

“© 2016 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.”

# The Fidelity of Recovery is Multiplicative

Mario Berta<sup>1</sup> and Marco Tomamichel<sup>2</sup>

<sup>1</sup>*Institute for Quantum Information and Matter, Caltech, Pasadena, California 91125, USA*

<sup>2</sup>*School of Physics, University of Sydney, Sydney, NSW 2006, Australia*

Fawzi and Renner [Commun. Math. Phys. 340(2):575, 2015] recently established a lower bound on the conditional quantum mutual information (CQMI) of tripartite quantum states  $\rho_{ABC}$  in terms of the fidelity of recovery (FoR), i.e. the maximal fidelity of the state  $\rho_{ABC}$  with a state reconstructed from its marginal  $\rho_{BC}$  by acting only on the  $C$  system. The FoR measures quantum correlations by the local recoverability of global states and has many properties similar to the CQMI. Here we generalize the FoR and show that the resulting measure is multiplicative by utilizing semi-definite programming duality. This allows us to simplify an operational proof by Brandão *et al.* [Phys. Rev. Lett. 115(5):050501, 2015] of the above-mentioned lower bound that is based on quantum state redistribution. In particular, in contrast to the previous approaches, our proof does not rely on de Finetti reductions.

## I. INTRODUCTION

The conditional quantum mutual information (CQMI) of a tripartite quantum state  $\rho_{ABC}$  is defined as

$$I(A:B|C)_\rho := H(AC)_\rho + H(BC)_\rho - H(ABC)_\rho - H(C)_\rho, \quad (1)$$

where  $H(X)_\rho := -\text{tr}[\rho_X \log \rho_X]$  denotes the von Neumann entropy. The CQMI is a measure for the correlations between  $A$  and  $B$  from the perspective of  $C$  and has an operational interpretation as the optimal quantum communication cost in quantum state redistribution [17, 46]. Apart from that the CQMI has found manifold applications in information theory [9, 14], physics [22, 23, 31, 35], as well as computer science [11–13, 39].

A celebrated result known as strong subadditivity of entropy states that the CQMI is always non-negative [27],

$$I(A:B|C)_\rho \geq 0. \quad (2)$$

Following a line of works (see [7, 22, 26, 47] and references therein), Fawzi and Renner have shown in a recent breakthrough result that the lower bound (2) can be improved to [18],

$$I(A:B|C)_\rho \geq -\log F(A;B|C)_\rho, \quad (3)$$

where we have the fidelity of recovery (FoR),

$$F(A;B|C)_\rho := \max_{\Gamma_{C \rightarrow AC}} F(\rho_{ABC}, (\mathcal{I}_B \otimes \Gamma_{C \rightarrow AC})(\rho_{BC})). \quad (4)$$

Here,  $\mathcal{I}_B$  denotes the identity channel on  $B$ , the supremum is taken over all quantum channels (completely positive and trace-preserving (CPTP) maps) from  $C$  to  $AC$ , and we use  $F(\cdot, \cdot)$  to denote Uhlmann's fidelity [40]:  $F(\rho, \sigma) := (\text{tr}|\sqrt{\sqrt{\rho}\sqrt{\sigma}}|)^2$ . The FoR was defined and explored in detail by Seshadreesan and Wilde in [32], where they show that it has similar properties as the CQMI. For example for pure states  $\sigma_{ABCD}$  the monogamy of entanglement implies the duality

$$I(A;B|C)_\sigma = I(A;B|D)_\sigma \quad \text{as well as} \quad F(A;B|C)_\sigma = F(A;B|D)_\sigma. \quad (5)$$

Similar to the squashed entanglement which is an entanglement measure based on the CQMI [14], the FoR then serves as the basis for a (pseudo) entanglement measure: the geometric squashed entanglement [32]. By its definition (4) the FoR is also connected to the local recoverability of global quantum states, a promising concept for understanding topological order in condensed matter systems [22, 23, 35].

In this paper we investigate and generalize the FoR, and give an information theoretic proof of the lower bound in (3). For any two bipartite states  $\rho_{AB}$  and  $\sigma_{AC}$  (that may or may not have the same marginal on  $A$ ) we define the generalized fidelity of recovery (FoR) as

$$F_{C \rightarrow B}(\rho_{AB} \parallel \sigma_{AC}) := \max_{\Gamma_{C \rightarrow B}} F(\rho_{AB}, \Gamma_{C \rightarrow B}(\sigma_{AC})). \quad (6)$$

We will drop the subscript  $C \rightarrow B$  in the following when it is evident from the context on which systems the maps act. The original FoR as in (4) is then simply given as  $F_{C \rightarrow AC}(\rho_{ABC} \parallel \rho_{BC}) = F(A;B|C)_\rho$ . We note that the generalized

form (6) gives a way of comparing quantum information that lives on different dimensional systems. In particular, this allows to study quantum correlations independent of the system used to represent them.

Our results about the FoR are then as follows. We study a semi-definite programming (SDP) formulation of the FoR and find the dual minimization problem (Section II).<sup>1</sup> Based on this dual SDP formulation, we establish our main technical result and show that the FoR is multiplicative for product states (Section III). Thus, we find that in particular for any two states  $\rho_{ABC}$  and  $\tau_{A'B'C'}$ ,

$$F(AA'; BB'|CC')_{\rho \otimes \tau} = F(A; B|C)_{\rho} \cdot F(A'; B'|C')_{\tau}. \quad (7)$$

This implies that there exists an optimal recovery map that has product structure as well. Additivity (multiplicativity) results are at the heart of quantum information theory, and using our finding (7) we provide an operational proof of the Fawzi-Renner lower bound (3) (Section IV). This proof utilizes a connection between the fidelity of recovery and one-shot quantum state redistribution, using the ideas of Brandão *et al.* [10].

## II. FIDELITY OF RECOVERY AS AN SDP

In the following we denote the set of quantum states on a finite-dimensional Hilbert space  $A$  by  $\mathcal{S}(A)$  and consequently use  $\mathcal{S}(ABC)$  to denote states on a tripartite quantum system  $ABC$ . We use subscripts to indicate on which Hilbert spaces an operator acts. The dimension of  $A$  is denoted by  $d_A$ .

First, note that if  $\rho_{AB} = \Phi_{AB}$  is a (normalized) maximally entangled state (MES) with  $d_B = d_A$  then we get for the FoR (6) by standard SDP duality the conditional min-entropy [25, Theorem 2],

$$F(\Phi_{AB} \|\sigma_{AC}) = \frac{1}{d_A} 2^{-H_{\min}(A|C)_{\sigma}} = \frac{1}{d_A} \min_{\omega_C \in \mathcal{S}(C)} \left\| \sqrt{\omega_C^{-1}} \sigma_{AC} \sqrt{\omega_C^{-1}} \right\|, \quad (8)$$

where  $\|\cdot\|$  denotes the operator norm. In general we do not know much about the optimal  $\omega_C$  in this expression except that for tensor-product states it is of tensor-product form as well. That is, the conditional min-entropy is additive [25]. Second, if  $\rho_{AB} = \psi_{AB}$  is a pure state with  $d_B = d_A$  then we get by standard SDP duality [25, Remark 1],

$$F(\psi_{AB} \|\sigma_{AC}) = \min_{\omega_C \in \mathcal{S}(C)} \left\| \sqrt{\psi_A \otimes \omega_C^{-1}} \sigma_{AC} \sqrt{\psi_A \otimes \omega_C^{-1}} \right\|, \quad (9)$$

This quantity was also studied by Barnum and Knill in the context of quantum error correction [3]. The fidelity of recovery can be formulated as an SDP in general.

**Lemma 1.** *Let  $\rho_{AB} \in \mathcal{S}(AB)$  and  $\sigma_{AC} \in \mathcal{S}(AC)$  and let  $\sigma_{ACD}$  be a purification of  $\sigma_{AC}$ . Then,  $F_{C \rightarrow B}(\rho_{AB} \|\sigma_{AC})$  as in (6) is the solution to the following minimization problem:*

$$\begin{aligned} \text{minimize : } & \text{tr} [\rho_{AB} R_{AB}^{-1}] \cdot \text{tr} [\sigma_{AD} Q_{AD}] \\ \text{subject to : } & R_{AB} > 0, Q_{AD} > 0 \\ & Q_{AD} \otimes 1_B \geq R_{AB} \otimes 1_D. \end{aligned} \quad (10)$$

The proof uses SDP duality following the footsteps of Watrous' lecture notes [41]. In particular Watrous discusses the dual SDP for the fidelity [42] in the form of Alberti [1],

$$F(\rho, \sigma) = \min_{R > 0} \text{tr} [\rho R^{-1}] \cdot \text{tr} [\sigma R]. \quad (11)$$

Our resulting dual program (10) can be thought of as the Alberti form of the fidelity of recovery (since it simplifies to (11) for trivial  $B$  and  $C$  systems).<sup>2</sup>

*Proof of Lemma 1.* First note that using the purification  $\sigma_{ACD}$ , we can write

$$\Gamma_{C \rightarrow B}(\sigma_{AC}) = \text{tr}_D [\Gamma_{C \rightarrow B}(\sigma_{ACD})] = \text{tr}_D \left[ \Gamma_{C \rightarrow B}(\sqrt{\sigma_{AD}} \Psi_{AD:C} \sqrt{\sigma_{AD}}) \right], \quad (12)$$

<sup>1</sup> SDPs are a powerful tool in quantum information theory with many applications (see [41] for an introduction).

<sup>2</sup> Interestingly this Alberti form (10) does not directly simplify to (8) and (9) for the special case of MES and pure states.

where we denote by  $\Psi_{AD:C}$  the (unnormalized) maximally entangled state between  $AD : C$  in the Schmidt decomposition of  $\sigma_{ACD}$ . Then, define the Choi-Jamiołkowski state (unnormalized) of the map  $\Gamma$  as

$$\tau_{ABD} = \Gamma_{C \rightarrow B}(\Psi_{AD:C}), \quad \text{tr}_B[\tau_{ABD}] = 1_{AD}. \quad (13)$$

Hence, we can write

$$\Gamma_{C \rightarrow B}(\sigma_{AC}) = \text{tr}_D [\sqrt{\sigma_{AD}} \tau_{ABD} \sqrt{\sigma_{AD}}], \quad (14)$$

and thus we can express the optimization problem for  $\Gamma_{C \rightarrow B}$  in terms of the Choi-Jamiołkowski state in (13). On the other hand, every state  $\tau_{ABD}$  satisfying (13) corresponds to a CPTP map  $\Gamma_{C \rightarrow B}$ . Hence, we can optimize over all Choi-Jamiołkowski states of the form (13) instead of CPTP maps from  $B$  to  $C$ . This leads to the following expression for the fidelity of recovery:

$$F(\rho_{AB} \|\sigma_{AC}) = \max \left\{ F\left(\rho_{AB}, \text{tr}_D [\sqrt{\sigma_{AD}} \tau_{ABD} \sqrt{\sigma_{AD}}]\right) : \tau_{ABD} \geq 0, \text{tr}_B[\tau_{ABD}] = 1_{AD} \right\}. \quad (15)$$

The primal problem above is obtained by considering an SDP for the root fidelity  $\sqrt{F(\rho, \sigma)} = \|\sqrt{\rho}\sqrt{\sigma}\|_1$  as in [42, Section 2.1] and [21]. The square root of the fidelity of recovery in (15) is then written as

$$\begin{aligned} & \text{maximize : } \frac{1}{2} \text{tr} [Z_{AB} + Z_{AB}^\dagger] \\ & \text{subject to : } \tau_{ABD} \geq 0, Z_{AB} \in \mathcal{L}(AB), \\ & \quad \text{tr}_B[\tau_{ABD}] = 1_{AD}, \\ & \quad \begin{pmatrix} \rho_{AB} & Z_{AB} \\ Z_{AB}^\dagger & \text{tr}_D [\sqrt{\sigma_{AD}} \tau_{ABD} \sqrt{\sigma_{AD}}] \end{pmatrix} \geq 0, \end{aligned} \quad (16)$$

where  $\mathcal{L}$  denotes the set of linear operators. In the next step we bring this program into standard form. We want to write the primal problem as a maximization over  $X \geq 0$  of the functional  $\text{tr}[XA]$  subject to  $\Phi(X) = B$ . Hence, we set

$$X = \begin{pmatrix} X_{11} & Z_{AB} & \cdot \\ Z_{AB}^\dagger & X_{22} & \cdot \\ \cdot & \cdot & \tau_{ABD} \end{pmatrix}, \quad A = \frac{1}{2} \begin{pmatrix} 0 & 1_{AB} & 0 \\ 1_{AB} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} \rho_{AB} & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1_{AD} \end{pmatrix}, \quad (17)$$

as well as

$$\Phi(X) = \begin{pmatrix} X_{11} & 0 & 0 \\ 0 & X_{22} - \text{tr}_D [\sqrt{\sigma_{AD}} \tau_{ABD} \sqrt{\sigma_{AD}}] & 0 \\ 0 & 0 & \text{tr}_B[\tau_{ABD}] \end{pmatrix}. \quad (18)$$

The variables with the placeholder ‘.’ are of no interest to us. The dual SDP is a minimization over self-adjoint  $Y$  of the functional  $\text{tr}[YB]$  subject to  $\Phi^\dagger(Y) \geq A$ . The dual variables and adjoint map can be determined to be

$$Y = \begin{pmatrix} L_{AB} & \cdot & \cdot \\ \cdot & R_{AB} & \cdot \\ \cdot & \cdot & Q_{AD} \end{pmatrix} \quad (19)$$

with

$$\Phi(Y) = \begin{pmatrix} L_{AB} & 0 & 0 \\ 0 & R_{AB} & 0 \\ 0 & 0 & -\sqrt{\sigma_{AD}}(R_{AB} \otimes 1_D)\sqrt{\sigma_{AD}} + 1_B \otimes Q_{AD} \end{pmatrix}. \quad (20)$$

This leads to the following dual problem:

$$\begin{aligned} & \text{minimize : } \text{tr}[\rho_{AB} L_{AB}] + \text{tr}[Q_{AD}] \\ & \text{subject to : } L_{AB}, R_{AB} \in \mathcal{H}(AB), Q_{AD} \in \mathcal{H}(AD), \\ & \quad Q_{AD} \otimes 1_B \geq \sqrt{\sigma_{AD}}(R_{AB} \otimes 1_D)\sqrt{\sigma_{AD}}, \\ & \quad \begin{pmatrix} L_{AB} & 0 \\ 0 & R_{AB} \end{pmatrix} \geq \frac{1}{2} \begin{pmatrix} 0 & 1_{AB} \\ 1_{AB} & 0 \end{pmatrix}, \end{aligned} \quad (21)$$

where  $\mathcal{H}$  denotes the set of self-adjoint operators. The Slater condition (cf. [41]) for strong duality is satisfied. The program (21) can be simplified further by the substitutions  $L_{AB} \rightarrow \frac{1}{2}L_{AB}$ ,  $R_{AB} \rightarrow \frac{1}{2}R_{AB}$  and  $Q_{AD} \rightarrow \frac{1}{2}\sqrt{\sigma_{AD}}Q_{AD}\sqrt{\sigma_{AD}}$ , leaving us with

$$\begin{aligned} & \text{minimize : } \frac{1}{2} \text{tr} [\rho_{AB}L_{AB}] + \frac{1}{2} \text{tr} [\sigma_{AD}Q_{AD}] \\ & \text{subject to : } L_{AB}, R_{AB} \in \mathcal{H}(AB), Q_{AD} \in \mathcal{H}(AD), \\ & \quad Q_{AD} \otimes 1_B \geq R_{AB} \otimes 1_D, \\ & \quad \begin{pmatrix} L_{AB} & -1_{AB} \\ -1_{AB} & R_{AB} \end{pmatrix} \geq 0. \end{aligned} \tag{22}$$

Now we note that the above matrix inequality holds if and only if  $L_{AB}, R_{AB} \geq 0$  and  $R_{AB} \geq L_{AB}^{-1}$ . Without loss of generality we can choose  $R_{AB} = L_{AB}^{-1}$ , and our problem simplifies to

$$\begin{aligned} & \text{minimize : } \frac{1}{2} \text{tr} [\rho_{AB}R_{AB}^{-1}] + \frac{1}{2} \text{tr} [\sigma_{AD}Q_{AD}] \\ & \text{subject to : } R_{AB}, Q_{AD} \geq 0, \\ & \quad Q_{AD} \otimes 1_B \geq R_{AB} \otimes 1_D. \end{aligned} \tag{23}$$

Finally, we follow the argument leading Watrous to Alberti's expression for the fidelity [41, Lecture 8]. We first remark that

$$\frac{1}{2} \text{tr} [\rho_{AB}R_{AB}^{-1}] + \frac{1}{2} \text{tr} [\sigma_{AD}Q_{AD}] \geq \sqrt{\text{tr} [\rho_{AB}R_{AB}^{-1}] \cdot \text{tr} [\sigma_{AD}Q_{AD}]} \tag{24}$$

by the arithmetic–geometric mean inequality, with equality when the two terms are equal. However, it is easy to see that for any feasible pair  $(R_{AB}, Q_{AD})$ , there exists a constant  $\lambda \in \mathbb{R}$  such that two trace terms evaluated for  $(\lambda R_{AB}, \lambda Q_{AD})$  are equal (and clearly  $(\lambda R_{AB}, \lambda Q_{AD})$  is also feasible). Hence, restricting our optimization to such rescaled pairs of operators, and going from the root fidelity to the fidelity again we find that

$$F(\rho_{AB} \parallel \sigma_{AC}) = \min_{\substack{R_{AB} > 0, Q_{AD} > 0 \\ Q_{AD} \otimes 1_B \geq R_{AB} \otimes 1_D}} \text{tr} [\rho_{AB}R_{AB}^{-1}] \cdot \text{tr} [\sigma_{AD}Q_{AD}]. \tag{25}$$

This concludes the proof.  $\square$

### III. FIDELITY OF RECOVERY IS MULTIPLICATIVE

As a direct consequence of this formulation of the problem we see that the fidelity of recovery is multiplicative.

**Proposition 2.** *For any  $\rho_{AB} \in \mathcal{S}(AB)$ ,  $\tau_{A'B'} \in \mathcal{S}(A'B')$ ,  $\sigma_{AC} \in \mathcal{S}(AC)$  and  $\omega_{A'C'} \in \mathcal{S}(A'C')$ , we have*

$$F(\rho_{AB} \otimes \tau_{A'B'} \parallel \sigma_{AC} \otimes \omega_{A'C'}) = F(\rho_{AB} \parallel \sigma_{AC}) \cdot F(\tau_{A'B'} \parallel \omega_{A'C'}). \tag{26}$$

*Proof.* From the definition in (6) it is evident that if we restrict to recovery maps that have a product structure, we immediately find

$$F(\rho_{AB} \otimes \tau_{A'B'} \parallel \sigma_{AC} \otimes \omega_{A'C'}) \geq F(\rho_{AB} \parallel \sigma_{AC}) \cdot F(\tau_{A'B'} \parallel \omega_{A'C'}). \tag{27}$$

To establish the equality, we take a closer look at (25). Here we simply note the following. For every two pairs of feasible operators  $(R_{AB}, Q_{AD})$  and  $(R_{A'B'}, Q_{A'D'})$  for  $F(\rho_{AB} \parallel \sigma_{AC})$  and  $F(\tau_{A'B'} \parallel \omega_{A'C'})$ , respectively, we have

$$\begin{aligned} Q_{AD} \otimes 1_B &\geq R_{AB} \otimes 1_D \wedge Q_{A'D'} \otimes 1_{B'} \geq R_{A'B'} \otimes 1_{D'} \\ &\implies \\ Q_{AD} \otimes Q_{A'D'} \otimes 1_{BB'} &\geq R_{AB} \otimes R_{A'B'} \otimes 1_{DD'}. \end{aligned} \tag{28}$$

To establish (28) we used twice that  $A \geq B \implies M \otimes A \geq M \otimes B$  for  $M \geq 0$ , which holds since taking the tensor product with  $M$  is a positive map. Hence,  $(R_{AB} \otimes R_{A'B'}, Q_{AD} \otimes Q_{A'D'})$  is a feasible pair for  $F(\rho_{AB} \otimes \tau_{A'B'} \parallel \sigma_{AC} \otimes \omega_{A'C'})$ , and, thus,

$$F(\rho_{AB} \otimes \tau_{A'B'} \parallel \sigma_{AC} \otimes \omega_{A'C'}) \leq \text{tr} [\rho_{AB}R_{AB}^{-1}] \cdot \text{tr} [\tau_{A'B'}R_{A'B'}^{-1}] \cdot \text{tr} [\sigma_{AD}Q_{AD}] \cdot \text{tr} [\omega_{A'D'}Q_{A'D'}]. \tag{29}$$

Since this holds for all feasible operators, we conclude that

$$F(\rho_{AB} \otimes \tau_{A'B'} \parallel \sigma_{AC} \otimes \omega_{A'C'}) \leq F(\rho_{AB} \parallel \sigma_{AC}) \cdot F(\tau_{A'B'} \parallel \omega_{A'C'}). \tag{30}$$

$\square$

#### IV. THE FAWZI-RENNER BOUND WITHOUT DE FINETTI REDUCTIONS

Brandão *et al.* [10] show that the Fawzi-Renner lower bound (3) can be deduced from the operational interpretation of the CQMI as (twice) the quantum communication cost in quantum state redistribution [17, 46]. We simplify their proof and in particular get rid of the continuity and representation theoretic arguments (de Finetti reductions). Instead we leverage on the multiplicativity of the fidelity of recovery (Proposition 2). We first give a precise definition for the information task of quantum state redistribution [17, 46] (also see Figure 1 for an intuitive description).

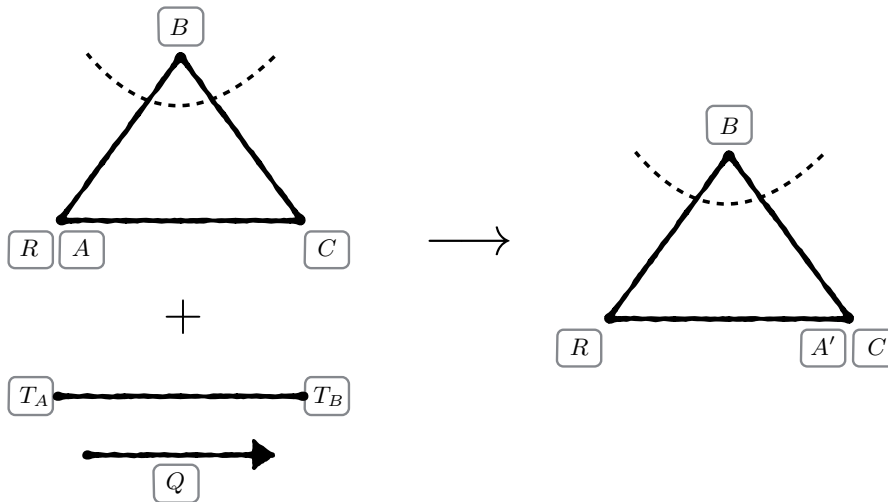


FIG. 1: Quantum state redistribution scheme. Starting from a four party pure state  $\rho_{ABCR}$  and arbitrary entanglement assistance  $T_A T_B$ , the objective of quantum state redistribution is to transfer  $A$  without altering the joint state. (See Definition 3). This is achieved by means of a local encoding operation  $\mathcal{E}_{ART_A \rightarrow QR}$ , transferring the system  $Q$ , and a local decoding operation  $\mathcal{D}_{CQT_B \rightarrow A'C}$ . One is then interested in the trade-off between the fidelity of the scheme versus the quantum communication cost  $q = \log d_Q$ .

**Definition 3.** Let  $\rho_{ABCR} \in \mathcal{S}(ABCR)$  be pure and let  $QT_A T_B$  be additional spaces. A quantum state redistribution protocol for  $A$  with fidelity  $1 - \delta$  is a pair of CPTP maps  $(\mathcal{E}_{ART_A \rightarrow QR}, \mathcal{D}_{CQT_B \rightarrow A'C})$ , the encoder and the decoder, together with  $\Phi_{T_A T_B} \in \mathcal{S}(T_A T_B)$  such that

$$F\left(\left(\mathcal{I}_{BR} \otimes \mathcal{D}_{CQT_B \rightarrow A'C}\right) \circ \left(\mathcal{E}_{ART_A \rightarrow QR} \otimes \mathcal{I}_{BCT_B}\right) \left(\rho_{ABCR} \otimes \Phi_{T_A T_B}\right), \rho_{A'BCR}\right) \geq 1 - \delta, \quad (31)$$

where  $\rho_{A'BCR} := (\mathcal{I}_{A \rightarrow A'} \otimes \mathcal{I}_{BCR}) \rho_{ABCR}$ . The number  $q := \log d_Q$  is called quantum communication cost of the protocol.

This one-shot version of quantum state redistribution was analyzed in [2, 4, 16].

**Lemma 4.** [4, Theorem 4] Let  $\rho_{ABCR} \in \mathcal{S}(ABCR)$  pure and  $\varepsilon > 0$  sufficiently small. Then, there exists a quantum state redistribution protocol for  $A$  with fidelity  $1 - 144\varepsilon^2$  and quantum communication cost

$$q \leq \frac{1}{2} \left( H_{\max}^{\varepsilon}(A|C)_{\rho} - H_{\min}^{\varepsilon}(A|BC)_{\rho} \right) + \log(4/\varepsilon^4), \quad (32)$$

where  $H_{\min}^{\varepsilon}$  and  $H_{\max}^{\varepsilon}$  denote the smooth conditional min- and max-entropy, respectively.

This follows straightforwardly by reading [4, Theorem 4] in terms of the fidelity (instead of the purified distance) and choosing appropriate error parameters. The precise definition of the smooth conditional min- and max-entropy and a discussion of their properties can be found in [38]. However, here we will only need that they both asymptotically converge to the conditional von Neumann entropy. That is, the fully quantum asymptotic equipartition property [37]

tells us that for any  $\varepsilon \in (0, 1)$ ,<sup>3</sup>

$$\lim_{n \rightarrow \infty} \frac{1}{n} H_{\max}^\varepsilon(A|C)_{\rho^{\otimes n}} \leq H(AC)_\rho - H(C)_\rho \quad \text{as well as} \quad \lim_{n \rightarrow \infty} \frac{1}{n} H_{\min}^\varepsilon(A|BC)_{\rho^{\otimes n}} \geq H(ABC)_\rho - H(BC)_\rho. \quad (33)$$

Hence, Lemma 4 implies the existence of a sequence (indexed by  $n \in \mathbb{N}$ ) of quantum state redistribution protocols for  $\rho_{ABC}^{\otimes n}$  with fidelity  $\delta_n = 1 - 144\varepsilon_n^2$  converging to one for  $n \rightarrow \infty$  and an asymptotic quantum communication cost rate  $q_n$  satisfying

$$\lim_{n \rightarrow \infty} \frac{q_n}{n} \leq \lim_{n \rightarrow \infty} \left\{ \frac{1}{n} \cdot \frac{1}{2} \left( H_{\max}^{\varepsilon_n}(A|C)_{\rho^{\otimes n}} - H_{\min}^{\varepsilon_n}(A|BC)_{\rho^{\otimes n}} \right) + \frac{1}{n} \log(4/\varepsilon_n^4) \right\} \quad (34)$$

$$\leq \frac{1}{2} \left( H(AC)_\rho - H(C)_\rho - H(ABC)_\rho + H(BC)_\rho \right) \quad (35)$$

$$= \frac{1}{2} I(A:B|C)_\rho. \quad (36)$$

Following the ideas of Brandão *et al.* [10], the existence of this protocol with a quantum communication cost rate given by (one-half) the CQMI can than be used to lower bound the CQMI.

**Theorem 5.** *Let  $\rho_{ABC} \in \mathcal{S}(ABC)$ . Then, we have*

$$I(A:B|C)_\rho \geq -\log F(A;B|C)_\rho. \quad (37)$$

*Proof.* The first part of the proof is the same as in [10]. Let  $\rho_{ABCR}$  be a purification of  $\rho_{ABC}$  and consider any quantum state redistribution protocol for  $A$  with encoder  $\mathcal{E}_{ART_A \rightarrow QR}$ , decoder  $\mathcal{D}_{CQT_B \rightarrow A'C}$ , and define

$$\sigma_{BCQRT_B} := (\mathcal{E}_{ART_A \rightarrow QR} \otimes \mathcal{I}_{BCT_B})(\rho_{ABCR} \otimes \Phi_{T_A T_B}). \quad (38)$$

The authors of [10] observe that the existence of a protocol with high fidelity is sufficient to give some bounds on the performance of the decoder even if the quantum communication is omitted. This is a consequence of the standard operator inequality  $d_X \cdot 1_X \otimes \omega_Y \geq \omega_{XY}$ . In our case,

$$\sigma_{BCQRT_B} \leq d_Q \cdot \sigma_{BCT_B} \otimes 1_Q = \rho_{BC} \otimes \left( d_Q^2 \cdot \frac{1_Q}{d_Q} \right) \otimes \frac{1_{T_B}}{d_{T_B}}, \quad (39)$$

which again implies

$$d_Q^2 \cdot \mathcal{D}_{CQRT_B \rightarrow AC} \left( \rho_{BC} \otimes \frac{1_Q}{d_Q} \otimes \frac{1_{T_B}}{d_{T_B}} \right) \geq \mathcal{D}_{CQRT_B \rightarrow A'C}(\sigma_{BCQRT_B}). \quad (40)$$

Now the following second part of the proof is different from [10]. Due to the operator monotonicity of the square root function we get

$$d_Q^2 \cdot F \left( \rho_{A'BC}, \mathcal{D}_{CQRT_B \rightarrow A'C} \left( \rho_{BC} \otimes \frac{1_Q}{d_Q} \otimes \frac{1_{T_B}}{d_{T_B}} \right) \right) \geq F(\rho_{A'BC}, \mathcal{D}_{CQRT_B \rightarrow A'C}(\sigma_{BCQRT_B})). \quad (41)$$

By the protocol for quantum state redistribution (Lemma 4), we find that for all  $\varepsilon > 0$  small enough there exists a protocol such that

$$F(\rho_{A'BC}, \mathcal{D}_{CQRT_B \rightarrow A'C}(\sigma_{BCQRT_B})) \geq 1 - 144\varepsilon^2 \quad (42)$$

for a quantum communication cost

$$\log d_Q \leq \frac{1}{2} \left( H_{\max}^\varepsilon(A|C)_\rho - H_{\min}^\varepsilon(A|BC)_\rho \right) + \log(4/\varepsilon^4). \quad (43)$$

---

<sup>3</sup> These inequalities are in fact equalities [36, Section 6.4].

Hence, we can use (41) and (42) to estimate

$$H_{\max}^\varepsilon(A|C)_\rho - H_{\min}^\varepsilon(A|BC)_\rho \geq -\log F\left(\rho_{A'BC}, \mathcal{D}_{CQT_B \rightarrow A'C}\left(\rho_{BC} \otimes \frac{1_Q}{d_Q} \otimes \frac{1_{T_B}}{d_{T_B}}\right)\right) - \log(16/\varepsilon^8) + \log(1 - 144\varepsilon^2)$$
(44)

$$\geq -\log \max_{\Gamma_{C \rightarrow A'C}} F(\rho_{A'BC}, \Gamma_{C \rightarrow A'C}(\rho_{BC})) - \log(16/\varepsilon^8) + \log(1 - 144\varepsilon^2),$$
(45)

and find that

$$H_{\max}^\varepsilon(A|C)_\rho - H_{\min}^\varepsilon(A|BC)_\rho \geq -\log F(A; B|C)_\rho - O(\log(1/\varepsilon)).$$
(46)

By applying this bound to  $\rho_{ABC}^{\otimes n}$ , multiplying the resulting inequality by  $1/n$ , and letting  $n \rightarrow \infty$  we find by the asymptotic equipartition property for the smooth conditional min- and max-entropy (33), and the multiplicativity of the fidelity of recovery (Proposition 2), that

$$I(A; B|C)_\rho \geq -\log F(A; B|C)_\rho.$$
(47)

□

## V. CONCLUSION

In this paper we have generalized the FoR and have shown that the resulting measure is multiplicative for product states (Proposition 2). It would be interesting to explore the consequences of this more for analyzing quantum correlations [32], or for possible applications in computer science [11–13, 39]. From the multiplicativity we also deduced an information theoretic proof of the Fawzi-Renner lower bound on the conditional quantum mutual information without making use of de Finetti reductions (Theorem 5). We note that Brandão *et al.* [10] also show a potentially stronger lower bound in terms of a regularized relative entropy distance,

$$I(A; B|C) \geq \lim_{n \rightarrow \infty} \frac{1}{n} \min_{\Gamma_{C^n \rightarrow A^n C^n}} D(\rho_{ABC}^{\otimes n} \| \Gamma_{C^n \rightarrow A^n C^n}(\rho_{BC}^{\otimes n})).$$
(48)

They then use de Finetti reductions to get rid of the regularization and arrive at a bound in terms of a measured relative entropy distance. On the other hand, our Proposition 2 rephrased in terms of the (sandwiched) quantum Rényi divergence of order  $\frac{1}{2}$  [28, 45] reads

$$\min_{\Gamma_{C^n \rightarrow A^n C^n}} D_{\frac{1}{2}}(\rho_{ABC}^{\otimes n} \| \Gamma_{C^n \rightarrow A^n C^n}(\rho_{BC}^{\otimes n})) = n \cdot \min_{\Gamma_{C \rightarrow AC}} D_{\frac{1}{2}}(\rho_{ABC} \| \Gamma_{C \rightarrow AC}(\rho_{BC})).$$
(49)

And hence the Fawzi-Renner bound then follows from the monotonicity of the quantum Rényi divergence in  $\alpha$ . Moreover, if such an additivity property would hold for any  $\alpha \in (\frac{1}{2}, 1]$  we could find stronger bounds. In particular, Li and Winter [26] have asked about a bound in terms of the relative entropy distance ( $\alpha = 1$ ). The corresponding problems can then no longer be phrased as SDPs but become complex optimization programs (for which duality is also available in principle [8]).<sup>4</sup> Another interesting question is if we can estimate the performance of the optimal map  $\Lambda_{C \rightarrow AC}$  in (4) with the Petz recovery map [29],

$$\Gamma_{C \rightarrow AC}^{\text{Petz}}(\cdot) := \rho_{AC}^{1/2} \rho_C^{-1/2}(\cdot) \rho_C^{-1/2} \rho_{AC}^{1/2},$$
(50)

in the sense that the Petz map should perform nearly as good as the optimal map. This in analogy to what Barnum and Knill have shown for the special case of pure states, i.e. for the quantity (9). Finally, the results of Fawzi and Renner were recently generalized to the multiparty setting [43] as well as to a new lower bound on the monotonicity of the quantum relative entropy under CPTP maps [6]. It should be insightful to study SDP techniques in these more general settings as well. We also note that Piani [30] recently established a family of lower bounds on quantum discord using (3)–(4) and SDPs similar to our primal problem in (16).

**Note added:** After completion of this work, improved lower bounds on the CQMI and on the monotonicity of the quantum relative entropy under CPTP maps were proven [20, 33, 34, 44]. Moreover, using complex optimization

---

<sup>4</sup> For studying additivity properties one could also try to adapt the techniques of [19].



duality the main result of this paper was extended to an additivity result for more general relative entropies of recovery [5]. It was also shown that the Petz recovery map (50) does not perform square-root optimal compared to the optimal recovery map [33, Appendix F] (even though some type of near optimality might still hold). Lastly it was pointed out very recently that there is a quantum interactive proof system whose maximum acceptance probability is equal to the fidelity of recovery [15], and hence the multiplicativity thereof also follows by a result of Kitaev and Watrous [24].

*Acknowledgments.* We thank Fernando Brandão, Omar Fawzi, Volkher Scholz, David Sutter, and Mark Wilde for discussions and feedback. MB acknowledges funding provided by the Institute for Quantum Information and Matter, an NSF Physics Frontiers Center (NSF Grant PHY-1125565) with support of the Gordon and Betty Moore Foundation (GBMF-12500028). Additional funding support was provided by the ARO grant for Research on Quantum Algorithms at the IQIM (W911NF-12-1-0521). MT is funded by an University of Sydney Postdoctoral Fellowship and acknowledges support from the ARC Centre of Excellence for Engineered Quantum Systems (EQUS). MB thanks the University of Sydney for hosting him while part of this work was done.

- 
- [1] P. M. Alberti. A Note on the Transition Probability over  $C^*$ -Algebras. *Lett. Math. Phys.*, 7:25–32, 1983. DOI: [10.1007/BF00398708](https://doi.org/10.1007/BF00398708).
- [2] A. Anshu, V. K. Devabathini, and R. Jain. Near Optimal Bounds on Quantum Communication Complexity of Single-Shot Quantum State Redistribution. 2014. [arXiv: 1410.3031](https://arxiv.org/abs/1410.3031).
- [3] H. Barnum and E. Knill. Reversing Quantum Dynamics with Near-Optimal Quantum and Classical Fidelity. *J. Math. Phys.*, 43(5):2097, 2002. DOI: [10.1063/1.1459754](https://doi.org/10.1063/1.1459754).
- [4] M. Berta, M. Christandl, and D. Touchette. Smooth Entropy Bounds on One-Shot Quantum State Redistribution. *IEEE Trans. on Inf. Theory*, PP(99):1–1, 2016. DOI: [10.1109/TIT.2016.2516006](https://doi.org/10.1109/TIT.2016.2516006).
- [5] M. Berta, O. Fawzi, and M. Tomamichel. On Variational Expressions for Quantum Relative Entropies. 2015. [arXiv: 1512.02615](https://arxiv.org/abs/1512.02615).
- [6] M. Berta, M. Lemm, and M. M. Wilde. Monotonicity of Quantum Relative Entropy and Recoverability. *Quant. Inf. Comput.*, 15(15/16):1333–1354, 2015.
- [7] M. Berta, K. Seshadreesan, and M. Wilde. Rényi Generalizations of the Conditional Quantum Mutual Information. *J. Math. Phys.*, 56(2):022205, 2015. DOI: [10.1063/1.4908102](https://doi.org/10.1063/1.4908102).
- [8] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.
- [9] F. G. S. L. Brandão, M. Christandl, and J. Yard. Faithful Squashed Entanglement. *Commun. Math. Phys.*, 306(3):805–830, 2011. DOI: [10.1007/s00220-011-1302-1](https://doi.org/10.1007/s00220-011-1302-1).
- [10] F. G. S. L. Brandão, A. W. Harrow, J. Oppenheim, and S. Strelchuk. Quantum Conditional Mutual Information, Reconstructed States, and State Redistribution. *Phys. Rev. Lett.*, 115(5):050501, 2015. DOI: [10.1103/PhysRevLett.115.050501](https://doi.org/10.1103/PhysRevLett.115.050501).
- [11] F. G. Brandao and A. W. Harrow. Product-State Approximations to Quantum Ground States. In *Proc. ACM STOC*, page 871, 2013. DOI: [10.1145/2488608.2488719](https://doi.org/10.1145/2488608.2488719).
- [12] F. G. Brandao and A. W. Harrow. Quantum de Finetti Theorems Under Local Measurements with Applications. In *Proc. ACM STOC*, page 861, 2013. DOI: [10.1145/2488608.2488718](https://doi.org/10.1145/2488608.2488718).
- [13] M. Braverman. Interactive Information Complexity. In *Proc. ACM STOC*, pages 505–524, 2012. DOI: [10.1145/2213977.2214025](https://doi.org/10.1145/2213977.2214025).
- [14] M. Christandl and A. Winter. Squashed Entanglement: An Additive Entanglement Measure. *J. Math. Phys.*, 45:829–840, 2004. DOI: [10.1063/1.1643788](https://doi.org/10.1063/1.1643788).
- [15] T. Cooney, C. Hirche, C. Morgan, J. P. Olson, K. P. Seshadreesan, and M. M. Wilde. Operational meaning of quantum measures of recovery. 2015. [arXiv: 1512.05324](https://arxiv.org/abs/1512.05324).
- [16] N. Datta, M.-H. Hsieh, and J. Oppenheim. An Upper Bound on the Second Order Asymptotic Expansion for the Quantum Communication Cost of State Redistribution. 2014. [arXiv: 1409.4352](https://arxiv.org/abs/1409.4352).
- [17] I. Devetak and J. Yard. Exact cost of redistributing multipartite quantum states. *Phys. Rev. Lett.*, 100:230501, 2008. DOI: [10.1103/PhysRevLett.100.230501](https://doi.org/10.1103/PhysRevLett.100.230501).
- [18] O. Fawzi and R. Renner. Quantum Conditional Mutual Information and Approximate Markov Chains. *Commun. Math. Phys.*, 340(2):575–611, 2015. DOI: [10.1007/s00220-015-2466-x](https://doi.org/10.1007/s00220-015-2466-x).
- [19] M. Hayashi and M. Tomamichel. Correlation Detection and an Operational Interpretation of the Rényi Mutual Information. 2014. [arXiv: 1408.6894](https://arxiv.org/abs/1408.6894).
- [20] M. Junge, R. Renner, D. Sutter, M. M. Wilde, and A. Winter. Universal recovery from a decrease of quantum relative entropy. 2015. [arXiv: 1509.07127](https://arxiv.org/abs/1509.07127).
- [21] N. Killoran. *Entanglement Quantification and Quantum Benchmarking of Optical Communication Devices*. PhD thesis, University of Waterloo, 2012.
- [22] I. H. Kim. *Conditional Independence in Quantum Many-Body Systems*. PhD thesis, California Institute of Technology, 2013.
- [23] I. H. Kim. On the Informational Completeness of Local Observables. 2014. [arXiv: 1405.0137](https://arxiv.org/abs/1405.0137).
- [24] A. Kitaev and J. Watrous. Parallelization, amplification, and exponential time simulation of quantum interactive proof

- systems. In *Proc. ACM STOC*, pages 608–617, 2000. DOI: [10.1145/335305.335387](https://doi.org/10.1145/335305.335387).
- [25] R. König, R. Renner, and C. Schaffner. The Operational Meaning of Min- and Max-Entropy. *IEEE Trans. on Inf. Theory*, 55(9):4337–4347, 2009. DOI: [10.1109/TIT.2009.2025545](https://doi.org/10.1109/TIT.2009.2025545).
- [26] K. Li and A. Winter. Squashed Entanglement, k-Extendibility, Quantum Markov Chains, and Recovery Maps. 2014. [arXiv: 1410.4184](https://arxiv.org/abs/1410.4184).
- [27] E. H. Lieb and M. B. Ruskai. Proof of the Strong Subadditivity of Quantum-Mechanical Entropy. *J. Math. Phys.*, 14(12):1938, 1973. DOI: [10.1063/1.1666274](https://doi.org/10.1063/1.1666274).
- [28] M. Müller-Lennert, F. Dupuis, O. Szechr, S. Fehr, and M. Tomamichel. On Quantum Rényi Entropies: A New Generalization and Some Properties. *J. Math. Phys.*, 54(12):122203, 2013. DOI: [10.1063/1.4838856](https://doi.org/10.1063/1.4838856).
- [29] M. Ohya and D. Petz. *Quantum Entropy and Its Use*. Springer, 1993.
- [30] M. Piani. Hierarchy of Efficiently Computable and Faithful Lower Bounds to Quantum Discord. 2015. [arXiv: 1501.06855](https://arxiv.org/abs/1501.06855).
- [31] D. Poulin and M. B. Hastings. Markov Entropy Decomposition: A Variational Dual for Quantum Belief Propagation. *Phys. Rev. Lett.*, 106(8):080403, 2011. DOI: [10.1103/PhysRevLett.106.080403](https://doi.org/10.1103/PhysRevLett.106.080403).
- [32] K. P. Seshadreesan and M. M. Wilde. Fidelity of Recovery, Geometric Squashed Entanglement, and Measurement Recoverability. *Phys. Rev. A*, 92(4):042321, 2015. DOI: [10.1103/PhysRevA.92.042321](https://doi.org/10.1103/PhysRevA.92.042321).
- [33] D. Sutter, O. Fawzi, and R. Renner. Universal Recovery Map for Approximate Markov Chains. *Proc. Roy. Soc. A*, 472(2186), 2016. DOI: [10.1098/rspa.2015.0623](https://doi.org/10.1098/rspa.2015.0623).
- [34] D. Sutter, M. Tomamichel, and A. W. Harrow. Strengthened Monotonicity of Relative Entropy via Pinched Petz Recovery Map. 2015. [arXiv: 1507.00303](https://arxiv.org/abs/1507.00303).
- [35] B. Swingle and I. H. Kim. Reconstructing Quantum States from Local Data. *Phys. Rev. Lett.*, 113(26):260501, 2014. DOI: [10.1103/PhysRevLett.113.260501](https://doi.org/10.1103/PhysRevLett.113.260501).
- [36] M. Tomamichel. *Quantum Information Processing with Finite Resources — Mathematical Foundations*. Springer. [arXiv: 1504.00233](https://arxiv.org/abs/1504.00233).
- [37] M. Tomamichel, R. Colbeck, and R. Renner. A Fully Quantum Asymptotic Equipartition Property. *IEEE Trans. on Inf. Theory*, 55(12):5840–5847, 2009. DOI: [10.1109/TIT.2009.2032797](https://doi.org/10.1109/TIT.2009.2032797).
- [38] M. Tomamichel, R. Colbeck, and R. Renner. Duality Between Smooth Min- and Max-Entropies. *IEEE Trans. on Inf. Theory*, 56(9):4674–4681, 2010. DOI: [10.1109/TIT.2010.2054130](https://doi.org/10.1109/TIT.2010.2054130).
- [39] D. Touchette. Quantum Information Complexity and Amortized Communication. 2014. [arXiv: 1404.3733](https://arxiv.org/abs/1404.3733).
- [40] A. Uhlmann. The Transition Probability for States of Star-Algebras. *Ann. Phys.*, 497(4):524–532, 1985.
- [41] J. Watrous. Theory of Quantum Information, Lecture Notes, 2011. Available online: <https://cs.uwaterloo.ca/~watrous/quant-info/>.
- [42] J. Watrous. Simpler Semidefinite Programs for Completely Bounded Norms. *Chicago J. of Th. Comp. Sci.*, 2013(8):1–19, 2013. Available online: <http://cjtcs.cs.uchicago.edu/articles/2013/8/contents.html>.
- [43] M. M. Wilde. Multipartite Quantum Correlations and Local Recoverability. *Proc. Roy. Soc. A*, 471(2177), 2015. DOI: [10.1098/rspa.2014.0941](https://doi.org/10.1098/rspa.2014.0941).
- [44] M. M. Wilde. Recoverability in Quantum Information Theory. *Proc. Roy. Soc. A*, 471(2182), 2015. DOI: [10.1098/rspa.2015.0338](https://doi.org/10.1098/rspa.2015.0338).
- [45] M. M. Wilde, A. Winter, and D. Yang. Strong Converse for the Classical Capacity of Entanglement-Breaking and Hadamard Channels via a Sandwiched Rényi Relative Entropy. *Commun. Math. Phys.*, 331(2):593–622, 2014. DOI: [10.1007/s00220-014-2122-x](https://doi.org/10.1007/s00220-014-2122-x).
- [46] J. T. Yard and I. Devetak. Optimal Quantum Source Coding with Quantum Side Information at the Encoder and Decoder. *IEEE Trans. on Inf. Theory*, 55:5339–5351, 2009. DOI: [10.1109/TIT.2009.2030494](https://doi.org/10.1109/TIT.2009.2030494).
- [47] L. Zhang. Conditional Mutual Information and Commutator. *Int. J. Theor. Phys.*, 52:2112–2117, 2013. DOI: [10.1007/s10773-013-1505-7](https://doi.org/10.1007/s10773-013-1505-7).