A new operational interpretation of relative entropy and trace distance between quantum states

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

Rahul Jain
Centre for Quantum Technologies and Department of Computer Science, National University of Singapore
rahul@comp.nus.edu.sg

Priyanka Mukhopadhyay
Centre for Quantum Technologies, National University of Singapore
a0109168@nus.edu.sg

Ala Shayeghi
Institute for Quantum Computing, Unversity of Waterloo
ashayeghi@uwaterloo.ca

Penghui Yao
Centre for Quantum Technologies, National University of Singapore
phyao1985@gmail.com

September 12, 2014

Technical version at: http://arxiv.org/abs/1404.1366

Our Results

Relative entropy is a widely used quantity of central importance in both classical and quantum information theory. In this paper we present a new operational meaning to quantum relative entropy in the form of the following protocol.

$\mathcal{P}$: Alice gets to know the eigen-decomposition of a quantum state ρ. Bob gets to know the eigen-decomposition of a quantum state σ. Both Alice and Bob know $\mathrm{S}(\rho\|\sigma) \stackrel{\text{def}}{=} \mathrm{Tr}\rho\log\rho - \rho\log\sigma$, the relative entropy between ρ and σ and an error parameter ε. Alice and Bob use shared entanglement and after communication of $\mathcal{O}((\mathrm{S}(\rho\|\sigma)+1)/\varepsilon^4)$ bits from Alice to Bob, with probability at least $1-4\varepsilon$, Bob ends up with a quantum state $\tilde{\rho}$ such that $\mathrm{F}(\rho,\tilde{\rho}) \geq 1-\varepsilon$, where $\mathrm{F}(\cdot)$ represents *fidelity*.

This result can be considered as a non-commutative generalization of a result due to Braverman and Rao [BR11] where they considered the special case when ρ and σ are classical probability distributions.

We also present a variant of protocol $\mathcal{P}$, with Bob possessing some side information about Alice's input. In such a case, the communication can be further reduced.

$\mathcal{P}'$: Alice and Bob know the description of a quantum channel $\mathcal{E} : A \to A'$. Alice is given the spectral decomposition of a state $\rho \in A$. Bob is given the spectral decompositions of a state $\sigma \in A$ and the state $\rho' = \mathcal{E}(\rho)$. Let $\mathrm{S}(\rho\|\sigma) - \mathrm{S}(\mathcal{E}(\rho)\|\mathcal{E}(\sigma))$ and $\varepsilon > 0$ be known to Alice and Bob. There exists a protocol, in which Alice and Bob use shared entanglement and Alice sends $\mathcal{O}((\mathrm{S}(\rho\|\sigma) - \mathrm{S}(\mathcal{E}(\rho)\|\mathcal{E}(\sigma)) + 1)/\varepsilon^4)$ bits of communication to Bob, such that with probability at least $1-4\varepsilon$, the state $\tilde{\rho}$ that Bob gets at the end of the protocol satisfies $\mathrm{F}(\rho,\tilde{\rho}) \geq 1-\varepsilon$.

Our second result provides a new operational meaning to *trace distance* between quantum states in the form of the following protocol.

$\mathcal{P}_1$: Alice gets to know the eigen-decomposition of a quantum state ρ. Bob gets to know the eigen-decomposition of a quantum state σ. Alice and Bob use shared entanglement, do local measurements (no communication) and at the end Alice outputs registers AA_1 and Bob outputs registers BB_1 such that the following holds:

1. The marginal state in A is ρ and the marginal state in B is σ.
2. For any projective measurement $M = \{M_1, \ldots, M_w\}$ in the support of the state in AA_1, the following holds. Let Alice perform M on AA_1 and Bob perform M on BB_1 and obtain outcome $I \in [w], J \in [w]$ respectively. Then,

$$\Pr[I = J] \geq \left(1 - \sqrt{\|\rho-\sigma\|_1 - \frac{1}{4}\|\rho-\sigma\|_1^2}\right)^3 .$$

The protocol above can be viewed as a quantum analogue of the *classical correlated-sampling protocol*, which is widely used for example by Holenstein [Hol07] in his proof of a *parallel-repetition theorem* for two-player one-round games. Recently Dinur, Steurer and Vidick [DSV14] have shown another version of a quantum correlated sampling protocol different from ours, and used it in their proof of a parallel-repetition theorem for two-prover one-round entangled projection games.

Our techniques

Approach for Protocol $\mathcal{P}$

Our protocol $\mathcal{P}$ is inspired by the protocol of Braverman and Rao [BR11], which as we mentioned, applies to the special case when inputs to Alice and Bob are classical probability distributions P, Q respectively.

In our protocol, Alice and Bob share infinite copies of the following quantum state

$$|\psi\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{NK}} \sum_{i=1}^{N} |i\rangle^A |i\rangle^B \otimes \left(\sum_{m=1}^{K} |m\rangle^{A_1} |m\rangle^{B_1} \right),$$

where registers A, B serve to sample a maximally mixed state in the support of ρ, σ and the registers A_1, B_1 serve to sample uniformly in the interval $[0, 1]$ (in the limit $K \to \infty$). Let us assume the simpler case first when Alice and Bob know $c = \mathrm{S}_\infty(\rho\|\sigma) \stackrel{\text{def}}{=} \min\{\lambda|\ \rho \leq 2^\lambda \sigma\}$ (here $\leq$ represent the Löwner order), the *relative min-entropy* between ρ and σ. Let $\rho = \sum_i a_i |a_i\rangle \langle a_i|$ and $\sigma = \sum_i b_i |b_i\rangle \langle b_i|$. Alice performs the following projection on registers AA_1 on each copy of $|\psi\rangle$ and accepts the index of a copy iff the projection succeeds.

$$P_A = \sum_i |a_i\rangle \langle a_i| \otimes \left(\sum_{m=1}^{Ka_i} |m\rangle \langle m| \right).$$

Similarly Bob performs the following projection (for appropriately chosen δ) on registers BB_1 on each copy of $|\psi\rangle$ and accepts the index of a copy iff the projection succeeds.

$$P_B = \sum_i |b_i\rangle \langle b_i| \otimes \left(\sum_{m=1}^{K \cdot \min\{2^c b_i/\delta, 1\}} |m\rangle \langle m| \right).$$

It is easily argued that (in the limit $K \to \infty$), the marginal state in B (and also in A) in the first copy of $|\psi\rangle$, with index i, in which Alice succeeds is ρ. Using crucially the fact that $\rho \leq 2^c \sigma$, we argue that after Alice's measurement succeeds in a copy, Bob's measurement also succeeds with high probability and hence (by the *gentle measurement lemma*) does not disturb the state much in the register B, conditioned on success. We also argue that Alice can communicate the index of this copy to Bob with communication of $\mathcal{O}(c)$ bits (for constant ε).

As can be seen, our protocol is a natural quantum analogue of the protocol of Braverman and Rao [BR11]. However, since ρ and σ may not commute, our analysis deviates significantly from the analysis of [BR11]. We are required to show several new facts related to the non-commuting case while arguing that the protocol still works fine.

We then consider the case in which $\mathrm{S}(\rho\|\sigma)$ (instead of $\mathrm{S}_\infty(\rho\|\sigma)$) is known to Alice and Bob. The *quantum substate theorem* [JRS09, JRS02, JN12] implies that there exists a quantum state ρ', having high fidelity with ρ such that $\mathrm{S}_\infty(\rho'\|\sigma) = \mathcal{O}(\mathrm{S}(\rho\|\sigma))$. We argue that our protocol is robust with respect to small perturbations in Alice's input and hence works well for the pair (ρ, σ) as well, and uses communication $\mathcal{O}(\mathrm{S}(\rho\|\sigma))$ bits. Again this requires us to show new facts related to the non-commuting case.

Approach for Protocol $\mathcal{P}_1$

For the Protocol $\mathcal{P}_1$, Alice and Bob use similar approach as followed in $\mathcal{P}$. They share infinite copies of the following quantum state

$$|\psi\rangle \stackrel{\text{def}}{=} \frac{1}{\sqrt{NK}} \sum_{i=1}^{N} |i\rangle^A |i\rangle^B \otimes \left(\sum_{m=1}^{K} |m\rangle^{A_1} |m\rangle^{B_1} \right),$$

.

Let $\rho = \sum_i a_i |a_i\rangle \langle a_i|$ and $\sigma = \sum_i b_i |b_i\rangle$. Alice performs the following projection on registers AA_1 on each copy of $|\psi\rangle$ and outputs the first copy where the projection succeeds.

$$P_A = \sum_i |a_i\rangle \langle a_i| \otimes \left(\sum_{m=1}^{Ka_i} |m\rangle \langle m| \right).$$

Similarly Bob performs the following projection (for appropriately chosen δ) on registers BB_1 on each copy of $|\psi\rangle$ and outputs the first copy where the projection succeeds.

$$P_B = \sum_i |b_i\rangle \langle b_i| \otimes \left(\sum_{m=1}^{Kb_i} |m\rangle \langle m| \right).$$

We show that the resulting state that Alice and Bob output together is well correlated between them. To give an intuitive picture, when ρ and σ are equal, then Alice and Bob succeed on same index and their output state is maximally entangled within the relevant subspace.

Implications

The protocol of Braverman and Rao [BR11], and slightly modified versions of it, were widely used to show several *direct sum* and *direct product* results in communication complexity, for example a direct sum theorem for all relations in the bounded-round public-coin communication model [BR11], direct product theorems for all relations in the public-coin one-way and public-coin bounded-round communication models [Jai13, JPY12, BRWY13].

Protocol $\mathcal{P}$ allows for compressing the communication in one-way entanglement-assisted quantum communication protocols to the *internal information* about the inputs carried by the message. Using this we obtain a direct-sum result for *entanglement assisted quantum one-way communication complexity* for all relations. This direct-sum result was shown previously by Jain, Radhakrishnan and Sen [JRS05, JRS08] and they obtained this result via a protocol that allowed them compression to *external information* carried in the message[1]. Their arguments were quite specific to one-way protocols and did not seem to generalize to multi-round communication protocols. Our proof however, is along the lines of a proof which has been generalized to bounded-round classical protocols [BR11] and hence it presents hope that our direct-sum result can also be generalized to bounded-round quantum protocols. The protocol of Braverman and Rao [BR11] was also used by Jain [Jai13] to obtain a direct-product for all relations in the model of one-way public-coin classical communication and later extended to multiple round public-coin classical communication [JPY12, BRWY13]. Hence protocol $\mathcal{P}$ also presents a hope of obtaining similar results for quantum communication protocols.

As mentioned before the classical correlated-sampling protocol has been widely used for example by Holenstein [Hol07] in his proof of a parallel-repetition theorem for two-player one-round games. It is possible that the protocol $\mathcal{P}_1$, which is the corresponding quantum analogue, finds similar uses, for example in showing a parallel repetition result for entangled two-player one-round games, which remains an important open question.

[1] Compression to external and internal information can be thought of as one-shot communication analogues of the celebrated results by Shannon [Sha48] and Slepian-Wolf [SW73] exhibiting compression of source to entropy and conditional entropy respectively.

References

[BR11] Mark Braverman and Anup Rao. Information equals amortized communication. In *Proceedings of the 52nd Symposium on Foundations of Computer Science*, FOCS '11, pages 748–757, Washington, DC, USA, 2011. IEEE Computer Society.

[BRWY13] Mark Braverman, Anup Rao, Omri Weinstein, and Amir Yehudayoff. Direct product via round-preserving compression. In *Proceedings of the 40th international conference on Automata, languages and programming*, ICALP'13, Berlin, Heidelberg, 2013. Springer-Verlag.

[DSV14] Irit Dinur, David Steurer, and Thomas Vidick. A parallel repetition theorem for entangled projection games. In *Proceedings of the 29th IEEE Annual Conference on Computational Complexity*, CCC '14, to appear, Washington, DC, USA, 2014. IEEE Computer Society.

[Hol07] Thomas Holenstein. Parallel repetition: simplifications and the no-signaling case. In *Proceedings of the thirty-ninth annual ACM Symposium on Theory of Computing*, STOC '07, pages 411–419, New York, NY, USA, 2007.

[Jai13] Rahul Jain. New strong direct product results in communication complexity. *Journal of the ACM*, to appear, 2013.

[JN12] Rahul Jain and Ashwin Nayak. Short proofs of the quantum substate theorem. *IEEE Transactions on Information Theory*, 58(6):3664–3669, 2012.

[JPY12] Rahul Jain, Attila Pereszlényi, and Penghui Yao. A direct product theorem for the two-party bounded-round public-coin communication complexity. In *Proceedings of the 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science*, FOCS '12, pages 167–176, Washington, DC, USA, 2012.

[JRS02] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. Privacy and interaction in quantum communication complexity and a theorem about the relative entropy of quantum states. In *Proceedings of the 43rd Symposium on Foundations of Computer Science*, FOCS '02, pages 429–438, Washington, DC, USA, 2002. IEEE Computer Society.

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

[JRS08] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. Optimal direct sum and privacy trade-off results for quantum and classical communication complexity. *CoRR*, abs/0807.1267, 2008.

[JRS09] Rahul Jain, Jaikumar Radhakrishnan, and Pranab Sen. A new information-theoretic property about quantum states with an application to privacy in quantum communication. *Journal of the ACM*, 56(6), September 2009. Article no. 33.

[Sha48] C. E. Shannon. A mathematical theory of communication. *Bell System Technical Journal*, 27(3):379–423, 1948.

[SW73] David Slepian and Jack K. Wolf. Noiseless coding of correlated information sources. *IEEE Transactions on Information Theory*, 19(4):471–480, 1973.