Quantum Shannon Theory: Patrick Hayden

Solutions

1. *More reasonable properties of the entropy function.*

a) Prove the Araki-Lieb inequality: $S(AB)_\rho \geq |S(A)_\rho - S(B)_\rho|$. *Hint:* Consider a purification of ρ to ABC and then use the nonnegativity of mutual information.

b) The conditional entropy is defined to be $S(A|B)_\rho = S(AB)_\rho - S(B)_\rho$. Show that conditioning cannot increase entropy: $S(A|B)_\rho \geq S(A|BC)_\rho$.

c) Show that adding an extra system can't cause the mutual information to increase too much: $I(A;BC)_\rho \leq I(A;B)_\rho + 2S(C)_\rho$.

Solution:

a) Let $|\varphi\rangle_{ABC}$ be a purification of ρ. Then, since the non-zero eigenvalues of the reduced density operators of the two halves of bipartite pure state are the same, the inequality $S(AB)_\rho \geq S(A)_\rho - S(B)_\rho$ is equivalent to $S(C)_\varphi \geq S(BC)_\varphi - S(B)_\varphi$. That is, $I(B;C) \geq 0$. The absolute value comes by interchanging the roles of A and B.

b) Expanding the inequality gives precisely strong subadditivity.

c) $I(A;BC) - I(A;B)$ is also known as the conditional mutual information $I(A;C|B)$, which can also be written $S(C|B) - S(C|AB)$. Since conditioning cannot increase entropy, $S(C|B) \leq S(C)$. On the other hand, Araki-Lieb implies that

$$S(C|AB) = S(ABC) - S(AB) \geq -S(C). \tag{1}$$

Thus,

$$I(A;BC) - I(A;B) = S(C|B) - S(C|AB) \leq S(C) - [-S(C)] = 2S(C). \tag{2}$$

2. *Minimal number of qubits required to destroy correlations.*

Given a quantum state ρ_{AB}, you will prove that it is necessary to discard at least $I(A;B)_\rho/2$ qubits in order to reduce the mutual information to zero or even near zero. Let $U : B \to K \otimes D$ be a Hilbert space isometry, in the sense that $U^\dagger U = I$. These are the most general noiseless quantum channels. K will represents the qubits kept and D those discarded.

Let $\sigma = (I_A \otimes U)\rho_{AB}(I_A \otimes U^\dagger)$. Under the assumption that $I(A;K)_\sigma \leq \varepsilon$, use Eq. (2) to show that

$$I(A;B)_\rho \leq \varepsilon + 2 \log \dim D. \tag{3}$$

That is, at least $I(A;B)_\rho/2 - \varepsilon/2$ qubits must be discarded.

Solution:

$$
\begin{aligned}
I(A;B)_\rho &= I(A;KD)_\sigma && (4)\\
&\le I(A;K)_\sigma + 2S(D)_\sigma && (5)\\
&\le I(A;K)_\sigma + 2\log\dim D. && (6)
\end{aligned}
$$

The first step is because U doesn't alter any non-zero eigenvalues so all entropies are unchanged. The second step is an application of Eq. (2) and the last step is because entropy is maximized by the state $I_D/\dim D$, whose entropy is $\log\dim D$.

3. *Entanglement of assistance and the Ryu-Takayanagi formula.*

The purpose of this problem is to show projecting away degrees of freedom from a state in the interior of a geometry with a boundary leads naturally to a state on the boundary obeying the Ryu-Takayanagi formula. Your route to get there will be repeated state merging. Don't be intimidated. The solution is much shorter than the problem itself!

In class, we constructed the classical communication version of state merging by investing entanglement between Alice and Bob, say I ebits. At the end of the procedure, Alice and Bob shared some number J of ebits and we declared the net ebit cost to be $I-J$. For merging Alice's portion of $|\varphi\rangle_{ABR}^{\otimes n}$ to Bob, we found a procedure with $(I-J)/n \to S(A|B)_\varphi$ as $n\to\infty$. It turns out that whenever $S(A|B)_\varphi$ is negative, there is a simple way to implement the procedure without investing any ebits at the beginning. The protocol is simply to apply Schumacher compression to Alice's system A^n and then measure in a random basis, communicating the measurement outcome to Bob. While it isn't *quite* true, assume for the purposes of this problem that for every measurement outcome, the resulting conditional state of R^nB^n is exactly a purification of $\varphi_R^{\otimes n}$.

a) Suppose that Alice, Bob and Charlie share n copies of the state $|\varphi\rangle_{ABC}$ and that Charlie wishes to help Alice and Bob establish pure state entanglement using an LOCC protocol. Argue that they can establish a pure state between Alice and Bob whose entanglement entropy is $n\min[S(A)_\varphi, S(B)_\varphi]$. *Hint:* Have Charlie try to merge his state to either Alice or Bob using classical communication and additional entanglement. What is the entanglement cost in each case? Can both costs be positive?

Now consider the more general problem of many Charlies holding subsystems $C_1, C_2, \ldots, C_k$ and n copies of the shared pure state $|\varphi\rangle_{ABC_1C_2\cdots C_k}$. The goal is again to establish a pure entangled state between Alice and Bob, but subject to the restriction of LOCC between Alice, Bob and each of the Charlies. Since the Charlies have to operate on their individual systems, the collective measurement of $C = C_1C_2\cdots C_k$ used in part (a) will generally no longer be an option. Instead, suppose that each Charlie in turn applies the compression and random measurement of part (a), effectively merging his state to Alice, Bob and the Charlies who have yet to participate. You will show that once all the Charlies have performed their measurements and communicated their outcomes that Alice and Bob will share a pure entangled state of entanglement entropy

$$
n \min_{T\subseteq\{C_1,\ldots,C_k\}} S(AT)_\varphi. \tag{7}
$$

This quantity is by definition the min-cut entanglement between A and B.

b) Show that Eq. (7) reduces to the result of part (a) when $k=1$.

c) Consider the measurement of C_1 and fix $R \subseteq \{C_2, \ldots C_k\}$. Show that, after measurement of C_1, the conditional states Ψ satisfy

$$S(A'^n)_\Psi = S(B'^n)_\Psi = n \min[S(AR)_\varphi, S(AR^c)_\varphi]. \tag{8}$$

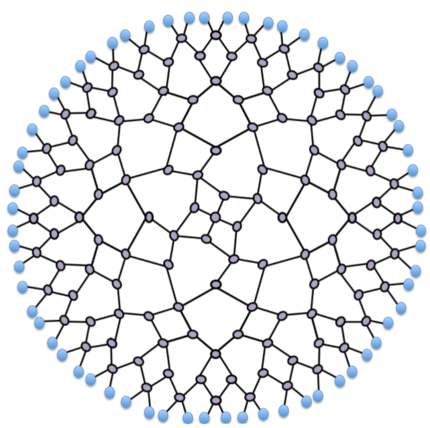
d) Conclude that

$$n \min_{R \subseteq \{C_2, \ldots, C_k\}} S(AR)_\Psi = n \min_{T \subseteq \{C_1, \ldots, C_k\}} S(AT)_\varphi. \tag{9}$$

Thus, the min-cut entanglement is left invariant by C_1's measurement.

Assuming that state merging continues to work for the subsequent measurements of C_2 through C_k, it follows by induction that once all Charlies have measured, Alice and Bob are left with a pure quantum state of entanglement entropy given by the min-cut entanglement of $|\varphi\rangle^{\otimes n}$, Eq. (7).

Now let's make things more concrete. Fix a connected graph $G = (V, E)$ with a vertex set V and edges E. The subset $\partial V \subseteq V$ of vertices of degree 1, that is, with only one edge, will be called the boundary of G. All other vertices will be called "bulk". For example, in the following graph, the blue vertices form the boundary set ∂V.



Suppose we have a d-dimensional state space $\mathcal{H}_v = \mathbb{C}^d$ at each vertex v so that the total Hilbert space is $\mathcal{H} = \otimes_{v \in V} \mathcal{H}_v$. Now suppose that $|\varphi\rangle \in \mathcal{H}$ is a state satisfying an area law. That is, for any subset of vertices $W \subseteq V$, $S(W)_\varphi = c|\partial W|$ for some constant C. Here $|\partial W|$ is the number of edges that cross from W to $V \backslash W$, the graph-theoretic analog of the area of W.

e) Fix $A \subseteq \partial V$ a subset of boundary vertices with $A^c = \partial V \backslash A$. Take n copies of $|\varphi\rangle$ and merge all the bulk subsystems to the boundary. Show that the resulting state $|\Psi\rangle_{AA^c}$ will satisfy

$$S(A)_\Psi = n \min\{c|\partial W| \ : \ W \subseteq V \text{ and } A \subseteq W\}. \tag{10}$$

That is, the entropy of A for the conditional state is the minimum area of a bulk region whose boundary is A. This matches the Ryu-Takayanagi formula.

For an interpretation of this observation in terms of the holographic properties of tensor networks, consult arXiv:1601.01694.

Solution:

a) From class, the entanglement cost rate of state merging with classical communication is $S(C|A)_\varphi$ for merging to Alice and $S(C|B)_\varphi$ for merging to Bob. But

$$
\begin{aligned}
S(C|A)_\varphi + S(C|B)_\varphi &= S(AC)_\varphi - S(A)_\varphi + S(BC)_\varphi - S(B)_\varphi && (11)\\
&= S(B)_\varphi - S(A)_\varphi + S(A)_\varphi - S(B)_\varphi && (12)\\
&= 0, && (13)
\end{aligned}
$$

where we are again using that the entropies of each half of a pure bipartite state are equal to each other. As a result, it is impossible for both $S(C|A)_\varphi$ and $S(C|B)_\varphi$ to be positive. If they are both equal to zero, the problem gets a bit tricky, so assume they are nonzero.

Suppose without loss of generality that it is $S(C|A)_\varphi$ that is negative. Then the final merged state shared between Alice and Bob has entanglement entropy $nS(B)_\varphi$ since C^n was merged to Alice. But $S(B)_\varphi - S(A)_\varphi = S(AC)_\varphi - S(A)_\varphi = S(C|A)_\varphi < 0$ so the state's entanglement entropy is indeed the lesser of $nS(A)_\varphi$ and $nS(B)_\varphi$.

b) This is simply the observation that when $k = 1$, $S(B) = S(AC)$.

c) Apply part (a) with $C' = C_1$, $A' = AR$ and $B' = BR^c$, where $R^c = \{C_2, \dots C_k\}\backslash R$. Since $|\Psi\rangle_{A'^n B'^n}$ is pure, $S(A'^n)_\Psi = S(B'^n)_\Psi$. Moreover, part (a) tells us that

$$S(A'^n)_\Psi = n \min[S(A')_\varphi, S(B')_\varphi] = n \min[S(AR)_\varphi, S(BR^c)_\varphi]. \tag{14}$$

d) From Eq. (14), we have that

$$\min_{R\subseteq\{C_2,\dots,C_k\}} S(AR)_\Psi = n \min_{R\subseteq\{C_2,\dots,C_k\}} \min[S(AR)_\varphi, S(BR^c)_\varphi] \tag{15}$$

Now let $T^* \subseteq \{C_1, \dots, C_k\}$ be a subset that minimizes $S(AT)_\varphi$. If $C_2 \notin T^*$ then we can choose $R = T^*$ in the equation above and get $S(AR)_\varphi = S(AT^*)_\varphi$. On the other hand, if $C_2 \in T^*$ then $C_2 \notin T^{*c} := \{C_1, \dots, C_k\}\backslash T^*$ so we can choose $R^c = T^{*c}$ and find $S(AT^*)_\varphi = S(BT^{*c})_\varphi = S(BR^c)_\varphi$. It follows that

$$\min_{R\subseteq\{C_2,\dots,C_k\}} \min[S(AR)_\varphi, S(BR^c)_\varphi] = \min_{T\subseteq\{C_1,\dots,C_k\}} S(AT)_\varphi. \tag{16}$$

e) Here the T of the min-cut formula Eq. (7) will be equal to $W\backslash A$ and we'll set $B = \partial V\backslash A$. There is actually nothing to prove. Using the min-cut formula and the area law assumption, we find that for any T consisting of bulk vertices,

$$S(AT)_\varphi = S(W)_\varphi = c|\partial W|. \tag{17}$$