Lecture 11, Tues Feb 21: Quantifying Entanglement, Mixed State Entanglement

How do you quantify how much entanglement there is between two quantum systems?

It's worth noting that we sort of get to decide what we think a measure of entanglement *ought* to mean. We've seen how it can be useful to think of entanglement as a resource, so we can phrase the question as "how many 'Bell pairs of entanglement' does a given state correspond to?"

A priori, there could be different, incomparable kinds of entanglement that are good for different things. And that's actually the case for entangled mixed states, or entangled pure states shared by three or more parties. But for the special case of an entangled pure state shared by two parties, Alice and Bob, it turns out that there's a single measure of entanglement, which counts "the number of Bell pairs needed to form this state, and equivalently the number that can be extracted from it."

So, given $\sum_{ij} \alpha_{ij} |i\rangle_A |j\rangle_B$, how do we calculate many Bell pairs it's worth?

Our first observation here is that given any bipartite state, you can always find a change of basis on Alice's side, and another change of basis on Bob's side, that puts the state into the simpler form

$$\sum \lambda_i |v_i\rangle |w_i\rangle,$$

where all $|v_i\rangle$'s are orthonormal, and all $|w_i\rangle$'s are also orthonormal. To put the state into this form, we use a tool from linear algebra called…

Schmidt Decomposition

Given a the matrix $A = \begin{bmatrix} \alpha_{11} & & \alpha_{1n} \\ & \ddots & \\ \alpha_{n1} & & \alpha_{nn} \end{bmatrix}$ representing the entire quantum state.

We can multiply A by two unitary matrices, one on each side, to get a diagonal matrix:

$$UAV = \Lambda$$

U and V can be found efficiently using linear algebra

U and V represent the changes of basis that Alice and Bob respectively would need to apply, in order to get their state into the Schmidt form

$$\sum \lambda_i |v_i\rangle |w_i\rangle.$$

Measuring in the $\{|v_i\rangle, |w_i\rangle\}$ basis would then yield the probability distribution

$$\begin{bmatrix} |\lambda_1|^2 \\ \vdots \\ |\lambda_n|^2 \end{bmatrix}$$

Now, recall that, for a classical probability distribution $D = (p_1, \ldots, p_n)$, its **Shannon entropy** is

$$H(D) = \sum_{i=1}^{n} P_i \log_2 \frac{1}{P_i}$$

So now we just need to calculate the ordinary Shannon entropy of our probability vector,

$$\sum_i |\lambda_i|^2 \log \frac{1}{|\lambda_i|^2},$$

in order to figure out how many Bell pairs our state is equivalent to.

To come at it a bit differently: there's a measure called **von Neumann entropy**, which generalizes Shannon entropy from classical probability distributions to quantum mixed states. We say that the von Neumann entropy of a mixed state ρ is

$$S(\rho) = \sum_{i=1}^{n} \lambda_i \log_2 \frac{1}{\lambda_i}$$

You could also say that von Neumann entropy *is* the Shannon entropy of the vector of eigenvalues of the density matrix of ρ. If you diagonalize the density matrix, the diagonal represents a probability distribution over n possible outcomes, and taking the Shannon entropy of *that* distribution gives you the von Neumann entropy of your quantum state.

Yet another way to think about it:

Say you looked at all the possible probability distributions, that could arise by measuring the mixed state ρ in all possible orthogonal bases. Then the von Neumann entropy of ρ is the *minimum* of the Shannon entropies of all those distributions.

$$S(\rho) = min_U \left\{ H(diag(U\rho U^\dagger)) \right.$$

where $diag(A)$ means the length-n vector obtained from the diagonal of the $n \times n$ matrix A.

So the von Neumann entropy of any pure state $|\Psi\rangle\langle\Psi|$ is 0, because there's always some measurement basis (namely, a basis containing $|\Psi\rangle$) that returns a definite outcome.

You could choose to measure $|+\rangle$ in the $\{|0\rangle, |1\rangle\}$ basis and you'll have complete uncertainty, and an entropy of 1. But if you measure $|+\rangle$ in the $\{|+\rangle, |-\rangle\}$ basis, you have an entropy of 0, because you'll always get the outcome at $|+\rangle$.

So $S(|\Psi\rangle\langle\Psi|) = 0$.

By contrast, the von Neumann entropy of the maximally mixed state, $\frac{I}{2}$, is 1.

Similarly, the von Neumann Entropy of the n-qubit maximally mixed state is n.

We can now talk about how much *entanglement entropy* is in a bipartite pure state.

Entanglement Entropy

Suppose Alice and Bob share a bipartite pure state $|\Psi\rangle = \sum_{i,j} \alpha_{ij} |i\rangle_A |j\rangle_B$

To quantify the entanglement entropy, we'll trace out Bob's part, and look at the von Neumann entropy of Alice's side, $S(\rho_A)$, in effect asking: if Alice made an optimal measurement, how much could she learn about Bob's state?

$$S(\rho_A) = S(\rho_B) = H\{\lambda_i\}$$

↑ This is the Shannon entropy of the vector of eigenvalues, which you can get by diagonalizing Alice's (or Bob's) density matrix, *or* by putting $|\Psi\rangle$ in Schmidt form, as we did in the previous lecture.

The entanglement entropy of any product state, $|\Psi\rangle \otimes |\Phi\rangle$, is 0.
The entanglement entropy of a Bell pair, $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, is 1.

You can think of entanglement entropy as either:

- The number of Bell pairs it would take to create the state
- The number of Bell pairs that you can extract from the state

It's not immediately obvious that these two values are the same, but for pure states, they are. (For mixed states, they need not be!)

A sample calculation...
Let $|\Psi\rangle = \frac{3}{5}|0\rangle_A|+\rangle_B + \frac{4}{5}|1\rangle_A|-\rangle_B$

This state is already in Schmidt form (otherwise, we'd have to put it in that form)

Then the entanglement entropy is

$$E = (\tfrac{3}{5})^2 \log_2(\tfrac{5}{3})^2 + (\tfrac{4}{5})^2 \log_2(\tfrac{5}{4})^2$$
$$= \;\sim .942$$

This means that if Alice and Bob shared 1000 copies of $|\Psi\rangle$, they'd be able to teleport about 942 qubits.

For bipartite *mixed* states, by contrast, there are two values to consider:

The Entanglement of Formation $E_F(\rho_{AB})$

is the number of ebits that Alice and Bob need to create one copy of the state ρ_{AB}, in the limit where they're creating many copies of it, and assuming they're allowed unlimited local operations and classical communication (called "LOCC" in the lingo) for free

The Distillable Entanglement $E_D(\rho_{AB})$

is the number of ebits that Alice and Bob can extract per copy of ρ_{AB}, again in the limit where they're given many copies of it, and assuming local operations and classical communication are free

Clearly $E_F \geq E_D$, since if you could ever get out more entanglement than you put in, it would give you a way to increase entanglement arbitrarily using LOCC, which is easily seen to be impossible. But what about the other direction?

It turns out that there exist bipartite pure states for which $E_F \gg E_D$, which is to say that those states take a lot of entanglement to make, but then you can only extract a small fraction of the entanglement that you put in. We won't have time to explain this in more detail.

We call a bipartite mixed state ρ_{AB} *separable* if there's any way to write it as a mixture of product states:

$$\rho_{AB} = \sum_i p_i |v_i\rangle\langle v_i| \otimes |w_i\rangle\langle w_i|$$

A mixed state is called entangled if and only if it's not separable.

This is subtle: it sometimes happens that a density matrix looks entangled, but there's some weird decomposition that shows that no, actually it's separable.

And indeed, in 2003 Leonid Gurvits proved a pretty crazy fact:

If you're given as input a density matrix ρ_{AB} for a bipartite state, then deciding whether ρ_{AB} represents a separable or entangled state is an NP-hard problem!

As a result, unless P = NP, there can be no "nice characterization" for telling apart entangled and unentangled bipartite mixed states—in contrast to the situation with bipartite pure states.

This helps to explain why there are endless paper writing opportunities in trying to classify different types of entanglement…