Quantum Conditional Mutual Information, Reconstructed States, and State Redistribution

Fernando G. S. L. Brandão,1 Aram W. Harrow,2 Jonathan Oppenheim,3 and Sergii Strelchuk4
1Department of Computer Science, University College London, Gower St, London WC1E 6BT, UK
2 and Quantum Architectures and Computation Group, Microsoft Research, Redmond, Washington 98052-6399, USA
3Center for Theoretical Physics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
4Department of Physics, University College London, Gower St, London WC1E 6BT, UK

Quantum information theory is the successful framework describing the transmission and storage of information. It not only generalized all of the classical information-theoretic results, but also developed a wealth of tools to analyze a number of scenarios beyond the reach of the latter, such as entanglement processing. One of the central quantities of the classical information theory is the conditional mutual information (CMI). For a tripartite state \( \rho_{BCR} \) it is defined as

\[
I(C:R|B)_p := S(BC)_{\rho} + S(BR)_{\rho} - S(BCR)_{\rho} - S(B)_{\rho},
\]

with \( S(X)_p = -\text{tr}(p_X \log p_X) \) as the von Neumann entropy. It measures the correlations of subsystems \( C \) and \( R \) relative to subsystem \( B \). The fact the classical CMI is non-negative is a simple consequence of the properties of the probability distributions; the same fact for the quantum CMI is equivalent to a deep result of quantum information theory—strong subadditivity of the von Neumann entropy [1]. Naturally, this lead to a variety of applications in different areas, ranging from quantum information theory [2–4] to condensed matter physics [5–7].

In the classical case, for every tripartite probability distribution \( p_{XYZ} \),

\[
I(X:Z|Y) = \min_{q \in \text{MC}} S(p\|q),
\]

for a probability distribution \( \{p_k\} \) and states \( \rho_{CB|I_k} \subset C \otimes B_{L,k} \) and \( \rho_{B|R_k} \in B_{R,k} \otimes R \). States of this form are called quantum Markov because in analogy to Markov chains, conditioned on the outcome of the measurement onto \( \{B_{L,k} \otimes B_{R,k}\} \), the resulting state on \( C \) and \( R \) is product.

Paralleling the classical case, \( \rho_{BCR} \) is a quantum Markov state if, and only if, there exists a reconstruction channel \( \Lambda : B \to BC \) such that \( \Lambda \otimes \text{id}_R(\rho_{BR}) = \rho_{BCR} \) [9]. Having generalized the definition of CMI, can we also retain the above equivalence, with the set of quantum Markov states taking the role of Markov chains? Surprisingly, it turns out that this is not the case, [10] and it seems not to be possible to connect states that are close to Markov states with states of small CMI in a meaningful way (see, however, [2,11]). Nonetheless, it might be possible to relate states with small CMI with those that can be approximately reconstructed from their bipartite reductions, i.e., such that \( \Lambda \otimes \text{id}_R(\rho_{BR}) \approx \rho_{BCR} \). Indeed, several conjectures appeared recently to this respect [5,12–14].
A recent breakthrough result from Fawzi and Renner gives the first such connection. They proved the following inequality [15]:\[
I(C: R | B)_\rho \geq \min_{\Lambda: B \rightarrow BC} S_{1/2}(\rho^\Lambda(B|C) || \Lambda \otimes \id_C(\rho^B|C)) \tag{4}
\]
with \(S_{1/2}(\rho||\sigma) = -\log F(\rho,\sigma)\) the order-1/2 Rényi relative entropy, where \(F(\rho,\sigma) = \text{tr}[\sigma^{1/2} \rho \sigma^{1/2}]\) is the fidelity [16]. It implies that if the CMI of \(\rho^B_{BCR}\) is small, there exists a reconstructing channel \(\Lambda: B \rightarrow BC\) such that \(\Lambda \otimes \id_C(\rho^B|C)\) has high fidelity with \(\rho^B_{BCR}\).

In this Letter, we prove a strengthened version of the Fawzi-Renner inequality. We also give a simpler proof of the inequality based on the task of state redistribution [4], which gives an operational interpretation to the CMI.

Result.—Let \(S(\rho||\sigma) := \text{tr}[\rho[\log \rho - \log \sigma]]\) be the quantum relative entropy of \(\rho\) and \(\sigma\). Define the measured relative entropy as\[
\mathcal{M}S(\rho||\sigma) = \max_{M \in \mathcal{M}} S(M(\rho)||M(\sigma)),
\]
where \(\mathcal{M}\) is the set of all quantum-classical channels \(M(\rho) = \sum_k \text{tr}(M_k \rho) |k\rangle \langle k|\), with \(\{M_k\}\) a positive operator-valued measure and \(\{\psi_k\}\) an orthonormal basis. The main result of this Letter is the following:

**Theorem 1:** For every state \(\rho^B_{BCR}\),\[
I(C: R | B)_\rho,
\]
Eq. (2) to quantum states, implying that it is optimal at least for classical states.\[
\min_{\Lambda: B \rightarrow BC} S_{1/2}(\rho^\Lambda(B|C) || \Lambda \otimes \id_C(\rho^B|C)) \geq \min_{\Lambda: B \rightarrow BC} S_{1/2}(\rho^\Lambda(B|C) || \Lambda \otimes \id_C(\rho^B|C)) \geq S_{1/2}(\rho^\Lambda(B|C) || \Lambda \otimes \id_C(\rho^B|C)) \tag{6c}
\]
equals to \(I(C: R) \approx \epsilon \log(d-1)\). The corresponding Fawzi-Renner bound (6d) becomes \(-\log F(\rho^B_{CR}, \rho^C \otimes \rho^R) \leq -\log(1-\epsilon) \approx \epsilon\). Thus, the lower bound (6c) is optimal for classical states.

Another application of our result is the well-known problem of classification of the short-range entangled states studied by Kitaev [19]. Defining such a class of states is nontrivial, and one of the natural properties to be required is the ability generate them locally: There must exist a \(O(1)\) quantum circuit that generates the designated state from a product state. In particular, one sees that states with low CMI can be generated from the product states according to the Fawzi-Renner bound. Our result improves the lower bound when we quantify the distance between the states using measured relative entropy.

Li and Winter conjectured in [11] that Eq. (6c) could be strengthened to have the relative entropy in the right-hand side (instead of the measured relative entropy). We leave this as an open question, but we note that Eq. (6b) shows that an asymptotic version of the conjectured inequality does hold true.

**Proof of Theorem 1:** The main tool in the proof will be the state redistribution protocol of Devetak and Yard [4,20,21], which gives an operational meaning for the CMI as twice the optimal quantum communication cost of the protocol. Consider the state \(|\psi\rangle_{ABCR}\) shared by two parties (Alice and Bob) and the environment (or reference system). Alice has \(A^nC^n\) (where we denote \(n\) copies of \(A\) by \(A^n\) and likewise for \(C, B\) and \(R\)). Bob has \(B^n\), and \(R^n\) is the reference system. In state redistribution, Alice wants to redistribute the \(C^n\) subsystem to Bob using preshared entanglement and quantum communication.

It was shown in [4,21] that using preshared entanglement Alice can send the \(C^n\) part of her state to Bob, transmitting approximately \((n/2)I(C: R | B)\) qubits in the limit of a large number of copies \(n\). More precisely:

**Lemma 2 (State redistribution protocol [4,21]):** For every state \(|\psi\rangle_{ABCR}\) there exist completely positive trace-preserving encoding maps \(E_n: A^nC^nX_n \rightarrow A^nG_n\) and decoding maps \(D_n: B^nG_nY_n \rightarrow B^nC^n\) such that\[
\lim_{n \to \infty} \|D_n \circ E_n(|\psi\rangle_{ABCR} \otimes \Phi_{X,Y}) - |\psi\rangle_{ABCR} \|_1 = 0 \tag{7}
\]
and\[
\lim_{n \to \infty} \frac{\log \text{dim}(G_n)}{n} = \frac{1}{2} I(C: R | B)_\rho \tag{8}
\]
where \(\rho^B_{BCR} := \text{tr}_A(|\psi\rangle_{ABCR} \otimes \Phi_{X,Y})\) and \(\Phi_{X,Y}\) is a maximally entangled state shared by Alice (who has \(X_n\)) and Bob (who has \(Y_n\)), and \(\| \cdot \|_1\) denotes the trace norm.

We split the proof of Theorem 1 into the proof of Proposition 3 and Eq. (17), below.

Proposition 3 follows from the state redistribution protocol outlined above. The main idea is the following:
Suppose that in the state redistribution protocol Bob does not receive any quantum communication from Alice, but instead he “mocks” the communication (locally preparing the maximally mixed state in $G_n$) and applies the decoding map $D_n$. It will follow that even though the output state might be very far from the target one, the relative entropy per copy of the output state and the original one cannot be larger than twice the amount of communication of the protocol (which is given by the conditional mutual information).

**Proposition 3:** For every state $\rho_{BCR}$,

$$I(C: R|B)_\rho \geq \lim_{n \to \infty} \min_{\Lambda: B^m \to B^m C^n} \frac{1}{n} \left( S[\rho_{BCR}^{\otimes n} \| (D_n \otimes \text{id}_{R^e})(\phi_{G_n Y_n B_n R^e})] \right).$$

(9)

**Proof.** Let $|\psi\rangle_{ABCR}$ be a purification of $\rho_{BCR}$. Consider the state redistribution protocol for sending from Alice (who has $AC$) to Bob (who has $B$). Let $\phi_{G_n Y_n A^m B^m R^e} := E_n \otimes \text{id}_{B^m R^e} |\psi\rangle_{ABCR} \otimes \Phi_{X_n Y_n}$ be the state after the encoding operation.

Using the operator inequality $\pi_{MN} \leq \text{dim}(M) I_M \otimes \pi_N$, valid for every state $\pi_{MN}$, we find

$$\phi_{G_n Y_n B^m R^e} \leq \text{dim}(G_n)^2 \tau_{G_n} \otimes \tau_{Y_n} \otimes \rho_{BR}^{\otimes n}$$

(10)

with $\tau_{Y_n}$, $\tau_{G_n}$ as the maximally mixed state on $Y_n$ and $G_n$, respectively. We used $\phi_{Y_n B^m R^e} = \tau_{Y_n} \otimes \rho_{BR}^{\otimes n}$, which holds true since $E_n$ only acts nontrivially on $A^n C^n X_n$.

Let $D_{\rho} := G_n Y_n B^m \to B^m C^n$ be the decoding operation of Bob in state redistribution (see Lemma 2) and define $\bar{D} := \left( 1 - 2^{-n} \right) D_n + 2^{-n} \Lambda_{\text{dep}}$, with $\Lambda_{\text{dep}}$ the depolarizing channel mapping all states to the maximally mixed. Since $\bar{D}_n$ is completely positive, using Eq. (10) we get

$$\left( \bar{D}_n \otimes \text{id}_{R^e} \right) \left( \tau_{G_n} \otimes \tau_{Y_n} \otimes \rho_{BR}^{\otimes n} \right) \geq \text{dim}(G_n)^{-2} \left( \bar{D}_n \otimes \text{id}_{R^e} \right) \left( \phi_{G_n Y_n B^m R^e} \right).$$

(11)

From the operator monotonicity of the log (see Lemma 1 in the Supplemental Material [22]),

$$S[\rho_{BCR}^{\otimes n} \| (D_n \otimes \text{id}_{R^e})(\phi_{G_n Y_n B^m R^e})] \leq S[\rho_{BCR}^{\otimes n} \| (D_n \otimes \text{id}_{R^e})(\phi_{G_n Y_n B^m R^e})] + 2 \log(\text{dim}(G_n)).$$

(12)

Equation (7) gives

$$\lim_{n \to \infty} \left\| \rho_{BCR}^{\otimes n} - \left( \bar{D}_n \otimes \text{id}_{R^e} \right) \left( \phi_{G_n Y_n B^m R^e} \right) \right\|_1 = 0.$$  

(13)

Because $\left( \bar{D}_n \otimes \text{id}_{R^e} \right) \left( \phi_{G_n Y_n B^m R^e} \right) = \left( 1 - 2^{-n} \right) \left( D_n \otimes \text{id}_{R^e} \right) \left( \phi_{G_n Y_n B^m R^e} \right) + 2^{-n} \rho_{BC}^{\otimes n} \rho_{BR}^{\otimes n}$ (with $\rho_{BC}$ the maximally mixed state on $BC$), Lemma 2 in the Supplemental Material [22] gives

$$\lim_{n \to \infty} \frac{1}{n} S[\rho_{BCR}^{\otimes n} \| (D_n \otimes \text{id}_{R^e})(\phi_{G_n Y_n B^m R^e})] = 0,$$  

(14)

and so

$$I(C: R|B)_\rho = 2 \lim_{n \to \infty} \frac{\log(\text{dim}(G_n))}{n} \geq \lim_{n \to \infty} \min_{\Lambda: B^m \to B^m C^n} \frac{1}{n} S[\rho_{BCR}^{\otimes n} \| (\Lambda_n \otimes \text{id}_{R^e})(\rho_{BR}^{\otimes n})].$$

(15)

Even though we do not know whether

$$\lim_{n \to \infty} \min_{\Lambda: B^m \to B^m C^n} \frac{1}{n} S[\rho_{BCR}^{\otimes n} \| (\Lambda_n \otimes \text{id}_{R^e})(\rho_{BR}^{\otimes n})] = \min_{\Lambda: B \to BC} S[\rho_{BCR}^{\otimes n} \| (\Lambda \otimes \text{id}_{R^e})(\rho_{BR}^{\otimes n})],$$

it turns out that a similar inequality holds true if we replace the relative entropy by its measured variant (see Sec. B in the Supplemental Material [22]): For every state $\rho_{BCR}$ one has

$$\lim_{n \to \infty} \min_{\Lambda: B^m \to B^m C^n} \frac{1}{n} S[\rho_{BCR}^{\otimes n} \| (\Lambda_n \otimes \text{id}_{R^e})(\rho_{BR}^{\otimes n})] \geq \min_{\Lambda: B \to BC} \langle M \rangle \rho_{BCR} \rho_{BCR},$$

(17)

**Discussion and open problems.**—The main result of this Letter, on one hand, and Theorem 4 of Ref. [10], on the other hand, give

$$\min_{\sigma \in \sigma_{\text{QMS}}} S(\rho_{BCR}^{\otimes n} | \sigma_{BCR}) \geq I(C: R|B)$$

(18)

with the set of quantum Markov states (QMS) given by Eq. (3). For probability distributions the lower and upper bounds in Eq. (18) coincide, giving Eq. (2). However, in the quantum case, the two can be very far from each other.

An interesting question is whether we can also have equality in the quantum case when minimizing over the set of reconstructed states. In particular, we can ask whether Eq. (9) holds with equality. It turns out that this is false and can be disproved using pure states of dimension $2 \times 2 \times 2$ and the transpose channel, defined for a tripartite state $\rho_{BCR}$ as

$$T(\pi) := \sqrt{\rho_{BC}^{1/2} \rho_B^{-1/2} \pi \rho_B^{-1/2} \rho_{BC}^{1/2}}.$$  

(19)

In Fig. 1 we plot the CMI against the reconstructed relative entropy using the transpose channel, i.e.,

$$S[\rho_{BCR}^{\otimes n} \| T_B \otimes \text{id}_{R}(\rho_{BR}^{\otimes n})],$$

for 10,000 randomly chosen pure states of dimension $2 \times 2 \times 2$. We see that for roughly 73%
of the points, the relative entropy is strictly smaller than the CMI when using the transpose channel. Since any particular reconstruction map also puts an upper bound on the minimum relative entropy, Eq. (9) must sometimes be a strict inequality. Similar numerical results were found in an unpublished early version of [11].

In the proof of Theorem 1 we were not able to give an explicit optimal reconstruction map. In the context of approximate recovery for pure states, the transpose channel is optimal up to a square factor [23] (using the fidelity as a figure of merit). We could ask whether the same holds for mixed states.

Another interesting open problem is whether we can improve the lower bound in Eq. (18) to have the relative entropy, instead of the measured relative entropy. Proposition 3 and Lemma 5 in the Supplemental Material [22] show that the result would follow from the following conjectured inequality: Given a state $\rho$, a convex closed set of states $S$, and a measure $\mu$ with support only on $S$,

$$\lim_{n \to \infty} \inf_n \frac{1}{n} S\left(\rho^{\otimes n}\left|\int \mu(\sigma)\sigma^{\otimes n}\right) \geq \min_{\sigma \in S} S(\rho\|\sigma). \right. \quad (20)$$

The case when $\rho_{BR} = \rho_B \otimes \rho_R$ was recently proven in [24]. We can also easily prove the inequality classically using hypothesis testing, which is universal for the alternative hypothesis. However, since there is no quantum hypothesis test universal for the alternative hypothesis [25] for general sets $S$, we leave the inequality in the quantum case as an open problem for future work.

F. G. S. L. B. and J. O. thank EPSRC for financial support. A. W. H. was funded by NSF Grants No. CCF-1111382 and CCF-1452616, ARO Contract No. W911NF-12-1-0486, and a grant from the Leverhulme Trust. S. S. acknowledges the support of Sidney Sussex College. We thank Omar Fawzi, Ke Li, Marco Tomamichel, Mark Wilde, and Lin Zhang for helpful comments and the Newton Institute for their hospitality while some of this research was conducted.

[9] Reference [8] shows that Markov states have perfect reconstruction maps; see Eq. (19) for an explicit formula. The converse is straightforward. If $\Lambda \otimes \mathrm{id}_\rho(\rho_{BR}) = \rho_{BCR}$, then $\Lambda(\rho_B) = \rho_{BC}$. Using the recovery condition, and the monotonicity of relative entropy after applying first $\Lambda \otimes \mathrm{id}_\rho$ and then $\mathrm{tr}_C$, we obtain $S(\rho_{BCR}\|\rho_B \otimes \rho_C) = S([\Lambda \otimes \mathrm{id}_\rho(\rho_{BR})]/(\rho_B \otimes \rho_C) \leq S(\rho_{BCR}\|\rho_B \otimes \rho_C) \leq S(\rho_{BCR}\|\rho_B \otimes \rho_C)$. Then it follows that $I(C : R|B) = S(\rho_{BCR}\|\rho_B \otimes \rho_C) - S(\rho_{BCR}\|\rho_B \otimes \rho_C) = 0$.


