Quantum Information Theory
Tips 6

HS 12
Lea and Norm

Preface: Recap of measurements on bipartite states

Suppose there is a state $\rho_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ and you want to perfom a measurement represented by the observable $O_A = \sum_y yP_y$ on subsystem A. Here $\{y\}_y$ are the eigenvalues of the operator and the projectors P_y have the form $P_y = \sum_\alpha |y^\alpha\rangle\langle y^\alpha|$, where $\{|y^\alpha\rangle\}_\alpha$ are the eigenvectors associated with eigenvalue y.
On the total system the measurement is represented by $O = O_A \otimes \mathbb{1}_B$. The probability of obtaining the outcome y is given by

$$\mathrm{Pr}_{O,\rho}(y) = \mathrm{Tr}([P_y \otimes \mathbb{1}_B]\rho_{AB})$$

and after the measurement (with outcome y) the state collapses to

$$\rho_B(y) = \frac{\mathrm{Tr}_A([P_y \otimes \mathbb{1}_B]\rho_{AB})}{\mathrm{Pr}_{O,\rho}(y)},$$

where Tr_A is the partial trace over subsystem A.

Exercise 6.1 Data hiding

Nah, there's enough information in the exercise sheet. This result means that to encode one bit of information with security ϵ (i.e., such that the agents' probability of successfully guessing the bit is just $1/2 + \epsilon$), you need a global system of approximately $4/\epsilon$ qubits (and give half the qubits to each agent). For instance, if you want $\epsilon = 1\%$, you need 400 qubits!

Exercise 6.2 Depolarizing channel (questions 2 and 3)

In this exercise we will see how to use quantum operations to define channels, which you surely remember from the second exercise series. The essential tools here are trace preserving completely positive maps (TCPMs). You can read all about them on pages 40 to 45 of the script. As the name suggests, TCPMs map positive operators to positive operators and preserve their trace — in particular they map density operators to density operators. The evolution of a system can always be represented by a TCPM: $\rho_{t_1} = \mathcal{E}(\rho_{t_0})$.
Let us examine the TCPM we are given in this exercise,

$$\mathcal{E}_p : \rho \mapsto \frac{p}{2}\mathbb{1} + (1-p)\rho,$$

where ρ is the density operator of a qubit. At first sight we notice that is redistributes the *weight* of the density operator: $1-p$ of it stays as before but p becomes fully mixed.
For now that channel seems maybe a bit abstract and that is why in part *a*) of the exercise we are asked to find a way of *implementing* it, ie. to express is in terms of operators qe know how to deal with — and in the case of qubits these will be Pauli matrices.
We have fo find an operator-sum representation of $\mathcal{E}_p$, meaning that we need to find operators $\{E_k\}_k$ such that

$$\frac{p}{2}\mathbb{1} + (1-p)\rho = \sum_k E_k \rho {E_k}^*.$$

My suggestion is that you start by using the Bloch sphere representation of qubits, $\rho = \frac{1}{2}(\mathbb{1} + \vec{r}\cdot\vec{\sigma})$ to express the identity in terms of Pauli matrices and ρ. Be careful with the properties of Pauli operators such as

$$\begin{aligned} {\sigma_i}^2 &= \mathbb{1} \\ [\sigma_i, \sigma_j] :&= \sigma_i\sigma_j - \sigma_j\sigma_i = 2 1 \varepsilon_{ijk}\sigma_k, \\ \{\sigma_i, \sigma_j\} :&= \sigma_i\sigma_j + \sigma_j\sigma_i = 2\delta_{ij}\mathbb{1}. \end{aligned}$$

You should obtain $\mathbb{1} = \frac{1}{2}(\rho + \sigma_x\rho\sigma_x + \sigma_y\rho\sigma_y + \sigma_z\rho\sigma_z)$.

Now insert that in the definition of $\mathcal{E}_p$ and in the end you should get

$$E_{\mathbb{1}} = \sqrt{1 - \frac{3p}{4}\mathbb{1}}, \qquad E_i = \frac{\sqrt{p}}{2}\sigma_i, \quad i = x, y, z.$$

Supposing that (eg. with a quantum computer) we know how to apply the Pauli matrices to a qubit, we are now able to implement $\mathcal{E}_p$.

In part *b*) they ask us what happens to the radius $|\vec{r}|$ of the Bloch vector of a state when we apply $\mathcal{E}_p$. Remember that the pure states lied on the surface of the sphere, with $|\vec{r}| = 1$, while the fully mixed state was in its centre, $|\vec{r}| = 0$. Check what happens to $|\vec{r}|$ (you don't need to use the operator-sum representation) and see what it means in terms of the purity of the state.

We can use TCPMs to describe channels — if you recall, sets of conditional probabilities that define maps from one probability distribution to another. In this case we will define it as

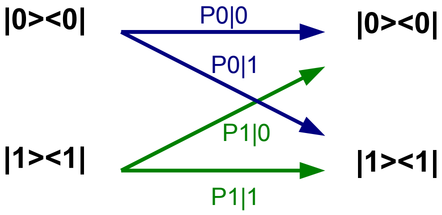

Figure 1: Our channel. Here $Pb|a$ stands for $P_{B|A=a}(b)$.

See what happens when you apply $\mathcal{E}_p(|0\rangle\langle 0|)$ and $\mathcal{E}_p(|1\rangle\langle 1|)$. You will get the conditional probabilities that define the channel from there if you look at the final states as ways of encoding probability distributions on $0, 1$. For instance, the state you obtain from $|0\rangle\langle 0|$ will be of the form of a *classical state* (pages 34-35 of the script),

$$\mathcal{E}_p(|0\rangle\langle 0|) = P_{B|A=0}(0)|0\rangle\langle 0| + P_{B|A=0}(1)|1\rangle\langle 1|.$$

More generally, you can apply $\mathcal{E}_p$ to the initial classical state $q|0\rangle\langle 0| + (1-q)|1\rangle\langle 1|$ and take the conditional probabilities from there.

Now that you have the channel defined in a classical way you can calculate its capacity just like in the second exercise series. What classical channel does it resemble?