Quantum Information Theory
Tips 10

HS 12
Lea and Norm

Exercise 10.1 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).