Lecture 9: Strong subadditivity CSE 599I, Spring 2021
Instructor: James R. Lee

1 Quantum entropy and subadditivity

Recall the von Neumann entropy of a density $\rho \in \mathcal{D}(\mathbb{C}^n)$ is defined as

$$\mathcal{S}(\rho) = -\mathrm{Tr}(\rho \log \rho).$$

This is precisely the Shannon entropy of the eigenvalues $\lambda_1, \ldots, \lambda_n$ of ρ:

$$H(\lambda_1, \ldots, \lambda_n) = \sum_{i=1}^{n} \lambda_i \log \frac{1}{\lambda_i},$$

with our standard convention that $0 \log 0 = 0$.

Remark 1.1. In most of what follows, we will assume that our density matrices ρ are strictly positive, i.e., that they don't have zero eigenvalues. Thus quantities like $\log(\rho)$ are well-defined. Our results extend to the general case by applying first an arbitrarily small perturbation and then taking a limit as the perturbation goes to zero. This will generally make sense in considering expressions like $\varepsilon \log \varepsilon$, which goes to 0 as $\varepsilon \to 0$.

1.1 Subadditivity and monotonicity

It is well-known that the Shannon entropy of two random variables X, Y is subadditive:

$$H(X, Y) \leqslant H(X) + H(Y). \tag{1.1}$$

This can be proved using the chain rule

$$H(X, Y) = H(X) + H(Y \mid X),$$

and then the monotonicity $H(Y \mid X) \leqslant H(Y)$.

Consider a density matrix on a bipartite system $\rho^{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, and define the reduced densities $\rho^A := \mathrm{Tr}_B(\rho^{AB})$ and $\rho^B := \mathrm{Tr}_A(\rho^{AB})$. We have already seen that a corresponding argument fails in the quantum case, as it can be that the joint entropy vanishes, i.e., $\mathcal{S}(\rho^{AB}) = 0$, and yet $\mathcal{S}(\rho^A) > 0$. Still, the analog of the subadditivity inequality (1.1) is true. The proof will use the quantum relative entropy

$$\mathsf{S}(\rho \,\|\, \sigma) = \mathrm{Tr}(\rho(\log \rho - \log \sigma)),$$

and the fact we established earlier that $\mathsf{S}(\rho \,\|\, \sigma) \geqslant 0$ with $\mathsf{S}(\rho \,\|\, \sigma) = 0 \iff \rho = \sigma$. Note that we take $\mathsf{S}(\rho \,\|\, \sigma) = +\infty$ if $\ker \sigma \not\subseteq \ker(\rho)$.

Theorem 1.2. *It holds that*

$$\mathcal{S}(\rho^{AB}) \leqslant \mathcal{S}(\rho^A) + \mathcal{S}(\rho^B) = \mathcal{S}(\rho^A \otimes \rho^B),$$

with equality if and only if $\rho^{AB} = \rho^A \otimes \rho^B$.

Proof. We have $\mathsf{S}(\rho^{AB} \,\|\, \rho^A \otimes \rho^B) \geqslant 0$, with equality if and only if $\rho^{AB} = \rho^A \otimes \rho^B$. As we have seen in the first homework, it holds that

$$\log(\rho^A \otimes \rho^B) = \log(\rho^A) \otimes I_B + \log(\rho^B) \otimes I_A,$$

hence

$$\begin{aligned} 0 \leqslant \mathsf{S}(\rho^{AB} \,\|\, \rho^A \otimes \rho^B) &= -\mathcal{S}(\rho^{AB}) - \operatorname{Tr}\left(\rho^{AB}\left(\log(\rho^A) \otimes I_B + \log(\rho^B) \otimes I_A\right)\right) \\ &= -\mathcal{S}(\rho^{AB}) - \operatorname{Tr}\left((\operatorname{Tr}_B \rho^{AB}) \log(\rho^A) + (\operatorname{Tr}_A \rho^{AB}) \log(\rho^B)\right) \\ &= -\mathcal{S}(\rho^{AB}) + \mathcal{S}(\rho^A) + \mathcal{S}(\rho^B). \end{aligned}$$

□

Although monotonicity of the entropy fails, we can recover the following quantum weakening of the classical fact that $H(X, Y) \geqslant \min(H(X), H(Y))$.

Theorem 1.3. *It holds that*

$$\mathcal{S}(\rho^{AB}) \geqslant |\mathcal{S}(\rho^A) - \mathcal{S}(\rho^B)|.$$

The only known argument is via purification. We require the following lemma.

Lemma 1.4. *Suppose that $\rho \in \mathcal{D}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ is a pure state and $\rho^1 = \operatorname{Tr}_2(\rho)$, $\rho^2 = \operatorname{Tr}_1(\rho)$. Then ρ^1 and ρ^2 have the same eigenvalues. In particular, $\mathcal{S}(\rho^1) = \mathcal{S}(\rho^2)$.*

Proof. Write $\rho = uu^*$ for a unit vector $u \in \mathcal{H}_1 \otimes \mathcal{H}_2$. Let $\{u_i\}$ and $\{v_j\}$ be orthonormal bases for $\mathcal{H}_1$ and $\mathcal{H}_2$ and write

$$\begin{aligned} u &= \sum_{i,j} a_{ij}(u_i \otimes v_j), \\ \rho &= \sum_{i,j,i',j'} a_{ij}\bar{a}_{i'j'}(u_i \otimes v_j)(u_{i'} \otimes v_{j'})^*. \end{aligned}$$

Then,

$$\rho^1 = \sum_{i,i'} (AA^*)_{ii'} u_i u_{i'}^*, \quad \rho^2 = \sum_{j,j'} (A^*A)_{jj'} v_j v_{j'}^*,$$

where A is the matrix defined by $A_{ij} = a_{ij}$.

Stated a different way: If we write u in the basis $\{u_i \otimes v_j\}$ and write each of ρ^1 and ρ^2 in the bases $\{u_i\}$ and $\{v_j\}$, respectively, then u is the matrix A (as a vector!), while ρ^1 is the matrix AA^* and ρ^2 is the matrix A^*A. As we have already seen from the singular-value decomposition, the matrices AA^* and A^*A always have the same non-zero eigenvalues—which are the singular values of A—although the multiplicity of the 0 eigenvalue will be different, to make up for the possibly unequal dimensions. □

Proof of Theorem 1.3. Let ρ^{ABC} denote a purification of ρ^{AB} so that $\rho^{AB} = \operatorname{Tr}_C(\rho^{ABC})$. Also define $\rho^C = \operatorname{Tr}_{AB}(\rho^{ABC})$ and $\rho^{AC} = \operatorname{Tr}_B(\rho^{ABC})$. By Lemma 1.4, it holds that $\mathcal{S}(\rho^C) = \mathcal{S}(\rho^{AB})$ and $\mathcal{S}(\rho^{AC}) = \mathcal{S}(\rho^B)$. Thus from Theorem 1.2, we have

$$\mathcal{S}(\rho^B) = \mathcal{S}(\rho^{AC}) \leqslant \mathcal{S}(\rho^A) + \mathcal{S}(\rho^C) = \mathcal{S}(\rho^A) + \mathcal{S}(\rho^{AB}),$$

whereby

$$\mathcal{S}(\rho^{AB}) \geqslant \mathcal{S}(\rho^B) - \mathcal{S}(\rho^A).$$

□

1.2 Quantum mutual information and strong subadditivity

The *mutual information* between two classical random variables X, Y is defined by

$$\mathbf{I}(X, Y) := \mathsf{D}(p_{XY} \,\|\, p_X \otimes p_Y),$$

where p_{XY} is the joint distribution on (X, Y) and p_X, p_Y are the respective marginal distributions. It is straightforward to verify that $\mathbf{I}(X, Y) = H(X) + H(Y) - H(X, Y)$.

Given a bipartite state $\rho \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$, one defines the classical mutual information across the A-B partition by

$$\mathbf{I}(A, B)_\rho := \mathsf{S}(\rho \,\|\, \rho^A \otimes \rho^B),$$

with $\rho^A = \mathrm{Tr}_B(\rho)$, $\rho^B = \mathrm{Tr}_A(\rho)$, and Theorem 1.2 asserts that the quantum mutual information is always nonnegative, since $\mathbf{I}(A, B)_\rho = \mathcal{S}(\rho^A) + \mathcal{S}(\rho^B) - \mathcal{S}(\rho)$ holds as well.

The classical *conditional mutual information* is defined by

$$\mathbf{I}(X, Y \mid Z) := \mathop{\mathbb{E}}_Z \left[\mathsf{D}(p_{XY|Z} \,\|\, p_{X|Z} \otimes p_{Y|Z}) \right],$$

where we use $p_{A|Z}$ to denote the distribution of the random variable A conditioned on Z. This definition does not extend nicely to the quantum setting since the notion of "conditioning" is not well-defined there. But since

$$\mathbf{I}(X, Y \mid Z) = H(X, Z) + H(Y, Z) - H(X, Y, Z) - H(Z)$$

holds, we can use this formula to define the quantum conditional mutual information for a tripartite state $\rho \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$:

$$\mathbf{I}(A, C \mid B)_\rho = \mathcal{S}(\rho^{AB}) + \mathcal{S}(\rho^{BC}) - \mathcal{S}(\rho) - \mathcal{S}(\rho^B),$$

where we make the definitions

$$\rho^{AB} = \mathrm{Tr}_C(\rho), \quad \rho^{BC} = \mathrm{Tr}_A(\rho), \quad \rho^A = \mathrm{Tr}_{BC}(\rho), \quad \rho^B = \mathrm{Tr}_{AC}(\rho).$$

Strong subadditivity asserts that $\mathbf{I}(X, Y \mid Z) \geqslant 0$ always holds, and the *strong subadditivity of quantum entropy* is the fact that this is also true in the quantum setting. The next assertion was conjectured by Robinson and Ruelle in 1966 and proved in 1973 by Lieb and Ruskai using Lieb's concavity thoerem. It was later discovered that it had already been proved by Kiefer in 1959 (in a paper entitled "Optimal Experimental Designs" that has no mention of anything quantum).

Theorem 1.5 (Quantum SSA)**.** *It holds that* $\mathbf{I}(A, C \mid B)_\rho \geqslant 0$*, i.e.,*

$$\mathcal{S}(\rho) + \mathcal{S}(\rho^B) \leqslant \mathcal{S}(\rho^{AB}) + \mathcal{S}(\rho^{BC}).$$

You will prove this in HW #2 using monotonicity of the relative entropy under partial trace, which we discuss next.