Expected communication cost of distributed quantum tasks

Amurag Anshu*, Ankit Garg†, Aram W. Harrow‡, Penghui Yao*
* Centre for Quantum Technologies, National University of Singapore, Singapore, a0109169@u.nus.edu
† Microsoft Research New England, USA, garga@microsoft.com
‡ Center for Theoretical Physics, Massachusetts Institute of Technology, aram@mit.edu
§ Joint Center for Quantum Information and Computer Science, University of Maryland, USA, phyao1985@gmail.com

Abstract—A central question in classical information theory is that of source compression, which is the task where Alice receives a sample from a known probability distribution and needs to transmit it to the receiver Bob with small error. This problem has a one-shot solution due to Huffman, in which the messages are of variable length and the expected length of the messages matches the asymptotic and i.i.d. compression rate of the Shannon entropy of the source.

In this work, we consider a quantum extension of above task, where Alice receives a sample from a known probability distribution and needs to transmit a part of a pure quantum state (that is associated to the sample) to Bob. We allow entanglement assistance in the protocol, so that the communication is possible through classical messages, for example using quantum teleportation. The classical messages can have a variable length and the goal is to minimize their expected length. We provide a characterization of the expected communication cost of this task, by giving a lower bound that is near optimal up to some additive factors.

A special case of above task, and the quantum analogue of the source compression problem, is when Alice needs to transmit the whole of her pure quantum state. Here we show that there is no one-shot interactive scheme which matches the asymptotic and i.i.d. compression rate of the von Neumann entropy of the average quantum state. This is a relatively rare case in quantum information theory where the cost of a quantum task is significantly different from its classical analogue. Further, we also exhibit similar results for the fully quantum task of quantum state redistribution, employing some different techniques. We show implications for the one-shot version of the problem of quantum channel simulation.

A full version of this paper is accessible at: https://arxiv.org/abs/1605.04601

I. Introduction

Shannon, in his celebrated work [1], initiated the idea of source compression by showing that in the asymptotic and i.i.d. setting (where i.i.d. refers to independent and identically distributed), compression could be achieved up to the Shannon entropy of the message source. This result was extended to the quantum domain by Schumacher [2], who showed that a quantum source could be compressed to the von Neumann entropy of the source in the asymptotic and i.i.d. setting. Since then, a large family of quantum source compression tasks and their compression schemes have been discovered. The communication task considered by Schumacher in [2], which is fundamental to all the subsequent tasks, can be formulated as a problem of classical-quantum state transfer. We informally define it below in the one-shot setting (which drops the asymptotic and i.i.d. assumption) and point out that it is a classical-quantum task, where the communicating parties receive a classical input from an external source.

Classical-quantum state transfer: Alice (henceforth the sender) receives an input $x$ with probability $p(x)$ associated with a pure quantum state $|\Psi_x\rangle$, where $p(\cdot)$ is a distribution over a finite set $\mathcal{X}$ and $x \in \mathcal{X}$. The goal is that Bob (henceforth the receiver) outputs a quantum state $\Phi^x$ such that the distance between $\Phi^x$ and $|\Psi_x\rangle\langle\Psi_x|$ is smaller than $\eta$ for all $x \in (0,1)$. We refer to $\eta$ as the average error.

The distance between the quantum states is measured in terms of the purified distance [3]. As mentioned above, the worst case quantum communication cost for this task in the asymptotic and i.i.d. setting is characterized by $S(\sum_x p(x)\Psi_x)$ [2], where $S(\cdot)$ denotes the von Neumann entropy. An-
other example of a classical-quantum task concerns the distribution of a pure bipartite quantum state between Alice and Bob. This task can be viewed as a classical-quantum analogue of the task of quantum state splitting [4] and is an extension of the task of classical-quantum state transfer.

**Classical-quantum state splitting:** Alice receives an input \( x \) with probability \( p(x) \) associated with a bipartite pure quantum state \( |\Psi^x\rangle_{AC} \). The goal for Alice and Bob is to share a state \( \Phi^x_{AC} \) with Alice holding \( A' \) and Bob holding \( C \), such that the distance between \( \Phi^x_{AC} \) and \( |\Psi^x\rangle\langle\Psi^x|_{AC} \), averaged over \( x \), is smaller than \( \eta \in (0, 1) \). We refer to \( \eta \) as the *average error*.

For this task, the worst case quantum communication cost in the asymptotic and i.i.d. setting is characterized by the *Holevo information:* \( S(\sum_x p(x)|\Psi^x_C\rangle - \sum_x S(|\Psi^x_C\rangle) \) [5].

A natural setting for the above two classical-quantum tasks is quantum communication complexity. Here, the communicating parties Alice and Bob receive inputs \( x \in \mathcal{X} \) and \( y \in \mathcal{Y} \) and their goal is to compute a joint function \( f(x, y) \) with minimum quantum communication. They may or may not have pre-shared entanglement. The two tasks correspond to the instances of a quantum communication protocol where Alice sends her first quantum message to Bob conditioned on \( x \).

A limitation of the classical-quantum tasks is that they do not completely capture the information theoretic properties of the quantum systems. This is achieved by the fully quantum or coherent quantum tasks, where Alice and Bob are required to maintain quantum correlation with the environment (which we shall refer to as the Reference system). A well known example of such tasks is quantum state merging [6], which provided the first operational interpretation to the negativity of quantum conditional information. A generalization of this is the task of *quantum state redistribution*, which was first introduced in [7], [8] and applied to the setting of quantum communication complexity in [9].

**Quantum state redistribution:** Alice (A,C), Bob (B) and Reference (R) share a joint pure quantum state \( |\Psi\rangle_{RBCA} \). Alice needs to transfer the register \( C \) to Bob such that the final state between Alice \( (A) \), Bob \( (B,C) \) and Reference (R) is \( |\Psi\rangle_{RBCA} \). It is required that the distance between \( |\Psi\rangle_{RBCA} \) and \( |\Psi\rangle_{RBCA} \) is smaller than \( \varepsilon \in (0, 1) \). We refer to \( \varepsilon \) as the *error*.

The worst case communication cost of this task in the asymptotic and i.i.d. setting is characterized by the *conditional quantum mutual information* \( I(C : R|B)_{\Psi} \) [7], [8].

Coherent quantum tasks such as quantum state merging [10], [6] have also found applications to the problems related to quantum channel coding, through the notion of quantum channel simulation. This task is informally defined as follows.

**Entanglement-assisted quantum channel simulation:** Given a quantum channel \( \mathcal{E} \) with input register \( A \) and output register \( B \), the goal of Alice and Bob is to simulate the action of \( \mathcal{E} \). That is, if Alice is given an input quantum state \( \rho_A \), Bob must output a quantum state \( \sigma_B \) such that the distance between \( \sigma_B \) and \( \mathcal{E}(\rho_A) \) is smaller than \( \eta \in (0, 1) \). We refer to \( \eta \) as the *error*.

The Quantum Reverse Shannon Theorem [11], [12] states that using the pre-shared entanglement, Alice and Bob can simulate the action of \( n \) copies of \( \mathcal{E} \) using a number of bits equal to \( n \) times the entanglement-assisted classical capacity of \( \mathcal{E} \), as \( n \to \infty \).

**Two communication costs of a protocol and their relevance**

There are two measures of the communication cost of a classical or quantum protocol. The worst case communication cost measures the total number of bits or qubits exchanged between the players. The *expected communication cost* measures the expected number of bits that are exchanged between the players. For the case of classical protocols that involve public or private randomness, the expectation is over the distribution of the inputs and all the randomness involved in the protocol. It can also be similarly defined in the classical-quantum or the fully-quantum case, by using quantum teleportation [13] to convert quantum messages into classical messages and taking expectation over the measurement outcomes (details appear in the full version of this work).

The first demonstration of the usefulness of the notion of expected communication cost was shown by Huffman [14]. For the task of communicating a sample from a probability distribution \( p \), he proved that by encoding each message into a codeword of different length, one could construct a code with expected length at most \( H(p) + 1 \). Here, the Shannon entropy \( H(\cdot) \) is the worst case communication cost for this task in the asymptotic and i.i.d. setting [1]. This, remarkably, led to an operational
interpretation of the Shannon entropy of a source in the one-shot setting.

In the subsequent works [15], [16], a number of elegant one-shot communication protocols were discovered that achieved the near-optimal expected communication costs for their respective tasks. Not only are these results significant in information theory, they have been proved to be useful in classical communication complexity, where interactive protocols play a crucial role [17]. The compression of interactive protocols up to their overall information cost (which is also known as the information complexity [18]) is difficult, since the error in the compression of each round can accumulate over the rounds. If one needs to compress an r round protocol in a round by round fashion, the error in each round must be $O(1/r)$, which can lead to a large overhead in the worst case communication cost. The notion of expected communication cost serves as the right tool for overcoming this difficulty, as the dependence on error is much weaker and it composes well across several rounds. Indeed, using this notion, the aforementioned results [15], [16] have obtained important applications to direct sum problems in communication complexity.

The notion of the expected communication cost has largely been left unexplored in the one-shot quantum domain. Protocols for various one-shot classical-quantum tasks [19], [20], [21] and fully quantum tasks [22], [12], [23], [24] have been investigated in the past two decades. However, all of these results only consider the worst case quantum communication cost. An exception is the work by Braunstein et al. [25], which considered the classical-quantum state transfer task and noted several issues in generalizing directly the techniques of the classical Huffman coding scheme to the quantum setting. Still, recent progress in the field of quantum communication complexity, such as the direct sum result for bounded-round entanglement-assisted quantum communication complexity [9], has raised the question of compressing quantum protocols in terms of the expected communication cost.

II. OUR RESULTS

We refer to a collection of pairs $\{(p(x), \Psi^x)\}_x$ as an ensemble of states, where $x$ is drawn from a distribution $p(\cdot)$ over a domain $\mathcal{X}$. The results obtained in this manuscript are as follows, which hold in the model of entanglement-assisted quantum communication. Proofs of these results can be found in the full version of this work.

**Classical - quantum state splitting:** We give a near optimal characterization of the expected communication cost of the task of classical-quantum state splitting, for the protocols that achieve this task with a bounded number of rounds. For this, we define a quantity $Q(\eta, r)$ that is a function of the ensemble $\{(p(x), \Psi^x)\}_x$, the average error $\eta$ and a positive integer $r$. $Q(\eta, 1)$ is as follows and $Q(\eta, r)$ is defined similarly.

**Definition 1:** Let $\mathbb{N}_+$ be the set of all positive integers and $\mathcal{D}(\mathcal{H}_C)$ be the set of all quantum states on the register $C$.

$$Q(\eta, 1) \overset{\text{def}}{=} \inf_{\{\omega^x; \varepsilon^x_i; p^x_i\}_{i \in \mathbb{N}_+, x \in \mathcal{X}}} \sum_x p(x)p^x_i \log i$$

s.t.

$$\sum_x p(x) \sum_i p^x_i (\varepsilon^x_i)^2 \leq \eta^2;$$

$$\forall x \in \mathcal{X}, \sum_i p^x_i = 1;$$

$$\forall i \in \mathbb{N}_+, x \in \mathcal{X}, 0 \leq p^x_i \leq 2^{-D_{\max}^x(\Psi^x; \omega^x)};$$

$$\omega^x \in \mathcal{D}(\mathcal{H}_C), \quad \varepsilon^x_i \in (0, 1).$$

The important constraint above is the upper bound on the probabilities $p^x_i$. Furthermore, for the optimum solution, the support of the probability distribution $\{p^x_i\}_i$ is finite for all $x \in \mathcal{X}$. We prove the following result.

**Theorem 1:** For any r-round entanglement-assisted interactive protocol for the classical-quantum state splitting task of the ensemble $\{(p(x), \Psi^x)\}_x$ with average error $\eta$, the expected communication cost is lower bounded by $Q(\eta, r)$. Further, for every $\delta \in (0, 1)$, there exists an entanglement-assisted one-way protocol that achieves the classical-quantum state splitting task of the above ensemble with average error $\eta + 3\sqrt{\delta}$ and expected communication cost

$$Q(\eta, r) + 2r \log Q(\eta, r) + 4r + 2\log \frac{4}{\delta}.$$  

The additive factor of $O(r \log Q(\eta, r))$ arises due to the prefix-free encoding of the integers [26]. The achievable one-way protocol uses a variant of the convex split lemma [27] and the classical-quantum rejection sampling approach of [19], [20].

**Classical - quantum state transfer:** Specializing to the sub-case of classical-quantum state transfer and by providing a lower bound to the corresponding $Q(\eta, r)$, we show a large separation between the expected communication cost and the quantum information cost (which is the worst case
quantum communication cost in the asymptotic and i.i.d setting). This shows that there exists no coding scheme for quantum messages that performs as well as the Huffman coding scheme [14] in the classical case. Our main result is as follows.

**Theorem 2:** Fix some parameter \( \delta \in (0,1) \) and an integer \( d \). There exists an ensemble \( \{(p(x), |\Psi^x\rangle \langle \Psi^x|)\}_x \) such that the quantum states \(|\Psi^x\rangle \langle \Psi^x|\) belong to a \( d \)-dimensional Hilbert space and the index \( x \) takes values over a set \( \mathcal{X} \) of size \( 8d^7 \). The following properties of this ensemble hold.

1) The quantum information cost, or the von Neumann entropy of the average state \( \sum_x p(x) |\Psi^x\rangle \langle \Psi^x| \), is \( \delta \log d + O(1) \).

2) Any one-way protocol achieving the classical-quantum state transfer of this ensemble with average error \( \eta < \left( \frac{1}{2} \right)^{\frac{1}{2}} \) must communicate at least \( (1 - \delta) \log (d\delta) - O(1) \) bits.

3) Any \( r \)-round interactive protocol achieving the classical-quantum state transfer of this ensemble with average error \( \eta < \left( \frac{1}{2} \right)^{\frac{1}{2}} \) must communicate at least
\[
\Omega \left( \max \left\{ \frac{\log(d\delta)}{\log \log \log d}, \frac{\log(d\delta)}{\log \log \log d} \right\} \right) \text{ bits.}
\]

Thus, arbitrarily large separations between the quantum information cost and the expected communication cost can be obtained for small enough average error, by choosing a small enough \( \delta \). For instance, setting \( \delta = \frac{1}{\log^2 q} \) and allowing an average error of at most \( O\left( \frac{\log^2 q}{\log \log \log q} \right) \), the quantum information cost is a constant, whereas the expected communication cost is \( \Omega \left( \frac{\log(d\delta)}{\log \log \log d} \right) \). In contrast, the separation between the information cost and the expected communication cost for the Huffman coding scheme [14] (which incurs no error) is at most by an additive factor of 1.

Another property of our construction is that the number of bits of input given to Alice is \( \approx 7 \log d \). Thus, the lower bound on the expected communication cost is of the order of the input size. This may be contrasted with the well known exponential separations between information and communication [28], [29] and their recent quantum counterpart [30], where the lower bound on the communication cost is doubly exponentially smaller than the input size.

**Quantum state redistribution:** We show the following result for the fully-quantum task of quantum state redistribution.

**Theorem 3:** Fix a \( p \in (0,1) \) and an \( \varepsilon \in [0, \left( \frac{1}{2} \right)^{\frac{1}{2}}] \). There exists a pure quantum state \( \Psi_{RBCA} \) such that any interactive entanglement-assisted communication protocol for its quantum state redistribution with error \( \varepsilon \) requires expected communication cost at least \( I(R:C|B)_{\Psi} \cdot \left( \frac{1}{2} \right)^p \).

While the lower bounds on the classical-quantum tasks imply the same lower bounds on their fully-quantum counterparts (as it is harder to maintain coherence with a Reference system), Theorem 3 is proved using techniques different from those used in Theorem 2. Furthermore, Theorem 3 has no dependence on the number of rounds, in contrast with Theorem 2.

**Entanglement-assisted quantum channel simulation:** For the task of one-shot entanglement-assisted simulation of a quantum channel, we show that the expected communication cost of simulating the quantum channel can be much larger than the entanglement-assisted classical capacity. This is in contrast with the corresponding classical result, since it was shown in [15] that a classical channel can be simulated with an expected communication cost close to its channel capacity.

We note that a part of this work has appeared in [31], where the one-way part of Theorem 2 has been proved.

### III. Conclusion

We have given a nearly optimal characterization of the expected communication cost of the classical-quantum state splitting task. For its special case of classical-quantum state transfer and the task of quantum state redistribution, we have shown large separations between the expected communication cost and the quantum information cost (which is the worst case quantum communication cost in the asymptotic and i.i.d setting). As an application of our main results, we show that in the one-shot setting, quantum channels cannot be simulated with an expected communication cost as small as their entanglement-assisted classical capacity. We have following questions for the future research.

- Theorem 2 has a dependence on the number of rounds. We conjecture that our techniques are not optimal and interactions cannot reduce the expected communication costs.
- Is there an operational interpretation of the fundamental quantum information theoretic quantities in the one-shot settings? Our result says that expected communication cost is not the right notion, but naturally we cannot rule out other notions.
ACKNOWLEDGEMENT

A.A. is supported by the National Research Foundation, Prime Minister’s Office, Singapore and the Ministry of Education, Singapore under the Research Centres of Excellence programme. Most of this research was done when A.G. was a graduate student at Princeton University and his research was partially supported by NSF grants CCF-1149888 and CCF-1525342, a Simons fellowship for graduate students in theoretical computer science and a Siebel scholarship. AWH is funded by NSF grants CCF-1629809 and CCF-1452616. P.Y. is supported by the Department of Defense. Part of this work was done when P.Y. was a postdoctoral fellow at IQC supported by NSERC and CIFAR.

REFERENCES

[1] C. E. Shannon, “A mathematical theory of communication,” The Bell System Technical Journal, vol. 27, no. 3, pp. 379–423, July 1948.
[2] B. Schumacher, “Quantum coding,” Phys. Rev. A., vol. 51, pp. 2738–2747, 1995.
[3] A. Gilchrist, N. K. Langford, and M. A. Nielsen, “Distance measures to compare real and ideal quantum processes,” Phys. Rev. A, vol. 71, p. 062310, Jun 2005.
[4] A. Abeysinghe, I. Devetak, P. Hayden, and A. Winter, “The mother of all protocols: Restructuring quantum information’s family tree,” Proceedings of the Royal Society of London, vol. A, pp. 2537–2563, 2009.
[5] A. S. Holevo, “Bounds for the quantity of information transmitted by a quantum communication channel,” Problems of Information Transmission, vol. 9, pp. 177–183, 1973.
[6] M. Horodecki, J. Oppenheim, and A. Winter, “Quantum state merging and negative information,” Communications in Mathematical Physics, vol. 269, pp. 107–136, 2007.
[7] I. Devetak and J. Yard, “Exact cost of redistributing multipartite quantum states,” Phys. Rev. Lett., vol. 100, 2008.
[8] J. T. Yard and I. Devetak, “Optimal quantum source coding with quantum side information at the encoder and decoder,” IEEE Transactions on Information Theory, vol. 55, no. 11, pp. 5339–5351, Nov 2009.
[9] D. Touchette, “Quantum information complexity,” in Proceedings of STOC ’15. New York, NY, USA: ACM, 2015, pp. 317–326.
[10] M. Horodecki, J. Oppenheim, and A. Winter, “Partial quantum information,” Nature, vol. 456, pp. 673 EP–, Aug 2005.
[11] C. H. Bennett, I. Devetak, A. W. Harrow, P. W. Shor, and A. Winter, “The quantum reverse shannon theorem and resource tradeoffs for simulating quantum channels,” IEEE Transactions on Information Theory, vol. 60, no. 5, pp. 2926–2959, May 2014.
[12] M. Berta, M. Christandl, and R. Renner, “The quantum reverse shannon theorem based on one-shot information theory,” Communications in Mathematical Physics, vol. 306, no. 3, p. 579, Aug 2011.
[13] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels,” Phys. Rev. Lett., vol. 70, pp. 1895–1899, Mar 1993.
[14] D. Huffman, “A method for the construction of minimum-redundancy codes,” Proceedings of IRE, vol. 40, no. 9, pp. 1098–1101, 1952.
[15] P. Harsha, R. Jain, D. McAllester, and J. Radhakrishnan, “The communication complexity of correlation,” IEEE Transactions on Information Theory, vol. 56, no. 1, pp. 438–449, Jan 2010.
[16] M. Braverman and A. Rao, “Information equals amortized communication,” in Proceedings of FOCS ’11. Washington, DC, USA: IEEE Computer Society, 2011, pp. 748–757.
[17] S. J. Ponzio, J. Radhakrishnan, and S. Venkatesh, “The communication complexity of pointer chasing,” Journal of Computer and System Sciences, vol. 62, no. 2, pp. 323–355, 2001.
[18] M. Braverman, “Interactive information complexity,” in Proceedings of STOC ’12. New York, NY, USA: ACM, 2012, pp. 505–524.
[19] R. Jain, J. Radhakrishnan, and P. Sen, “Prior entanglement, message compression and privacy in quantum communication,” in Proceedings of CCC. Washington, DC, USA: IEEE Computer Society, 2005, pp. 285–296.
[20] ——, “Optimal direct sum and privacy trade-off results for quantum and classical communication complexity,” 2008, http://arxiv.org/abs/0807.1267.
[21] A. Anshu, R. Jain, P. Muhkhopadhyay, A. Shayegehi, and P. Yao, “New one shot quantum protocols with application to communication complexity,” IEEE Transactions on Information Theory, vol. 62, no. 12, pp. 7566–7577, Dec 2016.
[22] M. Berta, “Single-shot quantum state merging,” 2009, master’s thesis, ETH Zurich.
[23] M. Berta, M. Christandl, and D. Touchette, “Smooth entropy bounds on one-shot quantum state redistribution,” IEEE Transactions on Information Theory, vol. 62, no. 3, pp. 1425–1439, 2016.
[24] A. Anshu, R. Jain, and N. A. Warsi, “A one-shot achievability result for quantum state redistribution,” IEEE Transactions on Information Theory, vol. PP, no. 99, pp. 1–1, 2017.
[25] S. L. Braunstein, C. A. Fuchs, D. Gottesman, and H.-K. Lo, “A quantum analog of huffman coding,” IEEE Transactions on Information Theory, vol. 46, no. 4, pp. 1644–1649, Jul 2000.
[26] P. Elias, “Universal codeword sets and representations of the integers,” IEEE Transactions on Information Theory, vol. 21, no. 2, pp. 194–203, March 1975.
[27] A. Anshu, V. K. Devabathini, and R. Jain, “Quantum communication using coherent rejection sampling,” Phys. Rev. Lett., vol. 110, p. 120506, Sep 2017.
[28] A. Ganor, G. Kol, and R. Raz, “Exponential separation of information and communication,” in Proceedings of FOCS ’14. Washington, DC, USA: IEEE Computer Society, Oct 2014, pp. 176–185.
[29] ——, “Exponential separation of information and communication for boolean functions,” in Proceedings of STOC ’15. New York, NY, USA: ACM, 2015, pp. 557–566.
[30] A. Anshu, D. Touchette, P. Yao, and N. Yu, “Exponential separation of quantum communication and classical information,” in Proceedings of STOC 2017. New York, NY, USA: ACM, 2017, pp. 277–288.
[31] A. Anshu, A. Garg, A. W. Harrow, and P. Yao, “Lower Bound on Expected Communication Cost of Quantum Huffman Coding,” in 11th Conference on TQC 2016, ser. Leibniz International Proceedings in Informatics (LIPIcs), A. Broadbent, Ed., vol. 61. Dagstuhl, Germany: Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik, 2016, pp. 3:1–3:18.