Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Quantum Information Theory
Tips 9

FS 11
Lídia del Rio

Handy properties of von Neumann entropy

1. Definition: $H(A)_\rho = -\mathrm{Tr}\big(\rho \log \rho\big) = -\sum_i \lambda_i \log \lambda_i$, where:
   (a) $\{\lambda_i\}_i$ are the eigenvalues of ρ;
   (b) the logarithm is $\log_2$;
   (c) to evaluate the entropies, $0 \log 0 = 0$;
   (d) nonation: we sometimes see just $H(A)$ or even $H(\rho)$.
2. Positivity: $H(A)_\rho \geq 0$ (because $0 \leq \lambda_i \leq 1$).
3. Entropy of pure states: $H(A)_{|\psi\rangle} = 0$ (because the density matrix has a single eigenvalue 1 for eigenvector $|\psi\rangle$).
4. Basis independence: $H(A)_\rho = H(A)_{U\rho U^\dagger}$ for unitaries U, because the eigenvalues are not affected by a change of basis.
5. Conditional entropy: $H(A|B)_\rho = H(AB)_\rho - H(B)_\rho$.
6. Strong subadditivity: $H(A|BC)_\rho \leq H(A|B)_\rho$. In other words, knowing more cannot hurt.

Exercise 9.1 Some properties of von Neumann entropy

In this exercise you have to prove some more properties of von Neumann entropy. The first one is rather surprising: if two systems share a pure state, then the entropy of each of the systems is the same, independently of their dimensions. In other words, if you have a pure state $|\psi\rangle$ in a system represented by the hilbert space $\mathcal{H}$, then you can decompose the system in two parts, $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$, in any way you want and the entropy of A will always be equal to the entropy of B, even if you choose to split $\mathcal{H}$ in a way such that $|\mathcal{H}_A| \ll |\mathcal{H}_B|$.

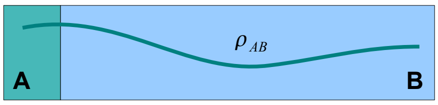

Figure 1: If ρ_{AB} is pure $H(A)_\rho = H(B)_\rho$, independently of dimensions of subsystems A and B.

To prove this, try writting a Schmidt decomposition of $|\psi\rangle$ (page 27 of the script). You should verify that the non-zero eigenvalues of the reduced state $\rho_A = \mathrm{Tr}_B(|\psi\rangle\langle\psi|)$ have to be the same as the eigenvalues of ρ_B. Then, if two operators share the same eigenvalues...
The next property studies two systems that are in a product state, $\rho_{AB} = \rho_A \otimes \rho_B$. The systems are independent of each other—whatever operations or measurements you perform on A will not affect ρ_B and vice-versa. In this non-correlated case one would expect that the uncertainty about the global state is just the sum of the uncertainty about the two local subsystems—and, for once, quantum mechanics respects common sense, with $H(AB) = H(A) + H(B)$.
To prove that property, you may start by expanding the reduced states in their eigenbases,

$$\rho_A = \sum_k \gamma_k |k\rangle\langle k|_A, \qquad \rho_B = \sum_\ell \lambda_\ell |\ell\rangle\langle \ell|_B.$$

Now expand the composed state $\rho_{AB} = \rho_A \otimes \rho_B$ in those bases and compute its entropy directly. The standard properties of the logarithm should give you the desired result.

In part b) we look at a special category of bipartite states, those that are classical on one of the subsystems. These states are introduced on pages 34–35 of the script. They have the form

$$\rho_{ZA} = \sum_z p_z |z\rangle\langle z|_Z \otimes \rho_A^z \tag{1}$$

for a fixed basis $\{z_Z\}_z$ of the first subsystem $\mathcal{H}_Z$ and a probability distribution $\{p_z\}_z$.
It help to look at one example of such a state. Consider two qubits, the computational basis and the classicaly correlated state

$$\rho_{ZA} = p\ |0\rangle\langle 0| \otimes \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} + (1-p)\ |1\rangle\langle 1| \otimes \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$$

Actually, the first system can be a classical bit, since no cross terms like $|0\rangle\langle 1|$ appear there. The reduced state of system A is just

$$\rho_A = \mathrm{Tr}_Z(\rho_{ZA}) = p\ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} + (1-p)\ \begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix},$$

and in general, for a hybrid classical-quantum state of the form of Eq. 1,

$$\rho_A = \sum_z p_z\ \rho_A^z.$$

The reduced state of the classical system is

$$\rho_Z = \mathrm{Tr}_A(\rho_{ZA}) = p(\alpha+\delta)\ |0\rangle\langle 0| + (1-p)(\alpha'+\delta')\ |1\rangle\langle 1|,$$

or, in general,

$$\rho_z = \sum_z p_z \mathrm{Tr}(\rho_A^z)\ |z\rangle\langle z|.$$

These hybrid states may be interpreted as "state ρ_A^z was prepared on system A with probability p_z, and in that case we have the pure state $|z\rangle\langle z|$ on system Z". A measurement on system Z performed in basis $\{z\}_z$ would allow us to determine which ρ_A^z had been prepared, because the total state would became $|z\rangle\langle z| \otimes \rho_A^z$. Since in that case the reduced state of A would be ρ_A^z, we call that the state of system A conditioned on the measurement outcome z of system Z, $\rho_A^z = \rho_{A|Z=z}$.
Let us now go back to the exercise. You are asked to prove that for states like that of Eq. 1,

$$\begin{aligned} H(AZ) &= H(Z)_\rho + \sum_z p_z\ H(A|Z=z) \\ &= H(Z)_\rho + \sum_z p_z\ H(A)_{\rho_A^z}. \end{aligned}$$

I suggest that you expand the matrices ρ_A^z in their eigenbases, for instance

$$\rho_A^z = \sum_k \lambda_k^z\ |k_z\rangle\langle k_z|.$$

If you now write ρ_{ZA} using those expressions for ρ_A^z and compute its entropy, you should get the desired result.
I won't help you in part b) 2. Part b) 3. asks you to show that for these states $H(Z|A) \geq 0$. One trick that may help is to imagine a system Y that is just a copy of Z and a state

$$\rho_{ZAY} = \sum_k p_z |z\rangle\langle z| \otimes \rho_A^z \otimes |y\rangle\langle y|.$$

You may check that the entropy of this state is the same than that of ρ_{AB}. In fact, you can show that $H(ZAY) = H(ZA)$ and $H(Z) = H(Y)$. Now use strong subaddivity to show what you want.

Exercise 9.2 Upper bound on von Neumann entropy

In this exercise you are going to use a long, sophisticated proof to show a very intuitive and otherwise easy to prove statement. You may ask: why?, and I may tell you: for the beauty/elegance/creativity/heck of it. The statement is the following: the entropy of a state of a system A with dimension $|A|$ is always less or equal to $\log |A|$. The intuition for this is simple: a mixed state of the form $\rho = \sum_k p_k |k\rangle\langle k|$ may be seen as "pure state $|k\rangle\langle k|$ was prepared with probability p_k"; entropy measures the uncertainty we have about what state was prepared; the worst case scenario happens when you have the fully mixed state, which corresponds to a uniform probability distribution of the possible pure states; the entropy of the fully mixed state is $\log |A|$. Now to our proof.

This proof is diveded in three parts. First you show that the entropy of the fully mixed state is what we want, $H(A)_{\frac{\mathbb{1}}{|A|}} = \log |A|$. This should be direct. Then you prove that this state may be written as $\frac{\mathbb{1}}{|A|} = \bar{\rho} = \int U\rho U^\dagger dU$, for any state ρ and where the integral is taken over all the unitaries U that can be applied on system A and dU is the Haar measure. I will give you a hand here. Finally you prove that $H(A)_\rho \leq H(A)_{\bar{\rho}}$.

Proving the second part is interesting. Here is a not-direct-at-all methotd, where you have to show that:

1. The fully mixed state is invariant under a change of basis, i.e. $V \frac{\mathbb{1}}{|A|} V^\dagger = \frac{\mathbb{1}}{|A|}$ for any unitary V.
2. The same is not true for any other state.
3. $\bar{\rho} = \int U\rho U^\dagger dU$ is invariant under a change of basis. To prove that use the property of the Haar measure $d(UV) = d(VU) = dU$.

To prove that $H(A)_\rho \leq H(A)_{\bar{\rho}}$ you are going to use the concavity result from the previous exercise, namely

$$\rho = \sum_k^0 p_k \sigma^k \quad \Rightarrow \quad H(A)_\rho \geq \sum_k^N p_k H(A)_{\sigma^k}, \qquad \{p_k\}_k \text{ probability distribution.}$$

Show that if that is true then in the limit $n \to \infty$, $p_k \to 0$ you can have

$$\rho = \int \sigma d\sigma \quad \Rightarrow \quad H(A)_\rho \geq \int H(A)_\sigma \, d\sigma, \qquad d\sigma \text{ any "good" measure,}$$

and replace $\int \sigma d\sigma$ by $\int U\rho' U^\dagger dU$.

By now you should have something like

$$H(A)_{\frac{\mathbb{1}}{|A|}} \geq \int H(A)_{U\rho U^\dagger} \, dU,$$

and getting what we want should be direct (look up the handy properties of the entropy if you are stuck).

Exercise 9.3 Quantum mutual information

All these exercises are simple and direct. You should be surprised with the result of the exercise about the cat state. Try to come with an intuition about why that should be true.