Quantum communication using coherent rejection sampling

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

Compression of a message up to the information it carries is key to many tasks involved in classical and quantum information theory. Schumacher [3] provided one of the first quantum *compression* schemes and several more general schemes have been developed ever since [5, 6, 9]. However, the one-shot characterization of these quantum tasks is still under development, and often lacks a direct connection with analogous classical tasks. Here we show a new technique for the compression of quantum messages with the aid of entanglement. We devise a new tool that we call the *convex split* lemma, which is a coherent quantum analogue of the widely used *rejection sampling* procedure in classical communication protocols. As a consequence, we exhibit new explicit protocols with tight communication cost for *quantum state merging, quantum state splitting* and *quantum state redistribution* (up to a certain optimization in the latter case). We also present a *port-based teleportation* scheme which uses less number of ports in presence of information about input.

Quantum teleportation [1], one of the most celebrated features of quantum information, allows Alice to send an unknown qubit to Bob using a classical message of 2 bits, assuming that both share a copy of the EPR state: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$. As an additional 'security' feature, the message sent by Alice is completely random: it carries no information about the state of the qubit being sent. It is not hard to imagine a similar *classical teleportation* scheme: Alice and Bob share a pair of perfectly correlated random coins, both taking values 0 or 1 with equal probability. Alice takes one sample from an unknown coin given to her, another sample from the aforementioned coin shared with Bob. If the values of samples match, Alice tells Bob to do nothing. Else she tells Bob to flip his coin. Once again, the message sent from Alice is completely random and independent of the unknown coin given to her.

Now, imagine a situation where Alice and Bob did not share any resource whatsoever, and Alice sent a random message to Bob. Clearly, this situation is completely futile for the purpose of transmitting an unknown qubit or a coin. This leads to a natural question: how does the presence of a shared resource bring such a dramatic change in this situation? The answer comes from the observation that the presence of a shared resource, whether classical or quantum, lends to Alice a complete *classical knowledge* or a *quantum knowledge* of the state of the system present with Bob. This knowledge allows Alice to orchestrate a desired state onto the system with Bob, an idea that has had profound implications in classical information theory.

The long history of classical information theory has seen various simplifications of the protocols for message transmission originally conceived, for example, by Shannon[4] and Slepian and Wolf[2]. An important simplification has been through the idea of one-shot information theory, which has surprisingly shown that studying single use of the channel can bring substantial clarity in the structure of the protocols. Another instance is the consideration of protocols that use shared coins or randomness, giving access of the aforementioned classical knowledge to Alice. These developments have been pivotal in constructing protocols in more complicated settings of classical network theory. An elegant technique that has come for wide use in one-shot classical information theory, as a consequence of above developments, is the rejection sampling technique as expressed in Figure 1. Several interesting generalizations of this idea have been used to obtain communication bounds in other more complicated settings in one-shot classical network theory [31–34].

On the other hand, quantum information is arguably more counter-intuitive than classical information, largely owing to the phenomena of entanglement. An interesting platform for studying quantum information is that of coherent quantum protocol, as depicted in Figure 2. Let's try to import the rejec-

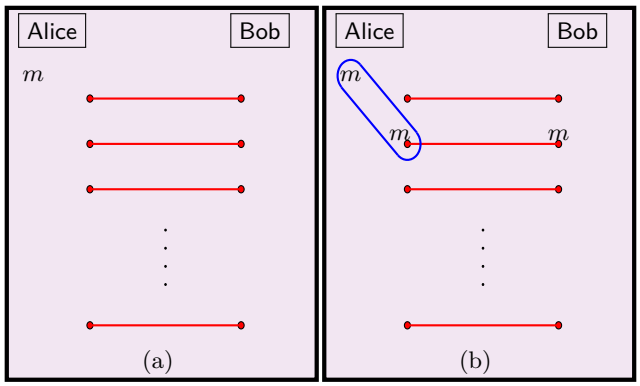

FIG. 1: The rejection sampling scheme: (a) Alice and Bob start with many copies of the shared randomness, equally taking the value m' with probability $p(m')$ (represented with red lines: red small circles represent the random variables connected by the red lines). Alice wishes to transmit m to Bob. (b) She finds a shared randomness which takes same value as her input. Then she sends the index of the shared randomness to Bob.

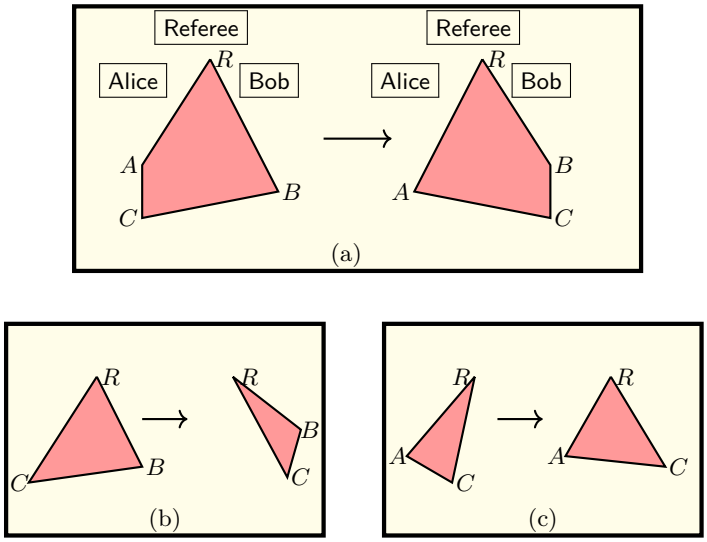

FIG. 2: A large body of work has been done towards quantum state redistribution (a) and its subtasks quantum state merging (b) and quantum state splitting (c) in asymptotic and i.i.d setting ([5], [9], [10], [11], [12]). Various one shot versions of these tasks have been developed in [7],[8],[17, 19]

tion sampling procedure to the coherent quantum setting, say in the simple setting when the registers A, B are absent in Figure 2. The key challenge comes from a very peculiar property of quantum information: monogamy of entanglement [40]. The failure of the tests, that Alice performs on her share of entanglement, lead to correlation between the register R and parts of shared entanglement with Alice, which is not compatible with the requirement that R be correlated only with register C to be output by Bob.

Thus, it comes as no surprise that some non-trivial techniques have been developed to handle quantum information, such as arguments that involve random unitaries (that have been employed in the works mentioned in Figure 2). Does this mean that quantum protocols are somehow inherently distinct from classical protocols and necessarily need more sophisticated techniques? In order to address this question, we revisit the rejection sampling and observe two of its important properties, one of which has been mentioned earlier.

- Using pre-shared randomness, Alice holds complete classical knowledge of the random variable present with Bob.
- Bob's strategy is simply to pick up the correct register based on Alice's message. Thus Alice is largely responsible for creating the right distribution on Bob's side.

We propose a quantum scheme that bases itself on these two properties and successfully performs the task of quantum message compression. The first property naturally lends itself in the setting of coherent quantum communication: Alice holds the purification of registers of both Bob and Referee, and thus has complete quantum knowledge of their registers. We incorporate the second property in our scheme by explicitly designing Bob's strategy (right hand side of Figure 3). For concreteness, we consider the following task: Alice (AM), Bob (B) and Referee (R) share a joint quantum state Ψ_{RABM} and Alice wishes to send the register M to Bob with error at most ε. This task may appear as a sub-routine in any other quantum protocol and the register M is to be interpreted as the message register. Our aim is to minimize the amount of communication needed to transfer M from Alice to Bob. We allow Alice and Bob to share arbitrary prior entanglement, which may be helpful in accomplishing this task.

For our compression protocol, we introduce a new quantum state σ_M. Its purification serves as the shared entanglement between Alice and Bob and both parties share n copies of this state, for a choice of n as made in Figure 3. The chosen value of n is in terms of an information theoretic quantity known as

max-relative entropy. For two quantum states ρ, σ it is defined as $\mathrm{D}_{\max}(\rho\|\theta) = \min\{\lambda : \rho \leq 2^{\lambda}\theta\}$. An intuitive explanation of this quantity is as follows: if we write θ as a convex combination $p\rho + (1-p)\rho'$ (for some arbitrary quantum state ρ'), then the largest value of p that we can choose is $2^{-\mathrm{D}_{\max}(\rho\|\theta)}$.

The quantum state depicted on the left hand side of Figure 3 is the reduced state on the registers involved with Bob and Referee, at the beginning of the protocol. The right hand side of Figure 3 depicts a quantum analogue of the second property mentioned above. It is a convex combination of states $\Phi_{RBM_j} \otimes \sigma_{M_1} \ldots \otimes \sigma_{M_{j-1}} \otimes \sigma_{M_{j+1}} \ldots \otimes \sigma_{M_n}$, such that if Bob knew which of these states he actually shared with the Referee, he could simply go ahead and pick the register M_j. Our main technical result is that the states on the left hand and the right hand side are close to each other (in fidelity) for sufficiently large n. We refer to it as the convex-split lemma.

At the beginning of the protocol, Alice holds the purification of the state on the left hand side in Figure 3. Appealing to Uhlmann's Theorem [36] gives us our desired protocol, as depicted in Figure 4. This protocol allows Alice to send the register M with error ε, and the number of qubits communicated is $\frac{1}{2}\log(n) = \frac{1}{2}\mathrm{D}_{\max}(\Psi_{RBM}\|\Psi_{RB} \otimes \sigma_M) + 2\log\frac{1}{\varepsilon}$. Now if we optimize over all possible σ_M, we can obtain the smallest possible cost of communication. This cost is naturally captured by a quantity called *max-information*, which is suitably defined as $\mathrm{I}_{\max}(RB : M)_{\Psi} = \min_{\sigma_M} \mathrm{D}_{\max}(\Psi_{RBM}\|\Psi_{RB} \otimes \sigma_M)$.

Above we have exhibited a scheme for quantum message compression which is based on a coherent quantum analogue of the classical rejection sampling technique. We point out that non-coherent analogues of classical rejection sampling already exist in literature [31–33]. Next we discuss several applications of our result. The first application is near optimal communication bounds for the tasks of quantum state splitting. We obtain a protocol which makes an error of at most 2ε, and its communication is upper bounded by: $\frac{1}{2}\mathrm{I}^{\varepsilon}_{\max}(R : C)_{\Psi} + \log\frac{1}{\varepsilon}$, where the *smooth max-information* is defined as $\mathrm{I}^{\varepsilon}_{\max}(A : B)_{\rho} \stackrel{\mathrm{def}}{=} \inf_{\rho'_{AB}:\mathrm{F}(\rho',\rho)\geq 1-\varepsilon} \mathrm{I}_{\max}(A : B)_{\rho'}$. It is known that any one-shot one-way entanglement assisted protocol for quantum state splitting that makes an error at most ε must communicate at least $\frac{1}{2}\mathrm{I}^{\varepsilon}_{\max}(R : C)_{\Psi}$ number of qubits [7]. 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 [7]. A slightly weaker form of our result was already known in [7], where the protocol used $\frac{1}{2}\mathrm{I}^{\varepsilon}_{\max}(R : C)_{\Psi} + \log\log\dim(C) + \log\left(\frac{1}{\varepsilon}\right)$ qubits of communication and embezzling quantum states as pre-shared entanglement. We show a similar statement for the case of quantum state redistribution, where the communication cost is tightly characterized by a quantity that captures how well Bob can decouple the registers RB and C using local operations and additional ancilla register T (without changing the state in the registers RB). We leave further understanding of the best possibly decoupling performed by Bob to future work, providing further details in online version of this work[24]. Quantum state redistribution can also be viewed in terms of other related forms of decoupling, as has been recently discussed in [22].

Another application of our work is in the context of port-based teleportation. The works [38, 39] introduced the elegant 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. Port-based teleportation has a very desirable property of being composable and has found important application in relating quantum communication complexity and *Bell-violations* [30]. Using the convex split lemma, we provide a scheme for port-based teleportation which can save on the number of ports (over the scheme by [39]) for a non-uniform ensemble.

Conclusion- In this work, we have provided a new framework for compression of quantum messages and have given applications to quantum state redistribution and port based teleportation. A key feature of our framework is that it is able to provide bounds which match in form to that of the best known bounds for analogous classical and classical-quantum network tasks, given that one is able to prove a suitable extension of the convex-split lemma. The simplicity of its proof allows it to be adapted to different settings. Very recently [25] have applied our framework to several important settings in quantum network theory, such as a quantum version of the *Gel'fand-Pinsker channel* and the *quantum broadcast channel*. The work [26] has used present framework to obtain a new achievability bound on quantum state redistribution, in terms of smooth-max information and hypothesis testing relative entropy. Convex-split lemma has also found application in the

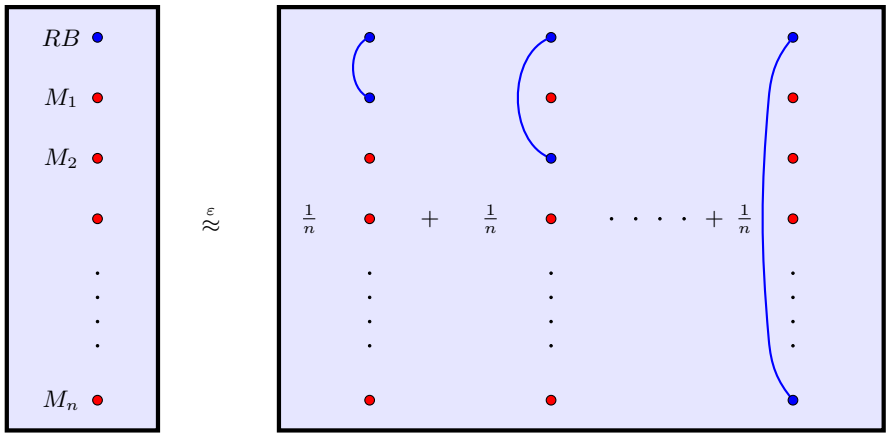

FIG. 3: The small circles refer to physical registers. The blue circles represent the state Ψ_{RB}, the red circles represents the state σ_M. The connected blue circles represent the state Ψ_{RBM}. The state on the left panel represents the actual state shared between Referee and Bob; σ_M is the reduced state on Bob's side in each copy of shared entanglement. If they shared the state on right panel and Bob were told that the j-th state of the n states appearing in the convex combination were actually shared, Bob would be able to directly pick up the corresponding register M_j to obtain the desired state. As a first step, we show that the states on left and right panels are close to each other up to error ε, as long as $\log n \geq \mathrm{D}_{\max}(\Psi_{RBM}\|\Psi_{RB}\otimes\sigma_M) + 2\log\frac{1}{\varepsilon}$. This we refer to as the convex-split lemma.

work [23], in the context of catalytic decoupling. We point out that the present version of this lemma (in supplementary material) further improves the corresponding result in [23]. Other recent applications of the convex-split lemma include privacy in quantum communication (the wiretap channel) in [29], a generalized quantum Slepian-Wolf result in [28] and a bound for the important and consequential task of measurement compression using classical shared randomness in [27]. Given the broad applicability of the convex-split technique as exhibited in these recent works, we expect more applications in quantum network theory in the future.

Acknowledgement- 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.

[1] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, William K. Wootters, Phys. Rev. Lett. **70(13)**, 1895-1899, 1993.
[2] D. Slepian and J. Wolf, IEEE Transactions on Information Theory **19 (4)**, 471-480, 1973.
[3] Benjamin Schumacher, Phys. Rev. A. **51 (4)**, 2738-2747, 1995.
[4] Claude Elwood Shannon, The Bell System Technical Journal **27 (3)**, 379-423, 1948.
[5] Michał Horodecki, Jonathan Oppenheim and Andreas Winter, Commun. Math. Phys. **269**, 107-136, 2007.
[6] Anura Abeyesinghe, Igor Devetak, Patrick Hayden and Andreas Winter, Proceedings of the Royal Society of London **A (465)**, 2537-2563, 2009.
[7] Mario Berta, Matthias Christandl and Renato Renner, Commun. Math. Phys., **306**, 579-615, 2011.
[8] Mario Berta, eprint arXiv:0912.4495, 2009.
[9] Igor Devetak and Jon Yard, Phys. Rev. Lett., **100**, 230501, 2008.
[10] Jonathan Oppenheim, eprint arXiv:0805.1065, 2008.
[11] Ming-Yong Ye, Yan-Kui Bai and Z. D. Wang, Phys. Rev. A. **78**, 030302(R), 2008.
[12] Jon T. Yard and Igor Devetak, IEEE Transactions on Information Theory **55**, 5339-5351, 2009.
[13] Frédéric Dupuis, eprint 1410.0664, 2010.
[14] Francesco Buscemi and Nilanjana Datta, IEEE Transactions on Information Theory **56**, 1447-1460, 2010.
[15] Nilanjana Datta and Min-Hsiu Hsieh, New Journal of Physics **13**, 093042, 2011.
[16] Frédéric Dupuis, Mario Berta, Jürg Wullschleger and Renato Renner, Commun. Math. Phys.,**328**, 251, 2014.
[17] Nilanjana Datta, Min-Hsiu Hsieh and Jonathan Oppenheim, Journal of Mathematical Physics **57**, 052203, 2016.
[18] Zhicheng Luo and Igor Devetak, IEEE Transactions on Information Theory **55**, 1331-1342, 2009.
[19] M. Berta and M. Christandl and D. Touchette, IEEE

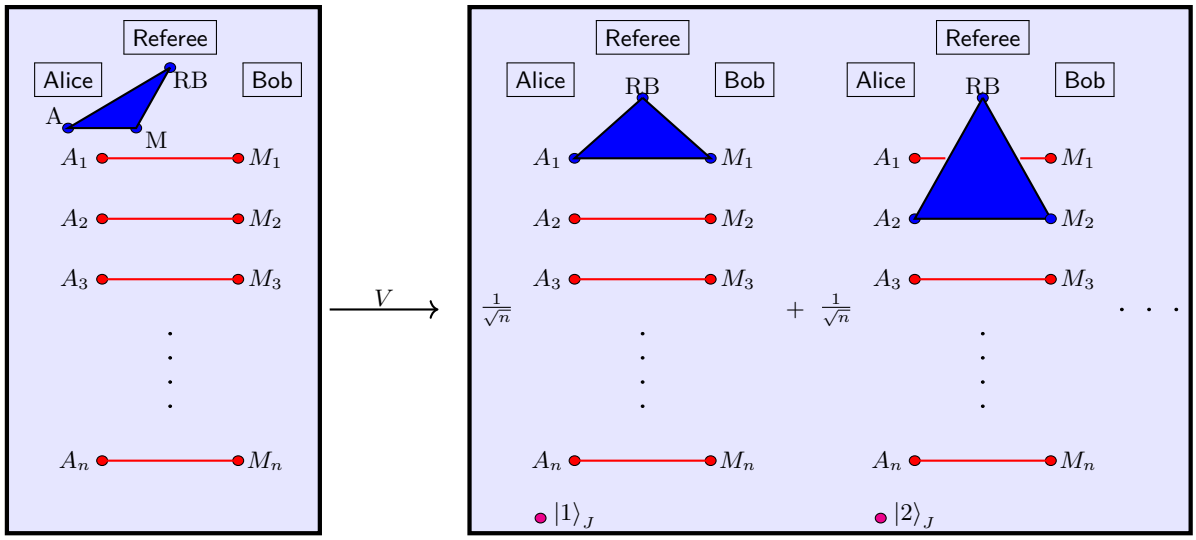

FIG. 4: The small circles represent the physical registers. The blue triangles represent the state Ψ_{RBAM}, the red connected circles represent the state σ_{AM} and the magenta circles represent the message register J. The state on the registers with Referee and Bob is nearly the same on the left panel and the right panel, as promised by the convex split lemma (Figure 3). Thus, as guaranteed by Uhlmann's Theorem [36], there is an isometry V that Alice can apply on her registers to produce a global state close to the state on the right panel. From this point, players can assume that they were sharing the state on the right panel, and Alice can measure the register J to send the outcome j to Bob. Bob now picks up the register M_j and outputs it. Alice outputs A_j. This finishes the protocol as players have obtained the correct state up to the error ε. The amount of entanglement consumed in this process is one copy of purification of σ_M. The quantum communication cost of this protocol is $\frac{1}{2}\log n$, as players can use superdense-coding scheme to achieve the task.

Transactions on Information Theory **62**, 1425-1439, 2016.

[20] Dave Touchette, Proceedings of the 47th Annual ACM on STOC, 317-326, 2015.

[21] Fernando G. S. L. Brandão , Aram W. Harrow, Jonathan Oppenheim and Sergii Strelchuk, Phys. Rev. Lett. **115** 050501, 2015.

[22] Mario Berta, Fernando G. S. L. Brandao, Christian Majenz and Mark M. Wilde, eprint arxiv.org/abs/1609.06994, 2016.

[23] Christian Majenz, Mario Berta, Frédéric Dupuis, Renato Renner and Matthias Christandl, Phys. Rev. Lett. **118 (8)** 080503, 2017.

[24] Anurag Anshu, Vamsi Krishna Devabathini, Rahul Jain, eprint arXiv:1410.3031, 2014.

[25] Anurag Anshu, Rahul Jain and Naqueeb Ahmad Warsi, eprint arXiv:1702.01940, 2017.

[26] Anurag Anshu, Rahul Jain and Naqueeb Ahmad Warsi, eprint arXiv:1702.02396, 2017.

[27] Anurag Anshu, Rahul Jain and Naqueeb Ahmad Warsi, eprint arXiv:1703.02342, 2017.

[28] Anurag Anshu, Rahul Jain and Naqueeb Ahmad Warsi, eprint arXiv:1703.09961, 2017.

[29] Mark M. Wilde, eprint arxiv:1703.01733, 2017.

[30] H. Buhrman, L. Czekaj, A. Grudka, M. Horodecki, P. Horodecki, M. Markiewicz, F. Speelman and S. Strelchuk, PNAS **113 (12)**, 3191-3196, 2016.

[31] Prahladh Harsha, Rahul Jain, David Mc.Allester and Jaikumar Radhakrishnan, IEEE Transcations on Information Theory **56**, 438-449, 2010.

[32] Rahul Jain, Jaikumar Radhakrishnan and Pranab Sen, Proceedings of 30th ICALP, 300-315, 2003.

[33] Rahul Jain, Jaikumar Radhakrishnan and Pranab Sen, Proceedings of the 20th Annual IEEE CCC, 285-296, 2005.

[34] Mark Braverman and Anup Rao, Proceedings of the 52nd Symposium on Foundations of Computer Science (FOCS' 11), 748–757, 2011.

[35] D. Dacunha-Castelle, H. Heyer and B. Roynette, Lecture Notes in Mathematics, Springer-Verlag **678**, 1978.

[36] A. Uhlmann, Rep. Math. Phys. **9**, 273-279, 1976.

[37] Charles H. Bennett and Stephen J. Wiesner, Phys. Rev. Lett. **69**, 2881-2884, 1992.

[38] Satoshi Ishizaka and Tohya Hiroshima, Phys. Rev. Lett. **101**, 240501, 2008.

[39] Satoshi Ishizaka and Tohya Hiroshima, Phys. Rev. A. **79**, 042306, 2009.

[40] B. M. Terhal, IBM Journal of Research and Development **48 (1)**, 71-78, 2004.

Supplementary material: Quantum communication using coherent rejection sampling

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

May 21, 2017

1 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 $\|X\|_1 \stackrel{\text{def}}{=} \text{Tr}\sqrt{X^\dagger X}$ and ℓ_2 norm is $\|X\|_2 \stackrel{\text{def}}{=} \sqrt{\text{Tr} X X^\dagger}$. 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 $\text{supp}(\rho)$ 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 $|A| \stackrel{\text{def}}{=} \dim(\mathcal{H}_A)$. 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

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

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 $VV^\dagger = I_B$. The set of all unitary operations on register A is denoted by $\mathcal{U}(A)$.

Definition 1.1. 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 $\rho_A \in \mathcal{D}(A)$,
$$\mathcal{B}^\varepsilon(\rho_A) \stackrel{\mathrm{def}}{=} \{\rho'_A \in \mathcal{D}(A) |\ \mathcal{P}(\rho_A, \rho'_A) \leq \varepsilon\}.$$

4. **Von-neumann entropy** For $\rho_A \in \mathcal{D}(A)$,
$$\mathrm{S}(\rho_A) \stackrel{\mathrm{def}}{=} -\mathrm{Tr}(\rho_A \log \rho_A).$$

5. **Relative entropy** For $\rho_A, \sigma_A \in \mathcal{D}(A)$ such that $\mathrm{supp}(\rho_A) \subset \mathrm{supp}(\sigma_A)$,
$$\mathrm{D}(\rho_A \| \sigma_A) \stackrel{\mathrm{def}}{=} \mathrm{Tr}(\rho_A \log \rho_A) - \mathrm{Tr}(\rho_A \log \sigma_A).$$

6. **Max-relative entropy** For $\rho_A, \sigma_A \in \mathcal{D}(A)$ such that $\mathrm{supp}(\rho_A) \subset \mathrm{supp}(\sigma_A)$,
$$\mathrm{D}_{\max}(\rho_A \| \sigma_A) \stackrel{\mathrm{def}}{=} \inf\{\lambda \in \mathbb{R} : 2^\lambda \sigma_A \geq \rho_A\}.$$

7. **Mutual information** For $\rho_{AB} \in \mathcal{D}(AB)$,
$$\mathrm{I}(A : B)_\rho \stackrel{\mathrm{def}}{=} \mathrm{S}(\rho_A) + \mathrm{S}(\rho_B) - \mathrm{S}(\rho_{AB}) = \mathrm{D}(\rho_{AB} \| \rho_A \otimes \rho_B) .$$

8. **Conditional mutual information** For $\rho_{ABC} \in \mathcal{D}(ABC)$,
$$\mathrm{I}(A : B|C)_\rho \stackrel{\mathrm{def}}{=} \mathrm{I}(A : BC)_\rho - \mathrm{I}(A : C)_\rho .$$

9. **Max-information** For $\rho_{AB} \in \mathcal{D}(AB)$,
$$\mathrm{I}_{\max}(A : B)_\rho \stackrel{\mathrm{def}}{=} \inf_{\sigma_B \in \mathcal{D}(B)} \mathrm{D}_{\max}(\rho_{AB} \| \rho_A \otimes \sigma_B) .$$

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 1.2 (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 1.3 ([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 1.4 (Monotonicity under quantum operations, [BCF+96],[Lin75])**.** For quantum states ρ, $\sigma \in \mathcal{D}(A)$, 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 1.5 (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 1.6 ([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 1.7 ([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 1.8 (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 1.9. *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 1.5) we get a pure state θ_{BC} such that

$$\begin{aligned}
1-\varepsilon &\leq \mathrm{F}(|\psi\rangle\langle\psi|_A, \rho_A) \\
&= \mathrm{F}(|\psi\rangle\langle\psi|_A \otimes |\theta\rangle\langle\theta|_{BC}, |\rho\rangle\langle\rho|_{ABC}) \\
&\leq \mathrm{F}(|\psi\rangle\langle\psi|_A \otimes \theta_B, \rho_{AB}). \quad \text{(monotonicity of fidelity under quantum operation, Fact 1.4)}
\end{aligned}$$

□

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

Lemma 1.10. *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

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

□

2 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 2.1 (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*

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

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,

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

Using Pinsker's inequality (Fact 1.8), 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 $\delta > 0$ 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 1.10 to express

$$\mathrm{D}(\tau_{PQ_1\ldots Q_n} \| \rho_P \otimes \sigma) = \frac{1}{n}\sum_j \mathrm{D}\left(\rho_{PQ_j} \otimes \sigma^{-j} \middle\| \rho_P \otimes \sigma\right) - \frac{1}{n}\sum_j \mathrm{D}\left(\rho_{PQ_j} \otimes \sigma^{-j} \middle\| \tau_{PQ_1Q_2\ldots Q_n}\right). \quad (2)$$

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 2, 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. □

A converse to Lemma 2.1

We now prove a converse in the following sense.

Lemma 2.2 (A converse to 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(σ_Q). Let $k \stackrel{\text{def}}{=} \mathrm{I}(P:Q)_\rho$. For an integer ℓ, define the following state*

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

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

$$\mathrm{D}_{\max}(\tau_{PQ_1Q_2\ldots Q_\ell} \| \tau_P \otimes \sigma_{Q_1} \otimes \sigma_{Q_2} \ldots \otimes \sigma_{Q_\ell}) \geq \log(\frac{2^k}{\ell} - 2).$$

Proof. For brevity, set $\mathrm{D}_{\max}(\tau_{PQ_1Q_2\ldots Q_\ell} \| \tau_P \otimes \sigma_{Q_1} \otimes \sigma_{Q_2} \ldots \otimes \sigma_{Q_\ell}) \stackrel{\text{def}}{=} \alpha$ and $\sigma_{Q_1} \otimes \sigma_{Q_2} \ldots \otimes \sigma_{Q_\ell} \stackrel{\text{def}}{=} \sigma^{(\ell)}$. Define the following state related to $\tau_{PQ_1Q_2\ldots Q_\ell}$, but on m registers, where m is a multiple of ℓ:

$$\tau_{PQ_1Q_2\ldots Q_m J} \stackrel{\text{def}}{=} \frac{1}{m}\sum_{j=1}^{m} \rho_{PQ_j} \otimes \sigma_{Q_1} \otimes \sigma_{Q_2} \ldots \otimes \sigma_{Q_{j-1}} \otimes \sigma_{Q_{j+1}} \ldots \otimes \sigma_{Q_m} \otimes |j\rangle\langle j|_J$$

It is easy to see that

$$\tau_{PQ_1Q_2\ldots Q_m} \stackrel{\text{def}}{=} \frac{\ell}{m}\sum_{j=1}^{m/\ell} \tau_{PQ_{\ell\cdot(j-1)+1}\ldots Q_{\ell\cdot(j-1)+\ell}} \otimes \sigma^{(\ell)}_{Q_1\ldots Q_\ell} \otimes \ldots \otimes \sigma_{Q_{\ell\cdot(j-2)+1}\ldots Q_{\ell\cdot(j-2)+\ell}} \otimes \sigma_{Q_{\ell\cdot(j)+1}\ldots Q_{\ell\cdot(j)+\ell}} \cdots$$

Then from Lemma 2.1, we conclude that

$$\mathrm{D}(\tau_{PQ_1Q_2\ldots Q_m} \| \tau_P \otimes \sigma_{Q_1} \ldots \sigma_{Q_m}) \leq \log(1 + \frac{2^\alpha \cdot \ell}{m}).$$

Now, observe that

$$\mathrm{I}(P : Q_1Q_2\ldots Q_mJ)_\tau \leq \mathrm{I}(P : Q_1Q_2\ldots Q_m)_\tau + \log m \leq \mathrm{D}(\tau_{PQ_1Q_2\ldots Q_m} \| \tau_P \otimes \sigma_{Q_1} \ldots \sigma_{Q_m}) + \log m.$$

Thus, we conclude that

$$\mathrm{I}(P : Q)_\rho = \mathrm{I}(P : Q_1Q_2\ldots Q_mJ)_\tau \leq \log(1 + \frac{2^\alpha \cdot \ell}{m}) + \log m = \log(m + 2^\alpha \cdot \ell).$$

Setting $m = 2\ell$, the lemma follows. □

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

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

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 $n \to \infty$).

3 Compression of one-way quantum message

Consider a state Φ_{RAMB} shared between $\mathsf{Alice}(AM)$, $\mathsf{Bob}(B)$ and $\mathsf{Referee}(R)$. 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 1.

Theorem 3.1 (Quantum message compression)**.** *There exists an entanglement-assisted one-way protocol $\mathcal{P}$, which takes as input $|\Phi\rangle_{RAMB}$ shared between three parties* $\mathsf{Referee}$ (R), Bob (B) *and* Alice (AM) *and outputs a state Φ'_{RAMB} shared between* $\mathsf{Referee}$ (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:*

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

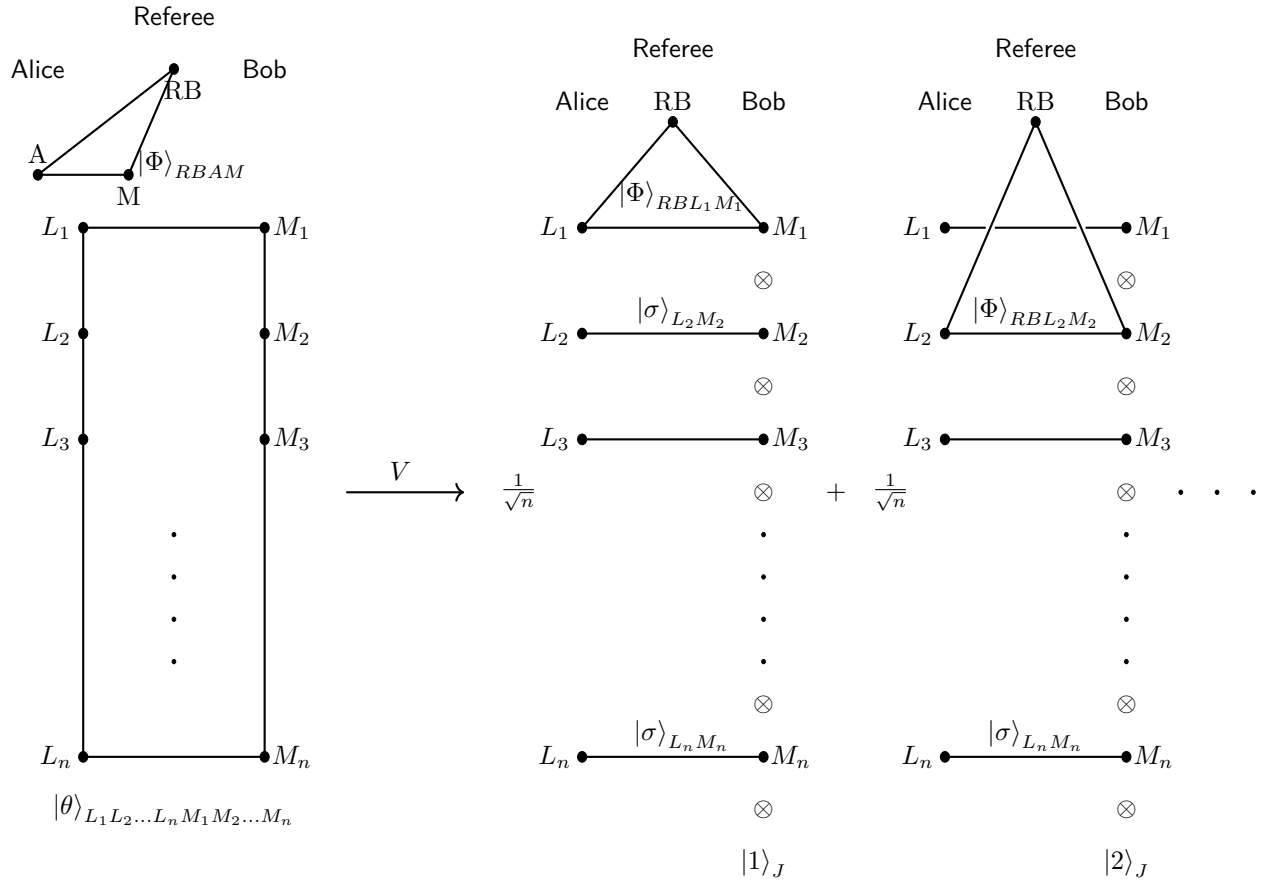

Figure 1: The state on left hand side $|\Phi\rangle_{RBAM} \otimes |\theta\rangle_{L_1L_2\ldots L_nM_1\ldots M_n}$, a purification of $\Phi_{RB} \otimes \tau_{M_1\ldots M_n}$. The state on right hand side is $|\mu\rangle_{JRBL_1L_2\ldots L_nM_1M_2\ldots M_n}$, a purification of $\tau_{RBM_1M_2\ldots M_n}$. 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.

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

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

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

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

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 $BM_1M_2\ldots M_n$.

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 1.5)

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 2.1) 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 $|\xi'\rangle_{RBJL_1\ldots L_nM_1\ldots M_n}$ be a purification of $\xi_{RBM_1\ldots M_n}$ (guaranteed by Uhlmann's theorem, Fact 1.5) such that,

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

Let $V' : \mathcal{H}_{AML_1\ldots L_n} \to \mathcal{H}_{JL_1\ldots L_n}$ be an isometry (guaranteed by Uhlmann's theorem, Fact 1.5) such that,

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

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

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

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

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 1.4), we have,

$$\mathrm{F}^2(\Phi_{RABM}, \Phi'_{RABM}) \geq \mathrm{F}^2(|\xi'\rangle\langle\xi'|_{RBJL_1\ldots L_nM_1\ldots M_n}, |\mu\rangle\langle\mu|_{RBJL_1\ldots L_nM_1\ldots M_n}) \geq 1 - \varepsilon^2. \tag{3}$$

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:

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

□

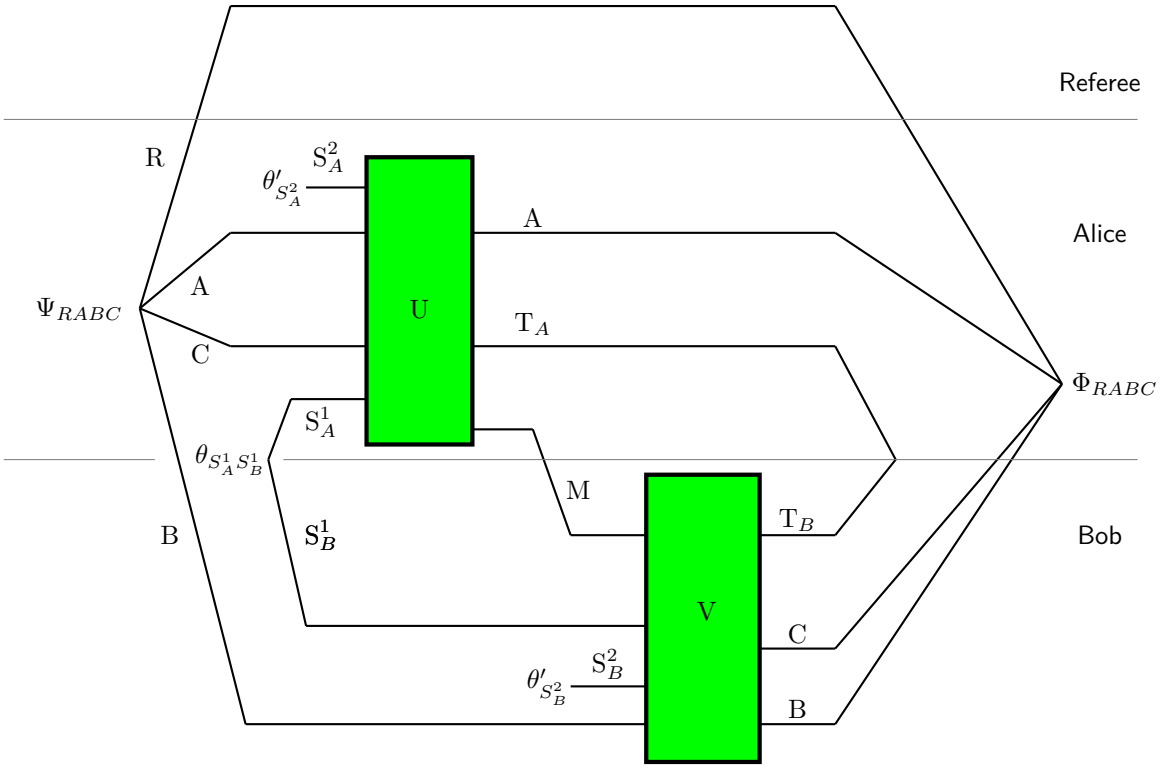

Figure 2: Graphical representation of one-way entanglement assisted quantum state redistribution.

4 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, DHO16] use EPR states and also take into account the amount of entanglement used by the protocol.

Definition 4.1 (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 $|\theta\rangle_{S_A^1 S_B^1}$, 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 1.3), 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 $S_A \stackrel{\text{def}}{=} S_A^1 S_A^2$ and $S_B \stackrel{\text{def}}{=} S_B^1 S_B^2$. Let the joint state in registers $S_A S_B$ be $|\theta\rangle_{S_A S_B}$. Then following is equivalent to Definition 4.1. 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.

Definition 4.2. 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

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

Lower bound

We have the following lower bound result.

Theorem 4.3 (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 2):

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 1.6, we know that there exists a state ω_M, such that:

$$2\log|M| \geq \mathrm{D}_{\max}(\kappa_{RBS_BM} \| \kappa_{RBS_B} \otimes \omega_M) = \mathrm{D}_{\max}(\kappa_{RBS_BM} \| \Psi_{RB} \otimes \theta_{S_B} \otimes \omega_M). \tag{4}$$

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 1.9 and monotonicity of fidelity under quantum operation (Fact 1.4) 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,

$$\Phi_{RBCT_B} = (I_R \otimes V_{BS_BM})\kappa_{RBS_BM}(I_R \otimes V^{\dagger}_{BS_BM}),\ \kappa_{RB} = \Psi_{RB}. \tag{5}$$

Recall that $S_BM \equiv CT_B$. Define $\sigma_{CT_B} \stackrel{\text{def}}{=} \theta_{S_B} \otimes \omega_M$. Eq. (4) and Eq. (5) imply,

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

with the conditions

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

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

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

□

Upper bound

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

Theorem 4.4 (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,

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

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

Define the state

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

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

$$|\kappa\rangle\langle\kappa|_{RBCTS} = V_1 \Psi_{RBAC} V_1^\dagger \tag{6}$$

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 3.1.

2. Using the protocol described in Theorem 3.1, 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,
$$\mathcal{P}(\kappa'_{RBCTS}, \kappa_{RBCTS}) \leq \varepsilon \tag{7}$$

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 $U_{BCT}\kappa'_{RBCT}U_{BCT}^\dagger$. By definition of ρ_{RBCT}, the relation $\mathcal{P}(\rho_{RBCT}, \Psi_{RBC} \otimes \sigma'_T) \leq \varepsilon$ and Equation 7, we find (using triangle inequality for purified distance (Fact 1.2)) that

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

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,

$$\mathcal{P}(\Psi_{RABC} \otimes |\sigma'\rangle\langle\sigma'|_{ET}, V_2 \otimes U_{BCT}\kappa'_{RBCTS}U_{BCT}^\dagger \otimes V_2^\dagger) \leq 2\varepsilon \tag{8}$$

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 8 and 6, 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:

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

□

5 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 4.4) and lower bound (Theorem 4.3) immediately gives the desired upper and lower bound on quantum communication cost of quantum state splitting.

Lemma 5.1. *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 4.2), we define the state

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

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 1.4). Consider,

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

Now,

$$\begin{aligned}
\mathrm{I}^{\varepsilon}_{\max}(R:C)_{\Psi_{RC}} &\geq \inf_{T,\sigma'_T} \mathrm{I}^{\varepsilon}_{\max}(R:CT)_{\Psi_{RC}\otimes\sigma'_T} \quad \text{(by setting } T \text{ to be trivial register)} \\
&= \inf_{T,\sigma'_T,\rho_{RCT}\in\mathcal{B}^{\varepsilon}(\Psi_{RC}\otimes\sigma'_T)} \mathrm{I}_{\max}(R:CT)_{\rho_{RCT}} \\
&\geq \inf_{\rho_{RC}\in\mathcal{B}^{\varepsilon}(\Psi_{RC})} \mathrm{I}_{\max}(R:C)_{\rho_{RC}} \\
&\quad \text{(using monotonicity of max-information under quantum operation, Fact 1.7)} \\
&= \mathrm{I}^{\varepsilon}_{\max}(R:C)_{\Psi_{RC}} .
\end{aligned}$$

Therefore,

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

□

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 5.2 ([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* 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 4.1), 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 1.5), 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. □

6 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 6.1. *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 $|\Psi\rangle_{RM} \stackrel{\text{def}}{=} \sum_i \sqrt{p_i}\,|i\rangle_R\,|\psi\rangle^i_M$. 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

$$\sum_i p_i\,\langle\psi|^i_M\,\mathcal{E}(\psi^i_M)\,|\psi\rangle^i_M = \sum_i p_i \sum_k |\mathrm{Tr}(\psi^i_M A_k)|^2,$$

which completes the proof. □

Now we proceed to our main theorem of this section.

Theorem 6.2. *Consider an ensemble of pure quantum states $\{p_i, |\psi\rangle\langle\psi|^i_M\}_i$, with $\psi^i_M \in \mathcal{D}(M)$. Introduce a register R and define the state $|\Psi\rangle_{RM} \stackrel{\text{def}}{=} \sum_i \sqrt{p_i}\,|i\rangle_R\,|\psi\rangle^i_M$. Let σ_M be an arbitrary state and $k \stackrel{\text{def}}{=} \mathrm{D}_{\max}(\Psi_{RM}\|\Psi_R \otimes \sigma_M)$. 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 $\phi^i_{M'}$ such that $\sum_i p_i \mathrm{F}^2(\psi^i_{M'}, \phi^i_{M'}) \geq 1 - \frac{2^k}{n}$.*

Proof. We define the state

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

Consider the following purification of $\tau^i_{RM_1M_2\ldots M_n}$,

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

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 2.1, 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 1.5), such that

$$\mathrm{F}^2(|\tau\rangle\langle\tau|_{JL_1L_2\ldots L_nRM_1M_2\ldots M_n}, V\,|\Psi\rangle\langle\Psi|_{RM}\otimes|\sigma\rangle\langle\sigma|_{L_1M_1}\otimes|\sigma\rangle\langle\sigma|_{L_2M_2}\ldots\otimes|\sigma\rangle\langle\sigma|_{L_nM_n}\,V^\dagger) \geq \frac{1}{1+\frac{2^k}{n}}. \quad (9)$$

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 9 and monotonicity of fidelity under quantum map (Fact 1.4), 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 6.1 to conclude that

$$\sum_i p_i \mathrm{F}^2(\phi^i_{M'}, \psi^i_{M'}) = \sum_i p_i \mathrm{F}^2(\mathcal{P}(\psi^i_M), \psi^i_M) \geq \mathrm{F}^2(\mathcal{P}(\Psi_{RM}), \Psi_{RM}) \geq 1 - \frac{2^k}{n}.$$

This proves the theorem.

□

Acknowledgement

We thank Ashwin Nayak, Nilanjana Datta, Joseph Fitzsimons, 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, Naqueeb Warsi and Jamie Sikora 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.

References

[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.

[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.

[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.

[DHO16] 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. *Journal of Mathematical Physics*, 57:052203, 2016.

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

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

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

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

[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.

[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.