New Journal of Physics

PAPER

Amortization does not enhance the max-Rains information of a quantum channel

Mario Berta[1,2] and Mark M Wilde[3,4]

1   Department of Computing, Imperial College London, London SW7 2AZ, United Kingdom
2   Institute for Quantum Information and Matter, California Institute of Technology, Pasadena, California 91125, United States of America
3   Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, United States of America
4   Author to whom any correspondence should be addressed.

E-mail: mwilde@gmail.com

Abstract

Given an entanglement measure E, the entanglement of a quantum channel is defined as the largest amount of entanglement E that can be generated from the channel, if the sender and receiver are not allowed to share a quantum state before using the channel. The amortized entanglement of a quantum channel is defined as the largest net amount of entanglement E that can be generated from the channel, if the sender and receiver are allowed to share an arbitrary state before using the channel. Our main technical result is that amortization does not enhance the entanglement of an arbitrary quantum channel, when entanglement is quantified by the max-Rains relative entropy. We prove this statement by employing semi-definite programming (SDP) duality and SDP formulations for the max-Rains relative entropy and a channel's max-Rains information, found recently in Wang *et al* (arXiv:1709.00200). The main application of our result is a single-letter, strong converse, and efficiently computable upper bound on the capacity of a quantum channel for transmitting qubits when assisted by positive-partial-transpose preserving (PPT-P) channels between every use of the channel. As the class of local operations and classical communication (LOCC) is contained in PPT-P, our result establishes a benchmark for the LOCC-assisted quantum capacity of an arbitrary quantum channel, which is relevant in the context of distributed quantum computation and quantum key distribution.

1. Introduction

One of the main goals of quantum information theory is to understand the fundamental limitations on communication when a sender and receiver are connected by a quantum communication channel [1–3]. Since it might be difficult to transmit information reliably by making use of a channel just once, a practically relevant setting is when the sender and receiver use the channel multiple times, with the goal being to maximize the rate of communication subject to a constraint on the error probability. The capacity of a quantum channel is defined to be the maximum rate of reliable communication, such that the error probability tends to zero in the limit when the channel is utilized an arbitrary number of times.

Among the various capacities of a quantum channel $\mathcal{N}$, the LOCC-assisted quantum capacity $Q^{\leftrightarrow}(\mathcal{N})$ [4] is particularly relevant for tasks such as distributed quantum computation. In the setting corresponding to this capacity, the sender and receiver are allowed to perform arbitrary local operations and classical communication (LOCC) between every use of the channel, and the capacity is equal to the maximum rate, measured in qubits per channel use, at which qubits can be transmitted reliably from the sender to the receiver [4]. Due to the teleportation protocol [5], this rate is equal to the maximum rate at which shared entangled bits (Bell pairs) can be generated reliably between the sender and the receiver [4]. The LOCC-assisted quantum capacity of certain channels such as the quantum erasure channel has been known for some time [6], but in general, it remains an open question to characterize $Q^{\leftrightarrow}(\mathcal{N})$. One can address this question by establishing either lower bounds or upper bounds on $Q^{\leftrightarrow}(\mathcal{N})$.

Figure 1. A protocol for PPT-P-assisted quantum communication that uses a quantum channel n times. Every channel use is interleaved by a PPT-preserving channel. The goal of such a protocol is to produce an approximate maximally entangled state in the systems M_A and M_B, where Alice possesses system M_A and Bob system M_B.
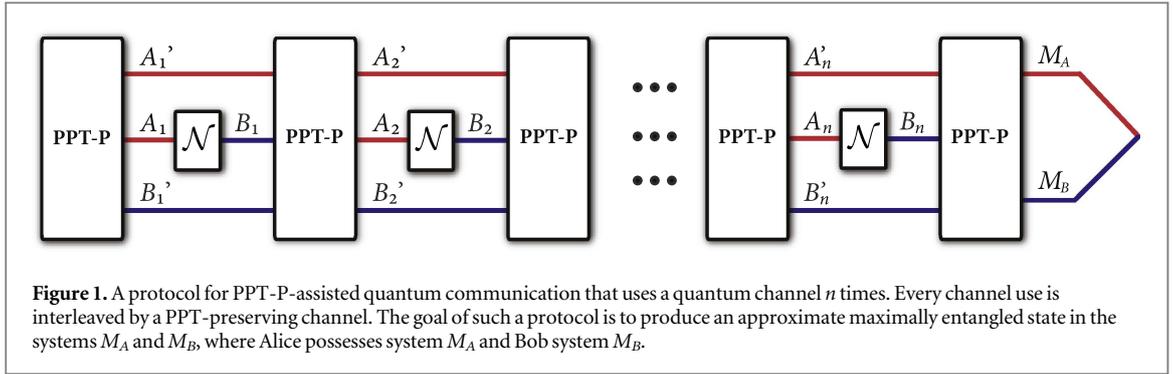
In this paper, we are interested in placing upper bounds on the LOCC-assisted quantum capacity, and one way of simplifying the mathematics behind this task is to relax the class of free operations that the sender and receiver are allowed to perform between each channel use. With this in mind, we follow the approach of [7, 8] and relax the set LOCC to a larger class of operations known as PPT-preserving (PPT-P), standing for channels that are positive-partial transpose preserving. The resulting capacity is then known as the PPT-P-assisted quantum capacity $Q^{\text{PPT-P},\leftrightarrow}(\mathcal{N})$, and it is equal to the maximum rate at which qubits can be communicated reliably from a sender to a receiver, when they are allowed to use a PPT-P channel in between every use of the actual channel $\mathcal{N}$. Figure 1 provides a visualization of such a PPT-P-assisted quantum communication protocol. Due to the containment LOCC $\subset$ PPT-P [7, 8], the inequality

$$Q^{\leftrightarrow}(\mathcal{N}) \leqslant Q^{\text{PPT-P},\leftrightarrow}(\mathcal{N}) \tag{1}$$

holds for all channels $\mathcal{N}$. Thus, if we find an upper bound on $Q^{\text{PPT-P},\leftrightarrow}(\mathcal{N})$, then by (1), such an upper bound also bounds the physically relevant LOCC-assisted quantum capacity $Q^{\leftrightarrow}(\mathcal{N})$.

A general approach for bounding these assisted capacities of a quantum channel has been developed recently in [9] (see [10–14] for related notions). The starting point is to consider an entanglement measure $E(A; B)_\rho$ [15], which is evaluated for a bipartite state ρ_{AB}. Given such an entanglement measure, one can define the entanglement $E(\mathcal{N})$ of a channel $\mathcal{N}$ in terms of it by taking an optimization over all pure, bipartite states that could be input to the channel:

$$E(\mathcal{N}) = \sup_{\psi_{RA}} E(R; B)_\omega, \tag{2}$$

where $\omega_{RB} = \mathcal{N}_{A \to B}(\psi_{RA})$. The channel's entanglement $E(\mathcal{N})$ characterizes the amount of entanglement that a sender and receiver can generate by using the channel if they do not share entanglement prior to its use. Due to the properties of an entanglement measure and the well known Schmidt decomposition theorem, it suffices to take system R isomorphic to the channel input system A and furthermore to optimize over pure states ψ_{RA}.

One can alternatively consider the amortized entanglement $E_A(\mathcal{N})$ of a channel $\mathcal{N}$ as the following optimization [9]:

$$E_A(\mathcal{N}) = \sup_{\rho_{A'AB'}} [E(A'; BB')_\tau - E(A'A; B')_\rho], \tag{3}$$

where $\tau_{A'BB'} = \mathcal{N}_{A \to B}(\rho_{A'AB'})$ and $\rho_{A'AB'}$ is a state. The supremum is with respect to all states $\rho_{A'AB'}$ and the systems $A'B'$ are finite-dimensional but could be arbitrarily large (so that the supremum might never be achieved for any particular finite-dimensional $A'B'$, but only in the limit of unbounded dimension). Thus, $E_A(\mathcal{N})$ is not known to be computable in general. The amortized entanglement quantifies the net amount of entanglement that can be generated by using the channel $\mathcal{N}$, if the sender and receiver are allowed to begin with some initial entanglement in the form of the state $\rho_{A'AB'}$. That is, $E(A'A; B')_\rho$ quantifies the entanglement of the initial state $\rho_{A'AB'}$, and $E(A'; BB')_\tau$ quantifies the final entanglement of the state after the channel acts. As observed in [9], the inequality

$$E(\mathcal{N}) \leqslant E_A(\mathcal{N}) \tag{4}$$

always holds for any entanglement measure E and for any channel $\mathcal{N}$, simply because one could take the B' system trivial in the optimization for $E_A(\mathcal{N})$, which is the same as not allowing entanglement between the sender and receiver before the channel acts. It is nontrivial if the opposite inequality

$$E_A(\mathcal{N}) \overset{?}{\leqslant} E(\mathcal{N}) \tag{5}$$

holds, which is known to occur generally for certain entanglement measures [9, 12, 16] or for certain channels with particular symmetries [9].

One of the main observations of [9], connected to earlier developments in [10–14], is that the amortized entanglement of a channel serves as an upper bound on the entanglement of the final state ω_{AB} generated by an LOCC- or PPT-P-assisted quantum communication protocol that uses the channel n times:

$$E(A; B)_\omega \leqslant n E_A(\mathcal{N}). \tag{6}$$

The basic intuition for why this bound holds is that, after a given channel use, the sender and receiver are allowed to perform a free operation such as LOCC or PPT, and thus the state that they share before the next channel use could have some entanglement. So the amount of entanglement generated by each channel use cannot exceed the amortized entanglement $E_A(\mathcal{N})$, and if the channel is used n times in such a protocol, then the entanglement of the final state ω_{AB} cannot exceed the channel's amortized entanglement multiplied by the number n of channel uses. Such a general bound can then be used to derive particular upper bounds on the assisted quantum capacities, such as strong converse bounds. Clearly, if the inequality in (5) holds, then $E_A(\mathcal{N}) = E(\mathcal{N})$ and the upper bound becomes much simpler because the channel entanglement $E(\mathcal{N})$ is simpler than the amortized entanglement $E_A(\mathcal{N})$. Thus, one of the main contributions of [9] was to reduce the physical question of determining meaningful upper bounds on the assisted capacities of $\mathcal{N}$ to a purely mathematical question of whether amortization can enhance the entanglement of a channel, i.e., whether the equality

$$E_A(\mathcal{N}) \overset{?}{=} E(\mathcal{N}) \tag{7}$$

holds for a given entanglement measure E and/or channel $\mathcal{N}$. Furthermore, it was shown in [9] how to incorporate the previous results of [4, 17, 18] into the amortization framework of [9].

In this paper, we solve the mathematical question posed above for the max-Rains information $R_{\max}(\mathcal{N})$ of a quantum channel $\mathcal{N}$, by proving that amortization does not enhance it; i.e., we prove that

$$R_{\max,A}(\mathcal{N}) = R_{\max}(\mathcal{N}), \tag{8}$$

for all channels $\mathcal{N}$, where $R_{\max,A}(\mathcal{N})$ denotes the amortized max-Rains information. Note that $R_{\max}(\mathcal{N})$ and $R_{\max,A}(\mathcal{N})$ are respectively defined by taking the entanglement measure E in (2) and (3) to be the max-Rains relative entropy, which we define formally in the next section. We note here that the equality in (8) solves an open question posed in the conclusion of [12], and we set our result in the context of the prior result of [12] and other literature in section 6. The max-Rains information of a quantum channel is a special case of a quantity known as the sandwiched Rényi–Rains information [19] and was recently shown to be equal to an information quantity discussed in [20, 21] and based on semi-definite programming (SDP). To prove our main technical result (the equality in (8)), we critically make use of the tools and framework developed in the recent works [20–22]. In particular, we employ SDP duality [23] and the well known Choi isomorphism to establish our main result, with the proof consisting of just a few lines once the framework from [20–22] is set in place.

The main application of the equality in (8) is an efficiently computable, single-letter, strong converse bound on $Q^{\mathrm{PPT\text{-}P},\leftrightarrow}(\mathcal{N})$, the PPT-P-assisted quantum capacity of an arbitrary channel $\mathcal{N}$. Due to (1), this is also an upper bound on the physically relevant LOCC-assisted quantum capacity $Q^\leftrightarrow(\mathcal{N})$. To arrive at this result, we simply apply the general inequality in (6) along with the equality in (8). For the benefit of the reader, we give technical details of this application in section 4. The quantity $R_{\max}(\mathcal{N})$ has already been shown in [21] to be efficiently computable via a semi-definite program, and in section 4, we explain how $R_{\max}(\mathcal{N})$ is both 'single-letter' and 'strong converse'.

The usefulness of the upper bound given in our paper is ultimately related with the importance of PPT-P channels. This is because the set of PPT-P channels contains the set of separable channels, and the set of separable channels strictly contains the set of LOCC channels, as shown in [24] and then in [25] for a classical scenario. Moreover, there is an entanglement monotone that can be increased by separable channels [26]. Thus, in general, PPT-P channels can increase entanglement, although this increase is not detectable by the max-Rains information. Thus, in this sense, the max-Rains information might be considered a rough measure for bounding LOCC-assisted quantum capacity. Therefore, as stressed earlier, the usefulness of our bound on the PPT-P assisted quantum capacity is directly related to PPT-P channels.

Our paper is organized as follows. In the next section, we review some background material before starting with the main development. Section 3 gives a short proof of our main technical result, and section 4 discusses its application as an efficiently computable, single-letter, strong converse bound on $Q^{\mathrm{PPT},\leftrightarrow}(\mathcal{N})$. In section 5, we revisit a result from [12], in which it was shown that amortization does not enhance a channel's max-relative entropy of entanglement. The authors of [12] proved this statement by employing complex interpolation theory [27]. We prove the main inequality underlying this statement using a method different from that used in [12], but along the lines of that given for our proof of (8) (i.e., convex programming duality), and we suspect that our alternative approach could be useful in future applications. In section 6, we discuss how our result fits into the prior literature on assisted quantum capacities and strong converses. We conclude with a brief summary in section 7.

2. Background and notation

In this section, we provide background on the Choi isomorphism, partial transpose, PPT states, separable states, PPT-P channels, max-relative entropy, max-Rains relative entropy, and max-Rains information. For basic concepts and standard notation used in quantum information theory, we point the reader to [3].

The Choi isomorphism represents a well known duality between channels and states, often employed in quantum information theory. Let $\mathcal{N}_{A \to B}$ be a quantum channel, and let $|\Upsilon\rangle_{RA}$ denote the maximally entangled vector

$$|\Upsilon\rangle_{RA} = \sum_i |i\rangle_R |i\rangle_A, \tag{9}$$

where the Hilbert spaces $\mathcal{H}_R$ and $\mathcal{H}_A$ are of the same dimension and $\{|i\rangle_R\}_i$ and $\{|i\rangle_A\}_i$ are fixed orthonormal bases. The Choi operator for a channel $\mathcal{N}_{A \to B}$ is defined as

$$J^{\mathcal{N}}_{RB} = (\mathrm{id}_R \otimes \mathcal{N}_{A \to B})(|\Upsilon\rangle\langle\Upsilon|_{RA}), \tag{10}$$

where id_R denotes the identity map on system R. One can recover the action of the channel $\mathcal{N}_{A \to B}$ on an arbitrary input state $\rho_{SA'}$ as follows:

$$\langle\Upsilon|_{A'R} \, \rho_{SA'} \otimes J^{\mathcal{N}}_{RB} \, |\Upsilon\rangle_{A'R} = \mathcal{N}_{A \to B}(\rho_{SA}), \tag{11}$$

where A' is a system isomorphic to the channel input A. The above identity can be understood in terms of a postselected variant [28, 29] of the quantum teleportation protocol [5]. Another identity we recall is that

$$\langle\Upsilon|_{RA}(X_{SR} \otimes I_A)|\Upsilon\rangle_{RA} = \mathrm{Tr}_R\{X_{SR}\}, \tag{12}$$

for an operator X_{SR} acting on $\mathcal{H}_S \otimes \mathcal{H}_R$.

For a fixed basis $\{|i\rangle_B\}_i$, the partial transpose is the following map:

$$(\mathrm{id}_A \otimes T_B)(X_{AB}) = \sum_{i,j}(I_A \otimes |i\rangle\langle j|_B) X_{AB}(I_A \otimes |i\rangle\langle j|_B), \tag{13}$$

where X_{AB} is an arbitrary operator acting on a tensor-product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. For simplicity we often employ the abbreviation $T_B(X_{AB}) = (\mathrm{id}_A \otimes T_B)(X_{AB})$. The partial transpose map plays a role in the following well known transpose trick identity:

$$(X_{SR} \otimes I_A)|\Upsilon\rangle_{RA} = (T_A(X_{SA}) \otimes I_R)|\Upsilon\rangle_{RA}. \tag{14}$$

The partial transpose map plays another important role in quantum information theory because a separable (unentangled) state

$$\sigma_{AB} = \sum_x p(x)\tau^x_A \otimes \omega^x_B \in \mathrm{SEP}(A:B), \tag{15}$$

for a distribution $p(x)$ and states τ^x_A and ω^x_B, stays within the set of separable states under this map [30, 31]:

$$T_B(\sigma_{AB}) \in \mathrm{SEP}(A:B). \tag{16}$$

This motivates defining the set of PPT states, which are those states σ_{AB} for which $T_B(\sigma_{AB}) \geqslant 0$. This in turn motivates defining the more general set of positive semi-definite operators [32]:

$$\mathrm{PPT}'(A:B) = \{\sigma_{AB} : \sigma_{AB} \geqslant 0 \wedge \|T_B(\sigma_{AB})\|_1 \leqslant 1\}, \tag{17}$$

where we have employed the trace norm, defined for an operator X as $\|X\|_1 = \mathrm{Tr}\{|X|\}$ with $|X| = \sqrt{X^\dagger X}$. We then have the containments $\mathrm{SEP} \subset \mathrm{PPT} \subset \mathrm{PPT}'$.

An LOCC quantum channel $\mathcal{N}_{AB \to A'B'}$ consists of an arbitrarily large but finite number of compositions of the following:

1. Alice performs a quantum instrument, which has both a quantum and classical output. She forwards the classical output to Bob, who then performs a quantum channel conditioned on the classical data received. This sequence of actions corresponds to a channel of the following form:

$$\sum_x \mathcal{F}^x_{A \to A'} \otimes \mathcal{G}^x_{B \to B'}, \tag{18}$$

where $\{\mathcal{F}^x_{A \to A'}\}_x$ is a collection of completely positive maps such that $\sum_x \mathcal{F}^x_{A \to A'}$ is a quantum channel and $\{\mathcal{G}^x_{B \to B'}\}_x$ is a collection of quantum channels.

2. The situation is reversed, with Bob performing the initial instrument, who forwards the classical data to Alice, who then performs a quantum channel conditioned on the classical data. This sequence of actions corresponds to a channel of the form in (18), with the A and B labels switched.

A quantum channel $\mathcal{N}_{AB \to A'B'}$ is a PPT-P channel if the map $T_{B'} \circ \mathcal{N}_{AB \to A'B'} \circ T_B$ is a quantum channel [7, 8]. Any LOCC channel is a PPT-P channel [7, 8].

The max-relative entropy of a state ρ relative to a positive semi-definite operator σ is defined as [33]

$$D_{\max}(\rho \| \sigma) = \inf\{\lambda : \rho \leqslant 2^{\lambda} \sigma\}. \tag{19}$$

If $\text{supp}(\rho) \not\subseteq \text{supp}(\sigma)$, then $D_{\max}(\rho \| \sigma) = \infty$. The max-relative entropy is monotone non-increasing under the action of a quantum channel $\mathcal{N}$ [33], in the sense that

$$D_{\max}(\rho \| \sigma) \geqslant D_{\max}(\mathcal{N}(\rho) \| \mathcal{N}(\sigma)). \tag{20}$$

The above inequality is also called the data processing inequality for max-relative entropy.

The max-Rains relative entropy of a state ρ_{AB} is defined as

$$R_{\max}(A; B)_{\rho} = \min_{\sigma_{AB} \in \text{PPT}'(A:B)} D_{\max}(\rho_{AB} \| \sigma_{AB}), \tag{21}$$

and it is monotone non-increasing under the action of a PPT-P quantum channel $\mathcal{N}_{AB \to A'B'}$ [19], in the sense that

$$R_{\max}(A; B)_{\rho} \geqslant R_{\max}(A'; B')_{\omega}, \tag{22}$$

for $\omega_{A'B'} = \mathcal{N}_{AB \to A'B'}(\rho_{AB})$. The max-Rains information of a quantum channel $\mathcal{N}_{A \to B}$ is defined by replacing E in (2) with the max-Rains relative entropy $R_{\max}$; i.e.,

$$R_{\max}(\mathcal{N}) = \max_{\phi_{SA}} R_{\max}(S; B)_{\omega}, \tag{23}$$

where $\omega_{SB} = \mathcal{N}_{A \to B}(\phi_{SA})$ and ϕ_{SA} is a pure state, with $|S| = |A|$. The amortized max-Rains information of a channel, denoted as $R_{\max,A}(\mathcal{N})$, is defined by replacing E in (3) with the max-Rains relative entropy $R_{\max}$.

Recently, in [22, equation (8)] (see also [21, equation (36)]), the max-Rains relative entropy of a state ρ_{AB} was expressed as

$$R_{\max}(A; B)_{\rho} = \log_2 W(A; B)_{\rho}, \tag{24}$$

where $W(A; B)_{\rho}$ is the solution to the following semi-definite program:

$$
\begin{aligned}
\text{minimize} \quad & \text{Tr}\{C_{AB} + D_{AB}\} \\
\text{subject to} \quad & C_{AB}, D_{AB} \geqslant 0, \\
& T_B(C_{AB} - D_{AB}) \geqslant \rho_{AB}.
\end{aligned} \tag{25}
$$

Similarly, in [21, equation (21)], the max-Rains information of a quantum channel $\mathcal{N}_{A \to B}$ was expressed as

$$R_{\max}(\mathcal{N}) = \log \Gamma(\mathcal{N}), \tag{26}$$

where $\Gamma(\mathcal{N})$ is the solution to the following semi-definite program:

$$
\begin{aligned}
\text{minimize} \quad & \|\text{Tr}_B\{V_{SB} + Y_{SB}\}\|_{\infty} \\
\text{subject to} \quad & Y_{SB}, V_{SB} \geqslant 0, \\
& T_B(V_{SB} - Y_{SB}) \geqslant J_{SB}^{\mathcal{N}}.
\end{aligned} \tag{27}
$$

These formulations of $R_{\max}(A; B)_{\rho}$ and $R_{\max}(\mathcal{N})$ are the tools that we use to prove our main technical result, proposition 1. It is worth mentioning that the formulations above follow by employing the theory of SDP and its duality.

3. Main technical result

The following proposition constitutes our main technical result, and an immediate corollary of it is that amortization does not enhance the max-Rains information of a quantum channel:

Proposition 1. *Let $\rho_{A'AB'}$ be a state and let $\mathcal{N}_{A \to B}$ be a quantum channel. Then*

$$R_{\max}(A'; BB')_{\omega} \leqslant R_{\max}(\mathcal{N}) + R_{\max}(A'A; B')_{\rho}, \tag{28}$$

where

$$\omega_{A'BB'} = \mathcal{N}_{A \to B}(\rho_{A'AB'}). \tag{29}$$

Proof. By removing logarithms and applying (24) and (26), the desired inequality is equivalent to the following one:

$$W(A'; BB')_{\omega} \leqslant \Gamma(\mathcal{N}) \cdot W(A'A; B')_{\rho}, \tag{30}$$

and so we aim to prove this one. Exploiting the identity in (25), we find that

$$W(A'A; B')_\rho = \min \mathrm{Tr}\{C_{A'AB'} + D_{A'AB'}\}, \tag{31}$$

subject to the constraints

$$C_{A'AB'}, D_{A'AB'} \geqslant 0, \tag{32}$$

$$T_{B'}(C_{A'AB'} - D_{A'AB'}) \geqslant \rho_{A'AB'}, \tag{33}$$

while the identity in (27) gives that

$$\Gamma(\mathcal{N}) = \min \| \mathrm{Tr}_B\{V_{SB} + Y_{SB}\} \|_\infty, \tag{34}$$

subject to the constraints

$$Y_{SB}, V_{SB} \geqslant 0, \tag{35}$$

$$T_B(V_{SB} - Y_{SB}) \geqslant J_{SB}^{\mathcal{N}}. \tag{36}$$

The identity in (25) implies that the left-hand side of (30) is equal to

$$W(A'; BB')_\omega = \min \mathrm{Tr}\{E_{A'BB'} + F_{A'BB'}\}, \tag{37}$$

subject to the constraints

$$E_{A'BB'}, F_{A'BB'} \geqslant 0, \tag{38}$$

$$\mathcal{N}_{A \to B}(\rho_{A'AB'}) \leqslant T_{BB'}(E_{A'BB'} - F_{A'BB'}). \tag{39}$$

With these SDP formulations in place, we can now establish the inequality in (30) by making judicious choices for $E_{A'BB'}$ and $F_{A'BB'}$. Let $C_{A'AB'}$ and $D_{A'AB'}$ be optimal for $W(A'A; B')_\rho$, and let Y_{SB} and V_{SB} be optimal for $\Gamma(\mathcal{N})$. Let $|\Upsilon\rangle_{SA}$ be the maximally entangled vector, as defined in (9). Pick

$$E_{A'BB'} = \langle\Upsilon|_{SA} \ C_{A'AB'} \otimes V_{SB} + D_{A'AB'} \otimes Y_{SB}|\Upsilon\rangle_{SA},$$

$$F_{A'BB'} = \langle\Upsilon|_{SA} \ C_{A'AB'} \otimes Y_{SB} + D_{A'AB'} \otimes V_{SB}|\Upsilon\rangle_{SA}.$$

We note that these choices are somewhat similar to those made in the proof of [21], Proposition 6, and they can be understood roughly via (11) as a postselected teleportation of the optimal operators of $W(A'A; B')_\rho$ through the optimal operators of $\Gamma(\mathcal{N})$, with the optimal operators of $W(A'A; B')_\rho$ being in correspondence with the input state $\rho_{A'AB'}$ through (33) and the optimal operators of $\Gamma(\mathcal{N})$ being in correspondence with the Choi operator $J_{SB}^{\mathcal{N}}$ through (36). We then have that $E_{A'BB'}, F_{A'BB'} \geqslant 0$ because $C_{A'AB'}, D_{A'AB'}, Y_{SB}, V_{SB} \geqslant 0$. Consider that

$$\begin{aligned} T_{BB'}(E_{A'BB'} - F_{A'BB'}) &= T_{BB'}[\langle\Upsilon|_{SA}(C_{A'AB'} - D_{A'AB'}) \otimes (V_{SB} - Y_{SB})|\Upsilon\rangle_{SA}] \\ &= \langle\Upsilon|_{SA} \ T_{B'}(C_{A'AB'} - D_{A'AB'}) \otimes T_B(V_{SB} - Y_{SB})|\Upsilon\rangle_{SA} \\ &\geqslant \langle\Upsilon|_{SA} \ \rho_{A'AB'} \otimes J_{SB}^{\mathcal{N}}|\Upsilon\rangle_{SA} \\ &= \mathcal{N}_{A \to B}(\rho_{A'AB'}). \end{aligned} \tag{40}$$

The inequality follows from (33) and (36), and the last equality follows from (11). Also consider that

$$\begin{aligned} \mathrm{Tr}\{E_{A'BB'} + F_{A'BB'}\} &= \mathrm{Tr}\{\langle\Upsilon|_{SA}(C_{A'AB'} + D_{A'AB'}) \otimes (V_{SB} + Y_{SB})|\Upsilon\rangle_{SA}\} \\ &= \mathrm{Tr}\{(C_{A'AB'} + D_{A'AB'}) T_A(V_{AB} + Y_{AB})\} \\ &= \mathrm{Tr}\{(C_{A'AB'} + D_{A'AB'}) T_A(\mathrm{Tr}_B\{V_{AB} + Y_{AB}\})\} \\ &\leqslant \mathrm{Tr}\{C_{A'AB'} + D_{A'AB'}\} \| T_A(\mathrm{Tr}_B\{V_{AB} + Y_{AB}\}) \|_\infty \\ &= \mathrm{Tr}\{C_{A'AB'} + D_{A'AB'}\} \| \mathrm{Tr}_B\{V_{AB} + Y_{AB}\} \|_\infty \\ &= W(A'A; B')_\rho \cdot \Gamma(\mathcal{N}). \end{aligned} \tag{41}$$

The second equality follows from (14) and (12). The inequality is a consequence of Hölder's inequality. The final equality follows because the spectrum of an operator is invariant under the action of a (full) transpose (note, in this case, that T_A is a full transpose because the operator $\mathrm{Tr}_B\{V_{AB} + Y_{AB}\}$ acts only on system A).

Thus, we can conclude that our choices of $E_{A'BB'}$ and $F_{A'BB'}$ are feasible for $W(A'; BB')_\omega$. Since $W(A'; BB')_\omega$ involves a minimization over all $E_{A'BB'}$ and $F_{A'BB'}$ satisfying (38) and (39), this concludes our proof of (30). ∎

An immediate corollary of proposition 1 is the following:

Corollary 2. *Amortization does not enhance the max-Rains information of a quantum channel* $\mathcal{N}_{A \to B}$; *i.e., the following equality holds*

$$R_{\max,A}(\mathcal{N}) = R_{\max}(\mathcal{N}). \tag{42}$$

Proof. The inequality $R_{\max,A}(\mathcal{N}) \geqslant R_{\max}(\mathcal{N})$ always holds, as reviewed in (4). The other inequality is an

immediate consequence of proposition 1. Letting $\rho_{A'AB'}$ denote an arbitrary input state, proposition 1 implies that

$$R_{\max}(A'; BB')_\omega - R_{\max}(A'A; B')_\rho \leqslant R_{\max}(\mathcal{N}), \tag{43}$$

where $\omega_{A'BB'} = \mathcal{N}_{A \to B}(\rho_{A'AB'})$. Since the inequality holds for any state $\rho_{A'AB'}$, it holds for the supremum over all such input states, leading to $R_{\max,A}(\mathcal{N}) \leqslant R_{\max}(\mathcal{N})$. ∎

4. Application to PPT-P-assisted quantum communication

We now give our main application of proposition 1, which is that the max-Rains information is a single-letter, strong converse upper bound on the PPT-P-assisted quantum capacity of any channel. The term 'single-letter' refers to the fact that the max-Rains information requires an optimization over a single use of the channel. As we remarked previously, the max-Rains information is efficiently computable via SDP, as observed in [20, 21]. Finally, the bound is a strong converse bound because, as we will show, if the rate of a sequence of PPT-P-assisted quantum communication protocols exceeds the max-Rains information, then the error probability of these protocols necessarily tends to one exponentially fast in the number of channel uses.

4.1. Protocol for PPT-P-assisted quantum communication

We begin by reviewing the structure of a PPT-P-assisted quantum communication protocol, along the lines discussed in [9]. In such a protocol, a sender Alice and a receiver Bob are spatially separated and connected by a quantum channel $\mathcal{N}_{A \to B}$. They begin by performing a PPT-P channel $\mathcal{P}^{(1)}_{\varnothing \to A_1'A_1B_1'}$, which leads to a PPT state $\rho^{(1)}_{A_1'A_1B_1'}$, where A_1' and B_1' are systems that are finite-dimensional but arbitrarily large. The system A_1 is such that it can be fed into the first channel use. Alice sends system A_1 through the first channel use, leading to a state $\sigma^{(1)}_{A_1'B_1B_1'} \equiv \mathcal{N}_{A_1 \to B_1}(\rho^{(1)}_{A_1'A_1B_1'})$. Alice and Bob then perform the PPT-P channel $\mathcal{P}^{(2)}_{A_1'B_1B_1' \to A_2'A_2B_2'}$, which leads to the state

$$\rho^{(2)}_{A_2'A_2B_2'} \equiv \mathcal{P}^{(2)}_{A_1'B_1B_1' \to A_2'A_2B_2'}(\sigma^{(1)}_{A_1'B_1B_1'}). \tag{44}$$

Alice sends system A_2 through the second channel use $\mathcal{N}_{A_2 \to B_2}$, leading to the state $\sigma^{(2)}_{A_2'B_2B_2'} \equiv \mathcal{N}_{A_2 \to B_2}(\rho^{(1)}_{A_2'A_2B_2'})$. This process iterates: the protocol uses the channel n times. In general, we have the following states for all $i \in \{2, \ldots, n\}$:

$$\rho^{(i)}_{A_i'A_iB_i'} \equiv \mathcal{P}^{(i)}_{A_{i-1}'B_{i-1}B_{i-1}' \to A_i'A_iB_i'}(\sigma^{(i-1)}_{A_{i-1}'B_{i-1}B_{i-1}'}), \tag{45}$$

$$\sigma^{(i)}_{A_i'B_iB_i'} \equiv \mathcal{N}_{A_i \to B_i}(\rho^{(i)}_{A_i'A_iB_i'}), \tag{46}$$

where $\mathcal{P}^{(i)}_{A_{i-1}'B_{i-1}B_{i-1}' \to A_i'A_iB_i'}$ is a PPT channel. The final step of the protocol consists of a PPT-P channel $\mathcal{P}^{(n+1)}_{A_n'B_nB_n' \to M_AM_B}$, which generates the systems M_A and M_B for Alice and Bob, respectively. The protocol's final state is as follows:

$$\omega_{M_AM_B} \equiv \mathcal{P}^{(n+1)}_{A_n'B_nB_n' \to M_AM_B}(\sigma^{(n)}_{A_n'B_nB_n'}). \tag{47}$$

Figure 1 depicts such a protocol.

The goal of the protocol is that the final state $\omega_{M_AM_B}$ is close to a maximally entangled state. Fix n, $M \in \mathbb{N}$ and $\varepsilon \in [0, 1]$. The original protocol is an (n, M, ε) protocol if the channel is used n times as discussed above, $|M_A| = |M_B| = M$, and if

$$F(\omega_{M_AM_B}, \Phi_{M_AM_B}) = \langle\Phi|_{M_AM_B} \omega_{M_AM_B}|\Phi\rangle_{M_AM_B} \tag{48}$$

$$\geqslant 1 - \varepsilon, \tag{49}$$

where the fidelity $F(\tau, \kappa) \equiv \|\sqrt{\tau}\sqrt{\kappa}\|_1^2$ [34] and the maximally entangled state $\Phi_{M_AM_B} = |\Phi\rangle\langle\Phi|_{M_AM_B}$ is defined from

$$|\Phi\rangle_{M_AM_B} \equiv \frac{1}{\sqrt{M}} \sum_{m=1}^{M} |m\rangle_{M_A} \otimes |m\rangle_{M_B}. \tag{50}$$

A rate R is achievable for PPT-P-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-P-assisted quantum capacity of a channel $\mathcal{N}$, denoted as $Q^{\text{PPT-P},\leftrightarrow}(\mathcal{N})$, is equal to the supremum of all achievable rates.

On the other hand, a rate R is a strong converse rate for PPT-P-assisted quantum communication if for all $\varepsilon \in [0, 1)$, $\delta > 0$, and sufficiently large n, there does not exist an $(n, 2^{n(R+\delta)}, \varepsilon)$ protocol. The strong converse PPT-P-assisted quantum capacity $Q^{\text{PPT-P},\leftrightarrow\dagger}(\mathcal{N})$ is equal to the infimum of all strong converse rates. We say that

a channel obeys the strong converse property for PPT-P-assisted quantum communication
if $Q^{\text{PPT-P},\leftrightarrow}(\mathcal{N}) = Q^{\text{PPT-P},\leftrightarrow\dagger}(\mathcal{N})$.

    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 $Q^{\leftrightarrow}(\mathcal{N})$ and the strong converse LOCC-assisted quantum capacity $Q^{\leftrightarrow\dagger}(\mathcal{N})$. It then immediately follows that

$$Q^{\leftrightarrow}(\mathcal{N}) \leqslant Q^{\text{PPT-P},\leftrightarrow}(\mathcal{N}), \tag{51}$$

$$Q^{\leftrightarrow\dagger}(\mathcal{N}) \leqslant Q^{\text{PPT-P},\leftrightarrow\dagger}(\mathcal{N}) \tag{52}$$

because every LOCC channel is a PPT channel.

4.2. Max-Rains information as a strong converse rate for PPT-P-assisted quantum communication

We now prove the following upper bound on the communication rate $\frac{1}{n}\log_2 M$ (qubits per channel use) of any (n, M, ε) PPT-P-assisted protocol:

Theorem 3. *Fix* $n, M \in \mathbb{N}$ *and* $\varepsilon \in (0, 1)$. *The following bound holds for an* (n, M, ε) *protocol for PPT-P-assisted quantum communication over a quantum channel* $\mathcal{N}$:

$$\log_2 M \leqslant n R_{\max}(\mathcal{N}) + \log_2\left(\frac{1}{1 - \varepsilon}\right). \tag{53}$$

Proof. For convenience of the reader, we give a complete proof, but we note that some of the essential steps are available in prior works [9, 12, 14]. From the assumption in (49), it follows that

$$\text{Tr}\{\Phi_{M_A M_B}\omega_{M_A M_B}\} \geqslant 1 - \varepsilon, \tag{54}$$

while [7, lemma 2] implies that

$$\text{Tr}\{\Phi_{M_A M_B}\sigma_{M_A M_B}\} \leqslant \frac{1}{M}, \tag{55}$$

for all $\sigma_{M_A M_B} \in \text{PPT}'(M_A : M_B)$. So under an 'entanglement test,' i.e., a measurement of the form $\{\Phi_{M_A M_B}, I_{M_A M_B} - \Phi_{M_A M_B}\}$ and applying the data processing inequality for the max-relative entropy, we find for all $\sigma_{M_A M_B} \in \text{PPT}'(M_A : M_B)$ that

$$D_{\max}(\omega_{M_A M_B}\|\sigma_{M_A M_B}) \geqslant D_{\max}(\{p, 1 - p\}\|\{q, \text{Tr}\{\sigma_{M_A M_B}\} - q\}) \tag{56}$$

$$= \log_2 \max\{p/q, (1 - p)/(\text{Tr}\{\sigma_{M_A M_B}\} - q)\} \tag{57}$$

$$\geqslant \log_2(p/q) \tag{58}$$

$$\geqslant \log_2[(1 - \varepsilon)M], \tag{59}$$

where $p \equiv \text{Tr}\{\Phi_{M_A M_B}\omega_{M_A M_B}\}$ and $q = \text{Tr}\{\Phi_{M_A M_B}\sigma_{M_A M_B}\}$. Since the above chain of inequalities holds for all $\sigma_{M_A M_B} \in \text{PPT}'(M_A : M_B)$, we conclude that

$$R_{\max}(M_A; M_B)_{\omega} \geqslant \log_2[(1 - \varepsilon)M]. \tag{60}$$

From the monotonicity of the Rains relative entropy with respect to PPT-P channels [8, 19], we find that

$$R_{\max}(M_A; M_B)_{\omega} \leqslant R_{\max}(A_n'; B_n B_n')_{\sigma^{(n)}} \tag{61}$$

$$= R_{\max}(A_n'; B_n B_n')_{\sigma^{(n)}} - R_{\max}(A_1' A_1; B_1')_{\rho^{(1)}} \tag{62}$$

$$= R_{\max}(A_n'; B_n B_n')_{\sigma^{(n)}} + \left[\sum_{i=2}^{n} R_{\max}(A_i' A_i; B_i')_{\rho^{(i)}} - R_{\max}(A_i' A_i; B_i')_{\rho^{(i)}}\right]$$
$$- R_{\max}(A_1' A_1; B_1')_{\rho^{(1)}} \tag{63}$$

$$\leqslant \sum_{i=1}^{n}[R_{\max}(A_i'; B_i B_i')_{\sigma^{(i)}} - R_{\max}(A_i' A_i; B_i')_{\rho^{(i)}}] \tag{64}$$

$$\leqslant n R_{\max}(\mathcal{N}). \tag{65}$$

The first equality follows because the state $\rho^{(1)}_{A_1' A_1 B_1'}$ is a PPT state with vanishing max-Rains relative entropy. The second equality follows by adding and subtracting terms. The second inequality follows because $R_{\max}(A_i' A_i; B_i')_{\rho^{(i)}} \leqslant R_{\max}(A_{i-1}'; B_{i-1} B_{i-1}')_{\sigma^{(i-1)}}$ for all $i \in \{2, \ldots, n\}$, due to monotonicity of the Rains relative entropy with respect to PPT-P channels. The final inequality follows by applying proposition 1 to each term $R_{\max}(A_n'; B_n B_n')_{\sigma^{(i)}} - R_{\max}(A_i' A_i; B_i')_{\rho^{(i)}}$. Combining (60) and (65), we arrive at the inequality in (53). ∎

Remark 4. The bound in (53) can also be rewritten in the following way:

$$1 - \varepsilon \leqslant 2^{-n[Q - R_{\max}(\mathcal{N})]}, \tag{66}$$

where we set the rate $Q = \frac{1}{n} \log_2 M$. Thus, if the communication rate Q is strictly larger than the max-Rains information $R_{\max}(\mathcal{N})$, then the fidelity of the transmission $(1 - \varepsilon)$ decays exponentially fast to zero in the number n of channel uses.

An immediate corollary of the above is the following strong converse statement:

Corollary 5. *The strong converse PPT-P-assisted quantum capacity is bounded from above by the max-Rains information:*

$$Q^{\mathrm{PPT-P}, \leftrightarrow \dagger}(\mathcal{N}) \leqslant R_{\max}(\mathcal{N}). \tag{67}$$

5. Amortization does not increase a channel's max-relative entropy of entanglement

One of the main results of [12] is that amortization does not increase a channel's max-relative entropy of entanglement; i.e.,

$$E_{\max, A}(\mathcal{N}) = E_{\max}(\mathcal{N}), \tag{68}$$

where $E_{\max}(\mathcal{N})$ denotes a channel's max-relative entropy of entanglement (we will define this shortly). The authors of [12] proved (68) by employing the methods of complex interpolation [27]. The main application of (68) is that $E_{\max}(\mathcal{N})$ is a strong converse upper bound on the secret-key-agreement capacity of a quantum channel [12] (this is defined as the private capacity of the channel, when arbitrary LOCC is allowed between every channel use—see [35] or [12] for a definition).

In this section, we provide an alternate proof of (68), which is along the lines of the proofs of proposition 1 and corollary 2. We think that this approach brings a different perspective to the result of [12] and could potentially be useful in future applications.

To begin with, let us recall the definition of the max-relative entropy of entanglement of a bipartite state ρ_{AB} [33]:

$$E_{\max}(A; B)_\rho = \min_{\sigma_{AB} \in \mathrm{SEP}(A:B)} D_{\max}(\rho_{AB} \| \sigma_{AB}). \tag{69}$$

Let $\overrightarrow{\mathrm{SEP}}(A:B)$ denote the cone of all separable operators, i.e., $X_{AB} \in \overrightarrow{\mathrm{SEP}}(A:B)$ if there exists a positive integer L and positive semi-definite operators $\{P_A^x\}_x$ and $\{Q_B^x\}_x$ such that $X_{AB} = \sum_{x=1}^{L} P_A^x \otimes Q_B^x$. The arrow in $\overrightarrow{\mathrm{SEP}}(A:B)$ is meant to remind the reader of 'cone' and is not intended to indicate any directionality between the A and B systems. In what follows, we sometimes employ the shorthands SEP and $\overrightarrow{\mathrm{SEP}}$ when the bipartite cuts are clear from the context. Then we have the following alternative expression for the max-relative entropy of entanglement:

Lemma 6. *Let ρ_{AB} be a bipartite state. Then*

$$E_{\max}(A; B)_\rho = \log_2 W_{\mathrm{sep}}(A; B)_\rho, \tag{70}$$

where

$$W_{\mathrm{sep}}(A; B)_\rho = \min_{X_{AB} \in \overrightarrow{\mathrm{SEP}}} \{\mathrm{Tr}\{X_{AB}\} : \rho_{AB} \leqslant X_{AB}\}. \tag{71}$$

Proof. Employing the definition in (69), consider that

$$\min_{\sigma_{AB} \in \mathrm{SEP}(A:B)} D_{\max}(\rho_{AB} \| \sigma_{AB}) = \log_2 \min_{\mu, \sigma_{AB}} \{\mu : \rho_{AB} \leqslant \mu \sigma_{AB}, \, \sigma_{AB} \in \mathrm{SEP}\} \tag{72}$$

$$= \log_2 \min_{X_{AB}} \{\mathrm{Tr}\{X_{AB}\} : \rho_{AB} \leqslant X_{AB}, \, X_{AB} \in \overrightarrow{\mathrm{SEP}}\}. \tag{73}$$

This concludes the proof. ∎

We can then define a channel's max-relative entropy of entanglement $E_{\max}(\mathcal{N})$ as in (2), by replacing E with $E_{\max}$. We can alternatively write $E_{\max}(\mathcal{N})$ as follows, by employing similar reasoning as given in the proof of [36, lemma 6]:

$$E_{\max}(\mathcal{N}) = \max_{\rho_S} \min_{\sigma_{SB} \in \mathrm{SEP}} D_{\max}(\rho_S^{1/2} J_{SB}^{\mathcal{N}} \rho_S^{1/2} \| \sigma_{SB}), \tag{74}$$

where ρ_S is a density operator and $J_{SB}^{\mathcal{N}}$ is the Choi operator for the channel $\mathcal{N}$, as defined in (10). We now prove the following alternative expression for $E_{\max}(\mathcal{N})$:

Lemma 7. *Let $\mathcal{N}_{A \to B}$ be a quantum channel. Then*

$$E_{\max}(\mathcal{N}) = \log_2 \Sigma(\mathcal{N}), \tag{75}$$

where

$$\Sigma(\mathcal{N}) = \min_{Y_{SB} \in \overrightarrow{\text{SEP}}} \{ \| \text{Tr}_B\{Y_{SB}\} \|_\infty : J_{SB}^{\mathcal{N}} \leqslant Y_{SB} \}. \tag{76}$$

Proof. Employing (74) and lemma 6, we find that

$$E_{\max}(\mathcal{N}) = \log \max_{\rho_S} \min_{Y_{SB} \in \overrightarrow{\text{SEP}}} \{ \text{Tr}\{Y_{SB}\} : \rho_S^{1/2} J_{SB}^{\mathcal{N}} \rho_S^{1/2} \leqslant Y_{SB} \}. \tag{77}$$

So our aim is to prove that the expression inside the logarithm is equal to $\Sigma(\mathcal{N})$. Taking the ansatz that ρ_S is an invertible density operator, we find that the condition $\rho_S^{1/2} J_{SB}^{\mathcal{N}} \rho_S^{1/2} \leqslant Y_{SB}$ is equivalent to the condition $J_{SB}^{\mathcal{N}} \leqslant \rho_S^{-1/2} Y_{SB} \rho_S^{-1/2} = Y'_{SB} \in \overrightarrow{\text{SEP}}(S : B)$. Noting that $Y_{SB} = \rho_S^{1/2} Y'_{SB} \rho_S^{1/2}$, this means that

$$\max_{\rho_S} \min_{Y_{SB} \in \overrightarrow{\text{SEP}}} \{ \text{Tr}\{Y_{SB}\} : \rho_S^{1/2} J_{SB}^{\mathcal{N}} \rho_S^{1/2} \leqslant Y_{SB} \} = \max_{\rho_S} \min_{Y'_{SB} \in \overrightarrow{\text{SEP}}} \{ \text{Tr}\{\rho_S Y'_{SB}\} : J_{SB}^{\mathcal{N}} \leqslant Y'_{SB} \}$$

$$= \min_{Y'_{SB} \in \overrightarrow{\text{SEP}}} \max_{\rho_S} \{ \text{Tr}\{\rho_S Y'_{SB}\} : J_{SB}^{\mathcal{N}} \leqslant Y'_{SB} \}$$

$$= \min_{Y'_{SB} \in \overrightarrow{\text{SEP}}} \max_{\rho_S} \{ \text{Tr}\{\rho_S \text{Tr}_B\{Y'_{SB}\}\} : J_{SB}^{\mathcal{N}} \leqslant Y'_{SB} \}$$

$$= \min_{Y'_{SB} \in \overrightarrow{\text{SEP}}} \{ \| \text{Tr}_B\{Y'_{SB}\} \|_\infty \} : J_{SB}^{\mathcal{N}} \leqslant Y'_{SB} \}$$

$$= \Sigma(\mathcal{N}). \tag{78}$$

The second equality follows from the Sion minimax theorem: the sets over which we are optimizing are convex, with the set of density operators additionally being compact, and the objective function $\text{Tr}\{\rho_S Y'_{SB}\}$ is linear in ρ_S and Y'_{SB}, and so the Sion minimax theorem applies. The third equality follows from partial trace, and the fourth follows because $\|D\|_\infty = \max_\rho \text{Tr}\{D\rho\}$, when the optimization is with respect to density operators. Finally, we note that the ansatz may be lifted by an appropriate limiting argument. ∎

We can now see that the expressions for $E_{\max}(A; B)_\rho$ in lemma 6 and $E_{\max}(\mathcal{N})$ in lemma 7 have a very similar form to those in (24) and (26) for $R_{\max}(A; B)_\rho$ and $R_{\max}(\mathcal{N})$, respectively. However, the optimization problems for $E_{\max}(A; B)_\rho$ and $E_{\max}(\mathcal{N})$ are not necessarily efficiently computable because they involve an optimization over the cone of separable operators, which is known to be difficult [37] in general. Regardless, due to the forms that we now have for $E_{\max}(A; B)_\rho$ and $E_{\max}(\mathcal{N})$, we can prove an inequality from [12], analogous to (28), with a proof very similar to that given in the proof of proposition 1:

Proposition 8. *[12] Let $\rho_{A'AB'}$ be a state and let $\mathcal{N}_{A \to B}$ be a quantum channel. Then*

$$E_{\max}(A'; BB')_\omega \leqslant E_{\max}(\mathcal{N}) + E_{\max}(A'A; B')_\rho, \tag{79}$$

where

$$\omega_{A'BB'} = \mathcal{N}_{A \to B}(\rho_{A'AB'}). \tag{80}$$

Proof. By removing logarithms and applying lemmas 6 and 7, the desired inequality is equivalent to the following one:

$$W_{\text{sep}}(A'; BB')_\omega \leqslant \Sigma(\mathcal{N}) \cdot W_{\text{sep}}(A'A; B')_\rho, \tag{81}$$

and so we aim to prove this one. Exploiting the identity in lemma 6, we find that

$$W_{\text{sep}}(A'A; B')_\rho = \min \text{Tr}\{C_{A'AB'}\}, \tag{82}$$

subject to the constraints

$$C_{A'AB'} \in \overrightarrow{\text{SEP}}(A'A : B'), \tag{83}$$

$$C_{A'AB'} \geqslant \rho_{A'AB'}, \tag{84}$$

while the identity in lemma 7 gives that

$$\Sigma(\mathcal{N}) = \min \| \text{Tr}_B\{Y_{SB}\} \|_\infty, \tag{85}$$

subject to the constraints

$$Y_{SB} \in \overrightarrow{\text{SEP}}(S : B), \tag{86}$$

$$Y_{SB} \geqslant J_{SB}^{\mathcal{N}}. \tag{87}$$

The identity in lemma 6 implies that the left-hand side of (81) is equal to

$$W_{\text{sep}}(A'; BB')_\omega = \min \text{Tr}\{E_{A'BB'}\}, \tag{88}$$

subject to the constraints

$$E_{A'BB'} \in \overrightarrow{\text{SEP}}(A' : BB'), \tag{89}$$

$$E_{A'BB'} \geqslant \mathcal{N}_{A \to B}(\rho_{A'AB'}). \tag{90}$$

With these optimizations in place, we can now establish the inequality in (81) by making a judicious choice for $E_{A'BB'}$. Let $C_{A'AB'}$ be optimal for $W_{\text{sep}}(A'A; B')_\rho$, and let Y_{SB} be optimal for $\Sigma(\mathcal{N})$. Let $|\Upsilon\rangle_{SA}$ be the maximally entangled vector, as defined in (9). Pick

$$E_{A'BB'} = \langle\Upsilon|_{SA} \, C_{A'AB'} \otimes Y_{SB}|\Upsilon\rangle_{SA}.$$

This choice is clearly similar to that in the proof of proposition 1. We need to prove that $E_{A'BB'}$ is feasible for $W_{\text{sep}}(A'; BB')_\omega$. To this end, consider that

$$\langle\Upsilon|_{SA} \, C_{A'AB'} \otimes Y_{SB}|\Upsilon\rangle_{SA} \geqslant \langle\Upsilon|_{SA} \, \rho_{A'AB'} \otimes J_{SB}^{\mathcal{N}}|\Upsilon\rangle_{SA}$$
$$= \mathcal{N}_{A \to B}(\rho_{A'AB'}), \tag{91}$$

which follows from (84), (87), and (11). Now, since $C_{A'AB'} \in \overrightarrow{\text{SEP}}(A'A : B')$, it can be written as $\sum_x P_{A'A}^x \otimes Q_{B'}^x$ for positive semi-definite $P_{A'A}^x$ and $Q_{B'}^x$. Furthermore, consider that since $Y_{SB} \in \overrightarrow{\text{SEP}}(S : B)$, it can be written as $\sum_y L_S^y \otimes M_B^y$ for positive semi-definite L_S^y and M_B^y. Then we have that

$$\langle\Upsilon|_{SA} \, C_{A'AB'} \otimes Y_{SB}|\Upsilon\rangle_{SA} = \sum_{x,y} \langle\Upsilon|_{SA} \, P_{A'A}^x \otimes Q_{B'}^x \otimes L_S^y \otimes M_B^y|\Upsilon\rangle_{SA}$$
$$= \sum_{x,y} \langle\Upsilon|_{SA} \, P_{A'A}^x \, T_A(L_A^y) \otimes Q_{B'}^x \otimes I_S \otimes M_B^y|\Upsilon\rangle_{SA}$$
$$= \sum_{x,y} \text{Tr}_A\{P_{A'A}^x \, T_A(L_A^y)\} \otimes Q_{B'}^x \otimes M_B^y \in \text{SEP}(A' : BB'). \tag{92}$$

The second equality follows from (14) and the third from (12). The last statement follows because $\text{Tr}_A\{P_{A'A}^x \, T_A(L_A^y)\} = \text{Tr}_A\{\sqrt{T_A(L_A^y)} \, P_{A'A}^x \, \sqrt{T_A(L_A^y)}\}$ is positive semi-definite for each x and y. Finally, consider that

$$\text{Tr}\{E_{A'BB'}\} = \text{Tr}\{\langle\Upsilon|_{SA} \, C_{A'AB'} \otimes Y_{SB}|\Upsilon\rangle_{SA}\}$$
$$= \text{Tr}\{C_{A'AB'} \, T_A(Y_{AB})\}$$
$$= \text{Tr}\{C_{A'AB'} \, T_A(\text{Tr}_B\{Y_{AB}\})\}$$
$$\leqslant \text{Tr}\{C_{A'AB'}\} \|T_A(\text{Tr}_B\{Y_{AB}\})\|_\infty$$
$$= \text{Tr}\{C_{A'AB'}\} \|\text{Tr}_B\{Y_{AB}\}\|_\infty$$
$$= W_{\text{sep}}(A'A; B')_\rho \cdot \Sigma(\mathcal{N}). \tag{93}$$

The reasoning for this chain is identical to that for (41).

Thus, we can conclude that our choice of $E_{A'BB'}$ is feasible for $W(A'; BB')_\omega$. Since $W(A'; BB')_\omega$ involves a minimization over all $E_{A'BB'}$ satisfying (89) and (90), this concludes our proof of (81). ∎

By the same reasoning employed in the proof of corollary 2, the equality in (68) follows as a consequence of the inequality in proposition 8.

We finally note that max-relative entropy of entanglement is subadditive as a function of quantum channels, in the following sense:

$$E_{\max}(\mathcal{N} \otimes \mathcal{M}) \leqslant E_{\max}(\mathcal{N}) + E_{\max}(\mathcal{M}), \tag{94}$$

where $\mathcal{N}$ and $\mathcal{M}$ are quantum channels. This follows as a consequence of the equality in (68) and [9, proposition 4], the latter of which states that the amortized entanglement is always subadditive as a function of quantum channels. It is an interesting open question to determine whether the max-relative entropy of entanglement is additive as a function of quantum channels.

6. On converses for quantum and private capacities

Here we discuss briefly how our strong converse result stands with respect to prior work on strong converses and quantum and private capacities [12, 18–21, 35, 38, 39].

6.1. Quantum capacities

Let $Q(\mathcal{N})$ and $Q^\dagger(\mathcal{N})$ denote the quantum capacity and the strong converse quantum capacity of a quantum channel $\mathcal{N}$. These quantities are defined similarly to $Q^{\text{PPT-P},\leftrightarrow}(\mathcal{N})$ and $Q^{\text{PPT-P},\leftrightarrow\dagger}(\mathcal{N})$, but there is no PPT assistance allowed. The partial transposition bound was defined in [38] as follows:

$$Q_\Theta(\mathcal{N}) = \log_2 \|T \circ \mathcal{N}\|_\diamond, \tag{95}$$

where T denotes the transpose map and $\|\cdot\|_\diamond$ is the diamond norm. In [38], $Q_\Theta(\mathcal{N})$ was established as a pretty-strong converse rate, in the sense of [40], for the quantum capacity of the channel $\mathcal{N}$. This result was subsequently improved in [39] to the following strong converse bound:

$$Q^\dagger(\mathcal{N}) \leqslant Q^{\text{PPT-P},\leftrightarrow\dagger}(\mathcal{N}) \leqslant Q_\Theta(\mathcal{N}). \tag{96}$$

The recent work in [20, 21] established the following two bounds:

$$R_{\max}(\mathcal{N}) \leqslant Q_\Theta(\mathcal{N}), \tag{97}$$

$$Q^\dagger(\mathcal{N}) \leqslant R_{\max}(\mathcal{N}). \tag{98}$$

Thus, in light of the above history, it is clear that the natural question was whether $Q^{\text{PPT-P},\leftrightarrow\dagger}(\mathcal{N}) \leqslant R_{\max}(\mathcal{N})$, and this is the question that our paper affirmatively answers. In summary, we now have that

$$Q(\mathcal{N}) \leqslant Q^\dagger(\mathcal{N}) \leqslant Q^{\text{PPT-P},\leftrightarrow\dagger}(\mathcal{N}) \leqslant R_{\max}(\mathcal{N}) \leqslant Q_\Theta(\mathcal{N}). \tag{99}$$

We now mention some other related results. The Rains relative entropy $R(A; B)_\rho$ of a bipartite state ρ_{AB} is defined as [7, 8, 32]

$$R(A; B)_\rho = \min_{\sigma_{AB} \in \text{PPT}'(A:B)} D(\rho_{AB} \| \sigma_{AB}), \tag{100}$$

where D denotes the quantum relative entropy [41, 42], defined as $D(\omega\|\tau) = \text{Tr}\{\omega[\log_2 \omega - \log_2 \tau]\}$ whenever $\text{supp}(\omega) \subseteq \text{supp}(\tau)$ and $+\infty$ otherwise. Then the Rains information $R(\mathcal{N})$ of a quantum channel $\mathcal{N}$ is defined by replacing E in (2) with $R(A; B)_\rho$ [19]. One can also define the amortized Rains information $R_A(\mathcal{N})$ via the recipe in (3). Due to the inequality $D(\omega\|\tau) \leqslant D_{\max}(\omega\|\tau)$ [33], the following inequality holds

$$R(\mathcal{N}) \leqslant R_{\max}(\mathcal{N}). \tag{101}$$

The following bound is known from [19]

$$Q^\dagger(\mathcal{N}) \leqslant R(\mathcal{N}), \tag{102}$$

and it is open to determine whether

$$Q^{\text{PPT-P},\leftrightarrow\dagger}(\mathcal{N}) \overset{?}{\leqslant} R(\mathcal{N}). \tag{103}$$

This latter inequality is known to hold if the channel $\mathcal{N}$ has sufficient symmetry [19].

The squashed entanglement $E_{\text{sq}}(A; B)_\rho$ of a quantum state ρ_{AB} is defined as [43]

$$E_{\text{sq}}(A; B)_\rho = \frac{1}{2} \inf_{\rho_{ABE}} \{I(A; B|E)_\rho : \text{Tr}_E\{\rho_{ABE}\} = \rho_{AB}\}, \tag{104}$$

where $I(A; B|E)_\rho = H(AE)_\rho + H(BE)_\rho - H(E)_\rho - H(ABE)_\rho$ and $H(F)_\sigma = -\text{Tr}\{\sigma_F \log_2 \sigma_F\}$. (See also discussions in [44, 45] for squashed entanglement.) One can also consider the squashed entanglement of a channel $E_{\text{sq}}(\mathcal{N})$ [16], as well as the amortized squashed entanglement $E_{\text{sq},A}(\mathcal{N})$. Another function of a quantum channel is its entanglement cost [46], which we write as $E_C(\mathcal{N})$ and for which a definition is given in [46]. The following bounds and relations are known regarding these quantities:

$$Q^{\leftrightarrow\dagger}(\mathcal{N}) \leqslant E_C(\mathcal{N}), \quad [44] \tag{105}$$

$$E_{\text{sq},A}(\mathcal{N}) = E_{\text{sq}}(\mathcal{N}), \quad [16] \tag{106}$$

$$Q^\leftrightarrow(\mathcal{N}) \leqslant E_{\text{sq}}(\mathcal{N}) \leqslant E_C(\mathcal{N}), \quad [16] \tag{107}$$

It is open to determine whether the following inequality holds

$$Q^{\leftrightarrow\dagger}(\mathcal{N}) \overset{?}{\leqslant} E_{\text{sq}}(\mathcal{N}). \tag{108}$$

6.2. Private capacities

One can also consider various private capacities and strong converse private capacities of a quantum channel, denoted as $P(\mathcal{N})$, $P^\leftrightarrow(\mathcal{N})$, $P^\dagger(\mathcal{N})$, and $P^{\leftrightarrow\dagger}(\mathcal{N})$. Defining the relative entropy of entanglement E_R [47] as

$$E_R(A; B)_\rho = \min_{\sigma_{AB} \in \text{SEP}(A:B)} D(\rho_{AB} \| \sigma_{AB}), \tag{109}$$

and the max-relative entropy of entanglement $E_{\max}$ as we did in (69), we can also define their channel versions $E_R(\mathcal{N})$ and $E_{\max}(\mathcal{N})$ and their amortized versions $E_{R,A}(\mathcal{N})$ and $E_{\max,A}(\mathcal{N})$. For these various quantities, we have that

$$E_R(\mathcal{N}) \leqslant E_{\max}(\mathcal{N}), \tag{110}$$

$$P^{\leftrightarrow}(\mathcal{N}) \leqslant E_{\mathrm{sq}}(\mathcal{N}), \quad [16, 46] \tag{111}$$

$$P^{\leftrightarrow\dagger}(\mathcal{N}) \leqslant E_C(\mathcal{N}), \quad [12] \tag{112}$$

$$E_{\max,A}(\mathcal{N}) = E_{\max}(\mathcal{N}), \quad [12] \tag{113}$$

$$P^{\leftrightarrow\dagger}(\mathcal{N}) \leqslant E_{\max}(\mathcal{N}), \quad [12] \tag{114}$$

$$P^{\dagger}(\mathcal{N}) \leqslant E_R(\mathcal{N}). \quad [33] \tag{115}$$

It is not known whether

$$P^{\leftrightarrow\dagger}(\mathcal{N}) \overset{?}{\leqslant} E_{\mathrm{sq}}(\mathcal{N}), \tag{116}$$

$$P^{\leftrightarrow\dagger}(\mathcal{N}) \overset{?}{\leqslant} E_R(\mathcal{N}), \tag{117}$$

but the latter inequality is known to hold for channels with sufficient symmetry [35].

An interesting question is whether the max-Rains information of a channel $\mathcal{N}$ could serve as an upper bound on one of its private capacities $P(\mathcal{N})$, $P^{\dagger}(\mathcal{N})$, $P^{\leftrightarrow}(\mathcal{N})$, or $P^{\leftrightarrow\dagger}(\mathcal{N})$. The guiding principle behind many strong converse bounds in quantum information theory is to compare the output of the actual protocol, with respect to a relative entropy-like measure, to a state or positive semi-definite operator that is 'useless' for the task. By 'useless,' we mean that the state or operator should have a probability of passing a test for the task that is no larger than inversely proportional to the dimension of the system being communicated. For example, this kind of result is known from [7, lemma 2] for operators in the set PPT$'(M_A : M_B)$ and the entanglement test, and we used this bound effectively in (55) in order to establish the max-Rains information as an upper bound on PPT-P-assisted quantum capacity. Furthermore, this kind of result is known from [35, 48, 49] for separable states and the privacy test, and prior work has used this result to establish upper bounds on various private capacities of a channel [12, 35]. However, it is not known how to obtain this kind of result for operators in the set PPT$'(M_A : M_B)$ and the privacy test, and it is for this reason that we have not been able to establish the max-Rains information as an upper bound on private capacity. We doubt whether this would be possible, given that there exist channels that produce PPT states with non-zero distillable secret-key [50, 51].

In the same spirit, one might wonder about differences between the max-Rains relative entropy and the max-relative entropy of entanglement. First, it is clear that the max-relative entropy of entanglement can increase under the action of a PPT-P channel, because there exist states that are PPT and entangled [48]. Furthermore, the aforementioned is related to the fact that there exist states for which there is a strict separation between the max-Rains relative entropy and the max-relative entropy of entanglement. Any state that is PPT and entangled has a max-Rains relative entropy equal to zero, while its max-relative entropy of entanglement is non-zero.

6.3. Summary: channel measures that do not increase under amortization
In summary, we know that amortization does not increase

1. the squashed entanglement $E_{\mathrm{sq}}(\mathcal{N})$ [16],

2. the max-relative entropy of entanglement $E_{\max}(\mathcal{N})$ [12],

3. or the max-Rains information $R_{\max}(\mathcal{N})$ (Corollary 2).

This is the main reason that these information quantities are single-letter converse bounds for assisted capacities. Is there any chance that the same could hold generally for $E_R(\mathcal{N})$ or $R(\mathcal{N})$? If so, then the known capacity bounds could be improved.

7. Conclusion

The main contribution of our paper was to show that the max-Rains information of a quantum channel does not increase under amortization. That is, when entanglement is quantified by the max-Rains relative entropy, the net entanglement that a channel can generate is the same as the amount of entanglement that it can generate if the sender and receiver do not start with any initial entanglement. This result then implies a single-letter, strong

converse, and efficiently computable bound for the capacity of a quantum channel to communicate qubits along with the assistance of PPT-P operations between every channel use. As such, the max-Rains information can be easily evaluated and is a general benchmark for this capacity. As we emphasized previously, our upper bound is also an upper bound on the physically relevant LOCC-assisted quantum capacity. The main tool that we used to prove our result is the formulation of the max-Rains relative entropy and max-Rains information as semi-definite programs [20–22] (in particular, we employed SDP duality—we note here that this kind of approach has previously been employed successfully for multiplicativity, additivity, or parallel repetition problems in quantum information theory [52–54]). We also compared our result to other results in the growing literature on the topic of bounds for the assisted capacities of arbitrary quantum channels [12, 16, 19, 35, 39].

We also provided an alternative proof for the fact that amortization does not enhance a channel's max-relative entropy of entanglement [12]: i.e., $E_{\max,A}(\mathcal{N}) = E_{\max}(\mathcal{N})$. This statement was proved in [12] by employing the methods of complex interpolation [27], but here we found a different proof by establishing alternative expressions for the max-relative entropy of entanglement (lemma 6) and a channel's max-relative entropy of entanglement (lemma 7). These alternative expressions then allowed us to employ reasoning similar to that in our proof of proposition 1 in order to establish a different proof for the equality $E_{\max,A}(\mathcal{N}) = E_{\max}(\mathcal{N})$. We suspect that our approach could be useful in future applications.

Finally, in [21], it was noted that the max-Rains information does not give a good upper bound on the quantum capacity of the qubit depolarizing channel. Our result gives a compelling reason for this observation: the max-Rains information finds its natural place as an upper bound on the PPT-P-assisted quantum capacity of the qubit depolarizing channel, and these assisting operations allowed between every channel use could result in a significant increase in capacity.

Acknowledgments

ORCID iDs

Mark M Wilde ● https://orcid.org/0000-0002-3916-4462

References

[1] Holevo A S 2012 *Quantum Systems, Channels, Information: A Mathematical Introduction* vol 16 (Berlin: Walter de Gruyter)
[2] Hayashi M 2006 *Quantum Information: An Introduction* (Berlin: Springer)
[3] Wilde M M 2017 *Quantum Information Theory* (Cambridge: Cambridge University Press) (https://doi.org/10.1017/9781316809976.001)
[4] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 Mixed-state entanglement and quantum error correction *Phys. Rev. A* **54** 3824–51
[5] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels *Phys. Rev. Lett.* **70** 1895–9
[6] Bennett C H, DiVincenzo D P and Smolin J A 1997 Capacities of quantum erasure channels *Phys. Rev. Lett.* **78** 3217–20
[7] Rains E M 1999 Bound on distillable entanglement *Phys. Rev. A* **60** 179–84
[8] Rains E M 2001 A semidefinite program for distillable entanglement *IEEE Trans. Inf. Theory* **47** 2921–33
[9] Kaur E and Wilde M M 2018 Amortized entanglement of a quantum channel and approximately teleportation-simulable channels *J. Phys. A: Math. Theor.* **51** 035303
[10] Bennett C H, Harrow A W, Leung D W and Smolin J A 2003 On the capacities of bipartite Hamiltonians and unitary gates *IEEE Trans. Inf. Theory* **49** 1895–911
[11] Leifer M S, Henderson L and Linden N 2003 Optimal entanglement generation from quantum operations *Phys. Rev. A* **67** 012306
[12] Christandl M and Müller-Hermes A 2017 Relative entropy bounds on quantum, private and repeater capacities *Commun. Math. Phys.* **353** 821–52
[13] Ben Dana K, García Díaz M, Mejatty M and Winter A 2017 Resource theory of coherence: beyond states *Phys. Rev. A* **95** 062327
[14] Rigovacca L, Kato G, Baeuml S, Kim M S, Munro W J and Azuma K 2018 Versatile relative entropy bounds for quantum networks *New J. Phys.* **20** 013033
[15] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Quantum entanglement *Rev. Mod. Phys.* **81** 865–942
[16] Takeoka M, Guha S and Wilde M M 2014 The squashed entanglement of a quantum channel *IEEE Trans. Inf. Theory* **60** 4987–98
[17] Müller-Hermes A 2012 Transposition in quantum information theory *Master's thesis* Technical University of Munich
[18] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 Fundamental limits of repeaterless quantum communications *Nat. Commun.* **8** 15043

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

[20] Wang X and Duan R 2016 A semidefinite programming upper bound of quantum capacity *2016 IEEE Int. Symp. on Information Theory (ISIT) (Barcelona, Spain, 10-15 July 2016)* pp 1690–4

[21] Wang X, Fang K and Duan R 2017 Semidefinite programming converse bounds for quantum communication arXiv:1709.00200

[22] Wang X and Duan R 2016 An improved semidefinite programming upper bound on distillable entanglement *Phys. Rev. A* **94** 050301

[23] Boyd S and Vandenberghe L 2004 *Convex Optimization* (Cambridge: Cambridge University Press)

[24] Bennett C H, DiVincenzo D P, Fuchs C A, Mor T, Rains E, Shor P W, Smolin J A and Wootters W K 1999 Quantum nonlocality without entanglement *Phys. Rev. A* **59** 1070–91

[25] Koashi M, Azuma K, Nakamura S and Imoto N 2013 Does 'quantum nonlocality without entanglement' have quantum origin? arXiv:1303.1269

[26] Chitambar E and Duan R 2009 Nonlocal entanglement transformations achievable by separable operations *Phys. Rev. Lett.* **103** 110502

[27] Bergh J and Löfström J 1976 *Interpolation Spaces* (Berlin: Springer)

[28] Horowitz G T and Maldacena J 2004 The black hole final state *J. High Energy Phys.* JHEP04(2004)008

[29] Bennett C H 2005 Simulated time travel, teleportation without communication, and how to conduct a romance with someone who has fallen into a black hole unpublished lecture

[30] Horodecki M, Horodecki P and Horodecki R 1996 Separability of mixed states: necessary and sufficient conditions *Phys. Lett. A* **223** 1–8

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

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

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

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

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

[36] Cooney T, Mosonyi M and Wilde M M 2016 Strong converse exponents for a quantum channel discrimination problem and quantum-feedback-assisted communication *Commun. Math. Phys.* **344** 797–829

[37] Harrow A W and Montanaro A 2013 Testing product states, quantum Merlin–Arthur games and tensor optimization *J. ACM* **60** 3:1–3:43

[38] Holevo A S and Werner R F 2001 Evaluating capacities of bosonic Gaussian channels *Phys. Rev. A* **63** 032312

[39] Müller-Hermes A, Reeb D and Wolf M M 2016 Positivity of linear maps under tensor powers *J. Math. Phys.* **57** 015202

[40] Morgan C and Winter A 2014 'Pretty strong' converse for the quantum capacity of degradable channels *IEEE Trans. Inf. Theory* **60** 317–33

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

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

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

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

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

[46] Berta M, Brandao F G S L, Christandl M and Wehner S 2013 Entanglement cost of quantum channels *IEEE Trans. Inf. Theory* **59** 6779–95

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

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

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

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

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

[52] Berta M and Tomamichel M 2016 The fidelity of recovery is multiplicative *IEEE Trans. Inf. Theory* **62** 1758–63

[53] Berta M, Fawzi O and Tomamichel M 2017 On variational expressions for quantum relative entropies *Lett. Math. Phys.* **107** 2239–65

[54] Vidick T and Watrous J 2016 Quantum proofs *Found. Trends Theor. Comput. Sci.* **11** 1–215

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