M M 2014 Fundamental rate-loss tradeoff for optical quantum key distribution *Nat. Commun.* 5 5235

Takeoka M, Guha S and Wilde M M 2014 Fundamental rate-loss tradeoff for optical quantum key distribution *Nat. Commun.* 5 5235

Takeoka M, Guha S and Wilde M M 2014 The squashed entanglement of a quantum channel *IEEE Trans. Inf. Theory* 60 4987–98

Takeoka M, Seshadreesan K P and Wilde M M 2016 Unconstrained distillation capacities of a pure-loss bosonic broadcast channel *IEEE Int. Symposium on Information Theory* pp 2484–8
[TSW17] Takeoka M, Seshadreesan K P and Wilde M M 2017 Unconstrained capacities of quantum key distribution and entanglement distillation for pure-loss bosonic broadcast channels Phys. Rev. Lett. 119 150501

[Tuc99] Tucci R R 1999 Quantum entanglement and conditional information transmission (arXiv:quant-ph/9909041)

[Tuc02] Tucci R R 2002 Entanglement of distillation and conditional mutual information (arXiv:quant-ph/0202144)

[TWW17] Tomamichel M, Wilde M M and Winter A 2017 Strong converse rates for quantum communication IEEE Trans. Inf. Theory 63 715–27

[Uhl76] Uhlmann A 1976 The ‘transition probability’ in the state space of a *-algebra Rep. Math. Phys. 9 273–9

[Ume62] Umegaki H 1962 Conditional expectations in an operator algebra IV (entropy and information) Kodai Math. Semin. Rep. 14 59–85

[VP98] Vedral V and Plenio M B 1998 Entanglement measures and purification procedures Phys. Rev. A 57 1619–33

[Wat15] Watrous J 2015 Theory Quantum Inf.

[Wer89] Werner R F 1989 Quantum states with Einstein–Podolsky–Rosen correlations admitting a hidden-variable model Phys. Rev. A 40 4277–81

[Wer01] Werner R F 2001 All teleportation and dense coding schemes J. Phys. A: Math. Gen. 34 7081

[Wil16a] Wilde M M 2016 From classical to quantum shannon theory (arXiv:1106.1445v7)

[Wil16b] Wilde M M 2016 Squashed entanglement and approximate private states Quantum Inf. Process. 15 4563–80

[Win16] Winter A 2016 Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints Commun. Math. Phys. 347 291–313

[WPGG07] Wolf M M, Pérez-García D and Giedke G 2007 Quantum capacities of bosonic channels Phys. Rev. Lett. 98 130501

[WR12] Wang L and Renner R 2012 One-shot classical-quantum capacity and hypothesis testing Phys. Rev. Lett. 108 200501

[WTB17] Wilde M M, Tomamichel M and Berta M 2017 Converse bounds for private communication over quantum channels IEEE Trans. Inf. Theory 63 1792–817

[WWY14] Wilde M M, Winter A and Yang D 2014 Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy Commun. Math. Phys. 331 593–622

[WY16] Winter A and Yang D 2016 Potential capacities of quantum channels IEEE Trans. Inf. Theory 62 1415–24