Quantum Conditional Mutual Information, Reconstructed States, and State Redistribution

Fernando G.S.L. Brandão\(^1\), Aram W. Harrow\(^2\), Jonathan Oppenheim\(^3\), Sergii Strelchuk\(^4\)

\(^1\) Department of Computer Science, University College London
\(^2\) Institute for Theoretical Physics, Massachusetts Institute of Technology
\(^3\) Department of Physics, University College London
\(^4\) Department of Applied Mathematics and Theoretical Physics, University of Cambridge

SUPPLEMENTAL MATERIAL

A. Auxiliary lemmas

**Lemma 1.** If \(\pi \leq 2^\lambda \sigma\), then \(S(\rho||\pi) \geq S(\rho||\sigma) - \lambda\).

The proof of the lemma follows directly from the operator monotonicity of the log function. \(\square\)

**Lemma 2** is due to Audenaert and Eisert:

**Lemma 2** (Theorem 3 of \([1]\)). For all states \(\rho\) and \(\sigma\) on a \(d\)-dimensional Hilbert space, with \(T = ||\rho - \sigma||_1\) and \(\beta = \lambda_{\min}(\sigma)\),

\[
S(\rho||\sigma) \leq T \log(d) + \min \left( -T \log T, \frac{1}{e} \right) - \frac{T \log \beta}{2}. \tag{1}
\]

The next lemma is due to M. Piani. It will suffice to state it for the case where \(M\) is the set of all measurements.

**Lemma 3.** \([Theorem~1~of~[2]]\) Consider two systems \(X\) and \(Y\) with joint Hilbert space \(\mathcal{H}_X \otimes \mathcal{H}_Y\), and a convex reference set \(K\). Suppose the reference set \(K\) is such that for all POVM elements \(M_i\) and all \(\sigma_{XY} \in K\), \(\text{tr}_X(M_i^\dagger \sigma_{XY}) \in \mathcal{P}(\text{up to normalization})\). Then for every \(\rho_{XY}\),

\[
\min_{\sigma_{XY} \in K} S(\rho_{XY}||\sigma_{XY}) \geq \min_{\sigma_X \in K} \mathbb{M}S(\rho_X||\sigma_X) + \min_{\sigma_Y \in K} S(\rho_Y||\sigma_Y). \tag{2}
\]

The following Lemma is due to Fawzi and Renner \([3]\) who stated it in a slightly more general form. It was used in their proof of Eq. (4) in the main text. Below is a very similar, but somewhat shorter, proof.

**Lemma 4.** Suppose \(\rho_{X^nY^n}\) satisfies \(\rho_{X^n} = \tau_{X^n}\) and \([\rho, P_{XY}(\pi)] = 0\) for all \(\pi \in S_n\). Then there exists a measure \(\mu\) over states \(\sigma_{XY}\) (independent of \(\rho\)) with each \(\sigma_X = \tau_X\) and

\[
\rho_{X^nY^n} \leq n^{\mathcal{O}(d_X^2 d_Y^2)} \int \sigma^n \mu(d\sigma), \tag{3}
\]

where \(d_X, d_Y\) are the dimensions of \(X\) and \(Y\).

**Proof.** First purify \(\rho\) to a state \(|\rho\rangle_{X^nY^nZ^n} \in \text{Sym}^n(\mathcal{H}_X \otimes \mathcal{H}_Y \otimes \mathcal{H}_Z)\) (the symmetric subspace in \((\mathcal{H}_X \otimes \mathcal{H}_Y \otimes \mathcal{H}_Z)^n\)) with \(d_Z = d_X d_Y\) using Lemma 4.2.2 of \([4]\). For \(V\) an isometry from \(X \rightarrow YZ\), define

\[
|\sigma(V)\rangle_{XYZ} = \frac{1}{\sqrt{d_X}} \sum_{i=1}^{d_X} |i\rangle V |i\rangle \tag{4}
\]

and \(\sigma(V) = |\sigma(V)\rangle \langle \sigma(V)|\). Observe that \(\sigma(V)_X = \tau_X\).

We will show that

\[
|\rho\rangle \langle \rho| \leq n^{\mathcal{O}(d_X^2 d_Y^2)} \int \sigma(V)^n \mu(d\sigma), \tag{5}
\]

which will imply Eq. (3).

Our strategy will be to expand both sides of Eq. (5) in the Schur basis. Schur duality uses the following notation:

\[
(\mathbb{C}^d)^\otimes n \cong \bigoplus_{\lambda \in \text{Par}(n,d)} \mathbb{Q}_d^{\lambda} \otimes P_\lambda. \tag{6}
\]

This is explained in detail in \([5]\), but briefly, \(\text{Par}(n,d)\) denotes the set of partitions of \(n\) into \(\leq d\) parts, \(\mathbb{Q}_d^{\lambda}\) is an irrep of the unitary group \(U_d\), \(P_\lambda\) is an irrep of the symmetric group \(S_n\), \(\otimes\) means that we interpret the tensor product as an irrep of \(U_d \times S_n\), and \(\cong\) means that the isomorphism respects this representation structure. Let \(U_{\text{Sch}}\) denote the unitary transform realizing the isomorphism in Eq. (6). We can write

\[
(U_{\text{Sch}}^X \otimes U_{\text{Sch}}^{YZ}) |\rho\rangle = \sum_{\lambda_1,\lambda_2} \sum_{\lambda \in \text{Par} (n,d_X,d_Y)} c_{\lambda_1,\lambda_2} |\lambda_1\rangle_X |\lambda_2\rangle_Y Z |\lambda\rangle_{\lambda_1,\lambda_2} \langle \theta_{\lambda_1,\lambda_2}| \Phi_\lambda\rangle, \tag{7}
\]

where \(\sum_{\lambda} |c_{\lambda}|^2 = 1\), \(|\lambda_1\rangle, |\lambda_2\rangle\), \(|\theta_{\lambda_1,\lambda_2}\rangle\) are arbitrary unit vectors in \(\mathbb{Q}_d^{\lambda_1} \otimes \mathbb{Q}_d^{\lambda_2} \otimes \mathbb{P}_\lambda\) and \(\mathbb{P}_\lambda \otimes \mathbb{P}_\lambda\), respectively. However, the permutation invariance and Schur’s Lemma mean that (following arguments along the lines of Section 6.4.1 of \([5]\)) the only nonzero terms have \(\lambda_1 = \lambda_2\) and \(|\theta_{\lambda_1,\lambda_2}\rangle = |\Phi_\lambda\rangle\) is the unique permutation-invariant state in \(\mathbb{P}_\lambda \otimes \mathbb{P}_\lambda\). Thus we can (using \(d_X \leq d_Y d_Z\)) rewrite Eq. (7) as

\[
(U_{\text{Sch}}^X \otimes \mathbb{P}^{YZ}) |\rho\rangle = \sum_{\lambda \in \text{Par} (n,d_X)} c_{\lambda} |\lambda\rangle_X |\lambda\rangle_Y Z |\lambda\rangle_{\lambda,\lambda} \langle \Phi_\lambda|, \tag{8}
\]
To calculate $c_\lambda$ we use the fact that $\rho_X = \tau_X$. Thus measuring the irrep label should yield outcome $\lambda$ with probability $\dim \mathcal{P}_\lambda \dim Q^d_{\lambda X} / d_X^n$, and we have

$$c_\lambda = \sqrt{\dim \mathcal{P}_\lambda \dim Q^d_{\lambda X} / d_X^n}. \tag{9}$$

A similar argument implies that

$$(U_{\text{Sch}} X \otimes U_{\text{Sch}} Y \otimes Z) |\sigma(V)\rangle \otimes^n = \sum_{\lambda \in \pi \in \mathcal{P}(n,d_X)} c_\lambda |\lambda\rangle_X |\lambda\rangle_Y |\lambda\rangle_Z |\chi_{\lambda}(V)| \Phi_{\lambda}\rangle, \tag{10}$$

for some states $|\chi_{\lambda}(V)\rangle$. The coefficients $c_\lambda$ are the same as in Eq. (9) because $\sigma(V)_{\otimes^n} = \tau_Q_{\otimes^n}$. Averaging $\sigma(V)_{\otimes^n}$ over all isometries $V$ yields a state that commutes with $(U_{\text{Sch}} X \otimes I_{\text{Sch}} Y) \otimes^n$ and $(I_{\text{Sch}} X \otimes U_{\text{Sch}} Y) \otimes^n$ for all $U_{\text{Sch}} X \otimes U_{\text{Sch}} Y \otimes \mathcal{U}_{d_X} Z \in \mathcal{U}_{d_Y} Z$. Thus

$$(U_{\text{Sch}} X \otimes U_{\text{Sch}} Y \otimes Z) |\sigma(V)\rangle \otimes^n (U_{\text{Sch}} X \otimes U_{\text{Sch}} Y) = \sum_{\lambda \in \pi \in \mathcal{P}(n,d_X)} |\lambda\rangle_X |\lambda\rangle_Y |\lambda\rangle_Z |\chi_{\lambda}(V)| \Phi_{\lambda}\rangle.$$

It follows from (8) and (11) that

$$|\rho\rangle \langle \rho| \leq (\max \dim Q^d_{\lambda X} \dim Q^d_{\lambda Y} \otimes \mathcal{V} \dim |\sigma(V)\rangle \otimes^n) \leq \left( d_X + n - 1 \right) \left( d_Y + n - 1 \right) \left( d_Z + n - 1 \right) \leq n^{d_X} n^{d_Y} d_Z \sum |\lambda\rangle_X |\lambda\rangle_Y |\lambda\rangle_Z |\chi_{\lambda}(V)| \Phi_{\lambda}\rangle.$$ 

\[\square\]

B. The measured entropy lower bound

To prove the inequality stated in the Eq. (17) of the main text, we first prove the following lemma which is a version of the postselection technique of [6] for quantum operations.

**Lemma 5.** For every permutation-invariant quantum operation $\Lambda : B^n \rightarrow B^n C^n$ and every state $\rho \in B^n$, $\lambda = \log(d_B)$.

$$\Lambda(\rho) \leq \log(d_B) \int S(\rho_{\otimes^n B^n C^n}) \mu(d\rho_{\otimes^n C^n}), \tag{12}$$

where $\mu$ is a measure over quantum operations $\mathcal{E} : B \rightarrow BC$.

**Proof.** Since $\Lambda : B^n \rightarrow B^n C^n$ is permutation-invariant, it follows that its Jamiołkowski state $J_{\Lambda} \in \mathcal{D}(\mathcal{B} \otimes B^n \otimes C^n)$ (with $\mathcal{B} \cong B$) is permutation-invariant. We now apply Lemma 4 in the Supplemental Material to find a distribution $\mu$ over $\sigma \in \mathcal{D}(\mathcal{B} \otimes B \otimes C)$ with

$$J_{\Lambda} \leq \log(d_B) \int \sigma \otimes^n \mu(d\sigma), \tag{13}$$

and each $\sigma_B = \tau_B$. This latter condition means that each $\sigma$ can be also thought of as $\lambda_{\mathcal{E}}$ for some $\mathcal{E} : B \rightarrow BC$. We complete the proof using the relation:

$$\text{tr}_{\mathcal{E}}(\langle (\pi^T \otimes I_{B^n C^n}) J_{\Lambda} \rangle) \leq \log(d_B) \int \text{tr}_{\mathcal{E}}((\pi^T \otimes I_{B^n C^n}) J_{\Lambda} \rangle) \mu(d\mathcal{E}), \tag{14}$$

and the fact that $\text{tr}_{\mathcal{E}}((\pi^T \otimes I_{B^n C^n}) J_{\Lambda} \rangle)$ is $\mathcal{E} \otimes^n (\pi) / \dim(B)^n$ and $\text{tr}_{\mathcal{E}}((\pi^T \otimes I_{B^n C^n}) J_{\Lambda} \rangle)$ is $\mathcal{E} \otimes^n (\pi) / \dim(B)^n$. \[\square\]

We now turn to proving the measured entropy lower bound:

**Proposition 6** (Eq. (17) in the main text). For every state $\rho_{BCR}$ one has

$$\min_{\Lambda : B \rightarrow BC} S(\rho_{\otimes^n C^n} |\Lambda \otimes \id_{R}(\rho_{BR})\rangle) \geq \min_{\Lambda : B \rightarrow BC} S(\rho_{\otimes^n C^n} |\Lambda \otimes \id_{R}(\rho_{BR})\rangle). \tag{15}$$

**Proof.** For $\Lambda : B^n \rightarrow B^n C^n$, define

$$\Lambda(\omega) := \frac{1}{n} \sum_{\pi \in \mathcal{S}_n} P_{BCR}(\pi) \Lambda(\rho_{BCR}(\pi)) P_{BCR}(\pi) \omega P_{BCR}(\pi), \tag{16}$$

with $P_{BCR}(\pi)$ a representation of a permutation $\pi$ from $\mathcal{S}_n$ (symmetric group of order $n$) in $X^n$ such that $P_{BCR}(\pi)(a_1, a_2, \ldots, a_n) = (a_{\pi^{-1}(a_1)}, a_{\pi^{-1}(a_2)}, \ldots, a_{\pi^{-1}(a_n)})$. Let Sym be the set of all permutation-invariant quantum operations, i.e. all $\Lambda$ such that $\Lambda = \Lambda_{n}\otimes \id_{n}$. Using Proposition 3 in the main text and the fact that the relative entropy is doubly convex we obtain [7]

$$\min_{n \rightarrow \infty} \min_{\Lambda : B^n \rightarrow B^n C^n} \frac{1}{n} S(\rho_{\otimes^n C^n} |\Lambda \otimes \id_{R}(\rho_{BR})\rangle) \geq \lim_{n \rightarrow \infty} \min_{\Lambda : B^n \rightarrow B^n C^n} \frac{1}{n} S(\rho_{\otimes^n C^n} |\Lambda \otimes \id_{R}(\rho_{BR})\rangle). \tag{17}$$

Lemma 5 gives that for every $\Lambda_n : B^n \rightarrow B^n C^n \in \text{Sym}$,

$$\langle \Lambda_n \otimes \id_{R}(\rho_{BR})\rangle \langle \rho_{BR} \rangle \geq \langle \rho_{BR} \rangle \langle \rho_{BR} \rangle \mu(d\rho_{BR}). \tag{18}$$

with $\mu(d\rho)$ a measure over quantum operations $\mathcal{E} : B \rightarrow BC$. Using the previous equation and the operator monotonicity of the log (see Lemma 1 above),

$$\min_{\Lambda : B^n \rightarrow B^n C^n} \frac{1}{n} S(\rho_{\otimes^n C^n} |\Lambda \otimes \id_{R}(\rho_{BR})\rangle) \geq \min_{\Lambda : B^n \rightarrow B^n C^n} \frac{1}{n} S(\rho_{\otimes^n C^n} |\Lambda \otimes \id_{R}(\rho_{BR})\rangle) \mu(d\rho_{BR}). \tag{19}$$

To complete the proof we make use of Lemma 3 above. Consider the state $\rho_{BCR}$ and let $X$ be the first
copy of $\rho_{BCR}$ in the tensor product and $Y$ the remaining $\otimes_{n-1}$. Define

$$K = \bigcup_{k \in \mathbb{N}} \left( \text{conv} \{ (\mathcal{E} \otimes \text{id}_R)(\rho_{BR})^\otimes k : \mathcal{E} : B \to BC \} \right),$$

(19)
i.e. the convex hull of tensor products of reconstructed states. It is easy to check that $K$ satisfies the assumption of Lemma 3 above. Therefore:

$$\min_{\mu_n} S \left( \rho_{BCR}^{\otimes n} \mid\mid \int (\mathcal{E} \otimes \text{id}_R(\rho_{BR}))^{\otimes n} \mu_n(d\mathcal{E}) \right) \geq \min_{\mu} MS \left( \rho_{BCR} \mid\mid \int (\mathcal{E} \otimes \text{id}_R(\rho_{BR})) \mu(d\mathcal{E}) \right)$$

(20)

$$+ \min_{\mu_{n-1}} S \left( \rho_{BCR}^{\otimes n-1} \mid\mid \int (\mathcal{E} \otimes \text{id}_R(\rho_{BR}))^{\otimes n-1} \mu_{n-1}(d\mathcal{E}) \right),$$

Iterating the equation above $n$ times gives Eq. (15). □

[7] In more detail: $S\left( \rho_{BCR}^{\otimes n} \mid\mid A(\rho_{BR}) \right) = \mathbb{E}_{\pi \in S_n} S\left( P_{CBR}^\pi \rho_{BCR}^{\otimes n} P_{CBR}^\pi \mid\mid P_{CBR}^\pi A(\rho_{BR}) P_{CBR}^\pi \right)$

$$= \mathbb{E}_{\pi \in S_n} S\left( \rho_{BCR}^{\otimes n} \mid\mid P_{CBR}^\pi A(\rho_{BR}) P_{CBR}^\pi \right) \geq S \left( \rho_{BCR} \mid\mid \mathbb{E}_{\pi \in S_n} P_{CB}^\pi A(\rho_{BR}) P_{CB}^\pi \right),$$

with $P_{CBR}^\pi := P_{CBR}(\pi)$. 
