Quantum message compression with applications

Anurag Anshu
Centre for Quantum Technologies,
National University of Singapore
a0109169@u.nus.edu

Vamsi Krishna Devabathini
Centre for Quantum Technologies,
National University of Singapore
devabathini92@gmail.com

Rahul Jain
Centre for Quantum Technologies and
Department of Computer Science,
National University of Singapore
MajuLab, CNRS-UNS-NUS-NTU
International Joint Research Unit,
UMI 3654, Singapore.
rahul@comp.nus.edu.sg

We present a new scheme for the compression of one-way quantum messages, in the setting of coherent entanglement assisted quantum communication. For this, we present a new technical tool that we call the *convex split* lemma, which is inspired by the classical compression schemes that use *rejection sampling* procedure. As a consequence, we show new bounds on the quantum communication cost of single-shot entanglement-assisted one-way *quantum state redistribution* task and for the sub-tasks *quantum state splitting* and *quantum state merging*. Our upper and lower bounds are tight upto a constant and hence stronger than previously known best bounds for above tasks. Our protocols use explicit quantum operations on the sides of Alice and Bob, which are different from the *decoupling by random unitaries* approach used in previous works. As another application, we present a port-based teleportation scheme which works when the set of input states is restricted to a known ensemble, hence potentially saving the number of required ports. Furthermore, in case of no prior knowledge about the set of input states, our average success fidelity matches the known average success fidelity, providing a new port-based teleportation scheme with similar performance as appears in literature.

Quantum message compression is a fundamental area of quantum information theory. Schumacher[Sch95] provided one of the first such schemes for source compression which was a direct quantum analogue of the celebrated classical source-coding scheme of Shannon [Sha]. To capture more general quantum tasks, such as those involving side information with the receiver, the work [HOW07] introduced the task of *quantum state merging*. This work also provided an operational interpretation to quantum conditional entropy, the negativity of which is a well known example of peculiarities of quantum information. The task of *quantum state splitting* was subsequently introduced in [ADHW09]. A central theme in these results is the notion of a purifying system (often termed as the reference system), which brings an element of coherence in quantum protocols. Originally studied in the asymptotic and i.i.d setting, these tasks were also subsequently studied the one-shot setting [Ber09, BCR11].

The task of *quantum state redistribution* elegantly captures the problem of coherent quantum message compression. In this task, Alice, Bob and Referee share a pure state $|\Psi\rangle_{RABC}$, with AC belonging to Alice, B to Bob and R to Referee. Alice wants to transfer the register C to Bob, such that the final state Φ_{RABC} satisfies $\mathrm{F}(\Phi_{RABC}, \Psi_{RABC}) \geq \sqrt{1-\varepsilon^2}$, for a given $\varepsilon \geq 0$. Here $\mathrm{F}(.,.)$ is fidelity.

This problem has been well studied in the literature both in the asymptotic and single-shot settings (see e.g. [DY08, Opp08, YBW08, YD09, Dup10, BD10, DH11, DBWR14, DHO14] and references therein). Quantum state merging is a special case of this task when register A is not present and quantum state splitting is the special case in which register B is not present. In the setting where Alice, Bob and Referee share n copies of independent and identical states $\Psi_{RABC}^{\otimes n}$, it was shown by Devatak and Yard [DY08, YD09] (see also Luo and Devatak [LD09]) that the quantum communication cost, using one-way communication and shared-entanglement, for quantum state redistribution approaches $n\mathrm{I}(C : R|B)_{\Psi}$ as $n \to \infty$ and error $\varepsilon \to 0$. Here, $\mathrm{I}(C : R|B)_{\Psi} = \mathrm{S}(\Psi_{RB}) + \mathrm{S}(\Psi_{BC}) - \mathrm{S}(\Psi_B) - \mathrm{S}(\Psi_{RBC})$ is the quantum *conditional mutual information* and $\mathrm{S}(.)$ is the von-neumann entropy. Subsequently, it was shown by Oppenheim [Opp08] that quantum state redistribution can be realized with two application of a protocol for quantum state merging. It was independently shown by Ye *et.al.* [YBW08] that quantum state redistribution can be realized with application of protocols for quantum state merging and quantum state splitting.

Recently, in independent works by Berta, Christandl, Touchette [BCT16] and Datta, Hsieh, Oppenheim [DHO14], single-shot entanglement-assisted one-way protocols for quantum state redistribution have been proposed. The work [BCT16] also provides several lower bounds with gaps between the upper and lower bounds and the question of closing these gaps has been left open. The upper bound of [BCT16] and [DHO14] has recently been used by Touchette [Tou15] to obtain a *direct-sum result* for bounded-round entanglement-assisted quantum communication complexity.

In this work, we introduce a novel technique for compressing coherent quantum information. As an immediate application, we exhibit a quantity that near-optimally captures the communication costs of quantum state re-distribution and present near optimal bounds for quantum state merging and quantum state splitting. We also give applications to the case of port- based teleportation, presenting schemes which allow port based teleportation when the states to be sent belong to a given ensemble. Our compression protocol has an important property of being explicit and using simple form of shared entanglement. Our techniques have also found recent application in the work [MBD$^+$16], in context of catalytic decoupling. We note that improved version of our main lemma, as presented below, also quantitatively improves one of the results in [MBD$^+$16].

Preliminaries

We represent the set of quantum states on a register A with the symbol $\mathcal{D}(A)$. A subscript to a quantum state represents the register associated to it. Fidelity between states ρ, σ is represented as $\mathrm{F}(\rho,\sigma) \stackrel{\mathrm{def}}{=} \|\sqrt{\rho}\sqrt{\sigma}\|_1$. We shall use the notation of *epsilon ball*, representing $\mathcal{B}^{\varepsilon}(\rho)$ as the set of all states σ such that $\mathrm{F}^2(\rho,\sigma) \geq 1-\varepsilon^2$. The *relative entropy* between quantum states ρ, σ is defined as $\mathrm{D}(\rho\|\sigma) = \mathrm{Tr}(\rho\log\rho) - \mathrm{Tr}(\rho\log\sigma)$. The *max-entropy* is defined as $\mathrm{D}_{\max}(\rho\|\sigma) \stackrel{\mathrm{def}}{=} \inf\{\lambda : \rho \leq 2^{\lambda}\sigma\}$, where $A \leq B$ (for hermitian matrices A, B) implies that $B-A$ is a positive semidefinite matrix. The *max-information* of a bipartite state ρ_{AB} is defined as $\mathrm{I}_{\max}(A:B)_{\rho} \stackrel{\mathrm{def}}{=} \inf_{\sigma\in\mathcal{D}(B)}\mathrm{D}_{\max}(\rho_{AB}\|\rho_A\otimes\sigma_B)$. The *smooth max-information is defined as* $\mathrm{I}^{\varepsilon}_{\max}(A:B)_{\rho} \stackrel{\mathrm{def}}{=} \inf_{\rho'_{AB}\in\mathcal{B}^{\varepsilon}(\rho_{AB})}\mathrm{I}_{\max}(A:B)_{\rho'}$.

One way protocols and convex split

We begin with the following classical protocol for message compression. Alice and Referee share the mixed state $\Psi_{RA} = \sum_i p_i |i\rangle\langle i|_R \otimes |i\rangle\langle i|_A$ and Alice needs to send the register A to Bob. A simple strategy using the technique of rejection sampling (see e.g. [HJMR10]) to achieve this task is that Alice and Bob share many copies of the state $\theta_{E_AE_B} \stackrel{\mathrm{def}}{=} \sum_i p_i |i\rangle\langle i|_{E_A} \otimes |i\rangle\langle i|_{E_B}$, and Alice sequentially checks in each copy whether the contents of registers A and E_A match. That is, she applies the projector $\sum_i |i\rangle\langle i|_A \otimes |i\rangle\langle i|_{E_A}$ and tries a fresh shared randomness upon failure. Upon success, she sends the index of the succeeding shared randomness, and Bob merely outputs his part of the shared randomness. A modification of this protocol also works when the state in register A is a mixed classical/quantum state, for each i [HJMR10, JRS03, JRS05].

Unfortunately, the technique fails when the state Ψ_{RA} is pure. The failure of the measurement leads to correlation between the register R and parts of shared entanglement with Alice which disrupts the requirement that R be correlated only with register output with Bob. To get around this problem, we design suitable operation on the Bob's side, and construct Alice's measurements in a coherent fashion. We outline our strategy more precisely below.

Given a one-way communication protocol that achieves certain task, let the shared state between Alice (A), Bob (B) and Referee (R) be ϕ_{RAB}. Here the registers A, B denote all the registers with Alice and Bob respectively. Let a measurement $\{M_1, M_2 \ldots\}$ be performed by Alice. Then conditioned on an outcome i, state on registers RB is $\mathrm{Tr}_A(M_i\phi_{RAB})$ (with slight abuse of notation for brevity). Thus, the measurement by Alice induces a *convex-split* of the state ϕ_{RB} as follows:

$$\phi_{RB} = \sum_i \mathrm{Tr}_A(M_i\phi_{RAB}).$$

Upon receiving the message i from Alice, Bob 'knows' that state on registers R, B is $\mathrm{Tr}_A(M_i\phi_{RAB})$. They can perform further operations to finish the protocol.

Alternatively, given a convex-split of the state ϕ_{RB} as $\phi_{RB} = \sum_i p_i\phi^i_{RB}$, one can construct a one-way communication protocol as follows. Consider the following purification of ϕ_{RB}:

$$|\phi\rangle_{RBA'J} = \sum_i \sqrt{p_i}\, |\phi^i\rangle_{RBA'} |i\rangle_J .$$

Here $|\phi^i\rangle_{RBA'}$ is a purification of ϕ^i_{RB}. Alice applies an isometry $V : A \to A'J$ to transform the shared state ϕ_{RAB} to $\phi_{RBA'J}$ and measures the register J. She then sends the measurement outcome to Bob. Upon receiving outcome i, Bob 'knows' that the state on registers RB is ϕ^i_{RB}, on which he can perform further operations.

We shall exploit this equivalence between convex-split and one-way communication protocols and construct a suitable convex-split corresponding to quantum state redistribution. Our idea is inspired by the aforementioned classical protocol, in which Bob simply outputs the correct register, receiving the message from Alice.

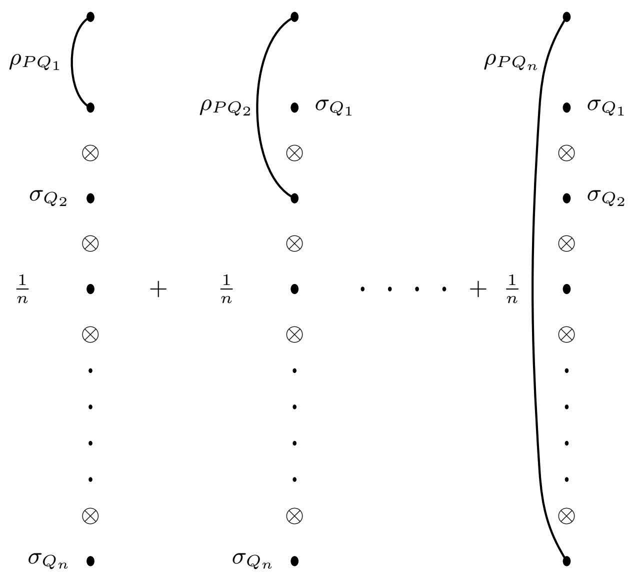

FIG. 1. The state $\tau_{PQ_1Q_2\ldots Q_n}$ considered in convex-split lemma. For large enough n, $\tau_{PQ_1Q_2\ldots Q_n}$ is approximately equal to the state $\tau_P \otimes \tau_{Q_1Q_2\ldots Q_n}$.

We shall show the following main lemma, which we apply to compression of quantum messages in next section.

Lemma (Convex-split lemma)**.** *Let $\rho_{PQ} \in \mathcal{D}(PQ)$ and $\sigma_Q \in \mathcal{D}(Q)$ be quantum states such that $\mathrm{supp}(\rho_Q) \subset \mathrm{supp}(\sigma_Q)$. Let $k \stackrel{\mathrm{def}}{=} \mathrm{D}_{\max}(\rho_{PQ} \| \rho_P \otimes \sigma_Q)$. Define the following state (please also refer to Figure 1)*

$$\tau_{PQ_1Q_2\ldots Q_n} \stackrel{\mathrm{def}}{=} \frac{1}{n}\sum_{j=1}^{n} \rho_{PQ_j} \otimes \sigma_{Q_1} \otimes \sigma_{Q_2} \ldots \otimes \sigma_{Q_{j-1}} \otimes \sigma_{Q_{j+1}} \ldots \otimes \sigma_{Q_n} \quad (1)$$

on $n+1$ registers $P, Q_1, Q_2, \ldots Q_n$, where $\forall j \in [n]$: $\rho_{PQ_j} = \rho_{PQ}$ and $\sigma_{Q_j} = \sigma_Q$. Then,

$$\mathrm{F}^2(\tau_{PQ_1Q_2\ldots Q_n}, \rho_P \otimes \sigma_{Q_1} \otimes \sigma_{Q_2} \ldots \otimes \sigma_{Q_n}) \geq \frac{1}{1+\frac{2^k}{n}}.$$

In particular, for $\delta \in (0, 1/3)$ and $n \stackrel{\mathrm{def}}{=} \lceil \frac{2^k}{\delta} \rceil$,

$$\mathrm{F}^2(\tau_{PQ_1Q_2\ldots Q_n}, \rho_P \otimes \sigma_{Q_1} \otimes \sigma_{Q_2} \ldots \otimes \sigma_{Q_n}) \geq 1-\delta.$$

Compressing one-way quantum message

Using the convex split lemma, we now present a scheme to compress an arbitrary quantum message. Consider a protocol in which Alice(AM), Bob(B) and Referee(R) share a joint quantum state Φ_{RAMB} and Alice sends the register M to Bob. This protocol may appear as a sub-routine in any other quantum protocol. We shall show the following theorem.

Theorem .1. *There exists a protocol $\mathcal{P}$ which starts with the state Φ_{RAMB} and produces a state Φ'_{RAMB} with the property $\mathrm{F}^2(\Phi_{RAMB}, \Phi'_{RAMB}) \geq 1-\varepsilon^2$, such that the register M is held by Bob. The number of qubits communicated from Alice to Bob is at most*

$$\frac{1}{2}\mathrm{I}_{\max}(RB : M)_{\Phi} + \log\left(\frac{1}{\varepsilon}\right).$$

An outline of the proof is as follows. The compression of message register M amounts to constructing a suitable convex split on the registers involved with Bob and Referee.

For any $\sigma \in \mathcal{D}(M)$, we set $\delta = \varepsilon^2$, $k = \mathrm{D}_{\max}(\Phi_{RBM} \| \Phi_{RB} \otimes \sigma_M)$, $n = 2^k/\delta$ and consider the state

$$\tau_{RBM_1M_2\ldots M_n} \stackrel{\mathrm{def}}{=} \frac{1}{n}\sum_{j=1}^{n} \Phi_{RBM_j} \otimes \sigma_{M_1} \ldots \otimes \sigma_{M_{j-1}} \otimes \sigma_{M_{j+1}} \ldots \otimes \sigma_{M_n}$$

Suppose Alice, Bob and Referee hold the following purification of $\tau_{RBM_1M_2\ldots M_n}$,

$$|\tau\rangle_{RBJL_1\ldots L_nM_1\ldots M_n} \stackrel{\mathrm{def}}{=} \frac{1}{\sqrt{n}}\sum_{j=1}^{n} |\tilde{\Phi}\rangle_{RBL_jM_j} \otimes |j\rangle_J \otimes |\sigma\rangle_{L_1M_1} \ldots \otimes |\sigma\rangle_{L_{j-1}M_{j-1}} \otimes |\sigma\rangle_{L_{j+1}M_{j+1}} \ldots \otimes |\sigma\rangle_{L_nM_n}$$

where, L_i is a register purifying M_i and $|\tilde{\Phi}\rangle_{RBL_jM_j}$ is a purification of Φ_{RBM_j}. Then Alice can send the register J to Bob via superdense coding. Upon receiving the message j, Bob can pick up the register M_j and Alice can purify the state Φ_{RBM_j} in her register A. The state in registers RBM_jA is then the desired output.

Obvious issue with this scheme is that the parties do not possess the state $\tau_{RBAJL_1L_2\ldots L_nM_1M_2\ldots M_n}$. But observe that $\tau_{RB} = \Phi_{RB}$ and $\tau_{RB}\otimes\sigma_{M_1}\otimes\sigma_{M_2}\ldots\otimes\sigma_{M_n}$ and $\tau_{RBM_1M_2\ldots M_n}$ are 2δ-close in fidelity (due to the convex split lemma). Thus, the parties can start with the state Φ_{RBAM} and the purification $|\sigma\rangle_{L_1M_1}\otimes\ldots|\sigma\rangle_{L_nM_n}$ of $\sigma_{M_1}\otimes\sigma_{M_2}\ldots\otimes\sigma_{M_n}$ as the pre-shared entanglement and Alice can apply an isometry V on her registers (guaranteed by Uhlmann's theorem [Uhl76]) such that the states $V(|\Phi\rangle_{RBAM}\otimes|\sigma\rangle_{L_1M_1}\otimes\ldots|\sigma\rangle_{L_nM_n})$ and $|\tau'\rangle_{RBAJL_1L_2\ldots L_nM_1M_2\ldots M_n}$ are δ-close to each other in fidelity. Alice then sends the register J, leading to a state Φ'_{RBM_jA} shared between all three parties, such that $\mathrm{F}^2(\Phi'_{RBM_jA},\Phi_{RBM_jA})\geq 1-2\delta$. The number of qubits communicated by Alice is $\frac{\log(n)}{2}$. The theorem follows when we choose σ such that $\mathrm{D}_{\max}(\Phi_{RBM}\|\Phi_{RB}\otimes\sigma_M) = \mathrm{I}_{\max}(RB:M)_\Phi$.

Application: Quantum state redistribution

An immediate application of our compression result is near optimal characterization of the task of quantum state redistribution. We begin with the case for quantum state splitting (in which register B is trivial). Referee(R) and Alice(AC) share the state Ψ_{RAC} and Alice needs to send the register C to Bob. From our compression result, a protocol in which Alice simply sends the register C to Bob can be compressed using a new protocol $\mathcal{P}$ which makes an error of at most 2ε, using the following number of qubits:

$$\frac{1}{2}\mathrm{I}^{\varepsilon}_{\max}(R:C)_\Psi + \log\left(\frac{2}{\varepsilon}\right).$$

It is known that any one-way entanglement assisted quantum protocol that makes an error at most ε must communicate at least $\frac{1}{2}\mathrm{I}^{\varepsilon}_{\max}(R:C)_\Psi$ number of qubits [BCR11]. Similar bounds also hold for quantum state merging (in which register A is trivial), as quantum state merging can be viewed as a time-reversed version of quantum state splitting [BCR11]. A slightly weaker form of our result was already known in [BCR11], where the protocol used $\frac{1}{2}\mathrm{I}^{\varepsilon}_{\max}(R:C)_\Psi + \log\log\dim(C) + \mathcal{O}(\log\left(\frac{1}{\varepsilon}\right))$ qubits of communication and embezzling quantum states as pre-shared entanglement. On the other hand, the communication cost in our protocol differs from the lower bound by a constant and uses a simple form of pre-shared entanglement: sufficiently many copies of purifications of certain state σ_C, that is obtained in the optimization in $\mathrm{I}^{\varepsilon}_{\max}(R:C)_\Psi$.

We show a similar statement for the case of quantum state redistribution, where the communication cost is tighly characterized by the following quantity.

Definition. Let $\varepsilon\geq 0$ and $|\Psi\rangle_{RABC}$ be a pure state. Define,

$$\mathrm{Q}^{\varepsilon}_{|\Psi\rangle_{RABC}} \stackrel{\mathrm{def}}{=} \inf_{T,U_{BCT},\sigma_T,\kappa_{RBCT}} \mathrm{I}_{\max}(RB:CT)_{\kappa_{RBCT}}$$

with the condition that U_{BCT} is a unitary on registers BCT, $\sigma_T\in\mathcal{D}(T)$, $\kappa_{RB}=\Psi_{RB}$ and

$$(I_R\otimes U_{BCT})\kappa_{RBCT}(I_R\otimes U^{\dagger}_{BCT})\in\mathcal{B}^{\varepsilon}(\Psi_{RBC}\otimes\sigma_T)\,.$$

It may be noted that in above quantity, we are not optimizing over all possible protocols. Rather, it quantifies (in terms of max-information) how well Bob can decouple the registers RB and CT using local operations and additional ancilla register T. In the special case where B is trivial (for quantum state splitting), there is no additional ancillary register T required by Bob for best possible decoupling and above quantity coincides with $\mathrm{I}^{\varepsilon}_{\max}(R:C)_\Psi$.

We show that any one-way entanglement assisted quantum protocol achieving quantum state redistribution of the state Ψ_{RABC} with error at most ε must communicate at least $\frac{1}{2}\mathrm{Q}^{\varepsilon}_{|\Psi\rangle_{RABC}}$ number of qubits. Furthemore, using our compression result, we exhibit a protocol that makes an error of at most 2ε and communicates at most $\frac{1}{2}\mathrm{Q}^{\varepsilon}_{|\Psi\rangle_{RABC}} + \log\left(\frac{2}{\varepsilon}\right)$ number of qubits. We leave further understanding of this quantity, to future work.

Application: Port-based teleportation

The work [IH08] introduced the technique of Port-based teleportation, where Alice and Bob share many copies of maximally entangled states (called *ports*), and upon receiving message from Alice (which she prepares after her local quantum operation), Bob simply picks up the desired state in one of the ports. It was shown in [IH09] that there is a Port-based teleportation scheme for d-dimensional quantum states that uses N copies of d-dimensional maximally entangled states and achieves average squared-fidelity of transmission at least $1-\frac{d^2}{N}$.

Using the convex split lemma, we provide a scheme for Port-based teleportation in the presence of side information about the set of input states. Given a collection of states on a register M and associated probabilities $\{p_i, \psi^i_M\}_i$, define the state $|\Psi\rangle_{RM} \stackrel{\text{def}}{=} \sum_i \sqrt{p_i}\, |i\rangle_R\, |\psi^i\rangle_M$ (where R is a register with sufficient large dimension). Then we present a protocol where Alice and Bob share N copies of purification of an arbitrary state σ_M and perform a port-based teleportation protocol for which the average squared-fidelity is at least $1 - \left(2^{\mathrm{D}_{\max}(\Psi_{RM}\|\Psi_R\otimes\sigma_M)}/N\right)$. In particular, if ψ^i_M form the set of all possible quantum states on d dimensional register M with uniform distribution, then choosing $\sigma_M = \frac{\mathrm{I}_M}{d}$, we find that $\mathrm{D}_{\max}(\Psi_{RM}\|\Psi_R\otimes\sigma_M) = 2\log(d)$. Thus, this scheme achieves the average squared-fidelity at least $1 - \frac{d^2}{N}$ for port-based teleportation of an arbitrary state, similar to the result obtained in [IH09]. But one can obtain better average squared-fidelity for a different collection $\{p_i, \psi^i_M\}_i$, since it always holds that $\inf_{\sigma_M}\mathrm{D}_{\max}(\Psi_{RM}\|\Psi_R\otimes\sigma_M) \le 2\log(d)$ (as shown in [BCR11]).

Conclusion

We have presented a new protocol for compressing one-way coherent quantum messages upto the *max information* between the message and joint system between receiver and reference. As a consequence, we have obtained optimal quantities characterizing the quantum communication cost of quantum state merging and quantum state splitting tasks. We have also exhibited a similar quantity for the task of quantum state redistribution, although it remains to better understand the optimization in it. We have also exhibited a port-based teleportation scheme that can potentially save the number of ports in presence of further information about the ensemble of the states to be teleported.

ACKNOWLEDGMENT

We thank Ashwin Nayak, Nilanjana Datta, Marco Tomamichel and Mark M. Wilde for helpful comments on previous versions of this paper and also for pointing us to many useful references. We thank Debbie Leung for pointing out the connection with Port-based teleportation. We thank Priyanka Mukhopadhyay and Naqueeb Warsi for helpful discussions. This work is supported by the Singapore Ministry of Education and the National Research Foundation, also through the Tier 3 Grant "Random numbers from quantum processes" MOE2012-T3-1-009.

[ADHW09] Anura Abeyesinghe, Igor Devetak, Patrick Hayden, and Andreas Winter. The mother of all protocols: Restructuring quantum information's family tree. *Proceedings of the Royal Society of London*, A(465):2537–2563, 2009.

[BCF+96] Howard Barnum, Carlton M. Cave, Christopher A. Fuch, Richard Jozsa, and Benjamin Schmacher. Noncommuting mixed states cannot be broadcast. *Phys. Rev. Lett.*, 76(15):2818–2821, 1996.

[BCR11] Mario Berta, Matthias Christandl, and Renato Renner. The Quantum Reverse Shannon Theorem based on one-shot information theory. *Commun. Math. Phys.*, 306(3):579–615, 2011.

[BCT16] M. Berta, M. Christandl, and D. Touchette. Smooth entropy bounds on one-shot quantum state redistribution. *IEEE Transactions on Information Theory*, 62(3):1425–1439, March 2016.

[BD10] Francesco Buscemi and Nilanjana Datta. The quantum capacity of channels with arbitrarily correlated noise. *IEEE Transactions on Information Theory*, 56:1447–1460, 2010.

[Ber09] Mario Berta. Single-shot quantum state merging. Master's thesis, ETH Zurich, http://arxiv.org/abs/0912.4495, 2009.

[BW92] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69(20):2881–2884, 1992.

[Car10] Eric Carlen. Trace inequalities and quantum entropy: an introductory course. entropy and the quantum. *Contemp. Math.*, 529:73–140, 2010.

[CHP07] I. Csiszár, F. Hiai, and D. Petz. Limit relation for quantum entropy and channel capacity per unit cost. *J. Math. Phys.*, 48(092102), 2007.

[CT91] Thomas M. Cover and Joy A. Thomas. *Elements of information theory*. Wiley Series in Telecommunications. John Wiley & Sons, New York, NY, USA, 1991.

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

[DBWR14] Frédéric Dupuis, Mario Berta, Jürg Wullschleger, and Renato Renner. One-shot decoupling. *Communications in Mathematical Physics*, 328(251), 2014.

[DCHR78] D. Dacunha-Castelle, H. Heyer, and B. Roynette. Ecole d'Eté de Probabilités de Saint-Flour VII. *Lecture Notes in Mathematics, Springer-Verlag*, 678, 1978.

[DH11] Nilanjana Datta and Min-Hsiu Hsieh. The apex of the family tree of protocols: optimal rates and resource inequalities. *New Journal of Physics*, 13(093042), 2011.

[DHO14] Nilanjana Datta, Min-Hsiu Hsieh, and Jonathan Oppenheim. An upper bound on the second order asymptotic expansion for the quantum communication cost of state redistribution. http://arxiv.org/abs/1409.4352, 2014.

[Dup10] Frédéric Dupuis. The decoupling approach to quantum information theory. PhD Thesis, Université de Montréal., http://arxiv.org/abs/1410.0664, 2010.

[DY08] Igor Devetak and Jon Yard. Exact cost of redistributing multipartite quantum states. *Phys. Rev. Lett.*, 100(230501), 2008.

[HHH99] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Phys. Rev. A*, 60:1888–1898, Sep 1999.

[HJMR10] Prahladh Harsha, Rahul Jain, David Mc.Allester, and Jaikumar Radhakrishnan. The communication complexity of correlation. *IEEE Transcations on Information Theory*, 56:438–449, 2010.

[HOW07] Michał Horodecki, Jonathan Oppenheim, and Andreas Winter. Quantum state merging and negative information. *Communications in Mathematical Physics*, 269(1):107–136, 2007.

[IH08] Satoshi Ishizaka and Tohya Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. *Phys. Rev. Lett.*, 101:240501, Dec 2008.

[IH09] Satoshi Ishizaka and Tohya Hiroshima. Quantum teleportation scheme by selecting one of multiple output ports. *Phys. Rev. A*, 79:042306, Apr 2009.

[JRS03] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A direct sum theorem in communication complexity via message compression. In *Proceedings of the 30th international conference on Automata, languages and programming*, ICALP'03, pages 300–315, Berlin, Heidelberg, 2003. Springer-Verlag.

[JRS05] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. Prior entanglement, message compression and privacy in quantum communication. In *Proceedings of the 20th Annual IEEE Conference on Computational Complexity*, pages 285–296, Washington, DC, USA, 2005. IEEE Computer Society.

[LD09] Zhicheng Luo and Igor Devetak. Channel simulation with quantum side information. *IEEE Transactions on Information Theory*, 55:1331–1342, 2009.

[Lin75] G. Lindblad. Completely positive maps and entropy inequalities. *Commun. Math. Phys.*, 40:147–151, 1975.

[MBD+16] Christian Majenz, Mario Berta, Frédéric Dupuis, Renato Renner, and Matthias Christandl. Catalytic decoupling of quantum information. 2016.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, Cambridge, UK, 2000.

[Opp08] Jonathan Oppenheim. State redistribution as merging: introducing the coherent relay. http://arxiv.org/abs/0805.1065, 2008.

[Ren05] Renato Renner. Security of quantum key distribution. PhD Thesis, ETH Zurich, Diss. ETH No. 16242, arXiv:quant-ph/0512258, 2005.

[Sch95] Benjamin Schumacher. Quantum coding. *Phys. Rev. A.*, 51:2738–2747, 1995.

[Sha] Claude Elwood Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423.

[Sti55] W. F. Stinespring. Positive functions on c*-algebras. *Proceedings of the American Mathematical Society*, page 211–216, 1955.

[TCR10] Marco Tomamichel, Roger Colbeck, and Renato Renner. Duality between smooth min- and max-entropies. *IEEE Transactions on Information Theory*, 56(9):4674 – 4681, 2010.

[Tom12] Marco Tomamichel. A framework for non-asymptotic quantum information theory. PhD Thesis, ETH Zurich, http://arXiv,org/abs/1203.2142, 2012.

[Tou15] Dave Touchette. Quantum information complexity. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, STOC '15, pages 317–326, New York, NY, USA, 2015. ACM.

[Uhl76] A. Uhlmann. The "transition probability" in the state space of a *-algebra. *Rep. Math. Phys.*, 9:273–279, 1976.

[Wat11] John Watrous. Theory of Quantum Information, lecture notes, 2011. https://cs.uwaterloo.ca/ watrous/LectureNotes.html.

[YBW08] Ming-Yong Ye, Yan-Kui Bai, and Z. D. Wang. Quantum state redistribution based on a generalized decoupling. *Physical Review A*, 78(030302(R)), 2008.

[YD09] Jon T. Yard and Igor Devetak. Optimal quantum source coding with quantum side information at the encoder and decoder. *IEEE Transactions on Information Theory*, 55:5339–5351, 2009.

Preliminaries

In this section we present some notations, definitions, facts and lemmas that we will use later in our proofs. Readers may refer to [CT91, NC00, Wat11] for good introduction to classical and quantum information theory.

Information theory

Consider a finite dimensional Hilbert space $\mathcal{H}$ endowed with an inner product $\langle \cdot, \cdot \rangle$ (in this paper, we only consider finite dimensional Hilbert-spaces). The ℓ_1 norm of an operator X on $\mathcal{H}$ is $\|X\|_1 \stackrel{\mathrm{def}}{=} \mathrm{Tr}\sqrt{X^\dagger X}$ and ℓ_2 norm is $\|X\|_2 \stackrel{\mathrm{def}}{=} \sqrt{\mathrm{Tr} X X^\dagger}$. A quantum state (or a density matrix or a state) is a positive semi-definite matrix on $\mathcal{H}$ with trace equal to 1. It is called *pure* if and only if its rank is 1. A sub-normalized state is a positive semi-definite matrix on $\mathcal{H}$ with trace less than or equal to 1. Let $|\psi\rangle$ be a unit vector on $\mathcal{H}$, that is $\langle \psi, \psi \rangle = 1$. With some abuse of notation, we use ψ to represent the state and also the density matrix $|\psi\rangle\langle\psi|$, associated with $|\psi\rangle$. Given a quantum state ρ on $\mathcal{H}$, *support of* ρ, called $\mathrm{supp}(\rho)$ is the subspace of $\mathcal{H}$ spanned by all eigen-vectors of ρ with non-zero eigenvalues.

A *quantum register* A is associated with some Hilbert space $\mathcal{H}_A$. Define $|A| \stackrel{\mathrm{def}}{=} \dim(\mathcal{H}_A)$. Let $\mathcal{L}(A)$ represent the set of all linear operators on $\mathcal{H}_A$. We denote by $\mathcal{D}(A)$, the set of quantum states on the Hilbert space $\mathcal{H}_A$. State ρ with subscript A indicates $\rho_A \in \mathcal{D}(A)$. If two registers A, B are associated with the same Hilbert space, we shall represent the relation by $A \equiv B$. Composition of two registers A and B, denoted AB, is associated with Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. For two quantum states $\rho \in \mathcal{D}(A)$ and $\sigma \in \mathcal{D}(B)$, $\rho \otimes \sigma \in \mathcal{D}(AB)$ represents the tensor product (Kronecker product) of ρ and σ. The identity operator on $\mathcal{H}_A$ (and associated register A) is denoted I_A.

Let $\rho_{AB} \in \mathcal{D}(AB)$. We define

$$\rho_B \stackrel{\mathrm{def}}{=} \mathrm{Tr}_A(\rho_{AB}) \stackrel{\mathrm{def}}{=} \sum_i (\langle i| \otimes I_B)\rho_{AB}(|i\rangle \otimes I_B),$$

where $\{|i\rangle\}_i$ is an orthonormal basis for the Hilbert space $\mathcal{H}_A$. The state $\rho_B \in \mathcal{D}(B)$ is referred to as the marginal state of ρ_{AB}. Unless otherwise stated, a missing register from subscript in a state will represent partial trace over that register. Given a $\rho_A \in \mathcal{D}(A)$, a *purification* of ρ_A is a pure state $\rho_{AB} \in \mathcal{D}(AB)$ such that $\mathrm{Tr}_B(\rho_{AB}) = \rho_A$. Purification of a quantum state is not unique.

A quantum map $\mathcal{E} : \mathcal{L}(A) \to \mathcal{L}(B)$ is a completely positive and trace preserving (CPTP) linear map (mapping states in $\mathcal{D}(A)$ to states in $\mathcal{D}(B)$). A *unitary* operator $U_A : \mathcal{H}_A \to \mathcal{H}_A$ is such that $U_A^\dagger U_A = U_A U_A^\dagger = I_A$. An *isometry* $V : \mathcal{H}_A \to \mathcal{H}_B$ is such that $V^\dagger V = I_A$ and $V V^\dagger = I_B$. The set of all unitary operations on register A is denoted by $\mathcal{U}(A)$.

Definition .2. We shall consider the following information theoretic quantities. Reader is referred to [Ren05, TCR10, Tom12, Dat09] for many of these definitions. We consider only normalized states in the definitions below. Let $\varepsilon \geq 0$.

1. **Fidelity** For $\rho_A, \sigma_A \in \mathcal{D}(A)$,

$$\mathrm{F}(\rho_A, \sigma_A) \stackrel{\mathrm{def}}{=} \|\sqrt{\rho_A}\sqrt{\sigma_A}\|_1 .$$

   For classical probability distributions $P = \{p_i\}, Q = \{q_i\}$,

$$\mathrm{F}(P, Q) \stackrel{\mathrm{def}}{=} \sum_i \sqrt{p_i \cdot q_i}.$$

2. **Purified distance** For $\rho_A, \sigma_A \in \mathcal{D}(A)$,

$$\mathcal{P}(\rho_A, \sigma_A) = \sqrt{1 - \mathrm{F}^2(\rho_A, \sigma_A)}.$$

3. ε**-ball** For $\rho_A \in \mathcal{D}(A)$,

$$\mathcal{B}^{\varepsilon}(\rho_A) \stackrel{\text{def}}{=} \{\rho'_A \in \mathcal{D}(A) |\ \mathcal{P}(\rho_A, \rho'_A) \leq \varepsilon\}.$$

4. **Von-neumann entropy** For $\rho_A \in \mathcal{D}(A)$,

$$\mathrm{S}(\rho_A) \stackrel{\text{def}}{=} -\mathrm{Tr}(\rho_A \log \rho_A).$$

5. **Relative entropy** For $\rho_A, \sigma_A \in \mathcal{D}(A)$ such that $\mathrm{supp}(\rho_A) \subset \mathrm{supp}(\sigma_A)$,

$$\mathrm{D}(\rho_A \| \sigma_A) \stackrel{\text{def}}{=} \mathrm{Tr}(\rho_A \log \rho_A) - \mathrm{Tr}(\rho_A \log \sigma_A).$$

6. **Max-relative entropy** For $\rho_A, \sigma_A \in \mathcal{D}(A)$ such that $\mathrm{supp}(\rho_A) \subset \mathrm{supp}(\sigma_A)$,

$$\mathrm{D}_{\max}(\rho_A \| \sigma_A) \stackrel{\text{def}}{=} \inf\{\lambda \in \mathbb{R} : 2^{\lambda} \sigma_A \geq \rho_A\}.$$

7. **Mutual information** For $\rho_{AB} \in \mathcal{D}(AB)$,

$$\mathrm{I}(A:B)_{\rho} \stackrel{\text{def}}{=} \mathrm{S}(\rho_A) + \mathrm{S}(\rho_B) - \mathrm{S}(\rho_{AB}) = \mathrm{D}(\rho_{AB} \| \rho_A \otimes \rho_B).$$

8. **Conditional mutual information** For $\rho_{ABC} \in \mathcal{D}(ABC)$,

$$\mathrm{I}(A:B|C)_{\rho} \stackrel{\text{def}}{=} \mathrm{I}(A:BC)_{\rho} - \mathrm{I}(A:C)_{\rho}.$$

9. **Max-information** For $\rho_{AB} \in \mathcal{D}(AB)$,

$$\mathrm{I}_{\max}(A:B)_{\rho} \stackrel{\text{def}}{=} \inf_{\sigma_B \in \mathcal{D}(B)} \mathrm{D}_{\max}(\rho_{AB} \| \rho_A \otimes \sigma_B).$$

10. **Smooth max-information** For $\rho_{AB} \in \mathcal{D}(AB)$,

$$\mathrm{I}^{\varepsilon}_{\max}(A:B)_{\rho} \stackrel{\text{def}}{=} \inf_{\rho' \in \mathcal{B}^{\varepsilon}(\rho)} \mathrm{I}_{\max}(A:B)_{\rho'}.$$

11. **Conditional min-entropy** For $\rho_{AB} \in \mathcal{D}(AB)$,

$$\mathrm{H}_{\min}(A|B)_{\rho} \stackrel{\text{def}}{=} -\inf_{\sigma_B \in \mathcal{D}(B)} \mathrm{D}_{\max}(\rho_{AB} \| I_A \otimes \sigma_B).$$

We will use the following facts.

Fact .3 (Triangle inequality for purified distance, [Tom12]). For states $\rho_A, \sigma_A, \tau_A \in \mathcal{D}(A)$,

$$\mathcal{P}(\rho_A, \sigma_A) \leq \mathcal{P}(\rho_A, \tau_A) + \mathcal{P}(\tau_A, \sigma_A).$$

Fact .4 ([Sti55]). (**Stinespring representation**) Let $\mathcal{E}(\cdot) : \mathcal{L}(A) \to \mathcal{L}(B)$ be a quantum operation. There exists a register C and an unitary $U \in \mathcal{U}(ABC)$ such that $\mathcal{E}(\omega) = \mathrm{Tr}_{A,C}\left(U(\omega \otimes |0\rangle\langle 0|^{B,C})U^{\dagger}\right)$. Stinespring representation for a channel is not unique.

Fact .5 (Monotonicity under quantum operations, [BCF+96],[Lin75]). For quantum states $\rho, \sigma \in \mathcal{D}(A)$, and quantum operation $\mathcal{E}(\cdot) : \mathcal{L}(A) \to \mathcal{L}(B)$, it holds that

$$\|\mathcal{E}(\rho) - \mathcal{E}(\sigma)\|_1 \leq \|\rho - \sigma\|_1 \quad \text{and} \quad \mathrm{F}(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \geq \mathrm{F}(\rho, \sigma) \quad \text{and} \quad \mathrm{D}(\rho\|\sigma) \geq \mathrm{D}(\mathcal{E}(\rho)\|\mathcal{E}(\sigma)).$$

In particular, for bipartite states $\rho_{AB}, \sigma_{AB} \in \mathcal{D}(AB)$, it holds that

$$\|\rho_{AB} - \sigma_{AB}\|_1 \geq \|\rho_A - \sigma_A\|_1 \quad \text{and} \quad \mathrm{F}(\rho_{AB}, \sigma_{AB}) \leq \mathrm{F}(\rho_A, \sigma_A) \quad \text{and} \quad \mathrm{D}(\rho_{AB}\|\sigma_{AB}) \geq \mathrm{D}(\rho_A\|\sigma_A).$$

Fact .6 (Uhlmann's theorem, [Uhl76])**.** Let $\rho_A, \sigma_A \in \mathcal{D}(A)$. Let $\rho_{AB} \in \mathcal{D}(AB)$ be a purification of ρ_A and $\sigma_{AC} \in \mathcal{D}(AC)$ be a purification of σ_A. There exists an isometry $V : \mathcal{H}_C \to \mathcal{H}_B$ such that,

$$\mathrm{F}(|\theta\rangle\langle\theta|_{AB}, |\rho\rangle\langle\rho|_{AB}) = \mathrm{F}(\rho_A, \sigma_A),$$

where $|\theta\rangle_{AB} = (I_A \otimes V)\,|\sigma\rangle_{AC}$.

Fact .7 ([BCR11], Lemma B.7)**.** For a quantum state $\rho_{AB} \in \mathcal{D}(AB)$,

$$\mathrm{I}_{\max}(A : B)_\rho \leq 2 \cdot \min\{\log|A|, \log|B|\}.$$

Fact .8 ([BCR11], Lemma B.14)**.** For a quantum state $\rho_{ABC} \in \mathcal{D}(ABC)$,

$$\mathrm{I}_{\max}(A : BC)_\rho \geq \mathrm{I}_{\max}(A : B)_\rho .$$

Fact .9 (Pinsker's inequality, [DCHR78])**.** For quantum states $\rho_A, \sigma_A \in \mathcal{D}(A)$,

$$\mathrm{F}(\rho, \sigma) \geq 2^{-\frac{1}{2}\mathrm{D}(\rho\|\sigma)}.$$

This implies,

$$1 - \mathrm{F}(\rho, \sigma) \leq \frac{\ln 2}{2} \cdot \mathrm{D}(\rho\|\sigma) \leq \mathrm{D}(\rho\|\sigma) .$$

Lemma .10. *Let $\epsilon > 0$. Let $|\psi\rangle\langle\psi|_A \in \mathcal{D}(A)$ be a pure state and let $\rho_{AB} \in \mathcal{D}(AB)$ be a state such that $\mathrm{F}(|\psi\rangle\langle\psi|_A, \rho_A) \geq 1 - \varepsilon$. There exists a state $\theta_B \in \mathcal{D}(B)$ such that $\mathrm{F}(|\psi\rangle\langle\psi|_A \otimes \theta_B, \rho_{AB}) \geq 1 - \varepsilon$.*

Proof. Introduce a register C such that $|C| = |A||B|$. Let $|\rho\rangle_{ABC} \in \mathcal{D}(ABC)$ be a purification of ρ_{AB}. Using Uhlmann's theorem (Fact .6) we get a pure state θ_{BC} such that

$$\begin{aligned}
1 - \varepsilon &\leq \mathrm{F}(|\psi\rangle\langle\psi|_A, \rho_A) \\
&= \mathrm{F}(|\psi\rangle\langle\psi|_A \otimes |\theta\rangle\langle\theta|_{BC}, |\rho\rangle\langle\rho|_{ABC}) \\
&\leq \mathrm{F}(|\psi\rangle\langle\psi|_A \otimes \theta_B, \rho_{AB}). \quad \text{(monotonicity of fidelity under quantum operation, Fact .5)}
\end{aligned}$$

□

The following lemma is a tighter version of (one-sided) convexity of relative entropy.

Lemma .11. *Let $\mu_1, \mu_2, \ldots \mu_n, \theta$ be quantum states and $\{p_1, p_2, \ldots p_n\}$ be a probability distribution. Let $\mu = \sum_i p_i \mu_i$ be the average state. Then*

$$\mathrm{D}(\mu\|\theta) = \sum_i p_i(\mathrm{D}(\mu_i\|\theta) - \mathrm{D}(\mu_i\|\mu)).$$

Proof. Proof proceeds by direct calculation. Consider

$$\begin{aligned}
&\sum_i p_i(\mathrm{D}(\mu_i\|\theta) - \mathrm{D}(\mu_i\|\mu)) = \sum_i p_i(\mathrm{Tr}(\mu_i \log \mu_i) - \mathrm{Tr}(\mu_i \log \theta) - \mathrm{Tr}(\mu_i \log \mu_i) + \mathrm{Tr}(\mu_i \log \mu)) \\
&= \mathrm{Tr}(\sum_i p_i \mu_i \log(\mu)) - \mathrm{Tr}(\sum_i p_i \mu_i \log \theta) = \mathrm{Tr}(\mu \log \mu) - \mathrm{Tr}(\mu \log \theta) = \mathrm{D}(\mu\|\theta) .
\end{aligned}$$

□

A convex-split lemma

We revisit the statement of convex split lemma and state its connection to a previous work. The lemma has been proved in main text.

Lemma .12 (Convex-split lemma). *Let $\rho_{PQ} \in \mathcal{D}(PQ)$ and $\sigma_Q \in \mathcal{D}(Q)$ be quantum states such that $supp(\rho_Q) \subset supp(\sigma_Q)$. Let $k \stackrel{\text{def}}{=} \mathrm{D}_{\max}(\rho_{PQ} \| \rho_P \otimes \sigma_Q)$. Define the following state*

$$\tau_{PQ_1Q_2\ldots Q_n} \stackrel{\text{def}}{=} \frac{1}{n}\sum_{j=1}^{n} \rho_{PQ_j} \otimes \sigma_{Q_1} \otimes \sigma_{Q_2} \ldots \otimes \sigma_{Q_{j-1}} \otimes \sigma_{Q_{j+1}} \ldots \otimes \sigma_{Q_n} \tag{2}$$

on $n+1$ registers $P, Q_1, Q_2, \ldots Q_n$, where $\forall j \in [n] : \rho_{PQ_j} = \rho_{PQ}$ and $\sigma_{Q_j} = \sigma_Q$. Then,

$$\mathrm{D}(\tau_{PQ_1Q_2\ldots Q_n} \| \tau_P \otimes \sigma_{Q_1} \otimes \sigma_{Q_2} \ldots \otimes \sigma_{Q_n}) \leq \log(1 + \frac{2^k}{n}).$$

Using Pinsker's inequality (Fact .9), we conclude,

$$\mathrm{F}^2(\tau_{PQ_1Q_2\ldots Q_n}, \tau_P \otimes \sigma_{Q_1} \otimes \sigma_{Q_2} \ldots \otimes \sigma_{Q_n}) \geq \frac{1}{1+\frac{2^k}{n}}.$$

In particular, for $\delta \in (0, 1/3)$ and $n = \lceil \frac{2^k}{\delta} \rceil$,

$$\mathrm{D}(\tau_{PQ_1Q_2\ldots Q_n} \| \tau_P \otimes \sigma_{Q_1} \otimes \sigma_{Q_2} \ldots \otimes \sigma_{Q_n}) \leq \log(1 + \delta)$$

and

$$\mathrm{F}^2(\tau_{PQ_1Q_2\ldots Q_n}, \tau_P \otimes \sigma_{Q_1} \otimes \sigma_{Q_2} \ldots \otimes \sigma_{Q_n}) \geq 1 - \delta.$$

The proof is as follows.

Proof of Convex-split Lemma. We use the abbreviation $\sigma^{-j} \stackrel{\text{def}}{=} \sigma_{Q_1} \ldots \otimes \sigma_{Q_{j-1}} \otimes \sigma_{Q_{j+1}} \ldots \otimes \sigma_{Q_n}$ and $\sigma \stackrel{\text{def}}{=} \sigma_{Q_1} \otimes \sigma_{Q_2} \ldots \sigma_{Q_n}$. Then $\tau_{PQ_1Q_2\ldots Q_n} = \frac{1}{n}\sum_{j=1}^{n} \rho_{PQ_j} \otimes \sigma^{-j}$. Now, we use Lemma .11 to express

$$\mathrm{D}(\tau_{PQ_1\ldots Q_n} \| \rho_P \otimes \sigma) = \frac{1}{n}\sum_j \mathrm{D}\left(\rho_{PQ_j} \otimes \sigma^{-j} \middle\| \rho_P \otimes \sigma\right) - \frac{1}{n}\sum_j \mathrm{D}\left(\rho_{PQ_j} \otimes \sigma^{-j} \middle\| \tau_{PQ_1Q_2\ldots Q_n}\right). \tag{3}$$

The first term in the summation on right hand side, $\mathrm{D}\left(\rho_{PQ_j} \otimes \sigma^{-j} \middle\| \rho_P \otimes \sigma\right)$, is equal to $\mathrm{D}\left(\rho_{PQ_j} \middle\| \rho_P \otimes \sigma_{Q_j}\right)$.

The second term $\mathrm{D}\left(\rho_{PQ_j} \otimes \sigma^{-j} \middle\| \tau_{PQ_1Q_2\ldots Q_n}\right)$ is lower bounded by $\mathrm{D}\left(\rho_{PQ_j} \middle\| \tau_{PQ_j}\right)$, as relative entropy decreases under partial trace. But observe that $\tau_{PQ_j} = \frac{1}{n}\rho_{PQ_j} + (1 - \frac{1}{n})\rho_P \otimes \sigma_{Q_j}$. By assumption, $\rho_{PQ_j} \leq 2^k \rho_P \otimes \sigma_{Q_j}$. Hence $\tau_{PQ_j} \leq (1 + \frac{2^k-1}{n})\rho_P \otimes \sigma_{Q_j}$. Since $\log(A) \leq \log(B)$ if $A \leq B$ for positive semidefinite matrices A and B (see for example, [Car10]), we have

$$\begin{aligned}
&\mathrm{D}\left(\rho_{PQ_j} \middle\| \tau_{PQ_j}\right) = \mathrm{Tr}(\rho_{PQ_j} \log \rho_{PQ_j}) - \mathrm{Tr}(\rho_{PQ_j} \log \tau_{PQ_j}) \\
&\geq \mathrm{Tr}(\rho_{PQ_j} \log \rho_{PQ_j}) - \mathrm{Tr}(\rho_{PQ_j} \log(\rho_P \otimes \sigma_{Q_j})) - \log(1 + \frac{2^k - 1}{n}) \\
&= \mathrm{D}\left(\rho_{PQ_j} \middle\| \rho_P \otimes \sigma_{Q_j}\right) - \log(1 + \frac{2^k - 1}{n}).
\end{aligned}$$

Using in Equation 3, we find that

$$\begin{aligned}
\mathrm{D}(\tau_{PQ_1Q_2\ldots Q_n} \| \rho_P \otimes \sigma) &\leq \frac{1}{n}\sum_j \mathrm{D}\left(\rho_{PQ_j} \middle\| \rho_P \otimes \sigma_{Q_j}\right) - \frac{1}{n}\sum_j \mathrm{D}\left(\rho_{PQ_j} \middle\| \rho_P \otimes \sigma_{Q_j}\right) + \log(1 + \frac{2^k - 1}{n}) \\
&= \log(1 + \frac{2^k - 1}{n}).
\end{aligned}$$

Thus, the lemma follows. $\square$

Connection to previous work: Following result appears as main theorem in the work of Csiszar *et. al.*[CHP07],

$$\lim_{n\to\infty} \mathrm{D}(\tau_{Q_1Q_2\ldots Q_n}\|\sigma_{Q_1}\otimes\sigma_{Q_2}\ldots\sigma_{Q_n}) = 0.$$

This is a special case of convex-split lemma in the limit $\delta \to 0$ (and hence $n \to \infty$) when the register P is trivial. But it is also equivalent to convex-split lemma in the limit $\delta \to 0$ (and hence $n \to \infty$), as we argue below. Given an arbitrary hermitian operator $M \in \mathcal{L}(P)$, consider the normalized states $\rho'_Q = \frac{\mathrm{Tr}_P(M\rho_{PQ})}{\mathrm{Tr}(M\rho_P)}$ and $\tau'_{Q_1Q_2\ldots Q_n} = \frac{\mathrm{Tr}_P(M\tau_{PQ_1Q_2\ldots Q_n})}{\mathrm{Tr}(M\tau_P)}$. It is easy to observe that

$$\tau'_{Q_1Q_2\ldots Q_n} \stackrel{\mathrm{def}}{=} \frac{1}{n}\sum_{j=1}^{n} \rho'_{Q_j}\otimes\sigma_{Q_1}\otimes\ldots\otimes\sigma_{Q_{j-1}}\otimes\sigma_{Q_{j+1}}\otimes\ldots\otimes\sigma_{Q_n}$$

From the main theorem in [CHP07], this state is arbitrarily close to $\sigma_{Q_1}\otimes\sigma_{Q_2}\ldots\otimes\sigma_{Q_n}$, for large enough n. This means that any measurement $M \in \mathcal{L}(P)$ on the state $\tau_{PQ_1Q_2\ldots Q_n}$ does not change the marginal on registers $Q_1Q_2\ldots Q_n$. Thus registers P and $Q_1Q_2\ldots Q_n$ are independent in the state $\tau_{PQ_1Q_2\ldots Q_n}$. This coincides with the statement of convex-split lemma if we let $\delta \to 0$ (and hence $n \to \infty$).

Compression of one-way quantum message

Consider a state Φ_{RAMB} shared between Alice(AM), Bob(B) and Referee(R). The register M serves as a message register, which Alice sends to Bob. Following theorem shows that this message can be compressed. An idea of the proof appears in the Figure 2.

Theorem .13 (Quantum message compression)**.** *There exists an entanglement-assisted one-way protocol $\mathcal{P}$, which takes as input $|\Phi\rangle_{RAMB}$ shared between three parties* Referee (R), Bob (B) *and* Alice (AM) *and outputs a state Φ'_{RAMB} shared between* Referee (R), Bob (BM) *and* Alice (A) *such that $\Phi'_{RAMB} \in \mathcal{B}^{\varepsilon}(\Psi_{RAMB})$ and the number of qubits communicated by* Alice *to* Bob *in $\mathcal{P}$ is upper bounded by:*

$$\frac{1}{2}\mathrm{I}_{\max}(RB:M)_{\Phi} + \log\left(\frac{1}{\varepsilon}\right).$$

Proof. Let $k \stackrel{\mathrm{def}}{=} \mathrm{I}_{\max}(RB:M)_{\Phi}$, $\delta \stackrel{\mathrm{def}}{=} \varepsilon^2$ and $n \stackrel{\mathrm{def}}{=} \lceil\frac{2^k}{\delta}\rceil$. Let σ_M be the state that achieves the infimum in the definition of $\mathrm{I}_{\max}(RB:M)_{\Phi}$. Consider the state,

$$\mu_{RBM_1\ldots M_n} \stackrel{\mathrm{def}}{=} \frac{1}{n}\sum_{j=1}^{n}\Phi_{RBM_j}\otimes\sigma_{M_1}\otimes\ldots\otimes\sigma_{M_{j-1}}\otimes\sigma_{M_{j+1}}\otimes\ldots\otimes\sigma_{M_n}.$$

Note that $\Phi_{RB} = \mu_{RB}$. Consider the following purification of $\mu_{RBM_1\ldots M_n}$,

$$|\mu\rangle_{RBJL_1\ldots L_nM_1\ldots M_n} \stackrel{\mathrm{def}}{=} \frac{1}{\sqrt{n}}\sum_{j=1}^{n}|j\rangle_J\left|\tilde{\Phi}\right\rangle_{RBL_jM_j}\otimes|\sigma\rangle_{L_1M_1}\otimes\ldots\otimes|\sigma\rangle_{L_{j-1}M_{j-1}}\otimes|\sigma\rangle_{L_{j+1}M_{j+1}}\otimes\ldots\otimes|\sigma\rangle_{L_nM_n}$$

Here, $\forall j\in[n] : |\sigma\rangle_{L_jM_j}$ is a purification of σ_{M_j} and $\left|\tilde{\Phi}\right\rangle_{RBL_jM_j}$ is a purification of Φ_{RBM_j}. Consider the following protocol $\mathcal{P}_1$.

1. Alice, Bob and Referee start by sharing the state $|\mu\rangle_{RBJL_1\ldots L_nM_1\ldots M_n}$ between themselves where Alice holds registers $JL_1\ldots L_n$, Referee holds the register R and Bob holds the registers $BM_1M_2\ldots M_n$.

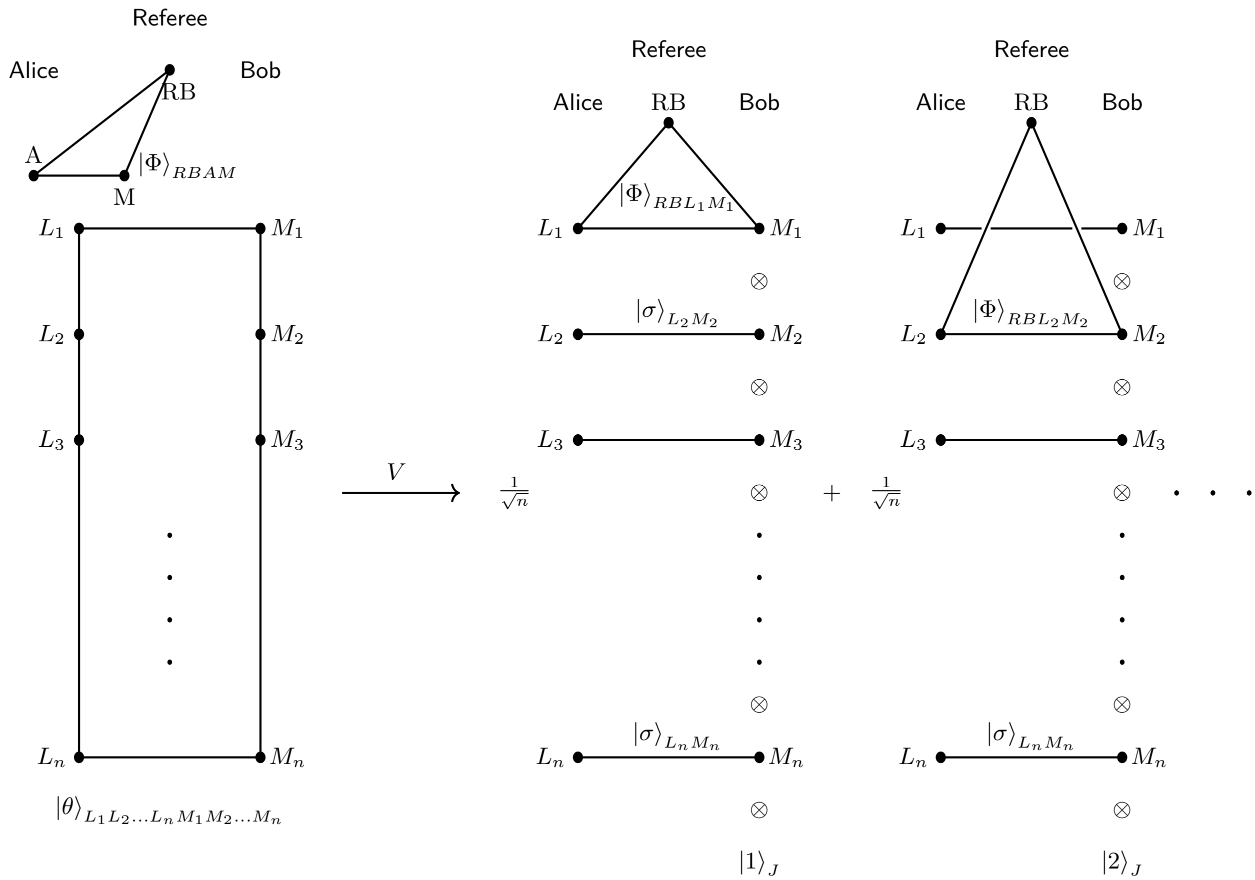

FIG. 2. The state on left hand side $|\Phi\rangle_{RBAM} \otimes |\theta\rangle_{L_1L_2\ldots L_nM_1\ldots M_n}$, a purification of $\Phi_{RB} \otimes \tau_{M_1\ldots M_n}$. The state on right hand side is $|\mu\rangle_{JRBL_1L_2\ldots L_nM_1M_2\ldots M_n}$, a purification of $\tau_{RBM_1M_2\ldots M_n}$. Using convex-split lemma, Alice can apply an isometry V on $|\Phi\rangle_{RBAM} \otimes |\theta\rangle_{L_1L_2\ldots L_nM_1\ldots M_n}$ to obtain $|\mu\rangle_{JRBL_1L_2\ldots L_nM_1M_2\ldots M_n}$ with high fidelity.

2. Alice measures the register J and sends the measurement outcome $j \in [n]$ to Bob using $\frac{\log(n)}{2}$ qubits of quantum communication. Alice and Bob employ superdense coding ([BW92]) using fresh entanglement to achieve this.

3. Alice swaps registers L_j and L_1 and Bob swaps registers M_j and M_1. Note that the joint state on the registers RBL_1F_1 at this stage is $\left|\tilde{\Phi}\right\rangle_{RBL_1M_1}$.

4. Alice applies an isometry $V : \mathcal{H}_{L_1} \to \mathcal{H}_A$ on the state $\left|\tilde{\Phi}\right\rangle_{RBL_1M_1}$ such that the joint state in registers RAM_1B is Φ_{RBAM_1}, as given by Uhlmann's theorem (Fact .6)

Consider the state,

$$\xi_{RBM_1\ldots M_n} \stackrel{\text{def}}{=} \Phi_{RB} \otimes \sigma_{M_1} \ldots \otimes \sigma_{M_n}.$$

Let $|\theta\rangle_{L_1\ldots L_nM_1\ldots M_n} = |\sigma\rangle_{L_1M_1} \otimes |\sigma\rangle_{L_2M_2} \ldots |\sigma\rangle_{L_nM_n}$ be a purification of $\sigma_{M_1} \otimes \ldots \sigma_{M_n}$. Let

$$|\xi\rangle_{RABML_1\ldots L_nM_1\ldots M_n} \stackrel{\text{def}}{=} |\Phi\rangle_{RABM} \otimes |\theta\rangle_{L_1\ldots L_nM_1\ldots M_n}.$$

Using convex-split lemma (Lemma .12) and choice of n we have,

$$\mathrm{F}^2(\xi_{RBM_1\ldots M_n}, \mu_{RBM_1\ldots M_n}) \geq 1 - \varepsilon^2.$$

Let $|\xi'\rangle_{RBJL_1\dots L_nM_1\dots M_n}$ be a purification of $\xi_{RBM_1\dots M_n}$ (guaranteed by Uhlmann's theorem, Fact .6) such that,

$$\mathrm{F}^2(|\xi'\rangle\langle\xi'|_{RBJL_1\dots L_nM_1\dots M_n}, |\mu\rangle\langle\mu|_{RBJL_1\dots L_nM_1\dots M_n}) = \mathrm{F}^2(\xi_{RBM_1\dots M_n}, \mu_{RBM_1\dots M_n}) \geq 1-\varepsilon^2.$$

Let $V' : \mathcal{H}_{AML_1\dots L_n} \to \mathcal{H}_{JL_1\dots L_n}$ be an isometry (guaranteed by Uhlmann's theorem, Fact .6) such that,

$$V'|\xi\rangle_{RABML_1\dots L_nM_1\dots M_n} = |\xi'\rangle_{RBJL_1\dots L_nM_1\dots M_n}.$$

Consider the following protocol $\mathcal{P}$.

1. Alice, Bob and Referee start by sharing the state $|\xi\rangle_{RABML_1\dots L_nM_1\dots M_n}$ between themselves where Alice holds registers $AML_1\dots L_n$, Referee holds the register R and Bob holds the registers $BM_1\dots M_n$. Note that $|\Psi\rangle_{RABM}$ is provided as input to the protocol and $|\theta\rangle_{L_1\dots L_nM_1\dots M_n}$ is additional shared entanglement between Alice and Bob.

2. Alice applies isometry V' to obtain state $|\xi'\rangle_{RBJL_1\dots L_nM_1\dots M_n}$, where Alice holds registers $JL_1\dots L_n$, Referee holds the register R and Bob holds the registers $BM_1\dots M_n$.

3. Alice and Bob simulate protocol $\mathcal{P}_1$ from Step 2. onwards.

Let Φ'_{RABM} be the output of protocol $\mathcal{P}$. Since quantum maps (the entire protocol $\mathcal{P}_1$ can be viewed as a quantum map from input to output) do not decrease fidelity (monotonicity of fidelity under quantum operation, Fact .5), we have,

$$\mathrm{F}^2(\Phi_{RABM}, \Phi'_{RABM}) \geq \mathrm{F}^2(|\xi'\rangle\langle\xi'|_{RBJL_1\dots L_nM_1\dots M_n}, |\mu\rangle\langle\mu|_{RBJL_1\dots L_nM_1\dots M_n}) \geq 1-\varepsilon^2. \tag{4}$$

This implies $\Phi_{RABM} \in \mathcal{B}^{\varepsilon}(|\Psi\rangle\langle\Psi|_{RABC})$.

The number of qubits communicated by Alice to Bob in $\mathcal{P}$ is upper bounded by:

$$\frac{\log(n)}{2} \leq \frac{1}{2}\mathrm{I}_{\max}(RB:M)_{\Phi} + \log\left(\frac{1}{\varepsilon}\right).$$

$\square$

Communication bounds on quantum state redistribution

We begin with definition of quantum state redistribution. Please note that we allow Alice and Bob to share arbitrary prior entanglement. In comparison, the previous works [BCT16, DHO14] use EPR states and also take into account the amount of entanglement used by the protocol.

Definition .14 (Quantum state redistribution)**.** The quantum state $|\Psi\rangle_{RABC} \in \mathcal{D}(RABC)$ is shared between three parties Referee (R), Bob (B) and Alice (AC). In addition, Alice and Bob are allowed to share an arbitrary pure state $|\theta\rangle_{S_A^1S_B^1}$, where register S_A^1 belongs to Alice and register S_B^1 belongs to Bob. Let M represent the message register. Alice applies an encoding map $\mathcal{E} : \mathcal{L}(ACS_A^1) \to \mathcal{L}(AM)$ and sends the message M to Bob. Bob applies a decoding map $\mathcal{D} : \mathcal{L}(MBS_B^1) \to \mathcal{L}(BC)$. The resulting state Φ_{RABC} is the *output* of the protocol. Quantum communication cost of the protocol is $\log|M|$.

Using Stinespring representation (Fact .4), the quantum maps $\mathcal{E}$ and $\mathcal{D}$ can be realized as unitary operations using additional ancillas. Let the ancillary register needed for map $\mathcal{E}$ by Alice be S_A^2, holding the state $\theta'_{S_A^2}$, and the ancillary register needed for map $\mathcal{D}$ by Bob be S_B^2, holding the state $\theta'_{S_B^2}$. Introduce registers $S_A \stackrel{\mathrm{def}}{=} S_A^1S_A^2$ and $S_B \stackrel{\mathrm{def}}{=} S_B^1S_B^2$. Let the joint state in registers S_AS_B be $|\theta\rangle_{S_AS_B}$. Then following is equivalent to Definition .14. Alice applies a unitary U_{ACS_A} on her registers, leading to the registers AMT_A on her side (with $MT_A \equiv CS_A$). She sends M to Bob, who applies a unitary V_{MBS_B} and discards all his registers except BC. Let the registers discarded by Bob be T_B. The output of protocol is the state Φ_{RABC} in register $RABC$. Figure 3 elaborates upon this description.

Before proceeding to our upper and lower bounds, we present the following definition.

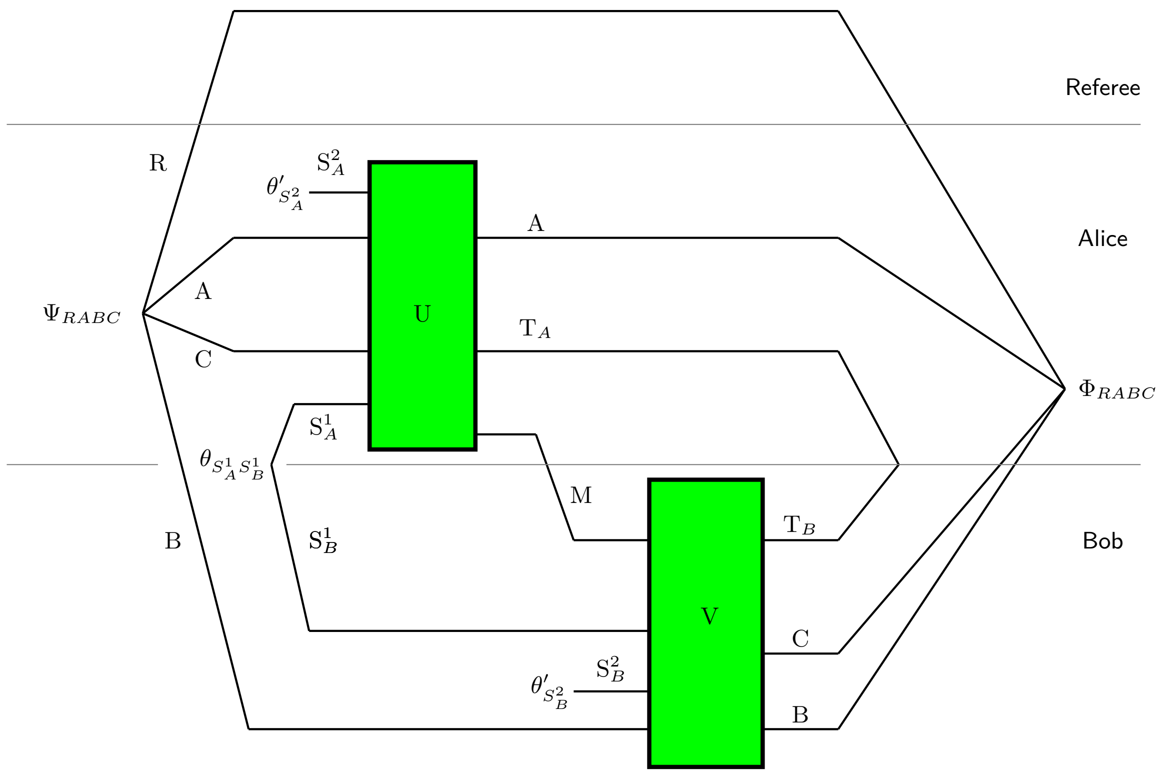

FIG. 3. Graphical representation of one-way entanglement assisted quantum state redistribution.

Definition .15. Let $\varepsilon \geq 0$ and $\Psi_{RABC} \in \mathcal{D}(RABC)$ be a pure state. Define,

$$\begin{aligned} \mathrm{Q}^{\varepsilon}_{|\Psi\rangle_{RABC}} &\stackrel{\text{def}}{=} \inf_{T, U_{BCT}, \sigma'_T, \kappa_{RBCT}} \mathrm{I}_{\max}(RB : CT)_{\kappa_{RBCT}} \\ &= \inf_{T, U_{BCT}, \sigma'_T, \sigma_{CT}, \kappa_{RBCT}} \mathrm{D}_{\max}(\kappa_{RBCT} \| \kappa_{RB} \otimes \sigma_{CT}) \end{aligned}$$

with the conditions $U_{BCT} \in \mathcal{U}(BCT), \sigma'_T \in \mathcal{D}(T), \sigma_{CT} \in \mathcal{D}(CT)$ and

$$(I_R \otimes U_{BCT})\kappa_{RBCT}(I_R \otimes U^{\dagger}_{BCT}) \in \mathcal{B}^{\varepsilon}(\Psi_{RBC} \otimes \sigma'_T), \kappa_{RB} = \Psi_{RB}.$$

Lower bound

We have the following lower bound result.

Theorem .16 (Lower bound)**.** *Let $\varepsilon > 0$ and $\Psi_{RABC} \in \mathcal{D}(RABC)$ be a pure state. Let $\mathcal{Q}$ be an entanglement-assisted one-way protocol (with communication from* Alice *to* Bob*), which takes as input $|\Psi\rangle_{RABC}$ shared between three parties* Referee *(R),* Bob *(B) and* Alice *(AC) and outputs a state Φ_{RABC} shared between* Referee *(R),* Bob *(BC) and* Alice *(A) such that $\Phi_{RABC} \in \mathcal{B}^{\varepsilon}(\Psi_{RABC})$. The number of qubits communicated by* Alice *to* Bob *in $\mathcal{Q}$ is lower bounded by:*

$$\frac{1}{2}\mathrm{Q}^{\varepsilon}_{|\Psi\rangle_{RABC}}.$$

Proof. Protocol $\mathcal{Q}$ can be written as follows (see Figure 3):

1. Alice and Bob get as input $|\Psi\rangle_{RABC}$ shared between Alice (AC), Referee (R) and Bob (B). In addition Alice and Bob use shared entanglement and local ancillas for their protocol. Let these additional resources be represented by a pure state $|\theta\rangle_{S_AS_B}$ where register S_A is held by Alice and register S_B is held by Bob.

2. Alice applies a unitary U_{ACS_A} on the registers ACS_A. Let $\kappa_{RMAT_ABS_B}$ be the joint state at this stage shared between Alice (MAT_A), Referee (R) and Bob (BS_B), where $MT_A \equiv CS_A$. Note that $\kappa_{RB} = \Psi_{RB}$ and $\kappa_{RBS_B} = \Psi_{RB} \otimes \theta_{S_B}$.

3. Alice sends the message register M to Bob.

4. Bob applies a unitary V_{BS_BM} on the registers BS_BM. Let $\Phi_{RABCT_AT_B}$ be the joint state at this stage shared between Alice (AT_A), Referee (R) and Bob (BCT_B) where $S_BM \equiv CT_B$.

5. The state Φ_{RABC} is considered the output of the protocol $\mathcal{Q}$.

Using Fact .7, we know that there exists a state ω_M, such that:

$$2\log|M| \geq \mathrm{D}_{\max}(\kappa_{RBS_BM} \| \kappa_{RBS_B} \otimes \omega_M) = \mathrm{D}_{\max}(\kappa_{RBS_BM} \| \Psi_{RB} \otimes \theta_{S_B} \otimes \omega_M)\,. \tag{5}$$

We have $\mathrm{F}^2(\Phi_{RABC}, |\Psi\rangle\langle\Psi|_{RABC}) \geq 1-\varepsilon^2$ and $|\Psi\rangle\langle\Psi|_{RABC}$ is a pure state. From Lemma .10 and monotonicity of fidelity under quantum operation (Fact .5) we get a state σ'_{T_B} such that,

$$\mathrm{F}^2(\Phi_{RBCT_B}, \Psi_{RBC} \otimes \sigma'_{T_B}) \geq 1-\varepsilon^2.$$

We have,

$$\Phi_{RBCT_B} = (I_R \otimes V_{BS_BM})\kappa_{RBS_BM}(I_R \otimes V^{\dagger}_{BS_BM}),\ \kappa_{RB} = \Psi_{RB}. \tag{6}$$

Recall that $S_BM \equiv CT_B$. Define $\sigma_{CT_B} \stackrel{\mathrm{def}}{=} \theta_{S_B} \otimes \omega_M$. Eq. (5) and Eq. (6) imply,

$$2\log|M| \geq \mathrm{D}_{\max}(\kappa_{RBCT_B} \| \Psi_{RB} \otimes \sigma_{CT_B})\,,$$

with the conditions

$$\mathrm{F}^2(\Phi_{RBCT_B}, \Psi_{RBC} \otimes \sigma'_{T_B}) > 1-\varepsilon^2, \Phi_{RBCT_B} = (I_R \otimes V_{BCT_B})\kappa_{RBCT_B}(I_R \otimes V^{\dagger}_{BCT_B}), \kappa_{RB} = \Psi_{RB}.$$

From above and the definition of $Q^{\varepsilon}_{|\Psi\rangle_{RABC}}$ we conclude

$$\log|M| \geq \frac{1}{2} Q^{\varepsilon}_{|\Psi\rangle_{RABC}}.$$

$\square$

Upper bound

We show a nearly matching upper bound on the quantum communication cost of quantum state redistribution.

Theorem .17 (Upper bound). *Let $\varepsilon \in (0, 1/3)$ and $\Psi_{RABC} \in \mathcal{D}(RABC)$ be a pure state. There exists an entanglement-assisted one-way protocol $\mathcal{P}$, which takes as input $|\Psi\rangle_{RABC}$ shared between three parties* Referee (R), Bob (B) *and* Alice (AC) *and outputs a state Φ_{RABC} shared between* Referee (R), Bob (BC) *and* Alice (A) *such that $\Phi_{RABC} \in \mathcal{B}^{2\varepsilon}(\Psi_{RABC})$. The number of qubits communicated by* Alice *to* Bob *in $\mathcal{P}$ is upper bounded by:*

$$\frac{1}{2} \mathrm{Q}^{\varepsilon}_{|\Psi\rangle_{RABC}} + \log\left(\frac{2}{\varepsilon}\right).$$

Proof. The definition of $\mathrm{Q}^{\varepsilon}_{|\Psi\rangle_{RABC}}$ involves an infimum over various quantities. There exists a collection $(T, U_{BCT}, \sigma'_T, \sigma_{CT}, \kappa_{RBCT})$ along with the conditions,

$$(I_R \otimes U_{BCT})\kappa_{RBCT}(I_R \otimes U^{\dagger}_{BCT}) \in \mathcal{B}^{\varepsilon}(\Psi_{RBC} \otimes \sigma'_T), \kappa_{RB} = \Psi_{RB},$$

such that $\mathrm{I}_{\max}(RB : CT)_{\kappa} \leq \mathcal{Q}^{\varepsilon}_{\Psi_{RABC}} + 1$.

Define the state

$$\rho_{RBCT} \stackrel{\text{def}}{=} (I_R \otimes U_{BCT})\kappa_{RBCT}(I_R \otimes U^{\dagger}_{BCT}).$$

Since $\kappa_{RB} = \Psi_{RB}$, then for any purification $|\kappa\rangle_{RBCTS}$ of κ_{RBCT}, there exists an isometry $V_1 : \mathcal{H}_{AC} \to \mathcal{H}_{CTS}$ such that

$$|\kappa\rangle\langle\kappa|_{RBCTS} = V_1 \Psi_{RBAC} V_1^{\dagger} \tag{7}$$

We start with the following protocol $\mathcal{P}_1$.

1. Alice(CTS), Bob(B) and Referee(R) start with the state $|\kappa\rangle_{RBCTS}$ and shared entanglement as required in the protocol described in Theorem .13.

2. Using the protocol described in Theorem .13, the parties produce a state κ'_{RBCTS} with registers BCT belonging to Bob, S belonging to Alice and R belonging to Referee, such that $\mathrm{F}^2(\kappa'_{RBCTS}, \kappa_{RBCTS}) \geq 1 - \varepsilon^2$. In other words,

$$\mathcal{P}(\kappa'_{RBCTS}, \kappa_{RBCTS}) \leq \varepsilon \tag{8}$$

3. Bob applies the unitary U_{BCT} on registers BCT.

The number of qubits communicated in $\mathcal{P}_1$ is $\frac{1}{2}\mathrm{I}_{\max}(RB : CT)_{\kappa} + \log(\frac{1}{\varepsilon})$.

At the end of the protocol, the state in registers $RBCT$ is $U_{BCT}\kappa'_{RBCT}U^{\dagger}_{BCT}$. By definition of ρ_{RBCT}, the relation $\mathcal{P}(\rho_{RBCT}, \Psi_{RBC} \otimes \sigma'_T) \leq \varepsilon$ and Equation 8, we find (using triangle inequality for purified distance (Fact .3)) that

$$\mathcal{P}(\Psi_{RBC} \otimes \sigma'_T, U_{BCT}\kappa'_{RBCT}U^{\dagger}_{BCT}) \leq 2\varepsilon.$$

Thus, there exists an isometry $V_2 : \mathcal{H}_S \to \mathcal{H}_{AE}$ such that for a purification $|\sigma'\rangle_{ET}$ of σ_T,

$$\mathcal{P}(\Psi_{RABC} \otimes |\sigma'\rangle\langle\sigma'|_{ET}, V_2 \otimes U_{BCT}\kappa'_{RBCTS}U^{\dagger}_{BCT} \otimes V_2^{\dagger}) \leq 2\varepsilon \tag{9}$$

Now, we describe the protocol $\mathcal{P}$ that achieves the desired task.

1. Alice(AC), Bob(B) and Referee(R) start with the state $|\Psi\rangle_{RABC}$ and the shared entanglement as required to run the protocol $\mathcal{P}_1$ below.

2. Alice applies the isometry V_1 on her registers. The parties run the protocol $\mathcal{P}_1$. Finally, Alice applies the isometry V_2 on her registers.

Let the final state produced in registers $RABC$ be Φ_{RABC}. Using equations 9 and 7, we find that $\mathcal{P}(\Psi_{RABC}, \Phi_{RABC}) \leq 2\varepsilon$.

Since the quantum communication cost of $\mathcal{P}$ is equal to the quantum communication cost of $\mathcal{P}_1$, the number of qubits communicated by Alice to Bob in $\mathcal{P}$ is upper bounded by:

$$\frac{\log(n)}{2} \leq \frac{1}{2}\mathrm{Q}^{\varepsilon}_{|\Psi\rangle_{RABC}} + \frac{1}{2} + \log\left(\frac{1}{\varepsilon}\right) \leq \frac{1}{2}\mathrm{Q}^{\varepsilon}_{|\Psi\rangle_{RABC}} + \log\left(\frac{2}{\varepsilon}\right).$$

□

Communication bounds on quantum state splitting and quantum state merging

In this section, we describe near optimal bound for quantum communication cost of quantum state splitting and quantum state merging protocols. We recall that quantum state splitting is a special case of quantum state redistribution in which the register B is trivial and quantum state merging is a special case of quantum state redistribution in which register A is trivial.

Quantum state splitting

We show the following lemma, which along with our upper bound (Theorem .17) and lower bound (Theorem .16) immediately gives the desired upper and lower bound on quantum communication cost of quantum state splitting.

Lemma .18. *Let $\Psi_{RABC} \in \mathcal{D}(RABC)$ be a pure quantum state and let B be a trivial register, that is, $|B| = 1$. Then $\mathrm{Q}^{\varepsilon}_{|\Psi\rangle_{RABC}} = \mathrm{I}^{\varepsilon}_{\max}(R:C)_{\Psi_{RC}}$.*

Proof. Since register B is trivial, we drop the notation B from the quantum states discussed below. Given the quantum state κ_{RCT} as appearing in definition of $Q^{\varepsilon}_{|\Psi\rangle_{RAC}}$ (Definition .15), we define the state

$$\rho_{RCT} \stackrel{\mathrm{def}}{=} (I_R \otimes U_{CT})\kappa_{RCT}(I_R \otimes U^{\dagger}_{CT}).$$

It holds that $\rho_{RCT} \in \mathcal{B}^{\varepsilon}(\Psi_{RC} \otimes \sigma'_T)$. Note that the condition $\kappa_R \in \mathcal{B}^{\varepsilon}(\Psi_R)$ is now redundant (is implied by above using $\rho_R = \kappa_R$ and monotonicity of fidelity under quantum operation, Fact .5). Consider,

$$\begin{aligned}
\mathrm{Q}^{\varepsilon}_{|\Psi\rangle_{RAC}} &= \inf_{T,U_{CT},\sigma_{CT},\sigma'_T,\kappa_{RCT}} \mathrm{D}_{\max}(\kappa_{RCT}\|\kappa_R \otimes \sigma_{CT}) \\
&= \inf_{T,U_{CT},\sigma_{CT},\sigma'_T,\kappa_{RCT}} \mathrm{D}_{\max}\left((I_R \otimes U^{\dagger}_{CT})\rho_{RCT}(I_R \otimes U_{CT})\middle\|\kappa_R \otimes \sigma_{CT}\right) \\
&= \inf_{T,U_{CT},\sigma_{CT},\sigma'_T,\kappa_{RCT}} \mathrm{D}_{\max}\left(\rho_{RCT}\middle\|\kappa_R \otimes U_{CT}\sigma_{CT}U^{\dagger}_{CT}\right) \\
&= \inf_{T,\mu_{CT},\sigma'_T,\kappa_{RCT}} \mathrm{D}_{\max}(\rho_{RCT}\|\kappa_R \otimes \mu_{CT}) \quad (\text{with } \mu_{CT} \stackrel{\mathrm{def}}{=} U_{CT}\sigma_{CT}U^{\dagger}_{CT}) \\
&= \inf_{T,\sigma'_T,\rho_{RCT}\in\mathcal{B}^{\varepsilon}\left(\Psi_{RC}\otimes\sigma'_T\right)} \mathrm{I}_{\max}(R:CT)_{\rho_{RCT}} \quad (\text{using } \rho_R = \kappa_R) \\
&= \inf_{T,\sigma'_T} \mathrm{I}^{\varepsilon}_{\max}(R:CT)_{\Psi_{RC}\otimes\sigma'_T}.
\end{aligned}$$

Now,

$$\begin{aligned}
\mathrm{I}^{\varepsilon}_{\max}(R:C)_{\Psi_{RC}} &\geq \inf_{T,\sigma'_T} \mathrm{I}^{\varepsilon}_{\max}(R:CT)_{\Psi_{RC}\otimes\sigma'_T} \quad (\text{by setting } T \text{ to be trivial register}) \\
&= \inf_{T,\sigma'_T,\rho_{RCT}\in\mathcal{B}^{\varepsilon}\left(\Psi_{RC}\otimes\sigma'_T\right)} \mathrm{I}_{\max}(R:CT)_{\rho_{RCT}} \\
&\geq \inf_{\rho_{RC}\in\mathcal{B}^{\varepsilon}(\Psi_{RC})} \mathrm{I}_{\max}(R:C)_{\rho_{RC}} \\
&\quad (\text{using monotonicity of max-information under quantum operation, Fact .8}) \\
&= \mathrm{I}^{\varepsilon}_{\max}(R:C)_{\Psi_{RC}}.
\end{aligned}$$

Therefore,

$$\mathrm{Q}^{\varepsilon}_{|\Psi\rangle_{RAC}} = \inf_{T,\sigma'_T} \mathrm{I}^{\varepsilon}_{\max}(R:CT)_{\Psi_{RC}\otimes\sigma'_T} = \mathrm{I}^{\varepsilon}_{\max}(R:C)_{\Psi_{RC}}.$$

$\square$

Quantum state merging

Now, we consider the case of quantum state merging. It has been noted in [BCR11] that quantum state merging can be viewed as 'time reversed' version of quantum state splitting, and their optimal quantum communication cost is the same.

Lemma .19 ([BCR11])**.** *Let $\varepsilon > 0$ be error parameter. Following two statements are equivalent, with registers A and B such that $A \equiv B$.*

1. *There exists an entanglement assisted quantum state splitting protocol $\mathcal{P}$ with quantum communication cost c, that starts with a state $\Psi_{RAC} \in \mathcal{D}(RAC)$, with AC on Alice's side and R on $\mathsf{Referee}$'s side, and outputs a state Φ_{RAC}, with C on Bob's side, such that $\Phi_{RAC} \in \mathcal{B}^{\varepsilon}(\Psi_{RAC})$.*
2. *There exists an entanglement assisted quantum state merging protocol $\mathcal{Q}$ with quantum communication cost c, that starts with the state $\Psi_{RBC} \in \mathcal{D}(RBC)$, with C on Alice's side and B on Bob's side, and outputs a state Φ'_{RBC}, with (BC) on Bob's side, such that $\Phi'_{RBC} \in \mathcal{B}^{\varepsilon}(\Psi_{RBC})$.*

Proof. We show that (1) $\implies$ (2). Let the protocol $\mathcal{P}$ start with the overall pure state $\Psi_{RAC} \otimes \mu_E$, where the register E include shared entanglement and other ancilla registers used by $\mathcal{P}$. Let the final pure state of the protocol be Φ_{RACE}, with $\mathrm{F}^2(\Phi_{RAC}, \Psi_{RAC}) \geq 1 - \varepsilon^2$. To describe the quantum state merging protocol, we now relabel register A with register B. Since protocol $\mathcal{P}$ is a collection of unitary operations (which are invertible, see discussion after Definition .14), it implies that there exists a protocol $\mathcal{P}'$ (which is inverse of the protocol $\mathcal{P}$) that starts with the state Φ_{RBCE}, and leads to the state $\Psi_{RBC} \otimes \mu_E$ with $\mathrm{F}^2(\Psi_{RBC}, \Phi_{RBC}) \geq 1 - \varepsilon^2$. From Uhlmann's theorem (Fact .6), there exists a pure state μ'_E that satisfies

$$\mathrm{F}^2(\Psi_{RBC} \otimes \mu'_E, \Phi_{RBCE}) = \mathrm{F}^2(\Psi_{RBC}, \Phi_{RBC}) \geq 1 - \varepsilon^2.$$

Let $\mathcal{Q}$ be a protocol that starts with the pure state $\Psi_{RBC} \otimes \mu'_E$, and then follows the protocol $\mathcal{P}'$. Let the overall state at the end of $\mathcal{Q}$ be Φ'_{RBCE}. Then,

$$\mathrm{F}^2(\Psi_{RBC}, \Phi'_{RBC}) \geq \mathrm{F}^2(\Psi_{RBC} \otimes \mu_E, \Phi'_{RBCE}) = \mathrm{F}^2(\Phi_{RBCE}, \Psi_{RBC} \otimes \mu'_E)) \geq 1 - \varepsilon^2.$$

It is clear that the communication between Alice and Bob is the same in $\mathcal{P}$ and $\mathcal{Q}$.

(2) $\implies$ (1) can be proved using similar arguments. ☐

Port-based teleportation

We consider the problem of port-based teleportation, when the sender Alice and the receiver Bob know that the set of possible states to be teleported belong to the ensemble $\{p_i, |\psi\rangle\langle\psi|^i\}_i$, with $\sum_i p_i = 1$. Alice is given the state $\left|\psi^i\right\rangle\left\langle\psi^i\right|$ with probability p_i which she wishes to teleport to Bob.

Before proving our result, we will prove the following useful Lemma. It can be seen as a one-sided analogue of the relation between optimal fidelity of teleportation and maximal singlet fraction as proven in [HHH99].

Lemma .20. *Given a quantum channel $\mathcal{E} : M \to M$ with Kraus-representation $\mathcal{E}(\rho) = \sum_k A_k \rho A_k^{\dagger}$ and an ensemble $\{p_i, |\psi\rangle\langle\psi|^i_M\}_i$ with $\psi^i_M \in \mathcal{D}(M)$, define the state $|\Psi\rangle_{RM} \stackrel{\mathrm{def}}{=} \sum_i \sqrt{p_i}\, |i\rangle_R\, |\psi\rangle^i_M$. Then it holds that*

$$\langle\Psi|_{RM}\, \mathcal{E}(\Psi_{RM})\, |\Psi\rangle_{RM} \leq \sum_i p_i\, \langle\psi|^i_M\, \mathcal{E}(\psi^i_M)\, |\psi\rangle^i_M\, .$$

Proof. We proceed as follows.

$$\begin{aligned}\langle\Psi|_{RM}\, \mathcal{E}(\Psi_{RM})\, |\Psi\rangle_{RM} &= \sum_k |\, \langle\Psi|_{RM}\, \mathrm{I}_R \otimes A_k\, |\Psi\rangle_{RM}\, |^2 = \sum_k |\sum_i p_i \mathrm{Tr}(\psi^i_M A_k)|^2 \\ &\leq \sum_k (\sum_i p_i) \cdot (\sum_i p_i |\mathrm{Tr}(\psi^i_M A_k)|^2) = \sum_i p_i \sum_k |\mathrm{Tr}(\psi^i_M A_k)|^2\end{aligned}$$

The inequality above is due to the Cauchy-Schwartz inequality. Now, we observe that

$$\sum_i p_i \langle\psi|_M^i \,\mathcal{E}(\psi_M^i)\,|\psi\rangle_M^i = \sum_i p_i \sum_k |\mathrm{Tr}(\psi_M^i A_k)|^2,$$

which completes the proof. □

Now we proceed to our main theorem of this section.

Theorem .21. *Consider an ensemble of pure quantum states $\{p_i, |\psi\rangle\langle\psi|_M^i\}_i$, with $\psi_M^i \in \mathcal{D}(M)$. Introduce a register R and define the state $|\Psi\rangle_{RM} \stackrel{\mathrm{def}}{=} \sum_i \sqrt{p_i}\,|i\rangle_R\,|\psi\rangle_M^i$. Let σ_M be an arbitrary state and $k \stackrel{\mathrm{def}}{=} \mathrm{D}_{\max}(\Psi_{RM}\|\Psi_R \otimes \sigma_M)$. Suppose* Alice *and* Bob *share n copies of a purification of σ_M. Then there exists a port-based teleportation protocol such that* Bob *outputs the register $M' \equiv M$ and for each i, the final state with* Bob *is $\phi_{M'}^i$ such that $\sum_i p_i \mathrm{F}^2(\psi_{M'}^i, \phi_{M'}^i) \geq 1 - \frac{2^k}{n}$.*

Proof. We define the state

$$\tau_{RM_1M_2\ldots M_n} \stackrel{\mathrm{def}}{=} \frac{1}{n}\sum_j \Psi_{RM_j} \otimes \sigma_{M_1} \otimes \ldots \sigma_{M_{j-1}} \otimes \sigma_{M_{j+1}} \ldots \otimes \sigma_{M_n}.$$

Consider the following purification of $\tau_{RM_1M_2\ldots M_n}^i$,

$$|\tau^i\rangle_{JL_1L_2\ldots L_nRM_1M_2\ldots M_n} \stackrel{\mathrm{def}}{=} \frac{1}{\sqrt{n}}\sum_j |j\rangle_J\,|\Psi\rangle_{RM_j}\,|\sigma\rangle_{L_1M_1}\otimes\ldots|\sigma\rangle_{L_{j-1}M_{j-1}}\otimes|0\rangle_{L_j}\otimes|\sigma\rangle_{L_{j+1}M_{j+1}}\ldots\otimes|\sigma\rangle_{L_nM_n},$$

where $|\sigma\rangle_{L_iM_i}$ is a purification of σ_{M_i} and $|0\rangle_{L_j}$ is some fixed state.

From convex split lemma .12, it holds that

$$\mathrm{F}^2(\tau_{RM_1M_2\ldots M_n}, \Psi_R \otimes \sigma_{M_1} \otimes \sigma_{M_2} \ldots \otimes \sigma_{M_n}) \geq \frac{1}{1+\frac{2^k}{n}}.$$

Thus, there exists an isometry $V : \mathcal{H}_{ML_1L_2\ldots L_n} \to \mathcal{H}_{JL_1L_2\ldots L_n}$ (guaranteed by Uhlmann's theorem, Fact .6), such that

$$\mathrm{F}^2(|\tau\rangle\langle\tau|_{JL_1L_2\ldots L_nRM_1M_2\ldots M_n}, V\,|\Psi\rangle\langle\Psi|_{RM}\otimes|\sigma\rangle\langle\sigma|_{L_1M_1}\otimes|\sigma\rangle\langle\sigma|_{L_2M_2}\ldots\otimes|\sigma\rangle\langle\sigma|_{L_nM_n}\,V^\dagger) \geq \frac{1}{1+\frac{2^k}{n}}. \quad (10)$$

We consider the following protocol $\mathcal{P}$:

1. Alice and Bob share n copies of the state $|\sigma\rangle_{LM}$ in registers $L_1M_1, L_2M_2, \ldots L_nM_n$.
2. Alice applies the isometry V and measures the register J. Then she sends the outcome j to Bob.
3. Upon receiving the outcome j, Bob picks up the register M_j and swaps it with his output register M'.

Consider the action of $\mathcal{P}$ when the input to it is the state Ψ_{RM}. Let the state in the registers RM' upon the completion of $\mathcal{P}$ be $\mathcal{P}(\Psi_{RM})$. From Equation 10 and monotonicity of fidelity under quantum map (Fact .5), it holds that $\mathrm{F}^2(\mathcal{P}(\Psi_{RM}), \Psi_{RM}) \geq \frac{1}{1+\frac{2^k}{n}} \geq 1 - \frac{2^k}{n}$.

Since $\mathcal{P}$ is a quantum map, we can apply Lemma .20 to conclude that

$$\sum_i p_i \mathrm{F}^2(\phi_{M'}^i, \psi_{M'}^i) = \sum_i p_i \mathrm{F}^2(\mathcal{P}(\psi_M^i), \psi_M^i) \geq \mathrm{F}^2(\mathcal{P}(\Psi_{RM}), \Psi_{RM}) \geq 1 - \frac{2^k}{n}.$$

This proves the theorem.

□

[ADHW09] Anura Abeyesinghe, Igor Devetak, Patrick Hayden, and Andreas Winter. The mother of all protocols: Restructuring quantum information's family tree. *Proceedings of the Royal Society of London*, A(465):2537–2563, 2009.

[BCF+96] Howard Barnum, Carlton M. Cave, Christopher A. Fuch, Richard Jozsa, and Benjamin Schmacher. Noncommuting mixed states cannot be broadcast. *Phys. Rev. Lett.*, 76(15):2818–2821, 1996.

[BCR11] Mario Berta, Matthias Christandl, and Renato Renner. The Quantum Reverse Shannon Theorem based on one-shot information theory. *Commun. Math. Phys.*, 306(3):579–615, 2011.

[BCT16] M. Berta, M. Christandl, and D. Touchette. Smooth entropy bounds on one-shot quantum state redistribution. *IEEE Transactions on Information Theory*, 62(3):1425–1439, March 2016.

[BD10] Francesco Buscemi and Nilanjana Datta. The quantum capacity of channels with arbitrarily correlated noise. *IEEE Transactions on Information Theory*, 56:1447–1460, 2010.

[Ber09] Mario Berta. Single-shot quantum state merging. Master's thesis, ETH Zurich, http://arxiv.org/abs/0912.4495, 2009.

[BW92] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Phys. Rev. Lett.*, 69(20):2881–2884, 1992.

[Car10] Eric Carlen. Trace inequalities and quantum entropy: an introductory course. entropy and the quantum. *Contemp. Math.*, 529:73–140, 2010.

[CHP07] I. Csiszár, F. Hiai, and D. Petz. Limit relation for quantum entropy and channel capacity per unit cost. *J. Math. Phys.*, 48(092102), 2007.

[CT91] Thomas M. Cover and Joy A. Thomas. *Elements of information theory*. Wiley Series in Telecommunications. John Wiley & Sons, New York, NY, USA, 1991.

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

[DBWR14] Frédéric Dupuis, Mario Berta, Jürg Wullschleger, and Renato Renner. One-shot decoupling. *Communications in Mathematical Physics*, 328(251), 2014.

[DCHR78] D. Dacunha-Castelle, H. Heyer, and B. Roynette. Ecole d'Eté de Probabilités de Saint-Flour VII. *Lecture Notes in Mathematics, Springer-Verlag*, 678, 1978.

[DH11] Nilanjana Datta and Min-Hsiu Hsieh. The apex of the family tree of protocols: optimal rates and resource inequalities. *New Journal of Physics*, 13(093042), 2011.

[DHO14] Nilanjana Datta, Min-Hsiu Hsieh, and Jonathan Oppenheim. An upper bound on the second order asymptotic expansion for the quantum communication cost of state redistribution. http://arxiv.org/abs/1409.4352, 2014.

[Dup10] Frédéric Dupuis. The decoupling approach to quantum information theory. PhD Thesis, Université de Montréal., http://arxiv.org/abs/1410.0664, 2010.

[DY08] Igor Devetak and Jon Yard. Exact cost of redistributing multipartite quantum states. *Phys. Rev. Lett.*, 100(230501), 2008.

[HHH99] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki. General teleportation channel, singlet fraction, and quasidistillation. *Phys. Rev. A*, 60:1888–1898, Sep 1999.

[HJMR10] Prahladh Harsha, Rahul Jain, David Mc.Allester, and Jaikumar Radhakrishnan. The communication complexity of correlation. *IEEE Transcations on Information Theory*, 56:438–449, 2010.

[HOW07] Michał Horodecki, Jonathan Oppenheim, and Andreas Winter. Quantum state merging and negative information. *Communications in Mathematical Physics*, 269(1):107–136, 2007.

[IH08] Satoshi Ishizaka and Tohya Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. *Phys. Rev. Lett.*, 101:240501, Dec 2008.

[IH09] Satoshi Ishizaka and Tohya Hiroshima. Quantum teleportation scheme by selecting one of multiple output ports. *Phys. Rev. A*, 79:042306, Apr 2009.

[JRS03] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A direct sum theorem in communication complexity via message compression. In *Proceedings of the 30th international conference on Automata, languages and programming*, ICALP'03, pages 300–315, Berlin, Heidelberg, 2003. Springer-Verlag.

[JRS05] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. Prior entanglement, message compression and privacy in quantum communication. In *Proceedings of the 20th Annual IEEE Conference on Computational Complexity*, pages 285–296, Washington, DC, USA, 2005. IEEE Computer Society.

[LD09] Zhicheng Luo and Igor Devetak. Channel simulation with quantum side information. *IEEE Transactions on Information Theory*, 55:1331–1342, 2009.

[Lin75] G. Lindblad. Completely positive maps and entropy inequalities. *Commun. Math. Phys.*, 40:147–151, 1975.

[MBD+16] Christian Majenz, Mario Berta, Frédéric Dupuis, Renato Renner, and Matthias Christandl. Catalytic decoupling of quantum information. 2016.

[NC00] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, Cambridge, UK, 2000.

[Opp08] Jonathan Oppenheim. State redistribution as merging: introducing the coherent relay. http://arxiv.org/abs/0805.1065, 2008.

[Ren05] Renato Renner. Security of quantum key distribution. PhD Thesis, ETH Zurich, Diss. ETH No. 16242, arXiv:quant-ph/0512258, 2005.

[Sch95] Benjamin Schumacher. Quantum coding. *Phys. Rev. A.*, 51:2738–2747, 1995.

[Sha] Claude Elwood Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423.

[Sti55] W. F. Stinespring. Positive functions on c*-algebras. *Proceedings of the American Mathematical Society*, page 211–216, 1955.

[TCR10] Marco Tomamichel, Roger Colbeck, and Renato Renner. Duality between smooth min- and max-entropies. *IEEE Transactions on Information Theory*, 56(9):4674 – 4681, 2010.

[Tom12] Marco Tomamichel. A framework for non-asymptotic quantum information theory. PhD Thesis, ETH Zurich, http://arXiv,org/abs/1203.2142, 2012.

[Tou15] Dave Touchette. Quantum information complexity. In *Proceedings of the Forty-Seventh Annual ACM on Symposium on Theory of Computing*, STOC '15, pages 317–326, New York, NY, USA, 2015. ACM.

[Uhl76] A. Uhlmann. The "transition probability" in the state space of a *-algebra. *Rep. Math. Phys.*, 9:273–279, 1976.

[Wat11] John Watrous. Theory of Quantum Information, lecture notes, 2011. https://cs.uwaterloo.ca/ watrous/LectureNotes.html.

[YBW08] Ming-Yong Ye, Yan-Kui Bai, and Z. D. Wang. Quantum state redistribution based on a generalized decoupling. *Physical Review A*, 78(030302(R)), 2008.

[YD09] Jon T. Yard and Igor Devetak. Optimal quantum source coding with quantum side information at the encoder and decoder. *IEEE Transactions on Information Theory*, 55:5339–5351, 2009.