CMSC 657: Introduction to Quantum Information Processing
Lecture 25

Instructor: Daniel Gottesman

Fall 2024

1 Examples of Quantum Channel Capacity

Example 1 (Dephasing Channel)**.** *The* dephasing channel *is* $\mathcal{D}_p(\rho) = (1-p)\rho + pZ\rho Z$*. It performs a* Z *gate with probability* p *and otherwise it leaves the state unchanged. Up to a basis change (by a Hadamard), the dephasing channel is equivalent to an essentially classical channel, the* binary symmetric channel*, which has a bit flip with probability* p*. Thus, classical codes in the Hadamard basis will suffice for the dephasing channel, just like the* 3*-qubit phase correcting code we saw before. A more rigorous analysis confirms that the quantum capacity for the dephasing channel is equal to the classical capacity of the binary symmetric channel, namely* $1 - h(p)$*, where* $h(x) = -x\log x - (1-x)\log(1-x)$*. Here,* $h(p)$ *is the entropy of the noise,* $nh(p) \approx \log \binom{n}{pn}$*.*

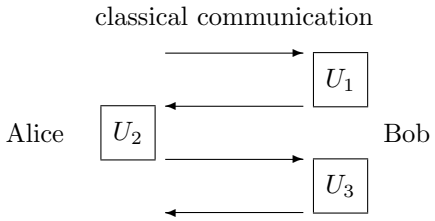
Example 2 (Depolarizing Channel)**.** *The* depolarizing channel *is* $\mathcal{C}_p(\rho) = (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$*. This is only slightly more complicated than the dephasing channel, but we don't know the capacity. The reason is this is a case where the coherent information is superadditive. If we calculate the single-shot coherent information (by maximizing only over states of the form* $\rho^{\otimes n}$ *in the formula for the channel capacity), we get the capacity* $1 - h(p) - p\log 3$*, where again* $h(x) = -x\log x - (1-x)\log(1-x)$*. Again,* $n(h(p) + p\log 3) \approx \log 3^{pn}\binom{n}{pn}$*. This rate can be achieved by essentially a random code. (It turns out that randomly chosen codes are quite good, albeit hard to decode efficiently.) However, we know that some non-random codes can do slightly better than this, and so the actual capacity of the depolarizing channel is still an open question.*

2 Measures of Entanglement

2.1 Entanglement Monotones

How do we measure how much entanglement is in a state? To discuss this, we generally consider a scenario where there are two or more parties who are spatially separated from each other. Let us consider *bipartite* entanglement, so there are only two people here, our old friends Alice and Bob. We want to distinguish entanglement from classical correlation, so we are not going to count as entanglement anything that Alice and Bob can do with classical resources. Certainly we want to consider the cases when Alice and Bob have quantum states, but if they have independent quantum states, that has no entanglement.

In particular, we don't want it to be possible to create entanglement via *LOCC* ("local operations and classical communication"). LOCC operations allow Alice and Bob to each do local CP maps by themselves and to do measurements and communicate with each other classically. The communications can go both ways.



A mixed state is unentangled if it can be created via LOCC.

Definition 1. *A mixed state ρ is* separable *if $\rho = \sum_i p_i \rho_{A,i} \otimes \rho_{B,i}$ for some $p_i > 0$, density matrices $\rho_{A,i}$, $\rho_{B,i}$. That is, it is separable if it can be written as a mixture of tensor product states.*

Note that any separable state can be created via LOCC: Alice chooses a random value of i with probability p_i. She sends it to Bob. Alice creates the quantum state $\rho_{A,i}$, Bob creates the quantum state $\rho_{B,i}$, and then both discard their records of i. Conversely, any state that they can create via LOCC must be separable: Consider the transcript of all the classical communication they do during the preparation protocol and use the full transcript as i. For any given i, there is some state held by Alice and Bob and it must be a tensor product state since they never did any joint quantum operations.

When we get to actually quantifying entanglement, there are some basic ground rules that a measure of entanglement should satisfy:

Definition 2. *An* entanglement monotone *is a function $f(\rho)$ from quantum states to non-negative real numbers with the following properties:*

1. *$f(\rho) = 0$ for unentangled states and $f(\rho) \neq 0$ for at least some entangled states.*
2. *$f((U_A \otimes U_B)\rho(U_A^\dagger \otimes U_B^\dagger)) = f(\rho)$.*
3. *$f(\rho)$ is non-increasing on average under LOCC.*

Property 1 indicates that the measure distinguishes entangled and non-entangled states. Because we conceive of entanglement as a property that is present non-locally in a basis independent way and can't be altered by local unitaries on Alice's or Bob's side, we need a good measure of entanglement to be invariant under local unitaries (property 2). Finally, since LOCC captures purely classical communication protocols, it should not be possible to increase the amount of entanglement we have this way, thus property 3.

We say that an entanglement monotone is *faithful* if $f(\rho) = 0$ implies that ρ is separable.

2.2 Entropy as a Measure of Entanglement

For a global pure state, we can look at the density matrix of Alice and calculate the entropy $S(A)$. This is equal to the entropy of Bob's density matrix $S(B)$. This quantity is known as the *entanglement entropy* of the state.

A separable pure state must be a tensor product state, and the marginal density matrix for a tensor product state is just another pure state. Thus, $S(A) = 0$ for a separable pure state. Conversely, if the pure state is entangled, Alice's state is *not* a pure state, and thus $S(A) > 0$. Local unitaries change Alice's density matrix, but they do not change its eigenvalues. Thus $S(\rho_A) = S(U_A \rho_A U_A^\dagger)$ and the entanglement entropy is unitarily invariant. In general, LOCC protocols will take a pure state to a mixed state, which we haven't talked about yet, but entropy seems like a good measure of entanglement for pure states. Indeed, in the problem set, you will see that the entanglement entropy properly quantifies how many maximally entangled states can be produced out of a pure entangled state, giving an operational justification of entropy as an entanglement measure. Indeed, it turns out that entanglement entropy is in some sense the unique correct measure of entanglement for pure states. (There are others but they can in general be related to the entanglement entropy.)

However, for global mixed states, the entanglement entropy no longer looks like a good candidate for a measure of entanglement. The entropy is still invariant under local unitaries, but it is no longer true that $S(A) = S(B)$, so we would have to pick either Alice or Bob to use as the preferred party to look at. In addition, purely classical states can have non-trivial entropy, including completely correlated states $\sum_i p_i |ii\rangle\langle ii|$ and tensor product mixed state $\rho_A \otimes \rho_B$. Thus, it is not true that $S(A) = 0$ for separable mixed states. Moreover, note that Alice's (and Bob's) density matrix for the separable state $\sum_i p_i |i\rangle|i\rangle$ is $\sum_i p_i |i\rangle\langle i|$, which is the same as Alice's (and Bob's) density matrix for the entangled pure state $\sum_i \sqrt{p_i}|ii\rangle$. Therefore, no property of Alice and Bob's density matrices by themselves can serve as a good measure of entanglement for mixed states — we need something that captures global properties.

2.3 Mixed State Entanglement

For mixed states, there are actually many possible sensible measures of entanglement. Unfortunately, they don't agree with each other. One strategy to find such measures is to think about operational measures by thinking up entanglement-related tasks.

One possibility is the *entanglement of formation*, which is the minimum amount of entanglement needed from which you can prepare ρ via LOCC:

$$E_f(\rho) = \min_{\{p_i, |\psi_i\rangle\}} \sum_i p_i S(\mathrm{Tr}_B |\psi_i\rangle\langle\psi_i|), \tag{1}$$

with the minimum taken over $\{p_i, |\psi_i\rangle\}$ such that $\sum_i p_i |\psi_i\rangle\langle\psi_i| = \rho$. That is, we make ρ out of a mixture of entangled states and average the entanglement entropies of the component entangled states. The entanglement of formation is the result for the best such decomposition.

It is not hard to see that $E_f(\rho)$ is an entanglement monotone. If we have a separable state, $E_f(\rho) = 0$, and if we have a pure entangled state, $E_f(\rho)$ is equal to the entanglement entropy of the pure state. Under local unitaries, we can just rotate the decomposition of ρ into states $|\psi_i\rangle$ by the same local unitaries and the entanglement entropy of the component pure states doesn't change. Thus, $E_f(\rho)$ doesn't change under local unitaries. In addition, E_f cannot increase under LOCC, since if σ can be reached from ρ, the best protocol to make σ via LOCC must at least as good (i.e., low on entanglement) as the best protocol to make ρ followed by the LOCC protocol to convert ρ to σ. Finally, E_f is faithful since we need some entangled states to make any non-separable state.

Unfortunately, not everything about the entanglement of formation is great. In particular, it is not *additive*:

$$E_f(\rho_{AB} \otimes \rho'_{AB}) \leq E_f(\rho_{AB}) + E_f(\rho'_{AB}). \tag{2}$$

There are cases where it is actually less, so you can save on the amount of entanglement you need to make a state by making other states at the same time. This means the entanglement of formation is not exactly a property of a state, but depends on the context in which you ask the question. In some cases, people will instead look at the *regularized* version, the *entanglement cost*:

$$E_c(\rho_{AB}) = \lim_{n\to\infty} \frac{1}{n} E_f(\rho_{AB}^{\otimes n}). \tag{3}$$

This is analogous to the regularized coherent information for the quantum channel capacity and is similarly impossible to calculate in most cases.

Another example of an operational entanglement measure is the *distillable entanglement*. Given a mixed state, suppose we process it by LOCC and try to get as many maximally entangled states as we can out of it on average. The maximum such value over all LOCC protocols is the distillable entanglement. This is clearly an entanglement monotone since it can't increase under LOCC, as we are already picking the best LOCC protocol. Again, the quantity is not additive, so frequently we regularize.

Note that the distillable entanglement is less than the entanglement of formation or the entanglement cost. It can't be greater, as if it were, we could increase the amount of entanglement we have through LOCC by building ρ and then running a distillation procedure on it. In most cases, the distillable entanglement

is strictly less. Indeed, there are some *bound entangled* states which have non-zero entanglement cost but 0 distillable entanglement. That is, they require entanglement to create, but you can't get any perfect (or almost-perfect) entanglement out of them.