Amortized entanglement of a quantum channel and approximately teleportationsimulable channels

Eneet Kaur
Louisiana State University

Mark M. Wilde
Louisiana State University

Recommended Citation

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

Eneet Kaur*   Mark M. Wilde*†

December 20, 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 ν-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.

*Department of Physics and Astronomy, Louisiana State University, Baton Rouge, Louisiana 70803, USA
†Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA

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, Fri15, 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
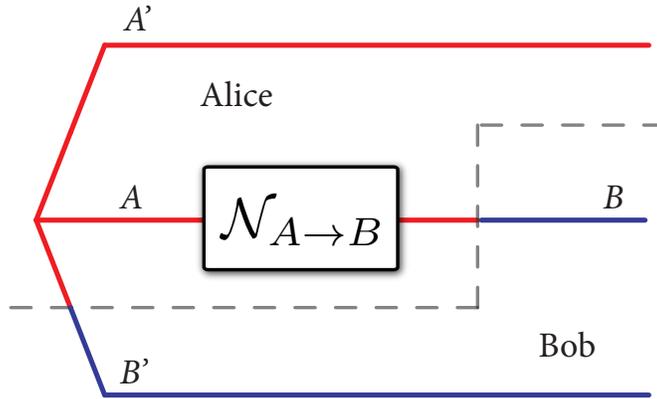
Figure 1: The amortized entanglement of a quantum channel $\mathcal{N}_{A \to B}$ is the largest difference in the entanglement between the output state on systems $A' : BB'$ and the input state on systems $A'A : B'$, the former of which is generated by the quantum channel $\mathcal{N}_{A \to B}$.

of resourcefulness that can be extracted from multiple calls to a quantum channel by inter-leaving calls to it with free channels. We also introduce the notion of a ν-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 [HHHH09], 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 $\mathcal{N}_{A \to B}$*

and an entanglement measure E, we define the channel's amortized entanglement as follows:

$$E_A(\mathcal{N}) \equiv \sup_{\rho_{A'AB'}} E(A'; BB')_\theta - E(A'A; B')_\rho, \tag{2.1}$$

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

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 and input of the channel.

Recall that the quantum relative entropy $D(\varsigma \| \xi)$ for a state ς and a positive semi-definite operator ξ is defined as [Ume62, Lin73]

$$D(\varsigma \| \xi) \equiv \operatorname{Tr}\{\varsigma [\log_2 \varsigma - \log_2 \xi]\}, \tag{2.2}$$

whenever $\operatorname{supp}(\varsigma) \subseteq \operatorname{supp}(\xi)$ 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, HHHO09] 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 $\mathcal{N}_{A \to B}$, its amortized relative entropy of entanglement is defined as follows:*

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

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

$$E_R(C; D)_\tau \equiv \inf_{\sigma_{CD} \in \operatorname{SEP}(C:D)} D(\tau_{CD} \| \sigma_{CD}), \tag{2.4}$$

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

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

$$R_A(\mathcal{N}) \equiv \sup_{\rho_{A'AB'}} R(A'; BB')_\theta - R(A'A; B')_\rho, \tag{2.5}$$

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

$$R(C; D)_\tau \equiv \inf_{\sigma_{CD} \in \operatorname{PPT}'(C:D)} D(\tau_{CD} \| \sigma_{CD}), \tag{2.6}$$

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

$$\operatorname{PPT}'(C:D) = \{\sigma_{CD} : \sigma_{CD} \geq 0 \wedge \|T_D(\sigma_{CD})\|_1 \leq 1\}, \tag{2.7}$$

and T_D denotes the partial transpose of system D.

Observe that SEP $\subset$ PPT$'$. Also, note that the quantities $E_{AR}(\mathcal{N})$ and $R_A(\mathcal{N})$ 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, RKB$^+$17]

$$E(\mathcal{N}) \equiv \sup_{\psi_{A'A}} E(A'; B)_\theta, \tag{2.8}$$

where

$$\theta_{A'B} \equiv \mathcal{N}_{A \to B}(\psi_{A'A}), \tag{2.9}$$

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:

$$E_R(\mathcal{N}) = \sup_{\psi_{A'A}} E_R(A'; B)_\theta, \tag{2.10}$$

$$R(\mathcal{N}) = \sup_{\psi_{A'A}} R(A'; B)_\theta. \tag{2.11}$$

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

$$E_A(\mathcal{N}) \geq E(\mathcal{N}), \tag{2.12}$$

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 $E_{\text{sq}}(\mathcal{N})$. A particular property of squashed entanglement was established as [TGW14b, Theorem 7]. We remark here (briefly) that [TGW14b, Theorem 7] implies the following inequality for the amortized version of squashed entanglement

$$E_{A,\text{sq}}(\mathcal{N}) \leq E_{\text{sq}}(\mathcal{N}), \tag{2.13}$$

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

$$E_{A,\text{sq}}(\mathcal{N}) = E_{\text{sq}}(\mathcal{N}). \tag{2.14}$$

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 entaglement

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

$$E(C;D)_{\rho^\lambda} \leq \lambda E(C;D)_{\rho^0} + (1-\lambda)E(C;D)_{\rho^1}, \tag{2.15}$$

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 $\lambda \in [0,1]$:*

$$E_A(\mathcal{N}^\lambda) \leq \lambda E_A(\mathcal{N}^0) + (1-\lambda)E_A(\mathcal{N}^1), \tag{2.16}$$

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

Proof. Let $\rho_{A'AB'}$ be a state and set $\tau_{A'BB'} = \lambda \mathcal{N}_{A\to B}^0(\rho_{A'AB'}) + (1-\lambda)\mathcal{N}^1(\rho_{A'AB'})$. Then consider that

$$\begin{aligned}
&E(A';BB')_\tau - E(A'A;B')_\rho \\
&= E(A';BB')_\tau - \lambda E(A'A;B')_\rho - (1-\lambda)E(A'A;B')_\rho & (2.17) \\
&\leq \lambda E(A';BB')_{\mathcal{N}^0(\rho)} + (1-\lambda)E(A';BB')_{\mathcal{N}^1(\rho)} - \lambda E(A'A;B')_\rho - (1-\lambda)E(A'A;B')_\rho & (2.18) \\
&= \lambda(E(A';BB')_{\mathcal{N}^0(\rho)} - E(A'A;B')_\rho) + (1-\lambda)(E(A';BB')_{\mathcal{N}^1(\rho)} - E(A'A;B')_\rho) & (2.19) \\
&\leq \lambda E_A(\mathcal{N}^0) + (1-\lambda)E_A(\mathcal{N}^1) & (2.20)
\end{aligned}$$

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. $\blacksquare$

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 ρ_{RA}, the output state $(\mathrm{id}_R \otimes \mathcal{N}_{A\to B})(\rho_{RA})$ 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 $\sigma_{A'BB'} = \mathcal{N}(\rho_{A'AB'})$ 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

$$E(A'; BB')_\sigma - E(A'A; B')_\rho \le E(A'A; B')_\rho - E(A'A; B')_\rho = 0. \tag{2.21}$$

The inequality follows from the fact that E is an entanglement measure and is thus monotone with respect to LOCC. Given that we always have $E_A(\mathcal{N}) \ge 0$, we conclude that $E_A(\mathcal{N}) = 0$.

Now we prove the second statement above: 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. From (2.12), we have that $E_A(\mathcal{N}) \ge E(\mathcal{N})$, which in turn implies that $E(\mathcal{N}) = 0$. Since the underlying entanglement measure E is faithful and $E(A'; B)_{\mathcal{N}(\rho)} \le E(\mathcal{N})$ for all mixed input states $\rho_{A'A}$, we conclude that for all mixed input states $\rho_{A'A}$, the output state $\mathcal{N}_{A\to B}(\rho_{A'A})$ is separable. Thus, $\mathcal{N}$ is entanglement breaking. ∎

2.4 (Sub)additivity of a channel's amortized entanglement

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 $\mathcal{M}$:*

$$E_A(\mathcal{N} \otimes \mathcal{M}) \le E_A(\mathcal{N}) + E_A(\mathcal{M}). \tag{2.22}$$

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 $\rho_{A'A_1A_2B'}$ denote a state to consider at the input of $\mathcal{N} \otimes \mathcal{M}$, when optimizing the amortized entanglement. Let $\theta_{A'B_1B_2B'} = (\mathcal{N}_{A_1\to B_1} \otimes \mathcal{M}_{A_2\to B_2})(\rho_{A'A_1A_2B'})$, which is the state at the output of the channel $\mathcal{N} \otimes \mathcal{M}$ when inputting $\rho_{A'A_1A_2B'}$. Define the intermediary state $\tau_{A'A_1B_2B'} = \mathcal{M}_{A_2\to B_2}(\rho_{A'A_1A_2B'})$. Then consider that

$$\begin{aligned} & E(A'; B_1B_2B')_\theta - E(A'A_1A_2; B')_\rho \\ &= E(A'; B_1B_2B')_\theta - E(A'A_1; B_2B')_\tau + E(A'A_1; B_2B')_\tau - E(A'A_1A_2; B')_\rho \tag{2.23} \\ &\le E_A(\mathcal{N}) + E_A(\mathcal{M}). \tag{2.24} \end{aligned}$$

The first equality follows by adding and subtracting $E(A'A_1; B_2B')_\tau$. The second inequality follows because the states $\tau_{A'A_1B_2B'}$ and $\theta_{A'B_1B_2B'}$ are particular states to consider at the respective input and output for the amortized entanglement of the channel $\mathcal{N}$, by making the identifications $A' \leftrightarrow A'$, $B' \leftrightarrow B'B_2$, $B \leftrightarrow B_1$, and $A \leftrightarrow A_1$, while the states $\rho_{A'A_1A_2B'}$ and $\tau_{A'A_1B_2B'}$ are particular states to consider at the respective input and output for the amortized entanglement of the channel $\mathcal{M}$, by making the identifications $A' \leftrightarrow A'A_1$, $B' \leftrightarrow B'$, $B \leftrightarrow B_2$, and $A \leftrightarrow A_2$. Since the inequality in (2.24) holds for all states $\rho_{A'A_1A_2B'}$, we can conclude the inequality in (2.22). ∎

An immediate consequence of Proposition 6 is the following inequality:

$$\sup_{\mathcal{M}} [E_A(\mathcal{N} \otimes \mathcal{M}) - E_A(\mathcal{M})] \le E_A(\mathcal{N}), \tag{2.25}$$

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

$$E(C_1C_2; D_1D_2)_\tau = E(C_1; D_1)_\xi + E(C_2; D_2)_\zeta, \qquad (2.26)$$

where $\tau_{C_1C_2D_1D_2} = \xi_{C_1D_1} \otimes \zeta_{C_2D_2}$ and $\xi_{C_1D_1}$ and $\zeta_{C_2D_2}$ are bipartite states. It is subadditive if

$$E(C_1C_2; D_1D_2)_\tau \leq E(C_1; D_1)_\xi + E(C_2; D_2)_\zeta, \qquad (2.27)$$

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 $\mathcal{M}$:*

$$E_A(\mathcal{N} \otimes \mathcal{M}) = E_A(\mathcal{N}) + E_A(\mathcal{M}). \qquad (2.28)$$

Proof. The inequality $\leq$ holds for all channels as shown in Proposition 6. To see the other inequality, let $\rho_{A_1'A_1B_1'} \otimes \kappa_{A_2'A_2B_2'}$ be an arbitrary state to consider for $E_A(\mathcal{N} \otimes \mathcal{M})$, and let

$$\theta_{A_1'B_1B_1'A_2'B_2B_2'} = \mathcal{N}_{A_1 \to B_1}(\rho_{A_1'A_1B_1'}) \otimes \mathcal{M}_{A_2 \to B_2}(\kappa_{A_2'A_2B_2'}). \qquad (2.29)$$

Then

$$E_A(\mathcal{N} \otimes \mathcal{M}) \geq E(A_1'A_2'; B_1B_2B_1'B_2')_\theta - E(A_1'A_2'A_1A_2; B_1'B_2')_{\rho \otimes \kappa} \qquad (2.30)$$

$$= E(A_1'; B_1B_1')_\theta - E(A_1'A_1; B_1')_\rho + E(A_2'; B_2B_2')_\theta - E(A_2'A_2; B_2')_\kappa \qquad (2.31)$$

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 $\rho_{A_1'A_1B_1'}$ and $\kappa_{A_2'A_2B_2'}$, 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 ω_{RB} shared between the sender A and receiver B. More generally, a channel $\mathcal{N}_{A \to B}$ with input system A and output system B is defined to be teleportation-simulable with associated resource state ω_{RB} if the following equality holds for all input states ρ_A [HHH99, Eq.(11)]:

$$\mathcal{N}_{A \to B}(\rho_A) = \mathcal{L}_{ARB \to B}(\rho_A \otimes \omega_{RB}), \qquad (2.32)$$

where $\mathcal{L}_{ARB \to B}$ is a quantum channel consisting of LOCC between the sender, who has systems A and R, and the receiver, who has system B ($\mathcal{L}_{ARB \to B}$ 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 $\mathcal{N}_{A \to B}$ is teleportation-simulable with associated state ω_{RB}, then the following bound holds*

$$E_{AS}(\mathcal{N}) \leq E_S(R; B)_\omega, \tag{2.33}$$

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

$$\mathcal{N}_{A \to B}(\rho_A) = \mathcal{L}_{ARB \to B}(\rho_A \otimes \omega_{RB}), \tag{2.34}$$

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

$$E_S(A'; BB')_{\mathcal{L}(\rho \otimes \omega)} - E_S(A'A; B')_\rho \leq E_S(A'AR; B'B)_{\rho \otimes \omega} - E_S(A'A; B')_\rho \tag{2.35}$$

$$\leq E_S(A'A; B')_\rho + E_S(R; B)_\omega - E_S(A'A; B')_\rho \tag{2.36}$$

$$= E_S(R; B)_\omega. \tag{2.37}$$

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 $\mathcal{N}_{A \to B}$ 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 Φ 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 $\mathcal{N}_{A \to B}$ is teleportation-simulable with associated state $\omega_{RB} = \mathcal{N}_{A \to B}(\rho_{RA})$ for some input state ρ_{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 $\rho_{A'B'A} = \rho_{RA}$, with the identification $A' \leftrightarrow R$ and $B' \leftrightarrow \emptyset$ (i.e., B' is a trivial system), and then we find that

$$E_{AS}(\mathcal{N}) = \sup_{\rho_{A'AB'}} E_S(A'; BB')_\theta - E_S(A'A; B')_\rho \geq E_S(R; B)_\omega. \tag{2.41}$$

This concludes the proof. ∎

Remark 11 *For several channels with sufficient symmetry, such as covariant channels, one can pick the input state ρ_{RA} in Proposition 10 to be the maximally entangled state Φ_{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 $\mathcal{N}_{A \to B}$ and $\mathcal{M}_{A \to B}$ is defined as [Kit97]

$$\|\mathcal{N}_{A \to B} - \mathcal{M}_{A \to B}\|_\Diamond = \sup_{\rho_{RA}} \|[\mathrm{id}_R \otimes (\mathcal{N}_{A \to B} - \mathcal{M}_{A \to B})](\rho_{RA})\|_1 \tag{2.42}$$

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

with $\|X\|_1 = \mathrm{Tr}\{\sqrt{X^\dagger X}\}$ and the second equality, with an optimization restricted to pure states ψ_{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

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

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

$$E_A(\rho, \mathcal{N}) \equiv E(A'; BB')_{\theta^{\mathcal{N}}} - E(A'A; B')_\rho, \tag{2.46}$$

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

$$\left| E_A(\rho, \mathcal{N}) - E_A(\rho, \mathcal{M}) \right| = \left| E(A'; BB')_{\theta^{\mathcal{N}}} - E(A'; BB')_{\theta^{\mathcal{M}}} \right|, \tag{2.47}$$

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

$$\left| E_A(\rho, \mathcal{N}) - E_A(\rho, \mathcal{M}) \right| \le 2\varepsilon \log_2 |B| + g(\varepsilon). \tag{2.48}$$

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

$$\frac{1}{2} \left\| \theta^{\mathcal{N}}_{A'BB'} - \theta^{\mathcal{M}}_{A'BB'} \right\|_1 \equiv \varepsilon_0 \le \varepsilon. \tag{2.49}$$

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

$$\Omega_{A'BB'} = \frac{\left[\theta^{\mathcal{N}}_{A'BB'} - \theta^{\mathcal{M}}_{A'BB'} \right]_+}{\text{Tr}\{ \left[\theta^{\mathcal{N}}_{A'BB'} - \theta^{\mathcal{M}}_{A'BB'} \right]_+ \}} = \frac{1}{\varepsilon_0} \left[\theta^{\mathcal{N}}_{A'BB'} - \theta^{\mathcal{M}}_{A'BB'} \right]_+, \tag{2.50}$$

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

$$\theta^{\mathcal{N}}_{A'BB'} = \theta^{\mathcal{N}}_{A'BB'} - \theta^{\mathcal{M}}_{A'BB'} + \theta^{\mathcal{M}}_{A'BB'} \tag{2.51}$$

$$\le \left[\theta^{\mathcal{N}}_{A'BB'} - \theta^{\mathcal{M}}_{A'BB'} \right]_+ + \theta^{\mathcal{M}}_{A'BB'} \tag{2.52}$$

$$= (1 + \varepsilon_0) \left(\frac{1}{1 + \varepsilon_0} \left[\theta^{\mathcal{N}}_{A'BB'} - \theta^{\mathcal{M}}_{A'BB'} \right]_+ + \frac{1}{1 + \varepsilon_0} \theta^{\mathcal{M}}_{A'BB'} \right) \tag{2.53}$$

$$= (1 + \varepsilon_0) \left(\frac{\varepsilon_0}{1 + \varepsilon_0} \Omega_{A'BB'} + \frac{1}{1 + \varepsilon_0} \theta^{\mathcal{M}}_{A'BB'} \right), \tag{2.54}$$

we can define

$$\xi_{A'BB'} \equiv \frac{\varepsilon_0}{1 + \varepsilon_0} \Omega_{A'BB'} + \frac{1}{1 + \varepsilon_0} \theta^{\mathcal{M}}_{A'BB'}, \tag{2.55}$$

and it follows that

$$\xi_{A'BB'} = \frac{\varepsilon_0}{1 + \varepsilon_0} \Omega'_{A'BB'} + \frac{1}{1 + \varepsilon_0} \theta^{\mathcal{N}}_{A'BB'}, \tag{2.56}$$

where the state $\Omega'_{A'BB'}$ is defined as

$$\Omega'_{A'BB'} \equiv \frac{1}{\varepsilon_0} \left[(1 + \varepsilon_0) \xi_{A'BB'} - \theta^{\mathcal{N}}_{A'BB'} \right]. \tag{2.57}$$

Consider that

$$\Omega_{A'B'} = \Omega'_{A'B'} \tag{2.58}$$

11

because

$$\mathrm{Tr}_B\left\{\frac{\varepsilon_0}{1+\varepsilon_0}\Omega_{A'BB'} + \frac{1}{1+\varepsilon_0}\theta^{\mathcal{M}}_{A'BB'}\right\} = \frac{\varepsilon_0}{1+\varepsilon_0}\Omega_{A'B'} + \frac{1}{1+\varepsilon_0}\theta^{\mathcal{M}}_{A'B'} \tag{2.59}$$

$$= \frac{\varepsilon_0}{1+\varepsilon_0}\Omega_{A'B'} + \frac{1}{1+\varepsilon_0}\rho_{A'B'}, \tag{2.60}$$

$$\mathrm{Tr}_B\left\{\frac{\varepsilon_0}{1+\varepsilon_0}\Omega'_{A'BB'} + \frac{1}{1+\varepsilon_0}\theta^{\mathcal{N}}_{A'BB'}\right\} = \frac{\varepsilon_0}{1+\varepsilon_0}\Omega'_{A'B'} + \frac{1}{1+\varepsilon_0}\theta^{\mathcal{N}}_{A'B'} \tag{2.61}$$

$$= \frac{\varepsilon_0}{1+\varepsilon_0}\Omega'_{A'B'} + \frac{1}{1+\varepsilon_0}\rho_{A'B'}, \tag{2.62}$$

and so

$$\frac{\varepsilon_0}{1+\varepsilon_0}\Omega_{A'B'} + \frac{1}{1+\varepsilon_0}\rho_{A'B'} = \frac{\varepsilon_0}{1+\varepsilon_0}\Omega'_{A'B'} + \frac{1}{1+\varepsilon_0}\rho_{A'B'}, \tag{2.63}$$

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

$$E(A';BB')_\xi \leq \frac{1}{1+\varepsilon_0}E(A';BB')_{\theta^{\mathcal{M}}} + \frac{\varepsilon_0}{1+\varepsilon_0}E(A';BB')_\Omega, \tag{2.64}$$

and from Lemma 25, we have that

$$\frac{1}{1+\varepsilon_0}E(A';BB')_{\theta^{\mathcal{N}}} + \frac{\varepsilon_0}{1+\varepsilon_0}E(A';BB')_{\Omega'} \leq E(A';BB')_\xi + h_2\left(\frac{\varepsilon_0}{1+\varepsilon_0}\right), \tag{2.65}$$

So this means that

$$E(A';BB')_{\theta^{\mathcal{N}}} \leq (1+\varepsilon_0)\,E(A';BB')_\xi + (1+\varepsilon_0)\,h_2\left(\frac{\varepsilon_0}{1+\varepsilon_0}\right) - \varepsilon_0 E(A';BB')_{\Omega'} \tag{2.66}$$

$$\leq E(A';BB')_{\theta^{\mathcal{M}}} + \varepsilon_0 E(A';BB')_\Omega + g(\varepsilon_0) - \varepsilon_0 E(A';BB')_{\Omega'} \tag{2.67}$$

$$= E(A';BB')_{\theta^{\mathcal{M}}} + g(\varepsilon_0) + \varepsilon_0\left[E(A';BB')_\Omega - E(A';BB')_{\Omega'}\right], \tag{2.68}$$

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

$$E(A';BB')_\Omega - E(A';BB')_{\Omega'} \leq 2\log_2|B| + E(A';B')_\Omega - E(A';B')_{\Omega'} \tag{2.69}$$

$$= 2\log_2|B|. \tag{2.70}$$

The first inequality follows from Lemma 23, the LOCC monotonicity of relative entropy of entanglement and the Rains relative entropy, and (2.58). So this implies that

$$E(A';BB')_{\theta^{\mathcal{N}}} - E(A';BB')_{\theta^{\mathcal{M}}} \leq g(\varepsilon_0) + 2\varepsilon_0\log_2|B| \tag{2.71}$$

$$\leq g(\varepsilon) + 2\varepsilon\log_2|B|, \tag{2.72}$$

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

$$E(A';BB')_{\theta^{\mathcal{M}}} - E(A';BB')_{\theta^{\mathcal{N}}} \leq g(\varepsilon) + 2\varepsilon\log_2|B| \tag{2.73}$$

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

$$E_A(\rho, \mathcal{N}) \leq \sup_\rho E_A(\rho, \mathcal{M}) + 2\varepsilon \log_2 |B| + g(\varepsilon) \tag{2.74}$$

$$= E_A(\mathcal{M}) + 2\varepsilon \log_2 |B| + g(\varepsilon). \tag{2.75}$$

Since the bound holds for all input states $\rho_{A'B'A}$, we can conclude that

$$E_A(\mathcal{N}) \leq E_A(\mathcal{M}) + 2\varepsilon \log_2 |B| + g(\varepsilon). \tag{2.76}$$

In a similar way, we obtain the opposite inequality

$$E_A(\mathcal{M}) \leq E_A(\mathcal{N}) + 2\varepsilon \log_2 |B| + g(\varepsilon), \tag{2.77}$$

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 [HHHO05b, 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 $\mathcal{N}_{A\to B}$. They begin by performing an LOCC channel $\mathcal{L}^{(1)}_{\emptyset \to A'_1 A_1 B'_1}$, which leads to a separable state $\rho^{(1)}_{A'_1 A_1 B'_1}$, 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 $\sigma^{(1)}_{A'_1 B_1 B'_1} \equiv \mathcal{N}_{A_1 \to B_1}(\rho^{(1)}_{A'_1 A_1 B'_1})$. They then perform the LOCC channel $\mathcal{L}^{(2)}_{A'_1 B_1 B'_1 \to A'_2 A_2 B'_2}$, which leads to the state

$$\rho^{(2)}_{A'_2 A_2 B'_2} \equiv \mathcal{L}^{(2)}_{A'_1 B_1 B'_1 \to A'_2 A_2 B'_2}(\sigma^{(1)}_{A'_1 B_1 B'_1}). \tag{3.1}$$

Alice feeds in the system A_2 to the second channel use $\mathcal{N}_{A_2 \to B_2}$, leading to the state $\sigma^{(2)}_{A'_2 B_2 B'_2} \equiv \mathcal{N}_{A_2 \to B_2}(\rho^{(1)}_{A'_2 A_2 B'_2})$. This process continues: the protocol uses the channel n times. In general, we have the following states for all $i \in \{2, \ldots, n\}$:

$$\rho^{(i)}_{A'_i A_i B'_i} \equiv \mathcal{L}^{(i)}_{A'_{i-1} B_{i-1} B'_{i-1} \to A'_i A_i B'_i}(\sigma^{(i-1)}_{A'_{i-1} B_{i-1} B'_{i-1}}), \tag{3.2}$$

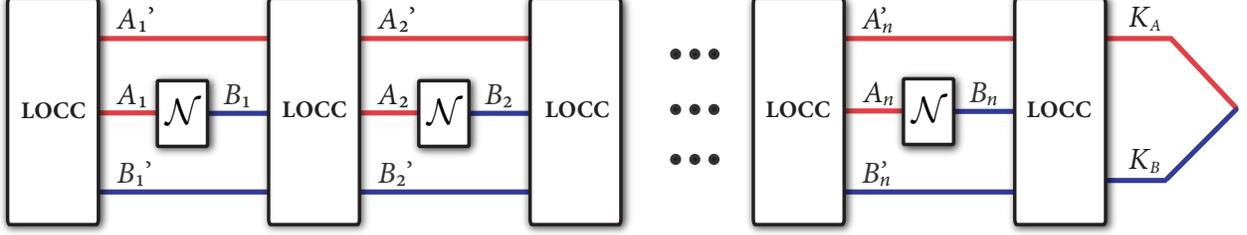$$\sigma^{(i)}_{A'_i B_i B'_i} \equiv \mathcal{N}_{A_i \to B_i}(\rho^{(i)}_{A'_i A_i B'_i}), \tag{3.3}$$

13

Figure 2: A protocol for secret key agreement over a quantum channel.

where $\mathcal{L}^{(i)}_{A'_{i-1}B_{i-1}B'_{i-1} \to A'_i A_i B'_i}$ is an LOCC channel. The final step of the protocol consists of an LOCC channel $\mathcal{L}^{(n+1)}_{A'_n B_n B'_n \to K_A K_B}$, 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:

$$\omega_{K_A K_B} \equiv \mathcal{L}^{(n+1)}_{A'_n B_n B'_n \to K_A K_B}(\sigma^{(n)}_{A'_n B_n B'_n}). \tag{3.4}$$

The goal of the protocol is that the final state $\omega_{K_A K_B}$ 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 $\rho^{(1)}_{A'_1 A_1 B'_1}$ is a separable state of the following form:

$$\rho^{(1)}_{A'_1 A_1 B'_1} \equiv \sum_{y_1} p_{Y_1}(y_1) \tau^{y_1}_{A'_1 A_1} \otimes \zeta^{y_1}_{B_1}. \tag{3.5}$$

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:

$$|\psi^{(1)}\rangle_{A'_1 A_1 S_{A_1} B'_1 S_{B_1} Y_1} \equiv \sum_{y_1} \sqrt{p_{Y_1}(y_1)} |\tau^{y_1}\rangle_{A'_1 A_1 S_{A_1}} \otimes |\zeta^{y_1}\rangle_{B_1 S_{B_1}} \otimes |y_1\rangle_{Y_1}, \tag{3.6}$$

where S_{A_1} and S_{B_1} are local "shield" systems that in principle could be held by Alice and Bob, respectively, $|\tau^{y_1}\rangle_{A'_1 A_1 S_{A_1}}$ and $|\zeta^{y_1}\rangle_{B_1 S_{B_1}}$ purify $\tau^{y_1}_{A'_1 A_1}$ and $\zeta^{y_1}_{B_1}$, respectively, and Eve possesses system Y_1, which contains a coherent classical copy of the classical data exchanged. Each LOCC channel $\mathcal{L}^{(i)}_{A'_{i-1}B_{i-1}B'_{i-1} \to A'_i A_i B'_i}$ can be written in the following form [Wat15], for all $i \in \{2, \ldots, n\}$:

$$\mathcal{L}^{(i)}_{A'_{i-1}B_{i-1}B'_{i-1} \to A'_i A_i B'_i} \equiv \sum_{y_i} \mathcal{E}^{y_i}_{A'_{i-1} \to A'_i A_i} \otimes \mathcal{F}^{y_i}_{B_{i-1}B'_{i-1} \to B'_i}, \tag{3.7}$$

where $\{\mathcal{E}^{y_i}_{A'_{i-1} \to A'_i A_i}\}_{y_i}$ and $\{\mathcal{F}^{y_i}_{B_{i-1}B'_{i-1} \to B'_i}\}_{y_i}$ 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:

$$U^{\mathcal{L}^{(i)}}_{A'_{i-1}B_{i-1}B'_{i-1} \to A'_i A_i S_{A_i} B'_i S_{B_i} Y_i} \equiv \sum_{y_i} U^{\mathcal{E}^{y_i}}_{A'_{i-1} \to A'_i A_i S_{A_i}} \otimes U^{\mathcal{F}^{y_i}}_{B_{i-1}B'_{i-1} \to B'_i S_{B_i}} \otimes |y_i\rangle_{Y_i}, \tag{3.8}$$

14

where $\{U^{\mathcal{E}^{y_i}}_{A'_{i-1} \to A'_i A_i S_{A_i}}\}_{y_i}$ and $\{U^{\mathcal{F}^{y_i}}_{B_{i-1} B'_{i-1} \to B'_i S_{B_i}}\}_{y_i}$ are collections of linear operators (each of which is a contraction, i.e., $\left\| U^{\mathcal{E}^{y_i}}_{A'_{i-1} \to A'_i A_i S_{A_i}} \right\|_\infty, \left\| U^{\mathcal{F}^{y_i}}_{B_{i-1} B'_{i-1} \to B'_i S_{B_i}} \right\|_\infty \leq 1$) 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

$$\mathcal{L}^{(n+1)}_{A'_n B_n B'_n \to K_A K_B} \equiv \sum_{y_{n+1}} \mathcal{E}^{y_{n+1}}_{A'_n \to K_A} \otimes \mathcal{F}^{y_{n+1}}_{B_n B'_n \to K_B}, \tag{3.9}$$

and it can be purified to an isometry similarly as

$$U^{\mathcal{L}^{(n+1)}}_{A'_n B_n B'_n \to K_A S_{A_{n+1}} K_B S_{B_{n+1}}} \equiv \sum_{y_{n+1}} U^{\mathcal{E}^{y_{n+1}}}_{A'_n \to K_A S_{A_{n+1}}} \otimes U^{\mathcal{F}^{y_{n+1}}}_{B_n B'_n \to K_B S_{B_{n+1}}} \otimes |y_{n+1}\rangle_{Y_{n+1}}. \tag{3.10}$$

Furthermore, each channel use $\mathcal{N}_{A_i \to B_i}$, for all $i \in \{1, \dots, n\}$ is purified by an isometry $U^{\mathcal{N}}_{A_i \to B_i E_i}$, 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_A 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 $|\omega\rangle_{K_A S_A K_B S_B E^n Y^{n+1}}$. Fix $n, K \in \mathbb{N}$ and $\varepsilon \in [0, 1]$. The original protocol is an (n, K, ε) protocol if

$$F(\omega_{K_A K_B E^n Y^{n+1}}, \overline{\Phi}_{K_A K_B} \otimes \xi_{E^n Y^{n+1}}) \geq 1 - \varepsilon, \tag{3.11}$$

where the fidelity $F(\tau, \kappa) \equiv \|\sqrt{\tau}\sqrt{\kappa}\|_1^2$ [Uhl76], the maximally correlated state $\overline{\Phi}_{K_A K_B}$ is defined as

$$\overline{\Phi}_{K_A K_B} \equiv \frac{1}{K} \sum_{k=1}^{K} |k\rangle\langle k|_{K_A} \otimes |k\rangle\langle k|_{K_B}, \tag{3.12}$$

and $\xi_{E^n Y^{n+1}}$ 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

$$F(\omega_{K_A S_A K_B S_B}, \gamma_{K_A S_A K_B S_B}) \geq 1 - \varepsilon, \tag{3.13}$$

where $\gamma_{K_A S_A K_B S_B}$ is a private state [HHHO05b, HHHO09] of the following form:

$$U_{K_A S_A K_B S_B}(\Phi_{K_A K_B} \otimes \theta_{S_A S_B}) U^\dagger_{K_A S_A K_B S_B}, \tag{3.14}$$

with $U_{K_A S_A K_B S_B}$ a twisting unitary of the form $U_{K_A S_A K_B S_B} = \sum_{i,j=1}^{K} |i\rangle\langle i|_{K_A} \otimes |j\rangle\langle j|_{K_B} \otimes U^{ij}_{S_A S_B}$, $\Phi_{K_A K_B}$ is a maximally entangled state of the form

$$\Phi_{K_A K_B} \equiv \frac{1}{K} \sum_{i,j=1}^{K} |i\rangle\langle j|_{K_A} \otimes |i\rangle\langle j|_{K_B}, \tag{3.15}$$

15

and $\theta_{S_A S_B}$ 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 $(n, 2^{n(R-\delta)}, \varepsilon)$ protocol. The secret-key-agreement capacity of $\mathcal{N}_{A \to B}$, denoted as $P^{\leftrightarrow}(\mathcal{N}_{A \to B})$, 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 ω_{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, ε) secret-key-agreement protocol conducted over a quantum channel $\mathcal{N}$:*

$$(1 - \varepsilon) \frac{\log_2 K}{n} \leq E_{AR}(\mathcal{N}) + \frac{1}{n} h_2(\varepsilon), \tag{3.16}$$

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, ε) 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$^+$08a, HHH$^+$08b]), which untwists the twisting unitary of the ideal target private state and projects onto the maximally entangled state of the key systems (cf., Section 3.3). Let F^* denote the probability of the actual state $\omega_{K_A S_A K_B S_B}$ 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 $\sigma_{K_A S_A K_B S_B}$ of systems $K_A S_A K_B S_B$ 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

$$-h_2(\varepsilon) + (1-\varepsilon)\log_2 K \leq D(\{1-\varepsilon, \varepsilon\}\|\{1/K, 1-1/K\}) \tag{3.17}$$

$$\leq D(\{F^*, 1-F^*\}\|\{p_{\text{SEP}}, 1-p_{\text{SEP}}\}) \tag{3.18}$$

$$\leq D(\omega_{K_A S_A K_B S_B}\|\sigma_{K_A S_A K_B S_B}). \tag{3.19}$$

The first inequality follows because

$$D(\{1-\varepsilon, \varepsilon\}\|\{1/K, 1-1/K\}) = (1-\varepsilon)\log_2\left(\frac{1-\varepsilon}{1/K}\right) + \varepsilon\log_2\left(\frac{\varepsilon}{1-1/K}\right) \tag{3.20}$$

$$= -h_2(\varepsilon) + (1-\varepsilon)\log_2 K + \varepsilon\log_2\left(\frac{K}{K-1}\right) \tag{3.21}$$

$$\geq -h_2(\varepsilon) + (1-\varepsilon)\log_2 K. \tag{3.22}$$

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 $\{p_{\text{SEP}}, 1-p_{\text{SEP}}\}$ are more distinguishable than the distributions $\{1-\varepsilon, \varepsilon\}$ and $\{1/K, 1-1/K\}$, due to the conditions $F^* \geq 1-\varepsilon$ and $p_{\text{SEP}} \leq 1/K$ (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 $\sigma_{K_A S_A K_B S_B}$, we find that

$$-h_2(\varepsilon) + (1-\varepsilon)\log_2 K \leq E_R(K_A S_A; K_B S_B)_\omega, \tag{3.23}$$

which can be rewritten as[1]

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

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

$$E_R(K_A S_A; K_B S_B)_\omega \leq E_R(A'_n; B_n B'_n)_{\sigma^{(n)}} \tag{3.25}$$

$$= E_R(A'_n; B_n B'_n)_{\sigma^{(n)}} - E_R(A'_1 A_1; B'_1)_{\rho^{(1)}} \tag{3.26}$$

$$= E_R(A'_n; B_n B'_n)_{\sigma^{(n)}} + \left[\sum_{i=2}^{n} E_R(A'_i A_i; B'_i)_{\rho^{(i)}} - E_R(A'_i A_i; B'_i)_{\rho^{(i)}}\right]$$

$$- E_R(A'_1 A_1; B'_1)_{\rho^{(1)}} \tag{3.27}$$

$$\leq \sum_{i=1}^{n} E_R(A'_i; B_i B'_i)_{\sigma^{(i)}} - E_R(A'_i A_i; B'_i)_{\rho^{(i)}} \tag{3.28}$$

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

---

[1]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 ε-relative entropy of entanglement [BD11] as an intermediary step to get that $\log_2 K \leq E_R^\varepsilon(K_A S_A; K_B S_B)_\omega \leq \frac{1}{1-\varepsilon}[E_R(K_A S_A; K_B S_B)_\omega + h_2(\varepsilon)]$, with the first bound following from [WTB17, Theorem 11] and the second from [WR12, MW14, KW17].

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 $E_R(A'_i A_i; B'_i)_{\rho^{(i)}} \leq E_R(A'_{i-1}; B_{i-1} B'_{i-1})_{\sigma^{(i-1)}}$ 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 $E_R(A'_n; B_n B'_n)_{\sigma^{(i)}} - E_R(A'_i A_i; B'_i)_{\rho^{(i)}}$ 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 $P^{\leftrightarrow}(\mathcal{N}_{A \to B})$ of a quantum channel $\mathcal{N}_{A \to B}$ cannot exceed its amortized relative entropy of entanglement:*

$$P^{\leftrightarrow}(\mathcal{N}) \leq E_{AR}(\mathcal{N}). \tag{3.30}$$

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

$$\frac{\alpha}{\alpha - 1} \log_2(1 - \varepsilon) \leq n \widetilde{E}^\alpha_{AR}(\mathcal{N}) - \log_2 K, \tag{3.31}$$

where

$$\widetilde{E}^\alpha_{AR}(\mathcal{N}) = \sup_{\rho_{A'AB'}} \widetilde{E}^\alpha_R(A'; BB')_\omega - \widetilde{E}^\alpha_R(A'A; B')_\rho, \tag{3.32}$$

and $\widetilde{E}^\alpha_R$ denotes the sandwiched Rényi relative entropy of entanglement [WTB17], defined from the sandwiched Rényi relative entropy [MLDS+13, WWY14]. One of the main results of [CMH17] is the bound $\widetilde{E}^\alpha_{AR}(\mathcal{N}) \leq E_{\max}(\mathcal{N})$, where $E_{\max}(\mathcal{N})$ denotes the channel's max-relative entropy of entanglement (cf., [Dat09]). The authors of [CMH17] observed that this latter bound in turn implies the following bound for all $\alpha > 1$:

$$\frac{\alpha}{\alpha - 1} \log_2(1 - \varepsilon) \leq n E_{\max}(\mathcal{N}) - \log_2 K. \tag{3.33}$$

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 $T_{B'} \circ \mathcal{N}_{AB \to A'B'} \circ T_B$ 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 $\rho \to \sum_{i,j} |i\rangle\langle j|\rho|i\rangle\langle j|$. 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 PPT′ 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

$$R(A;B)_\rho \geq R(A';B')_{\mathcal{P}(\rho)}, \tag{4.1}$$

where ρ_{AB} is a bipartite state and $\mathcal{P}_{AB \to A'B'}$ 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 (ω-PPT-simulable channel) *A channel $\mathcal{N}_{A \to B}$ with input system A and output system B is defined to be PPT-simulable with associated resource state ω_{RB} (ω-PPT-simulable for short) if the following equality holds for all input states ρ_A:*

$$\mathcal{N}_{A \to B}(\rho_A) = \mathcal{P}_{ARB \to B}(\rho_A \otimes \omega_{RB}), \tag{4.2}$$

where $\mathcal{P}_{ARB \to B}$ 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 ω_{RB} is PPT-simulable with associated resource state ω_{RB}.

4.2 Protocols for PPT-assisted quantum communication and their performance

The structure of an (n, M, ε) protocol for PPT-assisted quantum communication is quite similar to that for an (n, K, ε) 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 $\omega_{M_A M_B}$ instead of $\omega_{K_A K_B}$. Fixing $n, M \in \mathbb{N}$ and $\varepsilon \in [0, 1]$, the protocol is an (n, M, ε) PPT-assisted quantum communication protocol if

$$F(\omega_{M_A M_B}, \Phi_{M_A M_B}) \geq 1 - \varepsilon, \tag{4.3}$$

where the maximally entangled state $\Phi_{M_A M_B}$ 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 $(n, 2^{n(R-\delta)}, \varepsilon)$ protocol. The PPT-assisted quantum capacity of $\mathcal{N}_{A \to B}$, denoted as $Q^{\mathbf{PPT}, \leftrightarrow}(\mathcal{N}_{A \to B})$, 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 $Q^{\leftrightarrow}(\mathcal{N}_{A \to B})$. It then immediately follows that

$$Q^{\leftrightarrow}(\mathcal{N}_{A \to B}) \leq Q^{\mathbf{PPT}, \leftrightarrow}(\mathcal{N}_{A \to B}) \tag{4.4}$$

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

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

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 ω-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 ω_{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, ε) protocol and the fidelity, the probability for the final state $\omega_{M_A M_B}$ of the protocol to pass this test is larger than $1 - \varepsilon$. Furthermore, due to [Rai99, Lemma 2], the bound $\text{Tr}\{\Phi_{M_A M_B} \sigma_{M_A M_B}\} \leq 1/M$ holds for all states $\sigma_{M_A M_B} \in \text{PPT}'(M_A : M_B)$. 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, ε) PPT-assisted quantum communication protocol conducted over a quantum channel $\mathcal{N}$:*

$$(1 - \varepsilon)\frac{\log_2 M}{n} \leq R_A(\mathcal{N}) + \frac{1}{n}h_2(\varepsilon), \tag{4.6}$$

where $R_A(\mathcal{N})$ denotes the amortized Rains relative entropy from Definition 3.

Taking the limit in Proposition 17 as $n \rightarrow \infty$ and then as $\varepsilon \rightarrow 0$ leads to the following asymptotic statement:

Theorem 18 *The PPT-assisted quantum capacity $Q^{\mathbf{PPT},\leftrightarrow}(\mathcal{N}_{A \rightarrow B})$ of a quantum channel $\mathcal{N}_{A \rightarrow B}$ cannot exceed its amortized Rains relative entropy:*

$$Q^{\mathbf{PPT},\leftrightarrow}(\mathcal{N}) \leq R_A(\mathcal{N}). \tag{4.7}$$

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 $\mathcal{N}_{A \to B}$ is ε-approximately teleportation-simulable with associated resource state ω_{RB} if there exists a channel $\mathcal{M}_{A \to B}$ that is exactly teleportation-simulable with associated resource state ω_{RB} such that*

$$\frac{1}{2} \left\| \mathcal{N}_{A \to B} - \mathcal{M}_{A \to B} \right\|_{\diamond} \leq \varepsilon. \tag{5.1}$$

For short, we say that $\mathcal{N}_{A \to B}$ is $(\varepsilon, \omega_{RB})$-approximately teleportation-simulable. The same definition applies for an $(\varepsilon, \omega_{RB})$-approximately PPT-simulable channel, but the difference is that $\mathcal{M}_{A \to B}$ is exactly PPT-simulable with associated resource state ω_{RB}. Also, if a channel is $(\varepsilon, \omega_{RB})$-approximately teleportation-simulable, then it is $(\varepsilon, \omega_{RB})$-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, Theorem 12, and Theorem 14, and it constitutes one of the main results of our paper:

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

$$P^{\leftrightarrow}(\mathcal{N}_{A \to B}) \leq E_R(R; B)_{\omega} + 2\varepsilon \log_2 |B| + g(\varepsilon). \tag{5.2}$$

Similarly, the following theorem is an immediate consequence of Proposition 8, Theorem 12, and Theorem 18:

Theorem 21 *If a channel $\mathcal{N}_{A \to B}$ is $(\varepsilon, \omega_{RB})$-approximately PPT-simulable, then its PPT-assisted quantum capacity $Q^{\mathbf{PPT}, \leftrightarrow}(\mathcal{N}_{A \to B})$ is bounded from above as*

$$Q^{\mathbf{PPT}, \leftrightarrow}(\mathcal{N}_{A \to B}) \leq R(R; B)_{\omega} + 2\varepsilon \log_2 |B| + g(\varepsilon). \tag{5.3}$$

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:

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

where $p \in [0, 1]$ and ρ 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

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

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

$$K_2 = \sqrt{p}|0\rangle\langle 1|. \tag{6.4}$$

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

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

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 $\Phi(\mathcal{D}_p)$, 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 $(p^2/2, \Phi(\overline{\mathcal{N}}_p))$-approximately teleportation-simulable, where $\overline{\mathcal{N}}_p$ denotes the following teleportation-simulable channel:

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

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 $Q^{\mathbf{PPT},\leftrightarrow}(\mathcal{N}_p)$:

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

$$Q^{\mathbf{PPT},\leftrightarrow}(\mathcal{N}_p) \leq R(A;B)_{\Phi(\overline{\mathcal{N}}_p)} + p^2 + g(p^2/2). \tag{6.8}$$

By noting that the set PPT' contains the set of PPT states and applying the well known result that PPT states are equal to separable states for 2×2 systems [Per96, HHH96], we can conclude that

$$P^{\leftrightarrow}(\mathcal{N}_p),\ Q^{\mathbf{PPT},\leftrightarrow}(\mathcal{N}_p) \leq E_{\mathbf{PPT}}(A;B)_{\Phi(\overline{\mathcal{N}}_p)} + p^2 + g(p^2/2), \tag{6.9}$$

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

The upper bound in (6.9) is plotted in Figure 3. To calculate $E_{\mathbf{PPT}}(A;B)_{\Phi(\overline{\mathcal{N}}_p)}$, 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 $P^{\leftrightarrow}(\mathcal{N}_p)$ and $Q^{\mathbf{PPT},\leftrightarrow}(\mathcal{N}_p)$ 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 $\mathcal{N}_{A\to B}$ as the following optimization:

$$-H_{\mathrm{CB}}(\mathcal{N}) = \sup_{\rho} H(B|E)_{\mathcal{U}^{\mathcal{N}}(\rho)}, \tag{6.10}$$

where $\mathcal{U}^{\mathcal{N}}_{A\to BE}$ denotes an isometric channel that extends $\mathcal{N}_{A\to B}$. Due to the concavity of conditional entropy [LR73b, LR73a], it immediately follows that $H(B|E)_{\mathcal{U}^{\mathcal{N}}(\rho)}$ is concave with respect to the input density operator ρ, and thus the calculation of $-H_{\mathrm{CB}}(\mathcal{N})$ is a concave optimization problem.
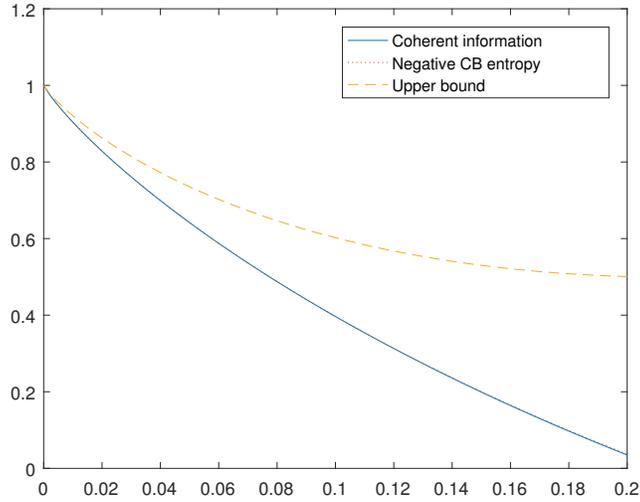
Figure 3: Upper and lower bounds on the secret-key-agreement capacity $P^{\leftrightarrow}(\mathcal{N}_p)$ and the PPT-assisted quantum capacity $Q^{\mathbf{PPT},\leftrightarrow}(\mathcal{N}_p)$ of the channel defined in (6.1). The vertical axis represents rate in either private bits or qubits per channel use. The horizontal axis represents the value of the channel parameter p.

For our example, we can further simplify the calculation of $-H_{\mathrm{CB}}(\mathcal{N}_p)$ by exploiting the symmetry of $\mathcal{N}_p$. 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

$$\mathcal{A}_p(U\rho U^\dagger) = U\mathcal{A}_p(\rho)U^\dagger, \qquad \mathcal{D}_p(U\rho U^\dagger) = U\mathcal{D}_p(\rho)U^\dagger, \tag{6.11}$$

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

$$\mathcal{U}^{\mathcal{N}_p}(Z\rho Z) = (Z \otimes \bar{Z})\mathcal{U}^{\mathcal{N}_p}(\rho)(Z \otimes \bar{Z}), \tag{6.12}$$

where $\mathcal{U}^{\mathcal{N}_p}$ is an isometric channel that extends $\mathcal{N}_p$ and $\bar{Z}$ 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

$$H(B|E)_{\mathcal{U}^{\mathcal{N}_p}(\rho)} = \frac{1}{2}\left[H(B|E)_{\mathcal{U}^{\mathcal{N}_p}(\rho)} + H(B|E)_{(Z\otimes\bar{Z})\mathcal{U}^{\mathcal{N}_p}(\rho)(Z\otimes\bar{Z})} \right] \tag{6.13}$$

$$= \frac{1}{2}\left[H(B|E)_{\mathcal{U}^{\mathcal{N}_p}(\rho)} + H(B|E)_{\mathcal{U}^{\mathcal{N}_p}(Z\rho Z)} \right] \tag{6.14}$$

$$\leq H(B|E)_{\mathcal{U}^{\mathcal{N}_p}(\frac{1}{2}(\rho+Z\rho Z))}. \tag{6.15}$$

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 $\mathcal{N}_p$ to an optimization over a single parameter.
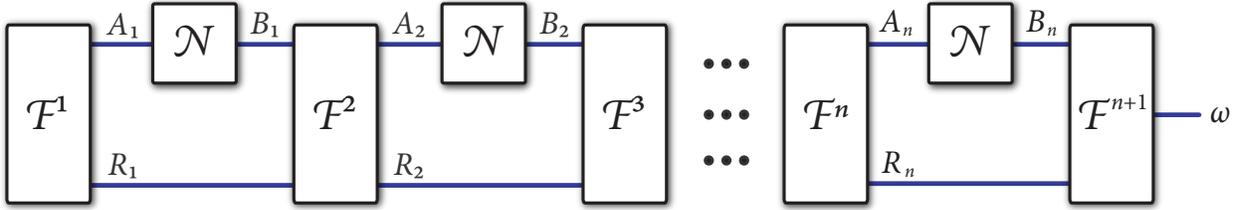
Figure 4: A protocol for extracting resourcefulness from a channel $\mathcal{N}$ by accessing it with free operations between each channel use.

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, Fri15, 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 ρ 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:

$$V_A(\mathcal{N}) = \sup_{\rho_{RA}} V((\mathrm{id}_R \otimes \mathcal{N}_{A \to B})(\rho_{RA})) - V(\rho_{RA}). \tag{7.1}$$

Suppose now that we have a protocol that accesses the channel $\mathcal{N}$ 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 ω denote the final state generated by the protocol, let $\rho_{R_i A_i}$

denote the state before the ith channel use, and let $\sigma_{R_i B_i}$ denote the state after the ith 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:

$$V(\omega) \leq V(\sigma_{R_n B_n}) \tag{7.2}$$

$$= V(\sigma_{R_n B_n}) - V(\rho_{R_1 A_1}) \tag{7.3}$$

$$= V((\mathrm{id}_R \otimes \mathcal{N}_{A_n \to B_n})(\rho_{R_n A_n})) - V(\rho_{R_1 A_1}) + \sum_{i=2}^{n} V(\rho_{R_i A_i}) - V(\rho_{R_i A_i}) \tag{7.4}$$

$$\leq V((\mathrm{id}_R \otimes \mathcal{N}_{A_n \to B_n})(\rho_{R_n A_n})) - V(\rho_{R_1 A_1})$$
$$+ \sum_{i=2}^{n} V((\mathrm{id}_R \otimes \mathcal{N}_{A_{i-1} \to B_{i-1}})(\rho_{R_{i-1} A_{i-1}})) - V(\rho_{R_i A_i}) \tag{7.5}$$

$$= \sum_{i=1}^{n} V((\mathrm{id}_R \otimes \mathcal{N}_{A_i \to B_i})(\rho_{R_i A_i})) - V(\rho_{R_i A_i}) \tag{7.6}$$

$$\leq n V_A(\mathcal{N}), \tag{7.7}$$

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 ω 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 ν-freely-simulable channels as a generalization of the teleportation-simulable channels of [BDSW96, HHH99] and the ω-PPT-simulable channels introduced in Definition 16:

Definition 22 (ν-freely-simulable channel) *A quantum channel $\mathcal{N}$ is ν-freely-simulable if there exists a resourceful state ν and a free channel $\mathcal{F}$ such that the following equality holds for all input states ρ:*

$$\mathcal{N}(\rho) = \mathcal{F}(\rho \otimes \nu). \tag{7.8}$$

For ν-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

$$V(\omega) \leq V(\nu^{\otimes n}), \tag{7.9}$$

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 ν. 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:

$$\frac{1}{n} V(\omega) \leq V(\nu). \tag{7.10}$$

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],
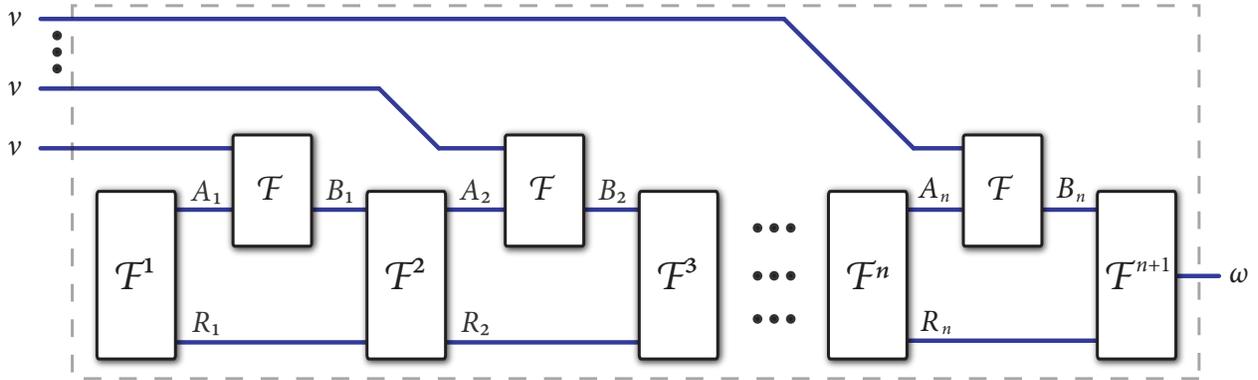
Figure 5: A protocol for extracting resourcefulness from a ν-freely simulable channel $\mathcal{N}$ by accessing it with free operations between each channel use. Any such protocol can be understood as the action of a single free channel (everything within the dotted box) acting on the resource state $\nu^{\otimes n}$.

asymmetry [MS14], or non-Gaussianity. We could certainly also consider approximately ν-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 ν-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 ν-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.

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 23 *Let E refer to either the relative entropy of entanglement or the Rains relative entropy. For ρ_{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 $\mathcal{S}$ refer to either SEP or PPT$'$. Consider that

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

$$\leq \min_{\sigma_{A:B}\in\mathcal{S}(A:B)} D(\rho_{ABC}\|\sigma_{A:B}\otimes\rho_C) \tag{A.4}$$

$$= \min_{\sigma_{A:B}\in\mathcal{S}(A:B)} [-H(ABC)_\rho - \mathrm{Tr}\{\rho_{ABC}\log_2(\sigma_{A:B}\otimes\rho_C)\}] \tag{A.5}$$

$$= \min_{\sigma_{A:B}\in\mathcal{S}(A:B)} [-H(ABC)_\rho - \mathrm{Tr}\{\rho_{ABC}\log_2(\sigma_{A:B})\} - \mathrm{Tr}\{\rho_{ABC}\log_2(\rho_C)\}] \tag{A.6}$$

$$= \min_{\sigma_{A:B}\in\mathcal{S}(A:B)} [-H(ABC)_\rho - \mathrm{Tr}\{\rho_{AB}\log_2(\sigma_{A:B})\} + H(C)_\rho] \tag{A.7}$$

$$= \min_{\sigma_{A:B}\in\mathcal{S}(A:B)} [-H(C|AB)_\rho - H(AB)_\rho - \mathrm{Tr}\{\rho_{AB}\log_2(\sigma_{A:B})\} + H(C)_\rho] \tag{A.8}$$

$$= -H(C|AB)_\rho + \min_{\sigma_{A:B}\in\mathcal{S}(A:B)} [-H(AB)_\rho - \mathrm{Tr}\{\rho_{AB}\log_2(\sigma_{A:B})\}] + H(C)_\rho \tag{A.9}$$

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

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

This concludes the proof. ∎

Lemma 24 *Let E refer to either the relative entropy of entanglement or the Rains relative entropy. For a classical–quantum state*

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

the following equality holds

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

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

$$\theta_{XAB} \equiv \sum_x p_X(x)|x\rangle\langle x|_X \otimes \sigma_{A:B}^x. \tag{A.14}$$

Then consider that

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

$$\leq D(\rho_{ABX}\|\theta_{A:BX}) \tag{A.16}$$

$$= \sum_x p_X(x)D(\rho^x_{AB}\|\sigma^x_{A:B}) \tag{A.17}$$

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

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

$$D(\rho_{ABX}\|\xi_{A:BX}) \geq D(\overline{\Delta}_X(\rho_{ABX})\|\overline{\Delta}_X(\xi_{A:BX})) \tag{A.19}$$

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

$$= \sum_x p_X(x)D(\rho^x_{AB}\|\xi^x_{A:B}) + D(p_X\|q_X) \tag{A.21}$$

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

where

$$\xi'_{A:BX} = \overline{\Delta}_X(\xi_{A:BX}) = \sum_x q_X(x)|x\rangle\langle x|_X \otimes \xi^x_{A:B}. \tag{A.23}$$

In the case that $\mathcal{S} = \mathrm{PPT}'$, 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 23 and 24 and the fact that $I(X;AB)_\rho \leq H(X)_\rho$ for a classical system X:

Lemma 25 *Let E refer to either the relative entropy of entanglement or the Rains relative entropy. Let $\{p_X(x), \rho^x_{AB}\}$ be an ensemble of states and let $\overline{\rho}_{AB} \equiv \sum_x p_X(x)\rho^x_{AB}$. Then we have that*

$$\sum_x p_X(x)E(A;B)_{\rho^x} \leq E(A;B)_{\overline{\rho}} + I(X;AB)_\rho \tag{A.24}$$

$$\leq E(A;B)_{\overline{\rho}} + H(X), \tag{A.25}$$

where $H(X)$ is the Shannon entropy of the distribution p_X.

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 $\mathcal{N}_{A \to B}$ is *covariant with respect to* $\{(U_A^g, V_B^g)\}_{g \in G}$ [Hol02], if

$$V_B^g \mathcal{N}(\cdot) V_B^{g\dagger} = \mathcal{N}(U_A^g(\cdot)U_A^{g\dagger}) \qquad \text{for all } g \in G.$$

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

$$\frac{1}{|G|} \sum_{g \in G} U_A^g \rho_A U_A^{g\dagger} = \pi_A \qquad \text{for all states } \rho_A,$$

where $\pi_A = \frac{1}{|A|} I_A$ 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 $\mathcal{N}_{A \to B}$, 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 $V_g^\dagger$ 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 26 *The twirled channel $\mathcal{N}_G$ can be simulated from $\mathcal{N} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ by means of a generalized teleportation protocol with a resource state equal to the Choi state $\omega_{AB} \equiv \mathcal{N}_{A'' \to B}(\Phi_{AA''})$ where $\mathcal{H}_A \simeq \mathcal{H}_{A'} \simeq \mathcal{H}_{A''}$, the POVM elements as*

$$\left\{ E_{A'A}^g \equiv \frac{|A|^2}{|G|} \left(U_{A'}^g \right)^\dagger \Phi_{A'A} U_{A'}^g \right\}_g, \tag{B.1}$$

with $\{U_A^g\}_{g \in G}$ a one-design, and teleportation correction operations given by $V_g^\dagger$ acting on the B system. That is, the following equality holds

$$\sum_g V_B^{g\dagger} \operatorname{Tr}_{AA'} \{ E_{A'A}^g (\rho_{A'} \otimes \omega_{AB}) \} V_B^g = \frac{1}{|G|} \sum_g V_B^{g\dagger} \mathcal{N}_{A \to B}(U_{A'}^g \rho_A U_{A'}^{g\dagger}) V_B^g. \tag{B.2}$$

Proof. We follow the proof of [WTB17, Appendix A] closely. Let $\mathcal{N} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ 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

$$\frac{1}{|G|} \sum_g U_A^g X_A \left(U_A^g \right)^\dagger = \operatorname{Tr}\{X_A\} \pi_A, \tag{B.3}$$

where $X_A \in \mathcal{L}(\mathcal{H}_A)$ and π denotes the maximally mixed state. (For notational convenience, we are placing the index g as a superscript.) Consider that

$$\frac{1}{|G|} \sum_g U_{A'}^g \Phi_{A'A} \left(U_{A'}^g\right)^\dagger = \pi_{A'} \otimes \pi_A, \tag{B.4}$$

where Φ 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 $\{E_{A'A}^g\}_g$, with A' a system isomorphic to A and each element $E_{A'A}^g$ defined as

$$E_{A'A}^g \equiv \frac{|A|^2}{|G|} \left(U_{A'}^g\right)^\dagger \Phi_{A'A} U_{A'}^g. \tag{B.5}$$

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

$$\sum_g V_B^{g\dagger} \operatorname{Tr}_{AA'}\{E_{A'A}^g(\rho_{A'} \otimes \omega_{AB})\} V_B^g. \tag{B.6}$$

The following analysis demonstrates that this protocol works (i.e., it simulates $\mathcal{N}_G$), by simplifying the form of the post-measurement state:

$$|G| \operatorname{Tr}_{AA'}\{E_{A'A}^g(\rho_{A'} \otimes \omega_{AB})\} = |A|^2 \operatorname{Tr}_{AA'}\{\left(U_{A'}^g\right)^\dagger |\Phi\rangle_{A'A}\langle\Phi|_{A'A} U_{A'}^g(\rho_{A'} \otimes \omega_{AB})\} \tag{B.7}$$

$$= |A|^2 \langle\Phi|_{A'A} U_{A'}^g(\rho_{A'} \otimes \omega_{AB}) \left(U_{A'}^g\right)^\dagger |\Phi\rangle_{A'A} \tag{B.8}$$

$$= |A|^2 \langle\Phi|_{A'A} U_{A'}^g \rho_{A'} \left(U_{A'}^g\right)^\dagger \otimes \mathcal{N}_{A''\to B}(\Phi_{AA''}))|\Phi\rangle_{A'A} \tag{B.9}$$

$$= |A|^2 \langle\Phi|_{A'A} \left[U_A^g \rho_A \left(U_A^g\right)^\dagger\right]^* \mathcal{N}_{A''\to B}(\Phi_{AA''})|\Phi\rangle_{A'A}. \tag{B.10}$$

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

$$\langle\Phi|_{A'A} M_{A'} = \langle\Phi|_{A'A} M_A^* \tag{B.11}$$

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

$$(\text{B.10}) = |A| \operatorname{Tr}_A \left\{ \left[U_A^g \rho_A \left(U_A^g\right)^\dagger\right]^* \mathcal{N}_{A''\to B}(\Phi_{AA''}) \right\} \tag{B.12}$$

$$= |A| \operatorname{Tr}_A \left\{ \mathcal{N}_{A''\to B}\left(\left[U_{A''}^g \rho_{A''} \left(U_{A''}^g\right)^\dagger\right]^\dagger \Phi_{AA''} \right) \right\} \tag{B.13}$$

$$= \mathcal{N}_{A''\to B}\left(\left[U_{A''}^g \rho_{A''} \left(U_{A''}^g\right)^\dagger\right]^\dagger \right) \tag{B.14}$$

$$= \mathcal{N}_{A''\to B}\left(U_{A''}^g \rho_{A''} \left(U_{A''}^g\right)^\dagger \right). \tag{B.15}$$

The first equality follows because $|A| \langle \Phi|_{A'A} (I_{A'} \otimes M_{AB}) |\Phi\rangle_{A'A} = \mathrm{Tr}_A\{M_{AB}\}$ 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:

$$\mathrm{Tr}_{AA'}\{E^g_{A'A}(\rho_{A'} \otimes \omega_{AB})\} = \frac{1}{|G|}\mathcal{N}_{A''\to B}\left(U^g_{A''}\rho_{A''}\left(U^g_{A''}\right)^\dagger\right), \tag{B.16}$$

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 27 (Approximate covariance [LKDW17]) *Fix a group G with unitary representations $g \mapsto U^g_A$ on $\mathcal{H}_A$ and $g \mapsto V^g_B$ on $\mathcal{H}_B$, respectively. For a given $\varepsilon \in [0,1]$, a channel $\mathcal{N}$ ε-covariant with respect to $\{(U^g_A, V^g_B)\}_{g\in G}$, if*

$$\frac{1}{2}\|\mathcal{N} - \mathcal{N}_G\|_\diamond \leq \varepsilon.$$

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 $(\varepsilon, \mathcal{N}(\Phi))$-approximately teleportation-simulable if it is ε-covariant, with $\{U^g_A\}_{g\in G}$ a one-design.

References

[ADMVW02] Koenraad Audenaert, Bart De Moor, Karl Gerd H. Vollbrecht, and Reinhard F. Werner. Asymptotic relative entropy of entanglement for orthogonally invariant states. *Physical Review A*, 66(3):032310, September 2002. arXiv:quant-ph/0204143.

[AML16] Koji Azuma, Akihiro Mizutani, and Hoi-Kwong Lo. Fundamental rate-loss trade-off for the quantum internet. *Nature Communications*, 7:13523, November 2016. arXiv:1601.02933.

[AMTdW00] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. *IEEE 41st Annual Symposium on Foundations of Computer Science*, pages 547–553, November 2000. arXiv:quant-ph/0003101.

[BA17] Stefan Bäuml and Koji Azuma. Fundamental limitation on quantum broadcast networks. *Quantum Science and Technology*, 2(2):024004, June 2017. arXiv:1609.03994.

[BaHO⁺13] Fernando G. S. L. Brandão, Michał Horodecki, Jonathan Oppenheim, Joseph M. Renes, and Robert W. Spekkens. Resource theory of quantum states out of thermal equilibrium. *Physical Review Letters*, 111:250404, Dec 2013.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, pages 175–179, Bangalore, India, December 1984.

[BBC+93]   Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, March 1993.

[BBP+96]   Charles H. Bennett, Gilles Brassard, Sandu Popescu, Benjamin Schumacher, John A. Smolin, and William K. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Physical Review Letters*, 76(5):722–725, January 1996. arXiv:quant-ph/9511027.

[BCY11]   Fernando G.S.L. Brandao, Matthias Christandl, and Jon Yard. Faithful squashed entanglement. *Communications in Mathematical Physics*, 306(3):805–830, September 2011. arXiv:1010.1750.

[BD11]   Fernando G. S. L. Brandao and Nilanjana Datta. One-shot rates for entanglement manipulation under non-entangling maps. *IEEE Transactions on Information Theory*, 57(3):1754–1760, March 2011. arXiv:0905.2673.

[BDGDMW17] Khaled Ben Dana, María García Díaz, Mohamed Mejatty, and Andreas Winter. Resource theory of coherence: Beyond states. *Physical Review A*, 95(6):062327, June 2017. arXiv:1704.03710.

[BDSW96]   Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824–3851, November 1996. arXiv:quant-ph/9604024.

[BG15]   Fernando G. S. L. Brandao and Gilad Gour. Reversible framework for quantum resource theories. *Physical Review Letters*, 115(7):070503, August 2015. arXiv:1502.03149.

[BHLS03]   Charles H. Bennett, Aram W. Harrow, Debbie W. Leung, and John A. Smolin. On the capacities of bipartite Hamiltonians and unitary gates. *IEEE Transactions on Information Theory*, 49(8):1895–1911, August 2003. arXiv:quant-ph/0205057.

[BK98]   Samuel L. Braunstein and H. J. Kimble. Teleportation of continuous quantum variables. *Physical Review Letters*, 80(4):869–872, January 1998.

[BSST99]   Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. Entanglement-assisted classical capacity of noisy quantum channels. *Physical Review Letters*, 83(15):3081–3084, October 1999. arXiv:quant-ph/9904023.

[BSST02]   Charles H. Bennett, Peter W. Shor, John A. Smolin, and Ashish V. Thapliyal. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. *IEEE Transactions on Information Theory*, 48(10):2637–2655, October 2002. arXiv:quant-ph/0106052.

[CDP09]   Giulio Chiribella, Giacomo Mauro DAriano, and Paolo Perinotti. Realization schemes for quantum instruments in finite dimensions. *Journal of Mathematical Physics*, 50(4):042101, April 2009. arXiv:0810.3211.

[Chr06]   Matthias Christandl. *The Structure of Bipartite Quantum States: Insights from Group Theory and Cryptography.* PhD thesis, University of Cambridge, April 2006. arXiv:quant-ph/0604183.

[CMH17]   Matthias Christandl and Alexander Müller-Hermes. Relative entropy bounds on quantum, private and repeater capacities. *Communications in Mathematical Physics*, 353(2):821–852, July 2017. arXiv:1604.03448.

[CW04]   Matthias Christandl and Andreas Winter. "Squashed entanglement": An additive entanglement measure. *Journal of Mathematical Physics*, 45(3):829–840, March 2004. arXiv:quant-ph/0308088.

[Dat09]   Nilanjana Datta. Min- and max-relative entropies and a new entanglement monotone. *IEEE Transactions on Information Theory*, 55(6):2816–2826, June 2009. arXiv:0803.2770.

[DDanM14]   Rafal Demkowicz-Dobrzański and Lorenzo Maccone. Using entanglement against noise in quantum metrology. *Physical Review Letters*, 113(25):250801, December 2014. arXiv:1407.2934.

[DJKR06]   Igor Devetak, Marius Junge, Christopher King, and Mary Beth Ruskai. Multiplicativity of completely bounded p-norms implies a new additivity result. *Communications in Mathematical Physics*, 266(1):37–63, August 2006. arXiv:quant-ph/0506196.

[dRKR15]   Lidia del Rio, Lea Kraemer, and Renato Renner. Resource theories of knowledge. November 2015. arXiv:1511.08818.

[DW05]   Igor Devetak and Andreas Winter. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A*, 461(2053):207–235, January 2005. arXiv:quant-ph/0306078.

[DW17]   Siddhartha Das and Mark M. Wilde. Quantum reading capacity: General definition and bounds. March 2017. arXiv:1703.03706.

[Eke91]   Artur K. Ekert. Quantum cryptography based on Bell's theorem. *Physical Review Letters*, 67(6):661–663, August 1991.

[FF17]   Hamza Fawzi and Omar Fawzi. Relative entropy optimization in quantum information theory via semidefinite programming approximations. May 2017. arXiv:1705.06671.

[Fri15]   Tobias Fritz. Resource convertibility and ordered commutative monoids. *Mathematical Structures in Computer Science*, page 189, 2015. arXiv:1504.03661.

[GEW16]   Kenneth Goodenough, David Elkouss, and Stephanie Wehner. Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels. *New Journal of Physics*, 18(6):063005, June 2016. arXiv:1511.08710.

[HHH96]   Michal Horodecki, Pawel Horodecki, and Ryszard Horodecki. Separability of mixed states: necessary and sufficient conditions. *Physics Letters A*, 223(1-2):1–8, November 1996. arXiv:quant-ph/9605038.

[HHH99]   Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Physical Review A*, 60(3):1888–1898, September 1999. arXiv:quant-ph/9807091.

[HHH$^+$08a] Karol Horodecki, Michał Horodecki, Paweł Horodecki, Debbie Leung, and Jonathan Oppenheim. Quantum key distribution based on private states: Unconditional security over untrusted channels with zero quantum capacity. *IEEE Transactions on Information Theory*, 54(6):2604–2620, June 2008. arXiv:quant-ph/0608195.

[HHH$^+$08b] Karol Horodecki, Michał Horodecki, Paweł Horodecki, Debbie Leung, and Jonathan Oppenheim. Unconditional privacy over channels which cannot convey quantum information. *Physical Review Letters*, 100(11):110502, March 2008. arXiv:quant-ph/0702077.

[HHHH09]   Ryszard Horodecki, Pawel Horodecki, Michal Horodecki, and Karol Horodecki. Quantum entanglement. *Reviews of Modern Physics*, 81(2):865–942, June 2009. arXiv:quant-ph/0702225.

[HHHO05a]   Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Locking entanglement with a single qubit. *Physical Review Letters*, 94(20):200501, May 2005. arXiv:quant-ph/0404096.

[HHHO05b]   Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Jonathan Oppenheim. Secure key from bound entanglement. *Physical Review Letters*, 94(16):160502, April 2005. arXiv:quant-ph/0309110.

[HHHO09]   Karol Horodecki, Michal Horodecki, Pawel Horodecki, and Jonathan Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898–1929, April 2009. arXiv:quant-ph/0506189.

[Hol02]   Alexander S. Holevo. Remarks on the classical capacity of quantum channel. December 2002. arXiv:quant-ph/0212025.

[Hol06]   Alexander S. Holevo. Multiplicativity of p-norms of completely positive maps and the additivity problem in quantum information theory. *Russian Mathematical Surveys*, 61(2):301–339, 2006.

[Hol12]   Alexander S. Holevo. *Quantum systems, channels, information: a mathematical introduction*, volume 16. Walter de Gruyter, 2012.

[HSR03]   Michal Horodecki, Peter W. Shor, and Mary Beth Ruskai. Entanglement breaking channels. *Reviews in Mathematical Physics*, 15(6):629–641, 2003. arXiv:quant-ph/0302031.

[KdR16]   Lea Kraemer and Lidia del Rio. Currencies in resource theories. May 2016. arXiv:1605.01064.

[Kit97]   Alexei Y. Kitaev. Quantum computations: algorithms and error correction. *Russian Mathematical Surveys*, 52(6):1191–1249, December 1997.

[KLR$^+$08] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland. Randomized benchmarking of quantum gates. *Physical Review A*, 77(1):012307, January 2008. arXiv:0707.0963.

[KW04]   Masato Koashi and Andreas Winter. Monogamy of quantum entanglement and other correlations. *Physical Review A*, 69:022309, February 2004. arXiv:quant-ph/0310037.

[KW17]   Eneet Kaur and Mark M. Wilde. Upper bounds on secret key agreement over lossy thermal bosonic channels. June 2017. arXiv:1706.04590.

[LG15]   Norbert Lütkenhaus and Saikat Guha. Quantum repeaters: Objectives, definitions and architectures. Available at http://wqrn.pratt.duke.edu/presentations.html, May 2015.

[LHL03]   Matthew S. Leifer, Leah Henderson, and Noah Linden. Optimal entanglement generation from quantum operations. *Physical Review A*, 67(1):012306, January 2003. arXiv:quant-ph/0205055.

[Lin73]   Göran Lindblad. Entropy, information and quantum measurements. *Communications in Mathematical Physics*, 33(4):305–322, December 1973.

[Lin75]   Göran Lindblad. Completely positive maps and entropy inequalities. *Communications in Mathematical Physics*, 40(2):147–151, June 1975.

[LKDW17]   Felix Leditzky, Eneet Kaur, Nilanjana Datta, and Mark M. Wilde. Approaches for approximate additivity of the Holevo information of quantum channels. September 2017. arXiv:1709.01111.

[LLS17]   Felix Leditzky, Debbie Leung, and Graeme Smith. Quantum and private capacities of low-noise channels. May 2017. arXiv:1705.04335.

[LPSW05]   Noah Linden, Sandu Popescu, Benjamin Schumacher, and Michael Westmoreland. Reversibility of local transformations of multiparticle entanglement. *Quantum Information Processing*, 4(3):241–250, August 2005. arXiv:quant-ph/9912039.

[LR73a]   Elliott H. Lieb and Mary Beth Ruskai. A fundamental property of quantum-mechanical entropy. *Physical Review Letters*, 30(10):434–436, March 1973.

[LR73b]   Elliott H. Lieb and Mary Beth Ruskai. Proof of the strong subadditivity of quantum-mechanical entropy. *Journal of Mathematical Physics*, 14:1938–1941, 1973.

[LW14]   Ke Li and Andreas Winter. Squashed entanglement, k-extendibility, quantum Markov chains, and recovery maps. October 2014. arXiv:1410.4184.

[MH12]   Alexander Müller-Hermes. Transposition in quantum information theory. Master's thesis, Technical University of Munich, September 2012.

[MLDS+13] Martin Müller-Lennert, Frédéric Dupuis, Oleg Szehr, Serge Fehr, and Marco Tomamichel. On quantum Rényi entropies: a new definition and some properties. *Journal of Mathematical Physics*, 54(12):122203, December 2013. arXiv:1306.3142.

[MS14]   Iman Marvian and Robert W. Spekkens. Modes of asymmetry: The application of harmonic analysis to symmetric quantum dynamics and quantum reference frames. *Physical Review A*, 90(6):062110, December 2014. arXiv:1312.0680.

[MW14]   William Matthews and Stephanie Wehner. Finite blocklength converse bounds for quantum channels. *IEEE Transactions on Information Theory*, 60(11):7317–7329, November 2014. arXiv:1210.4722.

[NFC09]   Julien Niset, Jaromír Fiurasek, and Nicolas J. Cerf. No-go theorem for Gaussian quantum error correction. *Physical Review Letters*, 102(12):120501, March 2009. arXiv:0811.3128.

[Per96]   Asher Peres. Separability criterion for density matrices. *Physical Review Letters*, 77(8):1413–1415, August 1996. arXiv:quant-ph/9604005.

[PLOB16]   Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. April 2016. arXiv:1510.08863v5.

[Rai99]   Eric M. Rains. Bound on distillable entanglement. *Physical Review A*, 60(1):179–184, July 1999. arXiv:quant-ph/9809082.

[Rai01]   Eric M. Rains. A semidefinite program for distillable entanglement. *IEEE Transactions on Information Theory*, 47(7):2921–2933, November 2001. arXiv:quant-ph/0008047.

[RGR+17]   Filip Rozpedek, Kenneth Goodenough, Jeremy Ribeiro, Norbert Kalb, Valentina Caprara Vivoli, Andreas Reiserer, Ronald Hanson, Stephanie Wehner, and David Elkouss. Realistic parameter regimes for a single sequential quantum repeater. May 2017. arXiv:1705.00043.

[RKB+17]   Luca Rigovacca, Go Kato, Stefan Baeuml, M. S. Kim, W. J. Munro, and Koji Azuma. Versatile relative entropy bounds for quantum networks. July 2017. arXiv:1707.05543.

[Shi16]   Maksim E. Shirokov. Continuity bounds for information characteristics of quantum channels depending on input dimension and on input energy. October 2016. arXiv:1610.08870.

[SN96]   Benjamin Schumacher and Michael A. Nielsen. Quantum data processing and error correction. *Physical Review A*, 54(4):2629–2635, October 1996. arXiv:quant-ph/9604022.

[SSW08]   Graeme Smith, John A. Smolin, and Andreas Winter. The quantum capacity with symmetric side channels. *IEEE Transactions on Information Theory*, 54(9):4208–4217, September 2008. arXiv:quant-ph/0607039.

[SSWR14]   David Sutter, Volkher B. Scholz, Andreas Winter, and Renato Renner. Approximate degradable quantum channels. December 2014. arXiv:1412.0980.

[STW16]   Kaushik P. Seshadreesan, Masahiro Takeoka, and Mark M. Wilde. Bounds on entanglement distillation and secret key agreement for quantum broadcast channels. *IEEE Transactions on Information Theory*, 62(5):2849–2866, May 2016. arXiv:1503.08139.

[TGW14a]   Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. Fundamental rate-loss trade-off for optical quantum key distribution. *Nature Communications*, 5:5235, October 2014. arXiv:1504.06390.

[TGW14b]   Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. The squashed entanglement of a quantum channel. *IEEE Transactions on Information Theory*, 60(8):4987–4998, August 2014. arXiv:1310.0129.

[TSW16]   Masahiro Takeoka, Kaushik P. Seshadreesan, and Mark M. Wilde. Unconstrained distillation capacities of a pure-loss bosonic broadcast channel. In *2016 IEEE International Symposium on Information Theory (ISIT)*, pages 2484–2488, July 2016.

[TSW17]   Masahiro Takeoka, Kaushik P. Seshadreesan, and Mark M. Wilde. Unconstrained capacities of quantum key distribution and entanglement distillation for pure-loss bosonic broadcast channels. *Physical Review Letters*, 119(15):150501, October 2017. arXiv:1706.06746.

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

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

[TWW17]   Marco Tomamichel, Mark M. Wilde, and Andreas Winter. Strong converse rates for quantum communication. *IEEE Transactions on Information Theory*, 63(1):715–727, January 2017. arXiv:1406.2946.

[Uhl76]   Armin Uhlmann. The "transition probability" in the state space of a *-algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.

[Ume62]   Hisaharu Umegaki. Conditional expectations in an operator algebra IV (entropy and information). *Kodai Mathematical Seminar Reports*, 14(2):59–85, 1962.

[VP98]   Vlatko Vedral and Martin B. Plenio. Entanglement measures and purification procedures. *Physical Review A*, 57(3):1619–1633, March 1998. arXiv:quant-ph/9707035.

[Wat15]   John Watrous. *Theory of Quantum Information*. November 2015.

[Wer89]   Reinhard F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, 40(8):4277–4281, October 1989.

[Wer01]   Reinhard F. Werner. All teleportation and dense coding schemes. *Journal of Physics A: Mathematical and General*, 34(35):7081, September 2001. arXiv:quant-ph/0003070.

[Wil16a]   Mark M. Wilde. *From Classical to Quantum Shannon Theory*. March 2016. arXiv:1106.1445v7.

[Wil16b]   Mark M. Wilde. Squashed entanglement and approximate private states. *Quantum Information Processing*, 15(11):4563–4580, November 2016. arXiv:1606.08028.

[Win16]   Andreas Winter. Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints. *Communications in Mathematical Physics*, 347(1):291–313, October 2016. arXiv:1507.07775.

[WPGG07]   Michael M. Wolf, David Pérez-García, and Geza Giedke. Quantum capacities of bosonic channels. *Physical Review Letters*, 98(13):130501, March 2007. arXiv:quant-ph/0606132.

[WR12]   Ligong Wang and Renato Renner. One-shot classical-quantum capacity and hypothesis testing. *Physical Review Letters*, 108(20):200501, May 2012. arXiv:1007.5456.

[WTB17]   Mark M. Wilde, Marco Tomamichel, and Mario Berta. Converse bounds for private communication over quantum channels. *IEEE Transactions on Information Theory*, 63(3):1792–1817, March 2017. arXiv:1602.08898.

[WWY14]   Mark M. Wilde, Andreas Winter, and Dong Yang. Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy. *Communications in Mathematical Physics*, 331(2):593–622, October 2014. arXiv:1306.1586.

[WY16]   Andreas Winter and Dong Yang. Potential capacities of quantum channels. *IEEE Transactions on Information Theory*, 62(3):1415–1424, March 2016. arXiv:1505.00907.