Communications in
**Mathematical
Physics**

CrossMark

Relative Entropy Bounds on Quantum, Private and Repeater Capacities

Matthias Christandl, Alexander Müller-Hermes

QMATH, Department of Mathematical Sciences, University of Copenhagen, Universitetsparken 5, 2100, Copenhagen, Denmark. E-mail: christandl@math.ku.dk; muellerh@posteo.net; muellerh@math.ku.dk

Abstract: We find a strong-converse bound on the private capacity of a quantum channel assisted by unlimited two-way classical communication. The bound is based on the max-relative entropy of entanglement and its proof uses a new inequality for the sandwiched Rényi divergences based on complex interpolation techniques. We provide explicit examples of quantum channels where our bound improves upon both the transposition bound (on the quantum capacity assisted by classical communication) and the bound based on the squashed entanglement. As an application, we study a repeater version of the private capacity assisted by classical communication and provide an example of a quantum channel with high private capacity but negligible private repeater capacity.

Contents

1. Introduction

The goal of Shannon theory [1] is to quantify the amount of information that can be reliably transmitted using many copies of a communication channel. To protect the information from errors induced by the channel, particular coding schemes may be applied. For a given class of coding schemes a capacity can be defined quantifying the optimal rate of reliable information transmission achievable using schemes from the class. In quantum Shannon theory there are many different capacities describing relevant coding scenarios where certain types of classical or quantum assistance are allowed. Here we are interested in capacities where arbitrary classical communication between the two communicating parties is allowed to assist the transmission of quantum or private information.

For a quantum channel $T : \mathcal{M}_{d_A} \rightarrow \mathcal{M}_{d_B}$ we denote by $\mathcal{Q}_\leftrightarrow(T)$ ($\mathcal{P}_\leftrightarrow(T)$) its quantum (private) capacity assisted by two-way classical communication. While it is true that $\mathcal{P}_\leftrightarrow(T)$ is an upper bound on $\mathcal{Q}_\leftrightarrow(T)$ it is important to have simpler upper bounds in terms of single-letter quantities only depending on the quantum channel T. Not many such bounds on $\mathcal{Q}_\leftrightarrow$ and $\mathcal{P}_\leftrightarrow$ are known: In [2] the squashed entanglement of a quantum channel has been defined and shown to be an upper bound on $\mathcal{P}_\leftrightarrow$ (and therefore also on $\mathcal{Q}_\leftrightarrow$). The transposition bound (see [3]) has been shown to be a strong-converse bound on $\mathcal{Q}_\leftrightarrow$ in [4]. Finally, in [5] the entanglement cost of a quantum channel has been defined and shown to be a strong-converse bound on $\mathcal{Q}_\leftrightarrow$.

For particular classes of channels other upper bounds are known. Recently, the class of teleportation covariant channels has received much attention in this context [6–11]. Special cases of such channels have been considered in [12], and recently more relevant examples have been identified. In particular, this family contains the Gaussian channels in infinite dimensions as an important subclass [6]. We will be interested mostly in the finite-dimensional case. For a finite-dimensional teleportation covariant channel T the capacity $\mathcal{P}_\leftrightarrow(T)$ is equal to the distillable key of the Choi–Jamiolkowski state C_T [13] corresponding to the channel (see teleportation stretching [6] for a generalization of these arguments to the case of infinite-dimensional quantum channels). Using that the relative entropy of entanglement E_R is an upper bound on the distillable key [14] any finite-dimensional teleportation covariant channel fulfills the bound (see [6])

$$\mathcal{P}_\leftrightarrow(T) = \mathcal{K}_\leftrightarrow(C_T) \le E_R(C_T) \tag{1}$$

and this is also a strong-converse bound (see [9]). It is still an open problem whether a similar bound based on the relative entropy of entanglement (possibly involving an optimization over the input state of the partial channel) holds for arbitrary quantum channels T.

In this article we establish an upper bound on $\mathcal{P}_\leftrightarrow$ for arbitrary quantum channels in terms of the max-relative entropy of entanglement. Given a quantum channel $T : \mathcal{M}_{d_A} \rightarrow \mathcal{M}_{d_B}$ its max-relative entropy of entanglement is defined as

$$E_{\max}(T) = \sup\{E_{\max}^{A':B}\left(T^{A\rightarrow B}\left(\rho_{A'A}\right)\right) \; : \; \rho_{A'A} \in \mathcal{D}\left(\mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_A}\right), d_{A'} \in \mathbb{N}\}. \tag{2}$$

Here $E_{\max}^{A':B}$ denotes the max-relative entropy of entanglement of states [15,16]. Our paper is structured as follows:

- In Sect. 3 we use complex interpolation techniques to prove a new inequality (the "data-processed triangle inequality") for the sandwiched α-Rényi divergence (see Sect. 2.1 for a definition).

- Using the data-processed triangle inequality we show in Sect. 4 that for any quantum channel $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ the quantity $E_{\max}(T)$ is a strong-converse bound on $\mathcal{P}_{\leftrightarrow}(T)$.
- In Sect. 5.1 we show that $E_{\max}(T)$ is non-lockable (see Corollary 5.1 for the precise statement). We use this feature of our bound in Sect. 6.1 to give examples of channels, where our bound improves upon the previously known bounds (transposition bound, squashed entanglement bound and entanglement cost).
- In Sect. 5.2 we give a weaker upper bound on $\mathcal{P}_{\leftrightarrow}(T)$ for any quantum channel $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ that is slightly easier to evaluate than our original $E_{\max}$ bound. As an application we then study a repeater version of the private capacity in Sect. 6.2, where the communicating parties can use an intermediate repeater station to perform private communication. We show that there are quantum channels T which have a high private capacity, but where the repeated private capacity can be arbitrarily close to zero. This is the channel version of a result demonstrated in [17] where states connecting the three parties are given.
- In the Appendix we give an example of a quantum channel that cannot be implemented via an LOCC-protocol from any state preparable by a single use of the channel (see Definition A.1). This property is needed to obtain a bound similar to (1) based on the relative entropy of entanglement using the arguments of [6].

2. Preliminaries

In the following we denote the complex $d \times d$-matrices by $\mathcal{M}_d$ and the cone of positive matrices by $\mathcal{M}_d^+$. The $d \times d$ identity matrix is denoted by $\mathbb{1}_d$. The set of $d \times d$ quantum states (i.e. positive $d \times d$ matrices with trace 1) is called $\mathcal{D}_d = \mathcal{D}(\mathbb{C}^d)$. Pure states will be denoted as projectors using the notation $|\psi\rangle\langle\psi| \in \mathcal{D}_d$ for $|\psi\rangle \in \mathbb{C}^d$ with $\langle\psi|\psi\rangle = 1$. On multipartite systems we will often use indices $A, B, \ldots$ to indicate the different tensor factors. For example we would write $\rho_{ABC} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_C})$ for a tripartite state. We use the common notation of omitting indices to denote partial traces (i.e. the state ρ_A would be the marginal of ρ_{ABC} on the A system). For general linear maps $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ we write $T^{A \to B}(\rho_{AA'}) \in \mathcal{D}(\mathbb{C}^{d_B} \otimes \mathbb{C}^{d_{A'}})$ to denote its partial application to the A system of the state $\rho_{AA'}$. In this sense the Choi matrix [13] of a linear map $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ is denoted by

$$C_T = T^{A \to B}(\omega_{A'A}), \tag{3}$$

where $\omega_{A'A} \in \mathcal{D}(\mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_A})$ for $d_A = d_{A'}$ denotes the maximally entangled state in the computational basis (i.e. $\omega_{A'A} = |\Omega_{A'A}\rangle\langle\Omega_{A'A}|$ for $|\Omega_{A'A}\rangle = \frac{1}{\sqrt{d_A}} \sum_{i=1}^{d_A} |i_{A'} i_A\rangle$). We will also use the notation $\omega_d \in \mathcal{D}(\mathbb{C}^d \otimes \mathbb{C}^d)$ to denote this state in the cases where the concrete systems are not important. Most linear maps we will use are quantum channels (i.e. trace-preserving and completely positive [13]). A well-known example of a positive, but not completely-positive, map is the transposition $\vartheta_d : \mathcal{M}_d \to \mathcal{M}_d$ given by $\vartheta_d(X) = X^T$ in the computational basis. We will also use the notation ϑ_A to denote the partial transposition on a particular system (named A in this case).

2.1. Sandwiched α-Rényi divergences. For quantum states $\rho, \sigma \in \mathcal{D}(\mathbb{C}^d)$ and a parameter $\alpha \in (1, \infty)$, the *sandwiched α-Rényi divergence* [18,19] is defined as

$$D_\alpha\left(\rho\|\sigma\right) = \begin{cases} \frac{1}{\alpha-1} \log\left(\operatorname{tr}\left[\left(\sigma^{\frac{1-\alpha}{2\alpha}} \rho \sigma^{\frac{1-\alpha}{2\alpha}}\right)^\alpha\right]\right), & \text{if } \operatorname{supp}[\rho] \subseteq \operatorname{supp}[\sigma] \\ +\infty, & \text{otherwise.} \end{cases} \tag{4}$$

In [18] it has been shown that the limiting cases $\alpha = 1$ and $\alpha = \infty$ of D_α coincide with quantities studied before: In the limit $\alpha \to 1$ we have

$$D_\alpha\left(\rho\|\sigma\right) \to D\left(\rho\|\sigma\right) = \operatorname{tr}\left[\rho\left(\log(\rho) - \log(\sigma)\right)\right]$$

which is the usual relative entropy [20]. We will sometimes write D_1 to denote the relative entropy. Taking the limit $\alpha \to \infty$ gives $D_\alpha\left(\rho\|\sigma\right) \to D_{\max}\left(\rho\|\sigma\right)$ which is the max-relative entropy [15]. For quantum states $\rho, \sigma \in \mathcal{D}\left(\mathbb{C}^d\right)$ this quantity can be defined in two equivalent ways as

$$D_{\max}\left(\rho\|\sigma\right) = \inf\{\lambda \in \mathbb{R}^+ : \rho \le 2^\lambda \sigma\} = \begin{cases} \log\left(\|\sigma^{-\frac{1}{2}} \rho \sigma^{-\frac{1}{2}}\|_\infty\right) & \text{if } \operatorname{supp}[\rho] \subseteq \operatorname{supp}[\sigma] \\ +\infty, & \text{otherwise} \end{cases} \tag{5}$$

using the convention $\inf \emptyset = +\infty$.

In [21] it has been noted that the sandwiched α-Rényi divergence D_α (see (4)) for $\alpha > 1$ can be written in terms of a non-commutative $L_{\alpha,\sigma}$-norm $\|\cdot\|_{\alpha,\sigma}$ defined as

$$\|X\|_{\alpha,\sigma} = \operatorname{tr}\left[\left|\sigma^{\frac{1}{2\alpha}} X \sigma^{\frac{1}{2\alpha}}\right|^\alpha\right]^{\frac{1}{\alpha}}$$

for any $X \in \mathcal{M}_d$ and $\sigma \in \mathcal{M}_d^+$. With the function $\Gamma_\sigma : \mathcal{M}_d \to \mathcal{M}_d$ given by $\Gamma_\sigma(X) = \sigma^{1/2} X \sigma^{1/2}$ we can write

$$D_\alpha\left(\rho\|\sigma\right) = \frac{1}{\alpha-1} \log\left(\|\Gamma_\sigma^{-1}\left(\rho\right)\|_{\alpha,\sigma}^\alpha\right) \tag{6}$$

for any quantum states $\rho, \sigma \in \mathcal{D}\left(\mathbb{C}^d\right)$ with $\operatorname{supp}\left(\rho\right) \subseteq \operatorname{supp}\left(\sigma\right)$ using the Moore-Penrose pseudo-inverse [22] in the case where σ is not full-rank.

For a linear map $L : \mathcal{M}_{d_1} \to \mathcal{M}_{d_2}$ we will use norms of the form

$$\|L\|_{(p,\sigma)\to(q,\sigma')} = \sup_{X \in \mathcal{M}_{d_1}} \frac{\|L(X)\|_{q,\sigma'}}{\|X\|_{p,\sigma}}, \tag{7}$$

which are the operator norms of the operator L as a mapping from the space $(\mathcal{M}_{d_1}, \|\cdot\|_{p,\sigma})$ to $(\mathcal{M}_{d_2}, \|\cdot\|_{q,\sigma'})$. For $\sigma = \mathbb{1}_{d_1}$ and $\sigma' = \mathbb{1}_{d_2}$ the above definition gives the usual $p \to q$-norms and we will use the common notation $\|\cdot\|_{p\to q}$ in this case. The main technical tool we will use, is the following non-commutative Riesz–Thorin-type theorem. It should be noted that similar interpolation theorems have a long history (see [23]).

Theorem 2.1 (Riesz–Thorin Theorem for $L_{p,\sigma}$ spaces [21]). *Let* $L : \mathcal{M}_{d_1} \to \mathcal{M}_{d_2}$ *be a linear map. For* $1 \le p_0 \le p_1 \le \infty$ *and* $1 \le q_0 \le q_1 \le \infty$ *and* $\theta \in (0, 1)$ *we define* p_θ *via*

$$\frac{1}{p_\theta} = \frac{\theta}{p_0} + \frac{1-\theta}{p_1}.$$

and q_θ *analogous. Then for positive definite matrices* $\sigma \in \mathcal{M}_{d_1}^+$ *and* $\sigma' \in \mathcal{M}_{d_2}^+$ *we have*

$$\|L\|_{(p_\theta,\sigma)\to(q_\theta,\sigma')} \le \|L\|_{(p_0,\sigma)\to(q_0,\sigma')}^\theta \|L\|_{(p_1,\sigma)\to(q_1,\sigma')}^{1-\theta}.$$

A consequence of the previous theorem is the monotonicity of the sandwiched α-Rényi divergences under quantum channels for $\alpha > 1$ (see [21]), i.e. the inequality

$$D_\alpha\left(T(\rho)\|T(\sigma)\right) \leq D_\alpha\left(\rho\|\sigma\right) \tag{8}$$

for any quantum channel $T : \mathcal{M}_{d_1} \to \mathcal{M}_{d_2}$ and quantum states $\rho, \sigma \in \mathcal{D}_{d_A}$. Inequality (8) also holds for trace-preserving positive maps T as shown in [24] and for quantum channels when $\alpha \geq \frac{1}{2}$ [18,25].

2.2. α-Relative entropies of entanglement and related measures.
For any $\alpha \geq 1$ we can introduce an α-relative entropy of entanglement generalizing the usual relative entropy of entanglement (also introduced recently in [9]).

Definition 2.1 (α-Relative Entropy of Entanglement). For a bipartite quantum state $\rho_{AB} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$ we define the α-relative entropy of entanglement as

$$E_\alpha^{A:B}(\rho_{AB}) = \min\{D_\alpha(\rho_{AB}\|\sigma_{AB}) \ : \ \sigma_{AB} \in \mathrm{Sep}_{A:B}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}\right)\}$$

where $\mathrm{Sep}_{A:B}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}\right)$ denotes the set of separable states w.r.t. the bipartition $A : B$.

Using the convergence of D_α it is clear that $E_\alpha^{A:B} \to E_R^{A:B}$ as $\alpha \to 1$ for the relative entropy of entanglement denoted by E_R. Similarly we can take the limit $\alpha \to \infty$ and obtain the max-relative entropy of entanglement[1]

$$E_{\max}^{A:B}(\rho_{AB}) = \min\{D_{\max}(\rho_{AB}\|\sigma_{AB}) \ : \ \sigma_{AB} \in \mathrm{Sep}_{A:B}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}\right)\},$$

which has been studied in [15,16,27]. For any $\alpha \geq 1$ the α-relative entropy of entanglement can be used to quantify the transmission of entanglement over a quantum channel. We will focus on the case $\alpha = \infty$ and the following quantity (also recently introduced in [9]):

Definition 2.2 (max-relative entropy of entanglement of a quantum channel). For a quantum channel $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ we define the max-relative entropy of entanglement of T as

$$E_{\max}(T) = \sup\{E_{\max}^{A':B}\left(T^{A \to B}(\rho_{A'A})\right) \ : \ \rho_{A'A} \in \mathcal{D}\left(\mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_A}\right), d_{A'} \in \mathbb{N}\}. \tag{9}$$

Using quasi-convexity of $D_{\max}$ (see [15, Lemma 9]) and the Schmidt-decomposition of pure quantum states it is not hard to show, that the dimension $d_{A'}$ appearing in the supremum can be chosen as the input dimension of the quantum channel. More specifically, for any quantum channel $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ we get the following equivalent expression

$$E_{\max}(T) = \max\{E_{\max}^{A':B}\left(T^{A \to B}(|\psi_{A'A}\rangle\langle\psi_{A'A}|)\right) \ : \ |\psi_{A'A}\rangle\langle\psi_{A'A}| \in \mathcal{D}\left(C^{d_{A'}} \otimes \mathbb{C}^{d_A}\right) \text{ for } d_{A'} = d_A\}.$$

In particular this shows that the max-relative entropy of a quantum channel is well-defined and we will use a max instead of the sup in (9) to indicate that the optimum is attained.

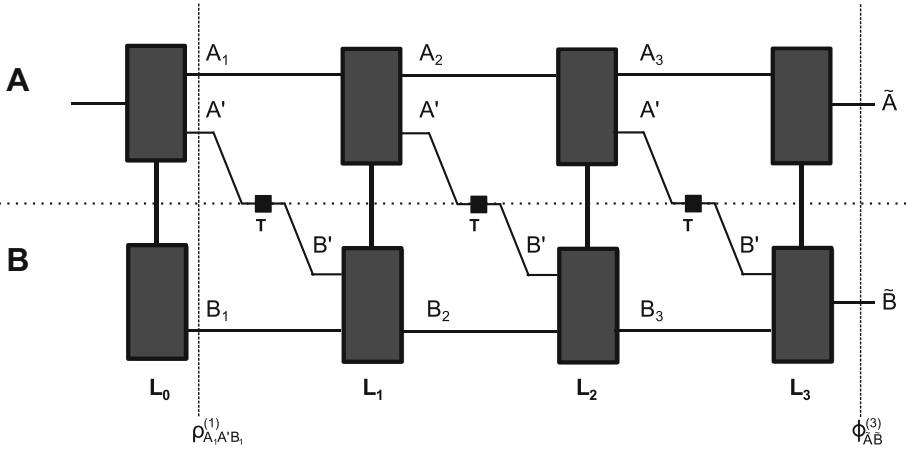[1] Also known as log-robustness [26].

Fig. 1. Coding scheme assisted by classical communication (cf. Definition 2.3) in the case of $m = 3$ uses of the channel $T : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{B'}}$. Here L_0 denotes an LOCC-operation used to create the separable initial state $\rho^{(1)}_{A_1 A' B_1}$

2.3. Quantum capacities assisted by classical communication. A quantum channel on bipartite systems $L : \mathcal{M}_{d_A} \otimes \mathcal{M}_{d_B} \to \mathcal{M}_{d_{A'}} \otimes \mathcal{M}_{d_{B'}}$ is called implementable via local operations and classical communications (w.r.t. bipartitions $A : B$ and $A' : B'$ of the input and output systems, respectively) if it can be written as a composition of any number of channels $L_{A_q : B_q \to A'_q A'_c : B'_q B'_c}$ of the following form ($X_{A_q B_q} \in \mathcal{M}_{d_{A_q}} \otimes \mathcal{M}_{d_{B_q}}$):

$$L_{A_q : B_q \to A'_q A'_c : B'_q B'_c}(X_{A_q B_q}) = \sum_{i,j} (K_i^A \otimes K_j^B) X_{A_q B_q} (K_i^A \otimes K_j^B)^\dagger \otimes |j\rangle\langle j|_{A'_c} \otimes |i\rangle\langle i|_{B'_c}.$$

(10)

Here $K_i^A : \mathbb{C}^{|A_q|} \to \mathbb{C}^{|A'_q|}$ and $K_j^B : \mathbb{C}^{|B_q|} \to \mathbb{C}^{|B'_q|}$ ($i \in I$, $j \in J$) are Kraus operators of quantum channels mapping system A_q to A'_q and system B_q to B'_q respectively (i.e. $\sum_i (K_i^A)^\dagger K_i^A = \mathbb{1}_{A_q}$ and $\sum_j (K_j^B)^\dagger K_j^B = \mathbb{1}_{B_q}$), and $|j\rangle_{A'_c}$ and $|i\rangle_{B'_c}$ are orthonormal bases belonging to (effectively classical) systems A_c and B_c of dimension $|J|$ and $|I|$ (see [28] for more details). In the following we will call a quantum channel implementable via local operations and classical communications simply an LOCC-operation.

We can now define coding schemes assisted by classical communication:

Definition 2.3 (*Coding schemes assisted by classical communication*). Let $T : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{B'}}$ be a quantum channel. A coding scheme assisted by classical communication with m uses of the channel T is given by a separable initial state

$$\rho^{(1)}_{A_1 A' B_1} \in \mathrm{Sep}_{A_1 A' : B_1}\left(\mathbb{C}^{d_{A_1} d_{A'}} \otimes \mathbb{C}^{d_{B_1}}\right)$$

and a set of LOCC-operations $\{L_i\}_{i=1}^m$ (see also Fig. 1). Here

$$L_i : \mathcal{M}_{d_{A_i}} \otimes \mathcal{M}_{d_{B'}} \otimes \mathcal{M}_{d_{B_i}} \to \mathcal{M}_{d_{A_{i+1}}} \otimes \mathcal{M}_{d_{A'}} \otimes \mathcal{M}_{d_{B_{i+1}}}$$

for each $i \in \{1, \dots, m-1\}$ and

$$L_m : \mathcal{M}_{d_{A_m}} \otimes \mathcal{M}_{d_{B'}} \otimes \mathcal{M}_{d_{B_m}} \to \mathcal{M}_{d_{\tilde{A}}} \otimes \mathcal{M}_{d_{\tilde{B}}}$$

are LOCC w.r.t. the bipartition into A and B systems for arbitrary dimensions d_{A_i}, d_{B_i}, $d_{\tilde{A}}$, $d_{\tilde{B}}$. The output state of the coding scheme will be denoted by

$$\phi_{\tilde{A}\tilde{B}}^{(m)} = L_m \circ \prod_{i=1}^{m-1} \left(T^{A' \to B'} \circ L_i \right) \circ T^{A' \to B'} \left(\rho_{A_1 A' B_1}^{(1)} \right).$$

We will first state the definition of the quantum capacity assisted by two-way classical communication. In the presence of unlimited classical communication we can use quantum teleportation [29] to turn any entanglement generation protocol into a quantum communication protocol. Therefore, we can define the quantum capacity assisted by two-way communication in terms of entanglement generation.

Definition 2.4 (*Entanglement generation assisted by classical communication*). Given a quantum channel $T : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{B'}}$ consider a coding scheme assisted by classical communication with m channel uses (as in Definition 2.3) given by LOCC-operations $\{L_i\}_{i=1}^{m+1}$, initial state $\rho_{A_1 A' B_1}^{(1)}$ and output state $\phi_{\tilde{A}\tilde{B}}^{(m)} \in \mathcal{D}\left(\mathbb{C}^{d_{\tilde{A}}} \otimes \mathbb{C}^{d_{\tilde{B}}}\right)$. Such a coding scheme is called an (n, m, ϵ)-coding scheme for entanglement generation assisted by classical communication iff the output dimensions fulfill $d_{\tilde{A}} = d_{\tilde{B}} = 2^n$ and the output state satisfies

$$\epsilon = \frac{1}{2} \| \phi_{\tilde{A}\tilde{B}}^{(m)} - \omega_{2^n} \|_1.$$

Definition 2.5 (*Quantum capacity assisted by classical communication*). We call $R \in \mathbb{R}^+$ an achievable rate for quantum communication over the channel T assisted by classical communication iff for each $\nu \in \mathbb{N}$ there exists a $(n_\nu, m_\nu, \varepsilon_\nu)$-coding scheme for entanglement generation assisted by classical communication (as in Definition 2.4) with $m_\nu \to \infty$ as $\nu \to \infty$ such that $R = \lim_{\nu \to \infty} \frac{n_\nu}{m_\nu}$ and $\lim_{\nu \to \infty} \varepsilon_\nu = 0$. The quantum capacity of T assisted by classical two-way communication $\mathcal{Q}_{\leftrightarrow}(T)$ is defined to be the supremum of all such achievable rates.

In a similar way we can define the private capacity assisted by classical two-way communication. It has been shown in [14] that the tasks of private communication using a quantum channel and public communication is equivalent to the task of distilling private states using a coding scheme assisted by classical communication (see also [9]). We will begin by defining these states:

Definition 2.6 (*Private states* [14]). A quantum state

$$\gamma_{A_k B_k A_s B_s} \in \mathcal{D}\left(\mathbb{C}^{d_{A_k}} \otimes \mathbb{C}^{d_{B_k}} \otimes \mathbb{C}^{d_{A_s}} \otimes \mathbb{C}^{d_{B_s}}\right)$$

with $d_{A_k} = d_{B_k} = K$ and $d_{A_s} = d_{B_s}$ is called a private state with K-dimensional key part iff it is of the form

$$\gamma_{A_k B_k A_s B_s} = U_{A_k B_k A_s B_s}^{\text{tw}} \left(\omega_{A_k B_k} \otimes \sigma_{A_s B_s} \right) (U_{A_k B_k A_s B_s}^{\text{tw}})^{\dagger}$$

for some quantum state $\sigma_{A_s B_s} \in \mathcal{D}\left(\mathbb{C}^{d_{A_s}} \otimes \mathbb{C}^{d_{B_s}}\right)$ where we applied a twisting unitary of the form

$$U_{A_k B_k A_s B_s}^{\text{tw}} = \sum_{i=1}^{d_{A_k}} \sum_{j=1}^{d_{B_k}} |i\rangle\langle i|_{A_k} \otimes |j\rangle\langle j|_{B_k} \otimes U_{A_s B_s}^{ij}$$

with $U_{A_s B_s}^{ij} \in \mathcal{U}_{d_{A_s} d_{B_s}}$ unitary for any i, j. The systems A_k, B_k are called the key part and A_s, B_s the shield part of the private state.

It can be shown (see [14]) that any private state with K-dimensional key part held by two parties A and B can be used to generate at least $\log_2(K)$ secret bits shared between the two parties (protected from any eavesdropper who might possess the purification of the state). Note that in the above definition there might be more than $\log_2(K)$ secret bits obtainable (i.e. the private state is not necessarily irreducible [14]).

Now we can define the private capacity assisted by classical communication as a private state generation capacity.

Definition 2.7 (*Coding scheme for private state generation assisted by classical communication*). Given a quantum channel $T : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{B'}}$ consider a coding scheme assisted by classical communication with m channel uses (as in Definition 2.3) given by LOCC-operations $\{L_i\}_{i=1}^{m+1}$, initial state $\rho_{A_1 A' B_1}^{(1)}$ and output state $\phi_{\tilde{A}\tilde{B}}^{(m)} \in \mathcal{D}\left(\mathbb{C}^{d_{\tilde{A}}} \otimes \mathbb{C}^{d_{\tilde{B}}}\right)$. Such a coding scheme is called a (k, m, ϵ)-coding scheme for private state generation assisted by classical communication iff the output dimensions factorize into $d_{\tilde{A}} = d_{A_k} d_{A_s}$ and $d_{\tilde{B}} = d_{B_k} d_{B_s}$ for $d_{A_k} = d_{B_k} = 2^k$ and $d_{A_s} = d_{B_s}$, and the output state satisfies

$$\epsilon = \frac{1}{2}\|\phi_{\tilde{A}\tilde{B}}^{(m)} - \gamma_{A_k B_k A_s B_s}\|_1.$$

for a private state $\gamma_{A_k B_k A_s B_s} \in \mathcal{D}\left(\mathbb{C}^{d_{\tilde{A}}} \otimes \mathbb{C}^{d_{\tilde{B}}}\right)$ with 2^k-dimensional key part.

Definition 2.8 (*Private capacity assisted by classical communication*). We call $R \in \mathbb{R}^+$ an achievable rate for private communication over the channel T assisted by classical communication iff for each $\nu \in \mathbb{N}$ there exists a $(k_\nu, m_\nu, \varepsilon_\nu)$-coding scheme for private state generation assisted by classical communication (as in Definition 2.7) with $m_\nu \to \infty$ as $\nu \to \infty$ such that $R = \lim_{\nu\to\infty} \frac{k_\nu}{m_\nu}$ and $\lim_{\nu\to\infty} \varepsilon_\nu = 0$. The private quantum capacity of T assisted by classical two-way communication $\mathcal{P}_\leftrightarrow(T)$ is defined to be the supremum of all such achievable rates.

In the remaining part of this section we will discuss some general upper and strong-converse bounds on $\mathcal{Q}_\leftrightarrow$ and $\mathcal{P}_\leftrightarrow$. Recall that an upper bound $B \geq 0$ on either $\mathcal{Q}_\leftrightarrow$ or $\mathcal{P}_\leftrightarrow$ is called a *strong converse bound* iff for any sequence of $(n_\nu, m_\nu, \varepsilon_\nu)$-coding schemes (for $\nu \in \mathbb{N}$) leading to a rate $R = \lim_{\nu\to\infty} \frac{n_\nu}{m_\nu} > B$ the error fulfills $\epsilon_\nu \to 1$ as $\nu \to \infty$. We will start with the transposition bound (originally introduced in [3]), based on the matrix transposition $\vartheta_d : \mathcal{M}_d \to \mathcal{M}_d$, i.e. $\vartheta_d(X) = X^T$ in any fixed basis.

Theorem 2.2 (Transposition bound [4]). *For any quantum channel $T : \mathcal{M}_{d_1} \to \mathcal{M}_{d_2}$ we have*

$$\mathcal{Q}_\leftrightarrow(T) \leq \log_2\left(\|\vartheta_{d_2} \circ T\|_\diamond\right)$$

and the above bound is a strong-converse bound.

Another bound is based on the squashed entanglement introduced in [30,31]. Recall the definition of the quantum conditional mutual information of a tripartite quantum state $\rho_{ABE} \in \mathcal{D}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}\right)$ given by

$$I(A; B|E)_{\rho_{ABE}} = S(\rho_{AE}) + S(\rho_{BE}) - S(\rho_E) - S(\rho_{ABE})$$

where $S(\sigma) = -\text{tr}\left(\sigma \log_2(\sigma)\right)$ denotes the von-Neumann entropy of a quantum state σ. Given a bipartite quantum state $\rho_{AB} \in \mathcal{D}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}\right)$ a quantum state $\sigma_{ABE} \in \mathcal{D}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}\right)$ is called an extension of ρ_{AB} iff $\sigma_{AB} = \rho_{AB}$. For a bipartite quantum state $\rho_{AB} \in \mathcal{D}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}\right)$ the squashed entanglement [30,31] (w.r.t. the bipartition $A : B$) is defined as

$$E_{\text{sq}}^{A:B}(\rho_{AB}) = \frac{1}{2}\inf\{I(A; B|E)_{\sigma_{ABE}} \ : \ \sigma_{ABE} \in \mathcal{D}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_E}\right) \text{ extension of } \rho_{AB}\}$$
(11)

where the dimension $d_E \in \mathbb{N}$ is arbitrary. Now the following bound holds:

Theorem 2.3 (Squashed entanglement of a quantum channel [2]). *For any quantum channel $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ we have*

$$Q_{\leftrightarrow}(T) \leq P_{\leftrightarrow}(T) \leq E_{sq}(T)$$

where $E_{sq}(T) = \sup\{E_{sq}^{A':B}\left(T^{A \to B}(\rho_{A'A})\right) \ : \ \rho_{A'A} \in \mathcal{D}\left(\mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_A}\right)\}$.

To our knowledge it is currently not known, whether $E_{\text{sq}}(T)$ is a strong-converse bound on either $Q_{\leftrightarrow}(T)$ or $P_{\leftrightarrow}(T)$.

Finally, another bound is based on the entanglement cost of a quantum channel [5]. For a bipartite quantum state $\rho_{AB} \in \mathcal{D}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}\right)$ the entanglement of formation is defined as

$$E_F^{A:B}(\rho_{AB}) = \sup_{\{p_i, |\psi_i\rangle_{AB}\}} \sum_i p_i S\left(\psi_i^A\right)$$

where the supremum is over all pure state decompositions $\rho_{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i|_{AB}$ and $\psi_i^A = \text{tr}_B\left(|\psi\rangle\langle\psi|_{AB}\right)$ denotes the reduced density matrix. The entanglement of formation of a quantum channel $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ is defined as

$$E_F(T) = \sup_{\rho_{A'A}} E_F^{A':B}\left(T^{A \to B}(\rho_{A'A})\right)$$

where the supremum is over bipartite states $\rho_{A'A} \in \mathcal{D}\left(\mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_A}\right)$ for any dimension $d_{A'}$. The following theorem has essentially been proven in [5]:

Theorem 2.4 (Entanglement cost of a quantum channel). *For any quantum channel $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ the entanglement cost of T defined as*

$$E_C(T) = \lim_{n \to \infty} \frac{1}{n} E_F\left(T^{\otimes n}\right) \leq E_F(T)$$
(12)

is a strong-converse bound on $P_{\leftrightarrow}(T)$.

It has been shown in [30, Proposition 5] that

$$E_{sq}(\rho_{AB}) \leq E_F(\rho_{AB})$$

for any bipartite quantum state $\rho_{AB} \in \mathcal{D}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}\right)$. Therefore, it follows from Theorem 2.3 that $E_C(T)$ is an upper bound on $P_{\leftrightarrow}(T)$. That $E_C(T)$ is a strong-converse bound on $Q_{\leftrightarrow}(T)$ has been shown in [5, Theorem 24]. The inequality in the previous theorem is [5, Lemma 14]. The fact that $E_C(T)$ is a strong-converse bound on $P_{\leftrightarrow}(T)$ has *not* been shown before, but follows easily from [5]. Specifically, the proof of [5,

Theorem 24] generalizes to the private capacity (possibly with modified error bounds) by simply using that $\mathcal{P}_\leftrightarrow (\mathrm{id}_2) = 1$ is a strong-converse capacity[2] instead of using [5, Corollary 22] in the original proof.

3. The Data-Processed Triangle Inequality

To establish new strong-converse bounds on the quantity $P_\leftrightarrow$ we need the following inequality for the sandwiched α-Rényi divergences (see Definition 4). We call this inequality the data-processed triangle inequality as it resembles a triangle inequality (although with changing distance measure) where some of the involved states are sent through a positive trace-preserving map.

Theorem 3.1 (Data-processed triangle inequality). *Let $P : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ be a positive and trace-preserving map. For any $\alpha \geq 1$ and any quantum states $\rho, \sigma' \in \mathcal{D}\left(\mathbb{C}^{d_A}\right)$ and $\sigma \in \mathcal{D}\left(\mathbb{C}^{d_B}\right)$ we have*

$$D_\alpha\left(P(\rho)\|\sigma\right) \leq D_\alpha(\rho\|\sigma') + D_{\max}(P(\sigma')\|\sigma).$$

Proof. Note that there is nothing to show whenever $\mathrm{supp}\,(\rho) \not\subseteq \mathrm{supp}\,(\sigma')$ or $\mathrm{supp}\,(P(\sigma')) \not\subseteq \mathrm{supp}\,(\sigma)$. If $\mathrm{supp}\,(\rho) \subseteq \mathrm{supp}\,(\sigma')$ holds true, then positivity of P implies $\mathrm{supp}\,(P(\rho)) \subseteq \mathrm{supp}\,(P(\sigma'))$. Hence, $\mathrm{supp}\,(P(\sigma')) \not\subseteq \mathrm{supp}\,(\sigma)$ has to hold whenever both $\mathrm{supp}\,(P(\rho)) \not\subseteq \mathrm{supp}\,(\sigma)$ and $\mathrm{supp}\,(\rho) \subseteq \mathrm{supp}\,(\sigma')$ are fulfilled. We can, therefore, restrict the proof to the cases where all the divergences in the inequality are finite, and w.l.o.g. to the case of full-rank σ and σ'.

Let $\rho, \sigma' \in \mathcal{D}\left(\mathbb{C}^{d_A}\right)$ and $\sigma \in \mathcal{D}\left(\mathbb{C}^{d_B}\right)$ be fixed quantum states with σ and σ' of full rank, and $P : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ a positive trace-preserving map. Consider some fixed $\alpha > 1$. By the definition of the $(\alpha, \sigma') \to (\alpha, \sigma)$-norm (see (7)) we have

$$\|\Gamma_\sigma^{-1} \circ P(\rho)\|_{(\alpha,\sigma)} \leq \|\Gamma_\sigma^{-1} \circ P \circ \Gamma_{\sigma'}\|_{(\alpha,\sigma')\to(\alpha,\sigma)} \|\Gamma_{\sigma'}^{-1}(\rho)\|_{(\alpha,\sigma')}. \tag{13}$$

Applying Theorem 2.1 for $p_0 = q_0 = 1$ and $p_1 = q_1 = \infty$ and $\theta = \frac{1}{\alpha}$ gives

$$\|\Gamma_\sigma^{-1} \circ P \circ \Gamma_{\sigma'}\|_{(\alpha,\sigma')\to(\alpha,\sigma)} \leq \|\Gamma_\sigma^{-1} \circ P \circ \Gamma_{\sigma'}\|_{(1,\sigma')\to(1,\sigma)}^{\frac{1}{\alpha}} \|\Gamma_\sigma^{-1} \circ P \circ \Gamma_{\sigma'}\|_{(\infty,\sigma')\to(\infty,\sigma)}^{1-\frac{1}{\alpha}}. \tag{14}$$

For any positive trace-preserving map we have

$$\|\Gamma_\sigma^{-1} \circ P \circ \Gamma_{\sigma'}\|_{(1,\sigma')\to(1,\sigma)} = \|P\|_{1\to1} = 1 \tag{15}$$

and, using the Russo-Dye theorem [32, Corollary 2.9], we have

$$\|\Gamma_\sigma^{-1} \circ P \circ \Gamma_{\sigma'}\|_{(\infty,\sigma')\to(\infty,\sigma)} = \|\Gamma_\sigma^{-1} \circ P \circ \Gamma_{\sigma'}\|_{\infty\to\infty} \tag{16}$$

$$= \|\Gamma_\sigma^{-1} \circ P \circ \Gamma_{\sigma'}(\mathbb{1}_{d_A})\|_\infty = \|\Gamma_\sigma^{-1} \circ P(\sigma')\|_\infty. \tag{17}$$

Combining equations (13), (14), (15) and (17) we obtain

$$\|\Gamma_\sigma^{-1} \circ P(\rho)\|_{(\alpha,\sigma)} \leq \|\Gamma_\sigma^{-1} \circ P(\sigma')\|_\infty^{1-\frac{1}{\alpha}} \|\Gamma_{\sigma'}^{-1}(\rho)\|_{(\alpha,\sigma')}$$

Taking logarithms, dividing by $1 - \frac{1}{\alpha}$ and writing the resulting inequality in terms of the sandwiched α-Rényi divergence (see (6)) finishes the proof for $\alpha > 1$. Taking the limit $\alpha \to 1$ gives the statement for $D_1 = D$. $\square$

---

[2] This follows e.g. from [9, Proposition 18] as id_2 is an erasure channel with erasure probability 0.

Note that Theorem 3.1 contains some well-known inequalities as special cases. Setting $\sigma = P(\sigma')$ gives the data processing inequality (8) for the trace-preserving positive map P. In the case where $P = \mathrm{id}_d$ the identity map we get the inequality

$$D_\alpha\left(\rho\|\sigma\right) \leq D_\alpha(\rho\|\sigma') + D_{\max}(\sigma'\|\sigma) \tag{18}$$

for any quantum states $\rho, \sigma, \sigma' \in \mathcal{D}\left(\mathbb{C}^d\right)$, which for $\alpha = \infty$ resembles a triangle inequality for $D_{\max}$ (which can easily be shown directly).

We will now apply Theorem 3.1 to prove a statement quantifying how the α-relative entropy of entanglement changes under partial application of a completely positive map:

Theorem 3.2. *For any quantum channel* $T : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{B'}}$ *and any quantum state* $\rho_{AA'B} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_B})$ *for* $d_A, d_B \in \mathbb{N}$ *arbitrary, we have*

$$E_\alpha^{A:BB'}\left(T^{A'\to B'}(\rho_{AA'B})\right) \leq E_{\max}(T) + E_\alpha^{AA':B}(\rho_{AA'B})$$

for any $\alpha \geq 1$.

Proof. Let $T : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{B'}}$ be a quantum channel and $\rho_{AA'B} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_B})$ a quantum state for some $d_A, d_B \in \mathbb{N}$. Furthermore let $\alpha > 1$. For any $\sigma_{AB'B} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_{B'}} \otimes \mathbb{C}^{d_B})$ and $\sigma'_{AA'B} \in \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_B})$ an application of Theorem 3.1 for $P = T^{A'\to B'}$ leads to

$$D_\alpha\left(T^{A'\to B'}(\rho_{AA'B})\|\sigma_{AB'B}\right) \leq D_{\max}\left(T^{A'\to B'}(\sigma'_{AA'B})\|\sigma_{AB'B}\right) + D_\alpha\left(\rho_{AA'B}\|\sigma'_{AA'B}\right).$$

Minimizing over $\sigma_{AB'B} \in \mathrm{Sep}_{A:B'B}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_{B'}} \otimes \mathbb{C}^{d_B}\right)$ and restricting to states $\sigma'_{AA'B} \in \mathrm{Sep}_{AA':B}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_B}\right)$ leads to

$$E_\alpha^{A:B'B}\left(T^{A'\to B'}(\rho_{AA'B})\right) \leq E_{\max}^{A:B'B}\left(T^{A'\to B'}(\sigma'_{AA'B})\right) + D_\alpha\left(\rho_{AA'B}\|\sigma'_{AA'B}\right)$$

$$\leq \max_{\tilde{\sigma}_{AA'B}\in\mathrm{Sep}(AA':B)} E_{\max}^{A:B'B}\left(T^{A'\to B'}(\tilde{\sigma}_{AA'B})\right) + D_\alpha\left(\rho_{AA'B}\|\sigma'_{AA'B}\right).$$

Now minimizing over $\sigma'_{AA'B} \in \mathrm{Sep}_{AA':B}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_B}\right)$ yields

$$E_\alpha^{A:B'B}\left(T^{A'\to B'}(\rho_{AA'B})\right) \leq \max_{\tilde{\sigma}_{AA'B}\in\mathrm{Sep}(AA':B)} E_{\max}^{A:B'B}\left(T^{A'\to B'}(\tilde{\sigma}_{AA'B})\right)$$

$$+ E_\alpha^{AA':B}\left(\rho_{AA'B}\right).$$

Let $\sigma'_0 \in \mathrm{Sep}_{AA':B}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_B}\right)$ attain the maximum in the previous equation. As σ'_0 is separable there is a decomposition of the form $\sigma'_0 = \sum_{i=1}^k p_i \gamma_{AA'}^i \otimes \phi_B^i$ with $k \in \mathbb{N}$, probabilities $p_i \in [0, 1]$ such that $\sum_{i=1}^k p_i = 1$, and states $\{\gamma_{AA'}^i\}_{i=1}^k \subset \mathcal{D}(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_{A'}})$ and $\{\phi_B^i\}_{i=1}^k \subset \mathcal{D}(\mathbb{C}^{d_B})$. Now let $\tau_{AB'}^i \in \mathrm{Sep}_{A:B'}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_{B'}}\right)$ be such that

$$E_{\max}^{A:B'}\left(T^{A'\to B'}(\gamma_{AA'}^i)\right) = D_{\max}\left(T^{A'\to B'}(\gamma_{AA'}^i)\|\tau_{AB'}^i\right)$$

for each $i \in \{1, \ldots, k\}$. With these states we get

$$
\max_{\tilde{\sigma}_{AA'B} \in \text{Sep}(AA':B)} E_{\max}^{A:B'B} \left(T^{A' \to B'} (\tilde{\sigma}_{AA'B}) \right)
$$

$$
= \min_{\sigma_{AB'B} \in \text{Sep}(A:B'B)} D_{\max} \left(T^{A' \to B'} (\sigma_0') \| \sigma_{AB'B} \right)
$$

$$
\leq D_{\max} \left(\sum_{i=1}^{k} p_i T^{A' \to B'} (\gamma_{AA'}^i) \otimes \phi_B^i \| \sum_{i=1}^{k} p_i \tau_{AB'}^i \otimes \phi_B^i \right)
$$

$$
\leq \max_{i \in \{1, \ldots, k\}} D_{\max} \left(T^{A' \to B'} (\gamma_{AA'}^i) \otimes \phi_B^i \| \tau_{AB'}^i \otimes \phi_B^i \right)
$$

$$
= \max_{i \in \{1, \ldots, k\}} D_{\max} \left(T^{A' \to B'} (\gamma_{AA'}^i) \| \tau_{AB'}^i \right)
$$

$$
= \max_{i \in \{1, \ldots, k\}} E_{\max}^{A:B'} \left(T^{A' \to B'} (\gamma_{AA'}^i) \right)
$$

$$
\leq E_{\max} (T).
$$

In the second line of the above computation we used that $\sum_{i=1}^{k} p_i \tau_{AB'}^i \otimes \phi_B^i \in \text{Sep}_{A:B'B} \left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_{B'}} \otimes \mathbb{C}^{d_B} \right)$ as $\tau_{AB'}^i \in \text{Sep}_{A:B'} \left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_{B'}} \right)$ by definition. In the third line we used that $D_{\max}$ is joint quasi-convex [15, Lemma 9] and in the fourth line that $D_{\max} (\rho_1 \otimes \sigma_1 \| \rho_2 \otimes \sigma_2) = D_{\max} (\rho_1 \| \rho_2) + D_{\max} (\sigma_1 \| \sigma_2)$ for any quantum states $\rho_1, \rho_2 \in \mathcal{D} \left(\mathbb{C}^d \right)$ and $\sigma_1, \sigma_2 \in \mathcal{D} \left(\mathbb{C}^{d'} \right)$ with $\text{supp} [\rho_1] \subseteq \text{supp} [\rho_2]$ and $\text{supp} [\sigma_1] \subseteq \text{supp} [\sigma_2]$ (see for instance [18, Theorem 2]). □

The following corollary bounds the α-relative entropy of entanglement of the state obtained from alternately applying an LOCC-operation and a partial quantum channel to some tripartite initial state.

Corollary 3.1. *Let* $T : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{B'}}$ *be a quantum channel,* $m \in \mathbb{N}$ *,and* $d_{A_i}, d_{B_i} \in \mathbb{N}$ *dimensions for each* $i \in \{1, \ldots, m\}$. *Consider LOCC-operations* $\{L_i\}_{i=1}^m$ *w.r.t. the bipartition into A and B systems acting as*

$$
L_i : \mathcal{M}_{d_{A_i}} \otimes \mathcal{M}_{d_{B'}} \otimes \mathcal{M}_{d_{B_i}} \to \mathcal{M}_{d_{A_{i+1}}} \otimes \mathcal{M}_{d_{A'}} \otimes \mathcal{M}_{d_{B_i}}
$$

for any $i \in \{1, \ldots, m\}$ *and*

$$
L_m : \mathcal{M}_{d_{A_m}} \otimes \mathcal{M}_{d_{B'}} \otimes \mathcal{M}_{d_{B_m}} \to \mathcal{M}_{d_{\tilde{A}}} \otimes \mathcal{M}_{d_{\tilde{B}}}
$$

for arbitrary $d_{\tilde{A}}, d_{\tilde{B}} \in \mathbb{N}$. *For any quantum state* $\rho_{A_1 A' B_1} \in \mathcal{D} \left(\mathbb{C}^{d_{A_1}} \otimes \mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_{B_1}} \right)$ *consider the state*

$$
\phi_{\tilde{A}\tilde{B}} = L_m \circ \prod_{i=1}^{m-1} \left(T^{A' \to B'} \circ L_i \right) \circ T^{A' \to B'} \left(\rho_{A_1 A' B_1} \right).
$$

Then we have

$$
E_{\alpha}^{\tilde{A}:\tilde{B}} \left(\phi_{\tilde{A}\tilde{B}} \right) \leq m E_{\max} (T) + E_{\alpha}^{A_1 A':B_1} \left(\rho_{A_1 A' B_1} \right)
$$

for any $\alpha > 1$.

Proof. For $i \in \{1, \ldots, m\}$ we define the states

$$\sigma_{A_i B' B_i}^{(i)} = \prod_{k=1}^{i-1} \left(T^{A' \to B'} \circ L_i \right) \circ T^{A' \to B'} \left(\rho_{A_1 A' B_1} \right).$$

By the data-processing inequality (8) it is easy to see that E_α is non-increasing under LOCC-operations as such operations preserve the set of separable states. Using this fact and Theorem 3.2 alternately gives

$$\begin{aligned}
E_\alpha^{\tilde{A}:\tilde{B}} \left(\phi_{\tilde{A}\tilde{B}} \right) &= E_\alpha^{\tilde{A}:\tilde{B}} \left(L_m \left(\sigma_{A_m B' B_m}^{(m)} \right) \right) \\
&\leq E_\alpha^{A_m : B' B_m} \left(\sigma_{A_m B' B_m}^{(m)} \right) \\
&\leq E_{\max}(T) + E_\alpha^{A_{m-1} : B' B_{m-1}} \left(\sigma_{A_{m-1} B' B_{m-1}}^{(m-1)} \right) \\
&\vdots \\
&\leq (m-1) E_{\max}(T) + E_\alpha^{A_1 B' B_1} \left(T^{A' \to B'} \left(\rho_{A_1 A' B_1} \right) \right) \\
&\leq m E_{\max}(T) + E_\alpha^{A_1 A' B_1} \left(\rho_{A_1 A' B_1} \right).
\end{aligned}$$

$\square$

In the next section we will apply the previous corollary to the output state of a protocol for $\mathcal{P}_\leftrightarrow$. This will establish the strong-converse bound in terms of $E_{\max}$.

4. Strong Converse Bound on $\mathcal{P}_\leftrightarrow$

To prove a strong converse bound on $\mathcal{P}_\leftrightarrow$ we will use some notions introduced in [9]. Consider a private state

$$\gamma_{A_k B_k A_s B_s} = U_{A_k B_k A_s B_s}^{\text{tw}} \left(\omega_{A_k B_k} \otimes \sigma_{A_s B_s} \right) (U_{A_k B_k A_s B_s}^{\text{tw}})^\dagger$$

where $U_{A_k B_k A_s B_s}^{\text{tw}}$ denotes a twisting unitary (see Definition 2.6). A privacy test corresponding to $\gamma_{A_k B_k A_s B_s}$ (see [9, Definition 6]) is a 2-outcome measurement given by the POVM

$$\{\Pi_{A_k B_k A_s B_s}, \mathbb{1}_{A_k B_k A_s B_s} - \Pi_{A_k B_k A_s B_s}\} \tag{19}$$

for the projector $\Pi_{A_k B_k A_s B_s} = U_{A_k B_k A_s B_s}^{\text{tw}} \left(\omega_{A_k B_k} \otimes \mathbb{1}_{A_s B_s} \right) \left(U_{A_k B_k A_s B_s}^{\text{tw}} \right)^\dagger$. It can be shown that a separable state only has a low probability of passing a privacy test (i.e. the measurement (19) giving the outcome corresponding to $\Pi_{A_k B_k A_s B_s}$) corresponding to a private state. More specifically (see [33, equation (281)] or [9, Lemma 8]) for a privacy test (19) corresponding to a private state $\gamma_{A_k B_k A_s B_s}$ with K-dimensional key part (i.e. $d_{A_k} = d_{B_k} = K$ as in Definition 2.6) it holds that

$$\text{tr} \left(\Pi_{A_k B_k A_s B_s} \sigma_{A_k B_k A_s B_s} \right) \leq \frac{1}{K} \tag{20}$$

for any separable state $\sigma_{A_k B_k A_s B_s} \in \text{Sep}_{A_k A_s : B_k B_s} \left(\mathbb{C}^{d_{A_k} d_{A_s}} \otimes \mathbb{C}^{d_{B_k} d_{B_s}} \right)$. At the same time the probability of a state passing the privacy test can be related to its distance to the private state. The following Lemma has been shown in [9]:

Lemma 4.1 (Lemma 7 in [9]). *Let* $\rho_{A_k B_k A_s B_s} \in \mathcal{D}\left(\mathbb{C}^{d_{A_k}} \otimes \mathbb{C}^{d_{B_k}} \otimes \mathbb{C}^{d_{A_s}} \otimes \mathbb{C}^{d_{B_s}}\right)$ *be a quantum state and* $\Pi_{A_k B_k A_s B_s}$ *the projector appearing in the privacy test* (*see* (19)) *corresponding to a private state* $\gamma_{A_k B_k A_s B_s}$. *Then*

$$tr\left(\Pi_{A_k B_k A_s B_s}\rho_{A_k B_k A_s B_s}\right) \geq F(\rho_{A_k B_k A_s B_s}, \gamma_{A_k B_k A_s B_s})$$

where $F(\rho, \sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$ *denotes the fidelity.*

Now we can prove a bound on the error of private state generation for protocols assisted by classical communication. The proof follows a method given in [19] and uses ideas from [9].

Lemma 4.2 (Bound on private communication error). *Let* $T : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{B'}}$ *be a quantum channel and* $\alpha \in (1, \infty)$. *For any* $k, m \in \mathbb{N}$ *the error* $\epsilon > 0$ *in an* (k, m, ϵ)-*coding scheme for private state generation assisted by classical communication* (*as in Definition* 2.7) *fulfills*

$$\epsilon \geq 1 - 2^{-\frac{\alpha-1}{2\alpha}(k - m E_{\max}(T))}.$$

Proof. Let $\phi_{\tilde{A}\tilde{B}}^{(m)} \in \mathcal{D}\left(\mathbb{C}^{d_{\tilde{A}}} \otimes \mathbb{C}^{d_{\tilde{B}}}\right)$ denote the output state of the (k, m, ϵ)-coding scheme, i.e.

$$\phi_{\tilde{A}\tilde{B}}^{(m)} = L_m \circ \prod_{i=1}^{m-1}\left(T^{A' \to B'} \circ L_i\right) \circ T^{A' \to B'}\left(\rho_{A_1 A' B_1}^{(1)}\right)$$

for LOCC-operations $\{L_i\}_{i=1}^m$ and initial state $\rho_{A_1 A' B_1} \in \mathrm{Sep}_{A_1 A':B_1}\left(\mathbb{C}^{d_{A_1}} \otimes \mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_{B_1}}\right)$ as in Definition 2.3. Note that by the form of $\phi_{\tilde{A}\tilde{B}}^{(m)}$ we can apply Lemma 3.1 to show

$$E_\alpha^{\tilde{A}:\tilde{B}}\left(\phi_{\tilde{A}\tilde{B}}^{(m)}\right) \leq m E_{\max}(T) \tag{21}$$

where we used that by separability $E_\alpha^{A_1 A':B_1}\left(\rho_{A_1 A' B_1}^{(1)}\right) = 0$.

By assumption (from Definition 2.7) we have $d_{\tilde{A}} = d_{A_k} d_{A_s}$ and $d_{\tilde{B}} = d_{B_k} d_{B_s}$ with $d_{A_k} = d_{B_k} = 2^k$ and $d_{A_s} = d_{B_s}$, and there exists a private state $\gamma_{A_k B_k A_s B_s} \in \mathcal{D}\left(\mathbb{C}^{d_{\tilde{A}}} \otimes \mathbb{C}^{d_{\tilde{B}}}\right)$ with 2^k-dimensional key part (see Definition 2.6) such that

$$\epsilon = \frac{1}{2}\|\phi_{\tilde{A}\tilde{B}}^{(m)} - \gamma_{A_k B_k A_s B_s}\|_1. \tag{22}$$

Let $\Pi_{A_k B_k A_s B_s}^{(k)}$ denote the projector in the privacy test corresponding to $\gamma_{A_k B_k A_s B_s}$ (see (19)). Then by Lemma 4.1 we have

$$F := tr\left(\Pi_{A_k B_k A_s B_s}^{(k)}\phi_{\tilde{A}\tilde{B}}^{(m)}\right) \geq F(\phi_{\tilde{A}\tilde{B}}^{(m)}, \gamma_{2^k}) \tag{23}$$

Now we define a binary flag channel $B : \mathcal{D}\left(\mathbb{C}^{d_{\tilde{A}}} \otimes \mathbb{C}^{d_{\tilde{B}}}\right) \to \mathcal{M}_2$ by

$$B(X) = tr\left(\Pi_{A_k B_k A_s B_s}^{(k)} X\right)|1\rangle\langle 1| + tr\left((\mathbb{1}_{A_k B_k A_s B_s} - \Pi_{A_k B_k A_s B_s}^{(k)})X\right)|0\rangle\langle 0|$$

where $|0\rangle, |1\rangle \in \mathbb{C}^2$ denote the computational basis states. For any separable state $\sigma_{\tilde{A}\tilde{B}} \in \mathrm{Sep}_{\tilde{A}:\tilde{B}} \left(\mathbb{C}^{d_{\tilde{A}}} \otimes \mathbb{C}^{d_{\tilde{B}}} \right)$ we can compute

$$
\begin{aligned}
D_\alpha \left(\phi_{\tilde{A}\tilde{B}}^{(m)} \| \sigma_{\tilde{A}\tilde{B}} \right) &\geq D_\alpha \left(B \left(\phi_{\tilde{A}\tilde{B}}^{(m)} \right) \| B \left(\sigma_{\tilde{A}\tilde{B}} \right) \right) \\
&= \frac{1}{\alpha - 1} \log_2 \left(F^\alpha p^{1-\alpha} + (1-F)^\alpha (1-p)^{1-\alpha} \right) \\
&\geq \frac{1}{\alpha - 1} \log_2 \left(F^\alpha p^{1-\alpha} \right) \\
&\geq \frac{1}{\alpha - 1} \log_2 \left(F^\alpha \left(\frac{1}{2^k} \right)^{1-\alpha} \right) \\
&= \frac{\alpha}{\alpha - 1} \log_2(F) + k.
\end{aligned}
$$

Here we introduced $p = \mathrm{tr}\left(\sigma_{\tilde{A}\tilde{B}} \Pi_{\tilde{A}\tilde{B}}^{(k)} \right)$ and used the data-processing inequality (8) of the sandwiched α-Rényi divergences for the first inequality. In the last inequality we used $p \leq \frac{1}{2^k}$ which follows from (20) and separability of $\sigma_{\tilde{A}\tilde{B}}$.

Minimizing over all separable states $\sigma_{\tilde{A}\tilde{B}} \in \mathrm{Sep}_{\tilde{A}:\tilde{B}} \left(\mathbb{C}^{d_{\tilde{A}}} \otimes \mathbb{C}^{d_{\tilde{B}}} \right)$ on the left-hand-side of the previous equation and using (21) gives

$$
m E_{\max}(T) \geq E_\alpha^{\tilde{A}:\tilde{B}} \left(\phi_{\tilde{A}\tilde{B}}^{(m)} \right) \geq \frac{\alpha}{\alpha - 1} \log_2(F) + k.
$$

By applying the Fuchs-van-de-Graaf inequality [34, Theorem 1] and (23) we get

$$
\epsilon \geq 1 - \sqrt{F(\phi_{\tilde{A}\tilde{B}}^{(m)}, \gamma_{2^k})} \geq 1 - \sqrt{F} \geq 1 - 2^{-\frac{\alpha-1}{2\alpha}(k - m E_{\max}(T))}
$$

for the communication error ϵ from (22). $\quad\square$

Theorem 4.1. *Let* $T : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{B'}}$ *be a quantum channel. Then the quantity* $E_{\max}(T)$ *is a strong-converse bound on* $\mathcal{P}_\leftrightarrow(T)$.

Proof. Consider $R > E_{\max}(T)$ such that for each $\nu \in \mathbb{N}$ there exists an $(k_\nu, m_\nu, \varepsilon_\nu)$-coding scheme for private state generation assisted by classical communication (as in Definition 2.4) with $m_\nu \to \infty$ as $\nu \to \infty$ and $R = \lim_{\nu \to \infty} \frac{k_\nu}{m_\nu}$. There exists a $\delta > 0$ and a $\nu_0 \in \mathbb{N}$ such that

$$
\frac{k_\nu}{m_\nu} > E_{\max}(T) + \delta
$$

for all $\nu \geq \nu_0$. Therefore, using Lemma 4.2 we have for any $\nu \geq \nu_0$ and $\alpha > 1$ that

$$
\begin{aligned}
\epsilon_\nu &\geq 1 - 2^{-\frac{\alpha-1}{2\alpha}(k_\nu - m_\nu E_{\max}(T))} \\
&\geq 1 - 2^{-\frac{\alpha-1}{2\alpha} m_\nu \delta} \to 1
\end{aligned}
$$

as $\nu \to \infty$.

Finally we can regularize the above bound. Consider the regularized max-relative entropy of a quantum channel $T : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{B'}}$

$$E_{\max}^{\infty}(T) := \lim_{n\to\infty} \frac{1}{n} E_{\max}\left(T^{\otimes n}\right).$$

As a special case of [9, Theorem 13] (which can also be shown directly following the proof of [35, Theorem 6] for the quantity $E_{\max}$) we have for any $n \in \mathbb{N}$

$$E_{\max}\left(T^{\otimes n}\right) \le n E_{\max}(T) + d_{A'} \log_2(n).$$

Dividing by n and taking the limit $n \to \infty$ implies

$$E_{\max}^{\infty}(T) \le E_{\max}(T).$$

We can therefore improve the bound from Theorem 4.1 (which is in particular an upper bound on $\mathcal{P}_{\leftrightarrow}$) by regularization. Note that by Definition 6.2 we have $\mathcal{P}_{\leftrightarrow}(T) = \lim_{n\to\infty} \frac{1}{n}\mathcal{P}_{\leftrightarrow}\left(T^{\otimes n}\right)$. Applying the bound from Theorem 4.1 for the channels $T^{\otimes n}$ and noting that $\mathcal{Q}_{\leftrightarrow} \le \mathcal{P}_{\leftrightarrow}$ (by Definition 6.2) implies:

Corollary 4.1 (Regularized upper bound on $\mathcal{P}_{\leftrightarrow}$). *For any quantum channel* $T : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{B'}}$ *we have*

$$\mathcal{Q}_{\leftrightarrow}(T) \le \mathcal{P}_{\leftrightarrow}(T) \le E_{\max}^{\infty}(T) \le E_{\max}(T).$$

5. Properties of $E_{\max}(T)$

5.1. Non-lockability. An entanglement measure is called non-lockable [36] if tracing out a subsystem of dimension $d \in \mathbb{N}$ can only change the measure by an amount logarithmic in d. Here we show that this is the case for the max-relative entropy of entanglement (cf. Theorem 5.1). As a consequence we show that for a quantum channel $T^{A\to BC} : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B d_C}$ the difference of the quantities $E_{\max}\left(T^{A\to BC}\right)$ and $E_{\max}\left(\mathrm{tr}_C \circ T^{A\to BC}\right)$ can be at most logarithmic in d_C. We start with an elementary lemma which is probably known:

Lemma 5.1. *For some $k \in \mathbb{N}$ consider a convex combination $\rho_{AB} = \sum_{i=1}^{k} p_i \rho_{AB}^i$ of bipartite quantum states $\rho_{AB}^i \in \mathcal{D}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}\right)$ and $p_i \in [0,1]$ for $i \in \{1,\dots,k\}$ such that $\sum_{i=1}^{k} p_i = 1$. Then we have*

$$\sum_{i=1}^{k} p_i E_{\max}^{A:B}\left(\rho_{AB}^i\right) \le E_{\max}^{A:B}(\rho_{AB}) + \sum_{i=1}^{k} p_i D_{\max}\left(\rho_{AB}^i \| \rho_{AB}\right).$$

Proof. Given states $\rho_i \in \mathcal{D}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}\right)$ for $i \in \{1,\dots,k\}$ and $\rho = \sum_{i=1}^{k} p_i \rho_{AB}^i$ with probabilities $\{p_i\}_{i=1}^{k} \subset [0,1]$ fulfilling $\sum_{i=1}^{k} p_i = 1$. Note that applying Theorem 3.1 for $P = \mathrm{id}_d$ and $\alpha = \infty$ gives

$$D_{\max}\left(\rho_{AB}^i \| \sigma_{AB}\right) \le D_{\max}(\rho_{AB} \| \sigma_{AB}) + D_{\max}\left(\rho_{AB}^i \| \rho_{AB}\right)$$

for any states $\sigma_{AB} \in \mathcal{D}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}\right)$. Minimizing over $\sigma_{AB} \in \mathrm{Sep}_{A:B}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}\right)$ leads to

$$E_{\max}^{A:B}\left(\rho_{AB}^i\right) \leq E_{\max}^{A:B}(\rho_{AB}) + D_{\max}\left(\rho_{AB}^i \| \rho\right).$$

Finally multiplying the above inequalities by p_i for each $i \in \{1, \ldots k\}$ and summing over i leads to the statement of the lemma. $\square$

With the previous lemma we can show that the max-relative entropy of entanglement is non-lockable. The argument is similar to an argument given in [36] for the relative entropy of entanglement.

Theorem 5.1 (Non-lockability of the max-relative entropy of entanglement). *For any tripartite state $\rho_{ABB'} \in \mathcal{D}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B} \otimes \mathbb{C}^{d_{B'}}\right)$ we have*

$$E_{\max}^{A:BB'}(\rho_{ABB'}) - E_{\max}^{A:B}(\rho_{AB}) \leq 2 \log_2(d_{B'}).$$

Proof. Note that

$$\rho_{AB} \otimes \frac{\mathbb{1}_{d_{B'}}}{d_{B'}} = \int_{\mathcal{U}_{d_{B'}}} \left(\mathbb{1}_{d_{AB}} \otimes U\right) \rho_{ABB'} \left(\mathbb{1}_{d_{AB}} \otimes U\right)^\dagger \mathrm{dU}$$

$$= \frac{1}{k} \sum_{i=1}^{k} \left(\mathbb{1}_{d_{AB}} \otimes U_i\right) \rho_{ABB'} \left(\mathbb{1}_{d_{AB}} \otimes U_i\right)^\dagger$$

where the integral is with respect to the Haar-measure on the unitary group $\mathcal{U}_{d_{B'}}$, and where we used unitaries $(U_i)_{i=1}^{k}$ forming a unitary 2-design (see [37]). Applying Lemma 5.1 for the above convex combination gives

$$\sum_{i=1}^{k} \frac{1}{k} E_{\max}^{A:BB'}\left(\left(\mathbb{1}_{d_{AB}} \otimes U_i\right) \rho_{ABB'} \left(\mathbb{1}_{d_{AB}} \otimes U_i\right)^\dagger\right) - E_{\max}^{A:BB'}\left(\rho_{AB} \otimes \frac{\mathbb{1}_{d_{B'}}}{d_{B'}}\right)$$

$$\leq \sum_{i=1}^{k} \frac{1}{k} D_{\max}\left(\left(\mathbb{1}_{d_{AB}} \otimes U_i\right) \rho_{ABB'} \left(\mathbb{1}_{d_{AB}} \otimes U_i\right)^\dagger \| \rho_{AB} \otimes \frac{\mathbb{1}_{d_{B'}}}{d_{B'}}\right)$$

$$= D_{\max}\left(\rho_{ABB'} \| \rho_{AB} \otimes \frac{\mathbb{1}_{d_{B'}}}{d_{B'}}\right)$$

$$\leq 2 \log_2(d_{B'}).$$

Here we used that $D_{\max}$ is invariant under unitary transformations applied to both of its arguments, and that $\rho_{ABB'} \leq d_{B'} \rho_{AB} \otimes \mathbb{1}_{d_{B'}}$, which by (5) implies the last inequality. Finally note that

$$E_{\max}^{A:BB'}\left(\rho_{AB} \otimes \frac{\mathbb{1}_{d_{B'}}}{d_{B'}}\right) = E_{\max}^{A:B}(\rho_{AB})$$

by monotonicity under local operations. $\square$

Finally by applying Theorem 5.1 to the quantity $E_{\max}$ (see (9)) we obtain the following:

Corollary 5.1. *Let* $T^{A \to BC} : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B} \otimes \mathcal{M}_{d_C}$ *be a quantum channel and consider the reduced quantum channel* $T^{A \to B} = tr_C \circ T^{A \to BC}$. *Then*

$$E_{\max}\left(T^{A \to BC}\right) \le 2 \log_2(d_C) + E_{\max}\left(T^{A \to B}\right)$$

The previous corollary is used in Sect. 6.1 to show that the bound from Corollary 4.1 improves on both the transposition bound (see Theorem 2.2) and the squashed entanglement bound (see Theorem 2.3).

5.2. Simplified upper bounds. The optimizations over input states and separable states make it hard to compute $E_{\max}(T)$ (see (9)) for a concrete quantum channel $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$. In the following we will give a slightly simpler bound in terms of the quantity

$$B_{\max}(T) = \min\{D_{\max}(C_T \| C_S) \; : \; S : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$$
$$\text{entanglement breaking quantum channel}\}.$$

Here C_T and C_S denote Choi matrices (see (3)) of the channels T and S. Recall that a quantum channel $S : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ is called entanglement breaking [38] iff $S^{A \to B}(\rho_{A'A})$ is separable for any bipartite state $\rho_{A'A} \in \mathcal{D}(\mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_A})$ and where A' is a system of any dimension. This is equivalent to separability of the Choi matrix C_S. Note that since $\text{tr}_B(C_S) = \mathbb{1}_{d_{A'}}/d_{A'}$ (where we used that $C_S = S^{A \to B}(\omega_{A'A})$ now for $d_{A'} = d_A$) the above quantity is in general different from $E_{\max}^{A':B}(C_T)$.

Theorem 5.2 (Simplified upper bound). *For a quantum channel* $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ *we have*

$$E_{\max}(T) \le B_{\max}(T).$$

Proof. Let $S : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ be an entanglement breaking channel. For any bipartite quantum state $\rho_{A'A} \in \mathcal{D}(\mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_A})$ the output state $S^{A \to B}(\rho_{A'A})$ is separable. Therefore we have

$$E_{\max}^{A':B}\left(T^{A \to B}(\rho_{A'A})\right)$$
$$= \inf\{D_{\max}\left(T^{A \to B}(\rho_{A'A}) \| \sigma_{A'B}\right) \; : \; \sigma_{A'B} \in \text{Sep}_{A':B}\left(\mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_B}\right)\}$$
$$\le D_{\max}\left(T^{A \to B}(\rho_{A'A}) \| S^{A \to B}(\rho_{A'A})\right)$$
$$= \inf\{\lambda \ge 0 : T^{A \to B}(\rho_{A'A}) \le 2^\lambda S^{A \to B}(\rho_{A'A})\}.$$

The condition in the last infimum is certainly fulfilled if the linear map $2^\lambda S - T$ is completely positive (in this case the condition holds for any state $\rho_{A'A}$). Expressing complete positivity of this linear map in terms of the Choi matrix [13] yields

$$E_{\max}^{A':B}\left(T^{A \to B}(\rho_{A'A})\right) \le \inf\{\lambda \ge 0 : C_T \le 2^\lambda C_S\} = D_{\max}(C_T \| C_S),$$

where $C_T = T^{A \to B}(\omega_{A'A})$ denotes the Choi matrix of T (and C_S the Choi matrix of S). As the previous bound holds for any input state $\rho_{A'A}$ and any entanglement breaking channel $S : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ the proof is finished. □

6. Applications

6.1. Flower channels. Here we will compare the bound from Corollary 4.1 to previously known bounds. Numerical computations show that for the qubit depolarizing channel, the qubit erasure channel, and the qubit amplitude damping channel our bound does not outperform the transposition bound. It should also be noted that for channels implementable from their image (see Definition A.1 in Appendix A) including all teleportation-covariant channels, the bound based on the relative entropy of entanglement (see [6]) performs better than our bound (based on the max-relative entropy of entanglement). However, for many important quantum channels (e.g. the channels considered in this section and in Sect. 6.2) it is currently not known whether they are implementable from their image. Moreover, in Appendix A we provide an example of a quantum channel which cannot be implemented from its image. Instead of estimating our bound for the commonly used standard examples, we will consider a particular construction of quantum channels in high dimensions. This exploits the non-lockability of our bound to outperform the previously known bounds. As the transposition bound (see Theorem 2.2) only upper bounds $\mathcal{Q}_\leftrightarrow$ and not $\mathcal{P}_\leftrightarrow$ we will only consider the former quantity in this section.

Here we will use a particular family of channels (so called flower channels) for which the transposition bound (see Theorem 2.2), the bound based on the squashed entanglement (see Theorem 2.3), and thereby also the entanglement cost bound (see Theorem 2.4) perform exceptionally badly. The reason of this bad performance is that all these bounds are lockable [36]. The new bound based on the max-relative entropy is non-lockable (cf. Corollary 5.1), which leads to an improvement compared to the other bounds. Moreover, the improvement can be made arbitrarily large by increasing the dimension of the channels.

For $d \in \mathbb{N}$ consider the so called "flower" states given by

$$\rho^f_{AA'BB'} = \frac{1}{2d} \sum_{i,k=1}^{d} \sum_{j,l=1}^{2} \langle k|U_l^\dagger U_j|i\rangle \, |ii\rangle\langle kk|_{AB} \otimes |jj\rangle\langle ll|_{A'B'} \in \mathcal{D}\left(\mathbb{C}^d \otimes \mathbb{C}^2 \otimes \mathbb{C}^d \otimes \mathbb{C}^2\right) \tag{24}$$

where $U_1 = \mathbb{1}_d$ and U_2 is the quantum Fourier transformation with entries

$$(U_2)_{j,k} = \frac{1}{\sqrt{d}} e^{2\pi i jk/d}$$

for $j, k \in \{1, \ldots, d\}$. In [36] and [39] several entanglement measures have been computed for these states. The squashed entanglement (see (11)) is given by (see [39, Proposition 4])

$$E_{\text{sq}}^{AA':BB'}\left(\rho^f_{AA'BB'}\right) = 1 + \frac{1}{2}\log_2(d), \tag{25}$$

and the logarithmic negativity is given by (see [36, p. 2])

$$\log_2\left(\|(\rho^f_{AA'BB'})^{T_{BB'}}\|_1\right) = \log_2\left(\sqrt{d} + 1\right). \tag{26}$$

Note that the previous quantities are unbounded in the limit $d \to \infty$. However, the actual entanglement in the states $\rho^f_{AA'BB'}$ is small, because tracing out the 2-dimensional system B' leads a separable state

$$\rho^f_{AA'B} = \frac{1}{2d} \sum_{i=1}^{d} \sum_{j=1}^{2} |ii\rangle\langle ii|_{AB} \otimes |j\rangle\langle j|_{A'}.$$

The two marginals of a flower state $\rho^f_{AA'BB'}$ fulfill $\rho^f_{BB'} = \rho^f_{AA'} = \mathbb{1}_{2d}/(2d)$. Therefore, by the Choi–Jamiolkowski isomorphism [13] there is a unital quantum channel $T^{AA' \to BB'}_f : \mathcal{M}_{2d} \to \mathcal{M}_{2d}$ with Choi matrix $\rho^f_{AA'BB'}$. We call this channel a flower channel. Note that the reduced channel $T^{AA' \to B}_f = \mathrm{tr}_{B'} \circ T^{AA' \to BB'}_f$ is entanglement breaking as its Choi matrix is the separable state $\rho^f_{AA'B}$. This implies that $E_{\max}\left(T^{AA' \to B}_f\right) = 0$ and using Corollary 5.1 and the non-regularized bound from Corollary 4.1 we get

$$Q_2\left(T^{AA' \to BB'}_f\right) \leq E_{\max}\left(T^{AA' \to BB'}_f\right) \leq 2 + E_{\max}\left(T^{AA' \to B}_f\right) = 2. \quad (27)$$

We can also estimate the transposition bound (see Theorem 2.2) and the bound based on the squashed entanglement (see Theorem 2.3). By (26) and (25) we have

$$\log_2\left(\|\vartheta_{BB'} \circ T^{AA' \to BB'}_f\|_\diamond\right) \geq \log_2\left(\|(\rho^f_{AA'BB'})^{T_{BB'}}\|_1\right) = \log_2\left(\sqrt{d}+1\right)$$

$$E_{sq}\left(T^{AA' \to BB'}_f\right) \geq E^{AA':BB'}_{sq}\left(\rho^f_{AA'BB'}\right) = 1 + \frac{1}{2}\log_2(d).$$

These computations show that (27) improves upon the squashed entanglement and by the discussion following Theorem 2.4 also upon the entanglement cost bound for $d > 2$. For $d > 9$ our bound also improves upon the transposition bound. All these improvements can be made arbitrary large by increasing the dimension d.

6.2. Non-repeatable private capacity.

In [17] a general paradigm has been introduced for sharing key using several quantum states sequentially connecting communication nodes to bridge a possibly long distance between the communicating parties A and B. Consider the case where only one intermediate node C connected to A and B by quantum states $\rho^{(1)}_{AC}$ and $\rho^{(2)}_{CB}$ is available. The supremum of rates with which private key can be established between A and B using arbitrary LOCC-operations acting on many copies of the two states is the repeatable key rate $\mathcal{K}_{A \leftrightarrow C \leftrightarrow B}\left(\rho^{(1)}_{AC}, \rho^{(2)}_{CB}\right)$ (see [17]).

It is clear that in the same scenario any pair of states with distillable entanglement [40] can be used to create entanglement between A and B by first distilling maximally entangled states between connecting A, C and C, B and then using a standard repeater protocol. A similar statement is false when distillable key (instead of distillable entanglement) is considered. In particular there are bipartite quantum states $\rho_d \in \mathcal{D}\left(\mathbb{C}^d \otimes \mathbb{C}^2 \otimes \mathbb{C}^d \otimes \mathbb{C}^2\right)$ (see [17]) from which private key can be extracted at rate close to 1, but for which the repeatable key rate fulfills $\mathcal{K}_{A \leftrightarrow C \leftrightarrow B}(\rho_d, \rho_d) \approx 0$.

Here we introduce the private repeater capacity of a pair of quantum channels. This is a channel-version of the repeatable key rate with one intermediate node. Again the two parties A and B communicate via an intermediate communication node C but now use two quantum channels (from A to C and from C to B) and arbitrary classical communication (between all three parties) to establish their secret key.

Note that this is a more realistic scenario than the state-version of [17]. It is conceivable that in an actual communication scenario the communicating parties have quantum channels to establish the quantum correlations for the creation of a secret key. But then it would be artificial to restrict possible protocols to those creating a number of copies of a fixed quantum state which are then used to obtain a secret key (see [17]). Here
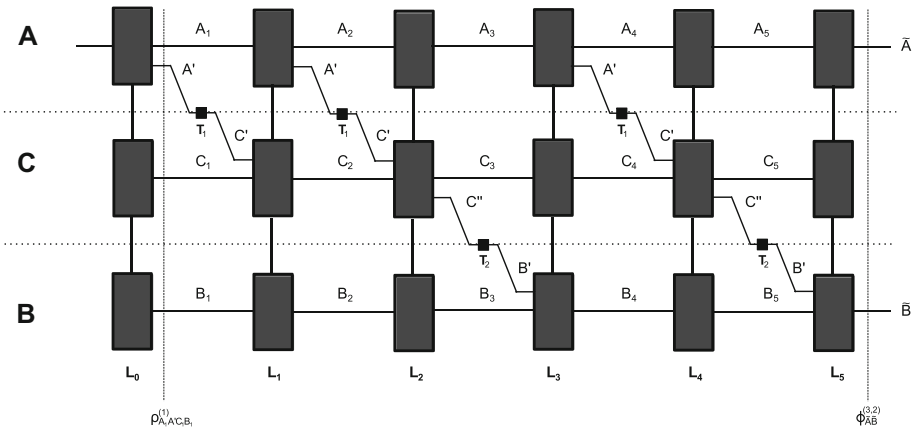
Fig. 2. Repeater coding scheme for private state generation assisted by classical communication (cf. Definition 6.1) in the case of $m^1 = 3$ uses of the channel $T_1 : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{C'}}$ and $m^2 = 2$ uses of the channel $T_2 : \mathcal{M}_{d_{C''}} \to \mathcal{M}_{d_{B'}}$ and channel order $w = (1, 1, 2, 1, 2)$. Here L_0 denotes an LOCC-operation used to create the separable initial state $\rho^{(1)}_{A_1 A' B_1}$.

we consider general protocols allowing for different inputs for the quantum channels at each stage of the protocol possibly depending on measurement outcomes and classical information shared at earlier stages.

Even in this general framework there are channels with non-repeatable private capacity. In particular we give an example of quantum channels (which are derived from the family of states considered in [17]) with private capacity $\mathcal{P}_\leftrightarrow$ close to 1, but arbitrarily small private repeater capacity. We begin with the definition of the private repeater capacity.

Definition 6.1 (*Repeater coding schemes assisted by classical communication.*) Let $T_1 : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{C'}}$ and $T_2 : \mathcal{M}_{d_{C''}} \to \mathcal{M}_{d_{B'}}$ denote two quantum channels where C' and C'' denote systems controlled by a party C. A (k, m^1, m^2, ϵ)-repeater coding scheme for private state generation assisted by classical communication (see Fig. 2) is given by a word $w \in \{1, 2\}^m$ for $m = m^1 + m^2$ with $|\{i : w_i = 1\}| = m^1$ (and $|\{i : w_i = 2\}| = m^2$), a separable initial state

$$\rho^{(1)} \in \begin{cases} \mathrm{Sep}_{A_1 A':C_1:B_1}\left(\mathbb{C}^{d_{A_1} d_{A'}} \otimes \mathbb{C}^{d_{C_1}} \otimes \mathbb{C}^{d_{B_1}}\right), & \text{if } w_1 = 1 \\ \mathrm{Sep}_{A_1:C_1 C':B_1}\left(\mathbb{C}^{d_{A_1}} \otimes \mathbb{C}^{d_{C_1} d_{C'}} \otimes \mathbb{C}^{d_{B_1}}\right), & \text{if } w_1 = 2 \end{cases}$$

and a set of LOCC-operations (w.r.t. the bipartition into A, B and C systems)

$$L_i : \mathcal{M}_{d_{A_i}} \otimes \mathcal{M}_{d_{C_i}} \otimes \mathcal{M}_{d_{B_i}} \otimes \mathcal{M}_{d_{D_{w_i}}} \to \mathcal{M}_{d_{A_{i+1}}} \otimes \mathcal{M}_{d_{C_{i+1}}} \otimes \mathcal{M}_{d_{B_{i+1}}} \otimes \mathcal{M}_{d_{E_{w_i}}}$$

for each $i \in \{1, \ldots, m - 1\}$ and

$$L_m : \mathcal{M}_{d_{A_m}} \otimes \mathcal{M}_{d_{C_m}} \otimes \mathcal{M}_{d_{B_m}} \otimes \mathcal{M}_{d_{D_{w_m}}} \to \mathcal{M}_{d_{\bar{A}}} \otimes \mathcal{M}_{d_{\bar{B}}}.$$

Here we set $D_1 = A'$ (i.e. a system at party A) and $D_2 = C''$ (i.e. a system at party C) and in the same way $E_1 = C'$ (i.e. a system at party C) and $E_2 = B'$ (i.e. a system at

party B). The dimensions $d_{A_i}, d_{B_i}, d_{C_i} \in \mathbb{N}$ and $d_{\tilde{A}} = d_{\tilde{B}}$ are arbitrary. Furthermore, we require the output state

$$\phi_{\tilde{A}\tilde{B}}^{(m^1, m^2)} = L_m \circ \prod_{i=1}^{m-1} \left(T_{w_i}^{D_{w_i} \to E_{w_i}} \circ L_i \right) \circ T_{w_1}^{D_{w_1} \to E_{w_1}} \left(\rho^{(1)} \right)$$

to fulfill

$$\epsilon = \frac{1}{2} \| \phi_{\tilde{A}\tilde{B}}^{(m^1, m^2)} - \gamma_{\tilde{A}\tilde{B}} \|_1$$

for a private state $\gamma_{\tilde{A}\tilde{B}}$ with 2^k-dimensional key part (see Definition 2.6).

Note that the order (and number) of channel applications (specified by the word w) in the protocols from Definition 6.1 is deterministic in the sense, that it cannot depend on outcomes of measurements made during the protocol. This is to avoid the complications from determining the rate of a protocol where the order and number of channel applications is not fixed.

Definition 6.2 (*Repeated private capacity assisted by classical communication*). We call $R \in \mathbb{R}^+$ an achievable rate for repeated private communication over the quantum channels $T_1 : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{C'}}$ and $T_2 : \mathcal{M}_{d_{C''}} \to \mathcal{M}_{d_{B'}}$ assisted by classical communication iff for each $\nu \in \mathbb{N}$ there exists a $(k_\nu, m_\nu^1, m_\nu^2, \varepsilon_\nu)$-repeater coding scheme for private state generation assisted by classical communication (as in Definition 6.1) with $m_\nu^1, m_\nu^2 \to \infty$ as $\nu \to \infty$ such that $R = \min \left(\lim_{\nu \to \infty} \frac{k_\nu}{m_\nu^1}, \lim_{\nu \to \infty} \frac{k_\nu}{m_\nu^2} \right)$ and $\lim_{\nu \to \infty} \varepsilon_\nu = 0$. The repeated private capacity $\mathcal{P}_{A \leftrightarrow C \leftrightarrow B}(T_1, T_2)$ is defined to be the supremum of all such achievable rates.

Before stating our main result we will discuss some properties of the repeated private capacity. For quantum channels $T_1 : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{C'}}$ and $T_2 : \mathcal{M}_{d_{C''}} \to \mathcal{M}_{d_{B'}}$ consider a sequence of coding schemes for $\mathcal{P}_{A \leftrightarrow C \leftrightarrow B}(T_1, T_2)$ achieving a rate $R > 0$. By combining the parties A and C (or C and B) any such sequence can be transformed into a sequence of coding schemes for $\mathcal{P}_{\leftrightarrow}(T_2)$ (or $\mathcal{P}_{\leftrightarrow}(T_1)$) achieving at least the same rate $R > 0$. Therefore the following bound holds

$$\mathcal{P}_{A \leftrightarrow C \leftrightarrow B}(T_1, T_2) \leq \min \left(\mathcal{P}_{\leftrightarrow}(T_1), \mathcal{P}_{\leftrightarrow}(T_2) \right). \tag{28}$$

We also have the following lemma similar to [17, Lemma 12]:

Lemma 6.1 (Transposition trick). *Let* $T_1 : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{C'}}$ *and* $T_2 : \mathcal{M}_{d_{C''}} \to \mathcal{M}_{d_{B'}}$ *be two quantum channels such that* $\vartheta_{d_{C'}} \circ T_1$ *and* $T_2 \circ \vartheta_{d_{C''}}$ *are quantum channels as well (here* $\vartheta_d : \mathcal{M}_d \to \mathcal{M}_d$ *denotes the matrix transposition in any fixed basis). Then we have*

$$\mathcal{P}_{A \leftrightarrow C \leftrightarrow B}(T_1, T_2) = \mathcal{P}_{A \leftrightarrow C \leftrightarrow B}(\vartheta_{d_{C'}} \circ T_1, T_2 \circ \vartheta_{d_{C''}}).$$

Proof. The proof goes by transforming any protocol for the channels T_1 and T_2 into a protocol for the channels $\tilde{T}_1 = \vartheta_{d_{C'}} \circ T_1$ and $\tilde{T}_2 = T_2 \circ \vartheta_{d_{C''}}$ leaving the output state unchanged. For $m^1, m^2 \in \mathbb{N}$ consider a word $w \in \{1, 2\}^m$ for $m = m^1 + m^2$ with $|\{i : w_i = 1\}| = m^1$ (and $|\{i : w_i = 2\}| = m^2$). Now consider a protocol for

repeated private state generation over the quantum channels $T_1 : \mathcal{M}_{d_{A'}} \to \mathcal{M}_{d_{C'}}$ and $T_2 : \mathcal{M}_{d_{C''}} \to \mathcal{M}_{d_{B'}}$ assisted by classical communication as in Definition 6.1 where w specifies the order of channel uses. This protocol is given by a the set of LOCC-operations $\{L_i\}_{i=1}^{m}$ (w.r.t. to the parties A, B and C) and initial state $\rho^{(1)}$, creating the output state (see Definition 6.1)

$$\phi_{\tilde{A}\tilde{B}}^{(m^1,m^2)} = L_m \circ \prod_{i=1}^{m-1} \left(T_{w_i}^{D_{w_i} \to E_{w_i}} \circ L_i \right) \circ T_{w_1}^{D_{w_1} \to E_{w_1}} \left(\rho^{(1)} \right).$$

For each $i \in \{1, \ldots, m-1\}$ we can define new LOCC-operations by

$$\tilde{L}_i = \vartheta_{\hat{C}_{i+1}} \circ L_i \circ \vartheta_{\hat{C}_i'}$$

where we denote by $\hat{C}_i'$ all systems at party C in step i after the channel (either T_1 or T_2) has been applied (see Definition 6.1). Similarly we denote by $\hat{C}_{i+1}$ all systems at party C before the channel has been applied. The $\tilde{L}_i$ are indeed LOCC-operations, which can be seen from writing L_i in its Kraus-decomposition (according to (10)) and applying the partial transpositions. In the final step we define

$$\tilde{L}_m = L_m \circ \vartheta_{\hat{C}_m'},$$

which is again LOCC (w.r.t. to the A, B and C systems) as there is no C system at the output of this map. We also define a new initial state $\tilde{\rho}^{(1)}$ by

$$\tilde{\rho}^{(1)} = \vartheta_{\hat{C}_1} \left(\rho^{(1)} \right), \tag{29}$$

which is a state since $\rho^{(1)}$ was chosen to be separable (see Definition 6.1).

Now note that the LOCC-operations $\{\tilde{L}_i\}_{i=1}^{m}$ with initial state $\tilde{\rho}^{(1)}$ define a new protocol for repeated private state generation (with the same word w as before) for the transposed channels $\tilde{T}_1 = \vartheta_{d_{C'}} \circ T_1$ and $\tilde{T}_2 = T_2 \circ \vartheta_{d_{C''}}$. The output state of the new protocol can be computed and is given by

$$\tilde{\phi}_{\tilde{A}\tilde{B}}^{(m^1,m^2)} = \tilde{L}_m \circ \prod_{i=1}^{m-1} \left(\tilde{T}_{w_i}^{D_{w_i} \to E_{w_i}} \circ \tilde{L}_i \right) \circ \tilde{T}_{w_1}^{D_{w_1} \to E_{w_1}} \left(\tilde{\rho}^{(1)} \right)$$

$$= L_m \circ \vartheta_{\hat{C}_m'} \circ \prod_{i=1}^{m-1} \left(\tilde{T}_{w_i}^{D_{w_i} \to E_{w_i}} \circ \vartheta_{\hat{C}_{i+1}} \circ L_i \circ \vartheta_{\hat{C}_i'} \right) \circ \tilde{T}_{w_1}^{D_{w_1} \to E_{w_1}} \left(\vartheta_{\hat{C}_1} \left(\rho^{(1)} \right) \right)$$

$$= L_m \circ \prod_{i=1}^{m-1} \left(T_{w_i}^{D_{w_i} \to E_{w_i}} \circ L_i \right) \circ T_{w_1}^{D_{w_1} \to E_{w_1}} \left(\rho^{(1)} \right) = \phi_{\tilde{A}\tilde{B}}^{(m^1,m^2)}$$

where we used that

$$\vartheta_{\hat{C}_i'} \circ \tilde{T}_{w_i}^{D_{w_i} \to E_{w_i}} \circ \vartheta_{\hat{C}_i} = T_{w_i}^{D_{w_i} \to E_{w_i}}$$

for each $i \in \{1, \ldots, m\}$. This shows that any protocol for the channels T_1 and T_2 corresponds to a protocol for the channels $\vartheta_{d_{C'}} \circ T_1$ and $T_2 \circ \vartheta_{d_{C''}}$ with the same output state and hence the same error. Therefore, the achievable rates for both scenarios are the same and so are their capacities. $\quad\square$

We will need a particular state constructed in [17]. Consider the state $\rho_d \in \mathcal{D}\left(\mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_A} \otimes \mathbb{C}^{d_{B'}} \otimes \mathbb{C}^{d_B}\right)$ for $d_A = d_B = d$ and $d_{A'} = d_{B'} = 2$ defined as

$$\rho_d = \frac{1}{2} \begin{pmatrix} (1 - p(d))\frac{\mathbb{1}_d}{d} \otimes \frac{\mathbb{1}_d}{d} & 0 & 0 & (1-p(d))X \\ 0 & p(d)\sqrt{YY^\dagger} & 0 & 0 \\ 0 & 0 & p(d)\sqrt{Y^\dagger Y} & 0 \\ (1-p(d))X^\dagger & 0 & 0 & (1-p(d))\frac{\mathbb{1}_d}{d} \otimes \frac{\mathbb{1}_d}{d} \end{pmatrix}. \tag{30}$$

Here we used $p(d) = \frac{1}{\sqrt{d}+1}$ and matrices

$$X = \frac{1}{d\sqrt{d}} \sum_{i,j=1}^{d} u_{ij}|ij\rangle\langle ji|$$

$$Y = \frac{1}{d} \sum_{i,j=1}^{d} u_{ij}|ii\rangle\langle jj|$$

where $U = (u_{ij})_{ij}$ denotes the quantum Fourier transform given by

$$U|k\rangle = \frac{1}{\sqrt{d}} \sum_{j=1}^{d} e^{2\pi ijk/d}|j\rangle.$$

The state ρ_d has been constructed such that it has positive partial transpose, but it is also close to a private state. More specifically we have

$$\|\rho_d - \gamma_2\|_1 \leq 2p(d) = \frac{2}{\sqrt{d}+1}$$

for the private state

$$\gamma_2 = \frac{1}{2} \begin{pmatrix} \frac{\mathbb{1}_d}{d} \otimes \frac{\mathbb{1}_d}{d} & 0 & 0 & X \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ X^\dagger & 0 & 0 & \frac{\mathbb{1}_d}{d} \otimes \frac{\mathbb{1}_d}{d} \end{pmatrix}$$

with 2-dimensional key part (see [17]). Now we can state the main result of this section:

Theorem 6.1 (Non-repeatable private capacity). *There is a quantum channel* $T_d : \mathcal{M}_2 \otimes \mathcal{M}_d \to \mathcal{M}_2 \otimes \mathcal{M}_d$ *such that*

$$\mathcal{P}_{\leftrightarrow}(T_d) \geq 1 - h_2\left(\frac{1}{\sqrt{d}+1}\right) \to 1,$$

but

$$\mathcal{P}_{A \leftrightarrow C \leftrightarrow B}(T_d, T_d) \leq \log_2\left(1 + \frac{1}{\sqrt{d}+1}\right) \to 0$$

as $d \to \infty$. *Here* $h_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ *denotes the binary entropy.*

Proof. Note that $\text{tr}_{BB'}(\rho_d) = \frac{\mathbb{1}_2}{2} \otimes \frac{\mathbb{1}_d}{d}$, which implies that ρ_d (see (30)) is the Choi matrix [13] of a quantum channel T_d. Moreover, since ρ_d has positive partial transpose both linear maps $\vartheta_{2d} \circ T_d$ and $T_d \circ \vartheta_{2d}$ are also quantum channels. The private capacity of T_d fulfills

$$\mathcal{P}_{\leftrightarrow}(T_d) \geq \mathcal{K}_{\leftrightarrow}(\rho_d) \geq 1 - h_2(\frac{1}{\sqrt{d}+1})$$

where the second inequality has been proved in [17, p. 27]. In order to show the second statement in the theorem we note that by Lemma 6.1 and (28)

$$\mathcal{P}_{A \leftrightarrow C \leftrightarrow B}(T_d, T_d) = \mathcal{P}_{A \leftrightarrow C \leftrightarrow B}(\vartheta_{2d} \circ T_d, T_d \circ \vartheta_{2d}) \leq \mathcal{P}_{\leftrightarrow}(\vartheta_{2d} \circ T_d).$$

By the non-regularized bound from Corollary 4.1 and the simpler bound from Theorem 5.2 we have

$$\mathcal{P}_{\leftrightarrow}(\vartheta_{2d} \circ T_d) \leq E_{\max}(\vartheta_{2d} \circ T_d) \leq B_{\max}(\vartheta_{2d} \circ T_d) \leq D_{\max}\left(\rho_d^{T_{B'B}} \| C_S\right)$$

where we choose the separable Choi matrix

$$C_S = \frac{1}{2(1+p(d))} \begin{pmatrix} (1-p(d))\frac{\mathbb{1}_d}{d} \otimes \frac{\mathbb{1}_d}{d} & 0 & 0 & 0 \\ 0 & 2p(d)\sqrt{YY^{\dagger}} & 0 & 0 \\ 0 & 0 & 2p(d)\sqrt{Y^{\dagger}Y} & 0 \\ 0 & 0 & 0 & (1-p(d))\frac{\mathbb{1}_d}{d} \otimes \frac{\mathbb{1}_d}{d} \end{pmatrix}.$$

It can be easily checked that C_S is the Choi matrix of an entanglement-breaking channel S. Note that

$$\rho_d^{T_{B'B}} = \frac{1}{2} \begin{pmatrix} (1-p(d))\frac{\mathbb{1}_d}{d} \otimes \frac{\mathbb{1}_d}{d} & 0 & 0 & 0 \\ 0 & p(d)\sqrt{YY^{\dagger}} & p(d)Y & 0 \\ 0 & p(d)Y^{\dagger} & p(d)\sqrt{Y^{\dagger}Y} & 0 \\ 0 & 0 & 0 & (1-p(d))\frac{\mathbb{1}_d}{d} \otimes \frac{\mathbb{1}_d}{d}. \end{pmatrix}$$

and a straightforward computation shows that $D_{\max}\left(\rho_d^{T_{B'B}} \| C_S\right) \leq \log_2(1+p(d))$. This implies that

$$\mathcal{P}_{A \leftrightarrow C \leftrightarrow B}(T_d, T_d) \leq \log_2(1+p(d)) = \log_2\left(1 + \frac{1}{\sqrt{d}+1}\right).$$

$\square$

7. Conclusion

We established a new inequality involving the sandwiched α-Rényi divergences and used it to study private communication via quantum channels assisted by classical communication. Specifically, we proved a strong-converse bound on the private capacity assisted by unlimited classical two-way communication. Moreover, this is the first such bound that is non-lockable. We exploited this fact to provide examples of quantum channels for which our bound improves on the transposition bound (Theorem 2.2), the squashed entanglement bound (Theorem 2.3) and the entanglement cost bound (Theorem 2.4).

Furthermore, we used the bound to analyze a quantum repeater version of the private capacity.

There are some open problems and directions of future research. The main open problem is to show that the relative entropy of entanglement of a quantum channel (instead of the max-relative entropy of entanglement, see (9)) is an upper bound (and possibly a strong-converse bound) on $P_{\leftrightarrow}$. So far, this bound has only been shown for teleportation-covariant quantum channels [6]. Such a result might be obtained from the bound in Theorem 4.1 (or Corollary 4.1) using a smoothing technique (cf. [27]).

It should be noted that quantities similar to (9) for different entanglement measures (replacing the max-relative entropy of entanglement) based on the sandwiched α-Rényi divergences have been studied before. In [35] the α-Rains information of a quantum channel (based on a generalization of the Rains bound on distillable entanglement [41]) has been introduced. Here instead of optimizing over separable states leading to a relative entropy of entanglement (cf. Definition 2.1) the optimization runs over a larger set (the so called Rains set) of positive matrices (see [35] for details). To our knowledge it is not known whether the α-Rains information (for any $\alpha \geq 1$) gives a strong converse bound (or even an upper bound) on $\mathcal{Q}_{\leftrightarrow}$. For $\alpha = \infty$ this follows almost from our work. The only problem seems to be in the final part of the proof of Theorem 3.2, where we cannot reduce the quantity involving the three systems A, B' and B to the Rains information (only involving two systems).

Finally, we should say that the main results from this paper can be extended to infinite dimensional systems using the general framework of non-commutative L_p-spaces [42]. This will be contained in future work.

Appendix A: Implementability of Quantum Channels via LOCC Operations

Here we study the class of quantum channels implementable via LOCC-operations from a bipartite state shared between the communicating parties. For such channels the interactive protocols of Definition 2.3 reduce to protocols involving only LOCC-operations performed on copies of the fixed state used for the implementation (see [12]). It is easy to see [6,9] that the distillable entanglement (key) of this state gives an upper bound on the performance of such protocols in the cases of quantum (private) communication.

The reduction of protocols described above is especially interesting when the state used for implementation of the quantum channel is itself preparable using the quantum channel exactly once (see below for a precise definition). This holds e.g. for teleportation-covariant channels (see [6]). In this case the capacities $\mathcal{Q}_{\leftrightarrow}$ and $\mathcal{P}_{\leftrightarrow}$ of the channel are equal to (not only upper bounded by) the distillable entanglement and distillable key respectively of the state used for implementation. Moreover, since this state can be produced using the channel, entanglement measures (e.g. squashed entanglement, relative entropy of entanglement, etc.) of the state can be related to the corresponding quantities of the channel (see also Theorem A.1 below). In this way [6,9] derive their upper bounds on the private capacity for particular classes of channels.

The quantum channels implementable from states using the teleportation protocol have been characterized in [43]. However, in the case of general protocols such a characterization is still missing, and it is not known which quantum channels can be implemented in this way. Here we give an example of a quantum channel, which cannot be implemented by any LOCC-protocol using a state preparable by only a single use of the quantum channel itself. We begin with a definition:

Definition A.1. We call a quantum channel $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ **implementable from its image** if there exists a bipartite quantum state $\sigma_{A''A'} \in \mathcal{D}\left(\mathbb{C}^{d_{A''}} \otimes \mathbb{C}^{d_{A'}}\right)$ for some $d_{A''} \in \mathbb{N}$ and $d_{A'} = d_A$ and an LOCC-operation $\Lambda : \mathcal{M}_{d_A d_{A''}} \otimes \mathcal{M}_{d_{B'}} \to \mathcal{M}_{d_B}$ for $d_{B'} = d_B$ with respect to the bipartition into A and B systems such that

$$T^{A \to B}(\rho_A) = \Lambda^{AA'':B' \to B}\left(\rho_A \otimes (\mathrm{id}_{A''} \otimes T^{A' \to B'})(\sigma_{A''A'})\right) \tag{31}$$

for any $\rho_A \in \mathcal{D}_{d_A}$.

Consider an LOCC-monotone $E^{A:B} : \mathcal{D}\left(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B}\right) \to \mathbb{R}_0^+$ for bipartite states. Formally, $E^{A:B}$ is a family of functions depending on the dimensions d_A and d_B decreasing under LOCC-operations applied to the input (LOCC with respect to the chosen bipartition $A : B$). To simplify notation we will omit the dependence on the dimensions. Now we define an associated quantity for quantum channels $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ by setting

$$E(T) = \sup_{\rho_{A'A}} E^{A':B}\left(\left(\mathrm{id}_{A'} \otimes T^{A \to B}\right)(\rho_{A'A})\right).$$

where the supremum is over states $\rho_{A'A} \in \mathcal{D}\left(\mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_A}\right)$ with arbitrary $d_{A'} \in \mathbb{N}$ (note that this quantity is not finite in general, but it will be in the examples we consider). We have the following simple consequence for quantum channels implementable from their image:

Theorem A.1. *For any LOCC-monotone $E^{A:B}$ and any quantum channel $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ implementable from its image, i.e. of the form* (31) *for some state $\sigma_{A''A'} \in \mathcal{D}\left(\mathbb{C}^{d_{A''}} \otimes \mathbb{C}^{d_{A'}}\right)$, we have*

$$E(T) = E^{A'':B'}\left(\left(\mathrm{id}_{A''} \otimes T^{A' \to B'}\right)(\sigma_{A''A'})\right).$$

Proof. The inequality "$\geq$" is clear. As $E^{A:B}$ is an LOCC-monotone we have

$$
\begin{aligned}
E(T) &= \sup_{\rho_{A'''A}} E^{A''':B}\left(\left(\mathrm{id}_{A'''} \otimes T^{A \to B}\right)(\rho_{A'''A})\right) \\
&= \sup_{\rho_{A'''A}} E^{A''':B}\left(\left(\mathrm{id}_{A'''} \otimes \Lambda^{AA'':B' \to B}\right)\left(\rho_{A'''A} \otimes (\mathrm{id}_{A''} \otimes T^{A' \to B'})(\sigma_{A''A'})\right)\right) \\
&\leq \sup_{\rho_{A'''A}} E^{A'''AA'':B'}\left(\rho_{A'''A} \otimes (\mathrm{id}_{A''} \otimes T^{A' \to B'})(\sigma_{A''A'})\right) \\
&= E^{A'':B'}\left((\mathrm{id}_{A''} \otimes T^{A' \to B'})(\sigma_{A''A'})\right).
\end{aligned}
$$

Here the last equality follows from the fact that removing or adding a local uncorrelated system is an LOCC-operation.

In the following we will only evaluate the LOCC-monotones E_R and E_{sq} on bipartite states where the systems in the bipartition are clear from context. Therefore, we will omit the indices denoting these systems to simplify notation. Now we can present the main result of this appendix:

Theorem A.2. *There exists a quantum channel $T : \mathcal{M}_{d_A} \to \mathcal{M}_{d_B}$ for some dimensions $d_A, d_B \in \mathbb{N}$ that is not implementable from its image, i.e. there is no state $\sigma_{A''A'}$ and LOCC protocol Λ such that T can be written as in* (31).

For the proof we will need some special states. The antisymmetric state $\alpha_d \in \mathcal{D}\left(\mathbb{C}^d \otimes \mathbb{C}^d\right)$ for $d \geq 2$ is defined as

$$\alpha_d = \frac{1}{d(d-1)} \left(\mathbb{1}_d \otimes \mathbb{1}_d - \mathbb{F}_d\right).$$

In [44, Lemma 6] it is shown that for even $d \in \mathbb{N}$

$$E_{sq}(\alpha_d) \leq \log_2\left(\frac{d+2}{d}\right). \tag{32}$$

It has also been shown in [44, Corollary 3] that for every $d \geq 2$ we have

$$\lim_{n \to \infty} \frac{1}{n} E_R\left(\alpha_d^{\otimes n}\right) \geq \log_2\left(\sqrt{\frac{4}{3}}\right).$$

Clearly, for any $\epsilon > 0$ this implies the existence of an $N_\epsilon \in \mathbb{N}$ such that

$$E_R\left(\alpha_d^{\otimes n}\right) \geq n\left(\log_2\left(\sqrt{\frac{4}{3}}\right) - \epsilon\right) \tag{33}$$

for all $n \geq N_\epsilon$. We will also use the flower states ρ_d^f from Sect. 6.1 considered as bipartite states with respect to the bipartition into A and B systems (both $2d$ dimensional, see (24)). Note that the squashed entanglement of the flower states has an easy formula (see (25)). Furthermore, as the partial trace $\text{tr}_{B'}\left(\rho_d^f\right)$ over the 2-dimensional B' system is separable we have (using non-lockability of E_R, see [36]) that

$$E_R\left(\rho_d^f\right) \leq 2. \tag{34}$$

Finally observe that for any $n, l \in \mathbb{N}$ and dimension $d = 2^n l^n$ we have

$$\tau_0 := \alpha_{2l}^{\otimes n} \in \mathcal{D}\left(\mathbb{C}^d \otimes \mathbb{C}^d\right) \tag{35}$$

and

$$\tau_1 := \rho_{2^{n-1}l^n}^f \in \mathcal{D}\left(\mathbb{C}^d \otimes \mathbb{C}^d\right). \tag{36}$$

Using the formulas for E_R and E_{sq} from above, and additivity of the squashed entanglement (see [30, Proposition 4]) we compute (with $N_{\frac{1}{2}}$ defined before (33))

$$E_R\left(\tau_0\right) \geq n\left(\log_2\left(\sqrt{\frac{4}{3}}\right) - \frac{1}{2}\right) \geq \frac{1}{2}n \text{ for all } n \geq N_{1/2}$$

$$E_R\left(\tau_1\right) \leq 2$$

$$E_{sq}\left(\tau_0\right) = nE_{sq}\left(\alpha_{2l}\right) \leq n\log_2\left(1 + \frac{1}{l}\right)$$

$$E_{sq}\left(\tau_1\right) = \frac{1}{2} + \frac{1}{2}n + \frac{1}{2}n\log_2\left(l\right).$$

Therefore, choosing n, l large enough we have

$$E_R\left(\tau_1\right) \ll E_R\left(\tau_0\right) \tag{37}$$

$$E_{sq}\left(\tau_1\right) \gg E_{sq}\left(\tau_0\right). \tag{38}$$

Proof of Theorem A.2. Choose $n, l \in \mathbb{N}$ large enough such that the states $\tau_0, \tau_1 \in \mathcal{D}\left(\mathbb{C}^d \otimes \mathbb{C}^d\right)$ (see (35) and (36)) for $d = 2^n l^n$ satisfy (37) and (38). Now define two channels $T_0, T_1 : \mathcal{M}_d \to \mathcal{M}_d$ with Choi matrices $C_{T_0} = \tau_0$ and $C_{T_1} = \tau_1$ (note that these maps are indeed trace-preserving).

The quantum channel T_0 is teleportation implementable (as the channel corresponding to the antisymmetric state is Weyl-covariant), i.e. it is of the form (31) with $\sigma = \tau_0$ and Λ the teleportation protocol (see [12]). Therefore, we can apply Theorem A.1 to conclude that

$$E_R\left(T_0\right) = E_R\left(\tau_0\right)$$

$$E_{sq}\left(T_0\right) = E_{sq}\left(\tau_0\right)$$

Let B' denote the 2-dimensional part of the output system of T_1 corresponding to the B' system of τ_1 (which is a flower state, see discussion following (24)). Then $\mathrm{tr}_{B'} \circ T_1$ is entanglement-breaking (as its Choi matrix is separable) and using non-lockability of E_R (see [36]) and the equations above we have

$$E_R\left(T_1\right) \leq 2 \ll E_R\left(\tau_0\right) = E_R\left(T_0\right). \tag{39}$$

For the squashed entanglement we obtain

$$E_{sq}\left(T_0\right) = E_{sq}\left(\tau_0\right) \ll E_{sq}\left(\tau_1\right) \leq E_{sq}\left(T_1\right). \tag{40}$$

Now consider the switch channel $T : \mathcal{M}_d \otimes \mathcal{M}_2 \to \mathcal{M}_d \otimes \mathcal{M}_2$ given by

$$T = T_0 \otimes P_0 + T_1 \otimes P_1$$

with projectors $P_i : \mathcal{M}_2 \to \mathcal{M}_2$ given by $P_i(\rho) = \langle i|\rho|i\rangle|i\rangle\langle i|$ for $i \in \{0, 1\}$. In the following we denote by "a" a 2-dimensional system at party A and by "b" a 2-dimensional system at party B. These will denote the switch systems used for the quantum channel T. As

$$\left(\mathrm{id}_{A'} \otimes T_i^{A \to B}\right)(\rho_{A'A}) \otimes |i\rangle\langle i|_b = \left(\mathrm{id}_{A'} \otimes T^{Aa \to Bb}\right)(\rho_{A'A} \otimes |i\rangle\langle i|_a),$$

for any $\rho_{A'A} \in \mathcal{D}\left(\mathbb{C}^{d_{A'}} \otimes \mathbb{C}^{d_A}\right)$ and $i \in \{0, 1\}$ we conclude that

$$E_R\left(T_i\right) \leq E_R\left(T\right) \tag{41}$$

$$E_{sq}\left(T_i\right) \leq E_{sq}\left(T\right). \tag{42}$$

Assume now that T is implementable from its image and let $\sigma_{A''A'a'} \in \mathcal{D}\left(\mathbb{C}^{d_{A''}} \otimes \mathbb{C}^{d_{A'}} \otimes \mathbb{C}^2\right)$ denote the state used for the implementation as in (31). Note that the dimension $d_{A''}$ is arbitrary and we consider the joint system $A'a'$ as the input (therefore taking the role of A' in (31)) for the channel. We can write

$$\sigma_{A''A'a'} = \sum_{i=0}^{1} \sum_{j=0}^{1} X_{A''A'}^{ij} \otimes |i\rangle\langle j|_{a'}$$

with matrices $X_{A''A'}^{ij} \in \mathcal{M}_{d_{A''}} \otimes \mathcal{M}_{d_{A'}}$. Positivity of $\sigma_{A''A'a'}$ implies positivity of $X_{A''A'}^{00}$ and $X_{A''A'}^{11}$. Now we have

$$\left(\mathrm{id}_{A''} \otimes T^{A'a'\to B'b'}\right)(\sigma_{A''A'a'}) = \sum_{i=0}^{1} \left(\mathrm{id}_{A''} \otimes T_i^{A'\to B'}\right)\left(X_{A''A'}^{ii}\right) \otimes |i\rangle\langle i|_{b'}.$$

As $\sigma_{A''A'a'}$ is normalized we can write

$$\left(\mathrm{id}_{A''} \otimes T^{A'a'\to B'b'}\right)(\sigma_{A''A'a'})$$
$$= p\left(\mathrm{id}_{A''} \otimes T_0^{A'\to B'}\right)\left(\sigma_{A''A'}^0\right) \otimes |0\rangle\langle 0|_{b'} + (1-p)\left(\mathrm{id}_{A''} \otimes T_1^{A'\to B'}\right)\left(\sigma_{A''A'}^1\right) \otimes |1\rangle\langle 1|_{b'} \tag{43}$$

for $p = \mathrm{tr}\left(X_{A''A'}^{00}\right) \in [0,1]$ and states

$$\sigma_{A''A'}^i = \begin{cases} \frac{1}{\mathrm{tr}\left(X_{A''A'}^{ii}\right)} X_{A''A'}^{ii}, & \text{if } \mathrm{tr}\left(X_{A''A'}^{ii}\right) \neq 0 \\ 0, & \text{else.} \end{cases}$$

Note that p only depends on σ. Now applying Theorem A.1 (as E_R and E_{sq} are LOCC-monotones) together with (43) and convexity of E_R and E_{sq} (see [30, Proposition 3] for the latter) we obtain

$$E_R(T) \leq pE_R(T_0) + (1-p)E_R(T_1) \tag{44}$$
$$E_{sq}(T) \leq pE_{sq}(T_0) + (1-p)E_{sq}(T_1) \tag{45}$$

Finally, it follows from (41), (44) and (39) that

$$E_R(T_0) \leq E_R(T) \leq pE_R(T_0) + (1-p)E_R(T_1) \leq E_R(T_0).$$

As $E_R(T_1) \ll E_R(T_0)$ this implies that $p = 1$. The same line of reasoning for the squashed entanglement using (42), (45) and (40) gives

$$E_{sq}(T_1) \leq E_{sq}(T) \leq pE_{sq}(T_0) + (1-p)E_{sq}(T_1) \leq E_{sq}(T_1).$$

As $E_{sq}(T_0) \ll E_{sq}(T_1)$ this implies that $p = 0$ which is a contradiction to the previous derivation. □

Note that the quantum channel T constructed in the previous example might be implementable using LOCC-operations and a state that can be prepared from two or more uses of the channel. This would be the case for example if the channel T_1 (coming from the flower state) would be implementable from its image. The reduction technique for interactive protocols (see [6]) would still apply then, however relating $\mathcal{Q}_{\leftrightarrow}$ (or $\mathcal{P}_{\leftrightarrow}$) to distillable entanglement (or distillable key) of a more complicated state. It is then not clear how to obtain e.g. the bound based on the relative entropy of entanglement of the quantum channel from the methods of [6] without an additional factor depending on the number of channel uses to prepare this state.

References

1. Shannon, C.: A mathematical theory of communication. Bell Syst. Tech. J. **27**(4), 623–656 (1948)
2. Takeoka, M., Guha, S., Wilde, M.M.: The squashed entanglement of a quantum channel. IEEE Trans. Inf. Theory **60**((8), 4987–4998 (2014)
3. Holevo, A.S., Werner, R.F.: Evaluating capacities of bosonic gaussian channels. Phys. Rev. A **63**, 032312 (2001)
4. Müller-Hermes, A., Reeb, D., Wolf, M.M.: Positivity of linear maps under tensor powers. J. Math. Phys. **57**((1), 015202 (2016)
5. Berta, M., Brando, F.G.S.L., Christandl, M., Wehner, S.: Entanglement cost of quantum channels. IEEE Trans. Inf. Theory **59**(10), 6779–6795 (2013)
6. Pirandola, S., Laurenza, R., Ottaviani, C., Banchi, L.: The ultimate rate of quantum cryptography. arXiv preprint arXiv:1510.08863 (2015)
7. Pirandola, S.: Optimal performance of a quantum network. arXiv preprint arXiv:1601.00966 (2016)
8. Takeoka, M., Seshadreesan, K.P., Wilde, M.M.: Unconstrained distillation capacities of a pure-loss bosonic broadcast channel. In: 2016 IEEE International Symposium on Information Theory (ISIT), pp. 2484–2488 (2016)
9. Wilde M.M., Tomamichel M., Berta M.: Converse bounds for private communication over quantum channels. IEEE Trans. Inf. Theory **63**(3), 1792–1817 (2017)
10. Pant, M., Krovi, H., Englund, D., Guha, S.: Rate-distance tradeoff and resource costs for all-optical quantum repeaters. Phys. Rev. A **95**, 012304 (2017)
11. Laurenza, R., Pirandola, S.: General bounds for sender–receiver capacities in multipoint quantum communications. arXiv preprint arXiv:1603.07262 (2016)
12. Bennett, C.H., DiVincenzo, D.P., Smolin, J.A., Wootters, W.K.: Mixed-state entanglement and quantum error correction. Phys. Rev. A **54**(5), 3824 (1996)
13. Choi, M.-D.: Completely positive linear maps on complex matrices. Linear Algebra Its Appl. **10**(3), 285–290 (1975)
14. Horodecki, K., Horodecki, M., Horodecki, P., Oppenheim, J.: Secure key from bound entanglement. Phys. Rev. Lett. **94**(16), 160502 (2005)
15. Datta, N.: Min- and max-relative entropies and a new entanglement monotone. IEEE Trans. Inf. Theory **55**(6), 2816–2826 (2009)
16. Datta, N.: Max-relative entropy of entanglement, alias log robustness. Int. J. Quantum Inf. **7**(02), 475–491 (2009)
17. Bäuml, S., Christandl, M., Horodecki, K., Winter, A.: Limitations on quantum key repeaters. Nat. Commun. **6**, 6908 (2015)
18. Müller-Lennert, M., Dupuis, F., Szehr, O., Fehr, S., Tomamichel, M.: On quantum Rényi entropies: a new generalization and some properties. J. Math. Phys. **54**(12), 122203 (2013)
19. Wilde, M.M., Winter, A., Yang, D.: 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)
20. Umegaki, H.: Conditional expectation in an operator algebra. IV. Entropy and information. Kodai Math. Sem. Rep. **14**(2), 59–85 (1962)
21. Beigi, S.: Sandwiched Rényi divergence satisfies data processing inequality. J. Math. Phys. **54**(12), 122202 (2013)
22. Penrose R.: A generalized inverse for matrices. Math. Proc. Cambridge Philos. Soc. **51**, 406–413 (1955)
23. Bergh, J., Löfström, J.: Interpolation Spaces: An Introduction, vol. 223. Springer, New York (2012)
24. Müller-Hermes, A., Reeb, D.: Monotonicity of the quantum relative entropy under positive maps. Ann. Henri Poincaré **18**(5), 1777–1788 (2017)
25. Frank, R.L., Lieb, E.H.: Monotonicity of a relative Rényi entropy. J. Math. Phys. **54**(12), 122201 (2013)
26. Brandão, F.G., Plenio, M.B.: A reversible theory of entanglement and its relation to the second law. Commun. Math. Phys. **295**(3), 829–851 (2010)
27. Brandão, F.G., Plenio, M.B.: A generalization of quantum Steins lemma. Commun. Math. Phys. **295**(3), 791–828 (2010)
28. Chitambar, E., Leung, D., Mančinska, L., Ozols, M., Winter, A.: Everything you always wanted to know about LOCC (but were afraid to ask). Commun. Math. Phys. **328**(1), 303–326 (2014)
29. Bennett, C.H., Brassard, G., Crépeau, C., Jozsa, R., Peres, A., Wootters, W.K.: Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels. Phys. Rev. Lett. **70**(13), 1895 (1993)
30. Christandl, M., Winter, A.: Squashed entanglement: an additive entanglement measure. J. Math. Phy. **45**(3), 829–840 (2004)
31. Tucci, R.R.: Entanglement of distillation and conditional mutual information. arXiv preprint arXiv:quant-ph/0202144 (2002)

32. Paulsen, V.: Completely Bounded Maps and Operator Algebras. Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge (2002)
33. Horodecki, K., Horodecki, M., Horodecki, P., Oppenheim, J.: General paradigm for distilling classical key from quantum states. IEEE Trans. Inf. Theory **55**(4), 1898–1929 (2009)
34. Fuchs, C.A., van de Graaf, J.: Cryptographic distinguishability measures for quantum-mechanical states. IEEE Trans. Inf. Theory **45**(4), 1216–1227 (1999)
35. Tomamichel, M., Wilde, M.M., Winter, A.: Strong converse rates for quantum communication. IEEE Trans. Inf. Theory **63**(1), 715–727 (2017)
36. Horodecki, K., Horodecki, M., Horodecki, P., Oppenheim, J.: Locking entanglement with a single qubit. Phys. Rev. Lett. **94**(20), 200501 (2005)
37. Roy, A., Scott, A.J.: Unitary designs and codes. Des. Codes Cryptogr. **53**(1), 13–31 (2009)
38. Horodecki, M., Shor, P.W., Ruskai, M.B.: Entanglement breaking channels. Rev. Math. Phys. **15**(06), 629–641 (2003)
39. Christandl, M., Winter, A.: Uncertainty, monogamy and locking of quantum correlations. In: Proceedings of the International Symposium on Information Theory, 2005. ISIT 2005, pp. 879–883 (2005)
40. Bennett, C.H., Bernstein, H.J., Popescu, S., Schumacher, B.: Concentrating partial entanglement by local operations. Phys. Rev. A **53**(4), 2046 (1996)
41. Rains, E.M.: A semidefinite program for distillable entanglement. IEEE Trans. Inf. Theory **47**(7), 2921–2933 (2001)
42. Pisier, G., Xu, Q.: Non-commutative Lp-spaces. Handb. Geom. Banach Spaces **2**, 1459–1517 (2003)
43. Bowen, G., Bose, S.: Teleportation as a depolarizing quantum channel, relative entropy, and classical capacity. Phys. Rev. Lett. **87**(26), 267901 (2001)
44. Christandl, M., Schuch, N., Winter, A.: Entanglement of the antisymmetric state. Commun. Math. Phys. **311**(2), 397–422 (2012)