Notes 8.370/18.435 Fall 2021

Lecture 16 Prof. Peter Shor

The Nobel Prize in Physics was given out Tuesday. On Wednesday, in honor of that, we explained the GHZ paradox, one of the many things that Anton Zeilinger won the Nobel Prize for on Tuesday. This paradox is named for its discoverers, Greenberger, Horne, and Zeilinger.

After that, we talked about quantum super-dense coding.

The GHZ paradox can be viewed as a game. It wasn't at first, but computer scientists love putting things in terms of games, because this has been a very fruitful way of thinking about several aspects of computer science. So when computer scientists started looking at quantum paradoxes, this was a natural way to view them.

This game is played by three players, Alice, Bob, and Carol, who are all cooperating, and a referee who plays randomly. Alice, Bob, and Carol cannot communicate once the game starts, but they can meet beforehand and agree on a strategy. The referee gives Alice, Bob, and Carol each a bit, which is either an X and a Y. He always gives an odd number of Xs, so either there are three Xs or one X and two Ys. More specifically, he gives the three players XXX, YYX, YXY, and CYY with equal probabilities.

When the players get these bits, they have to give a bit back to the referee, which will either be a $+$ or a $-$. The referee looks at the bits he receives, and decides whether the players win. The rule is that if all three players get an X, they must return an odd number of $+$s. However, if two players get a Y and one an X, the must return an even number of $+$s.

Can the players win this game with a classical strategy? The answer is "no", they can only win $3/4$ of the time. One way they can do this is to always return an even number of Xs, so for instance they could all return Ys. Then they win unless the referee gives them XXX, which only happens $1/4$ of the time.

Why can't the players do better? Let's consider what happens when they use a deterministic strategy. It's fairly easy to use probability theory to show that a probabilistic strategy cannot do better than a deterministic one, but we won't include the proof in these notes.

So what is a deterministic strategy? It's a table telling what each of Alice, Bob, and Carol will return if the referee gives them an X or a Y. For example, this might be the strategy:

player	X	Y
A	$+$	$-$
B	$+$	$-$
C	$+$	$+$

In this strategy, if they get XXX, they return $+++$, so they win. If they get XYY they return $+-+$, so they win. Similarly, if they get YXY, they return $-++$, so they win. But if they get YYX, they return $--+$, so they lose.

So let's consider the strategy table.

player	X	Y
A	a	d
B	b	e
C	c	f

There are only four possible challenges the referee can give the players, XXX YYX, YXY, XYY. The players' responses to these are abc, dec, dbf, aef, respectively. They must return an odd number of $+$s in one case, and an even number of $+$s in the other three. Thus, the responses abc, dec, dbf, aef, must contain an odd number of $+$s altogether. However, this is impossible, since each letter appears exactly twice in the sequence abc, dec, dbf, aef, so no matter how you assign $+$ and $-$ to the letters, the total number of $+$s is even.

Now, how can they win with by using quantum mechanics? What they do is share what is called a GHZ state before the game. This is the state $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. Then each of the players measures the state in either the x or the y basis, depending on whether they were given on X or a Y.

Suppose they were given three X's. Then the probability they measure $|+++\rangle$ is

$$\frac{1}{\sqrt{2}^4}(\langle 0| + \langle 1|)(\langle 0| + |1\rangle)(\langle 0| + |1\rangle)(|000\rangle + |111)\rangle = \frac{1}{4}(1+1)$$

You can see that there are only two terms that appear in the final sum: $\langle 0|\langle 0|\langle 0|000\rangle$ and $\langle 1|\langle 1|\langle 1|111\rangle$, and they both contribute $\frac{1}{4}$ to the amplitude. The amplitude is thus $\frac{1}{2}$, and the probability of getting this oucome is its square, $\frac{1}{4}$. Similarly, the probability of getting the outcome $|+--\rangle$ is

$$\frac{1}{\sqrt{2}^4}(\langle 0| + \langle 1|)(\langle 0| - |1\rangle)(\langle 0| - |1\rangle)(|000\rangle + |111)\rangle = \frac{1}{4}(1+1),$$

because the two -1 coefficients from the two $|-\rangle$ multiply to give $+1$. However, if we have just one $-$, as in $|+-+\rangle$, then the amplitude coming from the term $|111\rangle$ would be -1, and the amplitude from the term $|000\rangle$ would still be 1. Adding these gives 0 meaning that the probability of seeing exactly one $-$ is 0.

It is fairly easy to see that if the players were given XYY, then the chance of seeing $+++$ is

$$\frac{1}{\sqrt{2}^4}(\langle 0| + \langle 1|)(\langle 0| + i\,|1\rangle)(\langle 0| + i\,|1\rangle)(|000\rangle + |111)\rangle = \frac{1}{4}(1-1),$$

as the two i's multiply to give -1. Thus the probability of seeing $|+++\rangle$ is 0. You need an even number of $+$s in an outcome to get $1+1$, and thus a chance of seeing that outcome.

Thus, if they are allowed to share a GHZ state, the players can measure it and win with probability 1.

Now, we will talk about superdense coding. Recall that last time, we talked about quantum teleportation. If the sender and receiver share entanglement, they can send

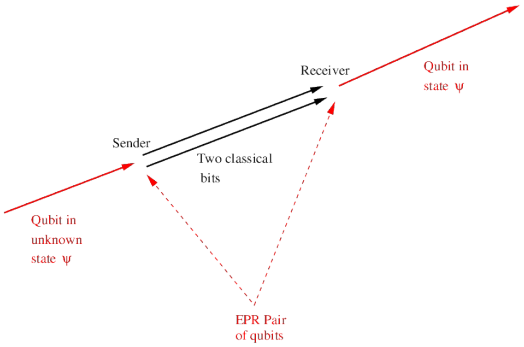

Figure 1: teleportation

one qubit from the sender to the receiver by encoding it using two classical bits. One can represent teleportation schematically as follows:

Here, as we saw last class, if the sender and receiver each hold one qubit in an EPR pair $\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$, the send can make a joint measurement on the unknown qubit $|\psi\rangle$ and her half of the EPR pair, and send the results of the measurement to the receiver. The receiver can apply a Pauli matrix to his half of the EPR pair to recover $|\psi\rangle$.

Superdense coding is the converse process; the send and receiver can send two classical bits using one quantum bit. A schematic representation of this process is:

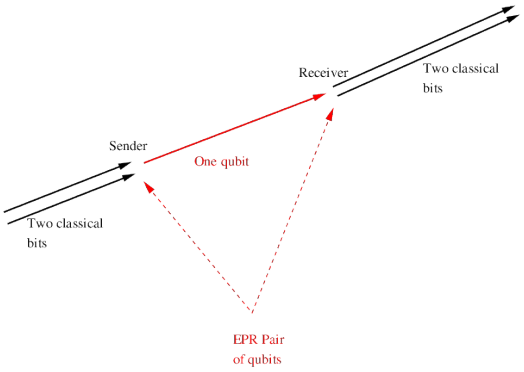

Figure 2: superdense coding

As we will see, for superdense coding, the sender encodes using the same process the receiver uses to decode in teleportation, and the receiver decodes using the process the sender uses to encode in teleportation.

How does the process work? Recall the Bell basis is four entangled states, and can

be obtained from the state $|00\rangle + |11\rangle$ by applying a Pauli matrix. We have:

$$\begin{aligned}
&\frac{1}{\sqrt{2}}\big(\,|00\rangle + |11\rangle\,\big) \\
&\frac{1}{\sqrt{2}}\big(\,|00\rangle - |11\rangle\,\big) = \frac{1}{\sqrt{2}}(\sigma_z \otimes I)\big(\,|00\rangle + |11\rangle\,\big) \\
&\frac{1}{\sqrt{2}}\big(\,|01\rangle + |10\rangle\,\big) = \frac{1}{\sqrt{2}}(\sigma_x \otimes I)\big(\,|00\rangle + |11\rangle\,\big) \\
&\frac{1}{\sqrt{2}}\big(\,|01\rangle - |10\rangle\,\big) = \frac{1}{\sqrt{2}}(\sigma_z\sigma_x \otimes I)\big(\,|00\rangle + |11\rangle\,\big)
\end{aligned}$$

Thus, Alice can convert the EPR pair she shares with Bob to any one of the Bell basis states. When she sends her qubit to Bob, he measures in the Bell basis, and gets one of four values, giving him two classical bits. So superdense coding works.

You can also use superdense coding to show that teleportation is optimal. Even with an arbitrarily large number of Bell pairs, you cannot send a qubit using fewer than two classical bits. Why not? Suppose you could find a protocol that sent a qubit using 1.9 classical bits on average. Then, encoding two classical bits using superdense coding, and encoding the resulting qubit with the improved teleportation protocol, you could send 2 classical bits using entanglement and 1.9 classical bits on average. Repeating this k times, for large n you could send n classical bits using $(0.95)^k n$ classical bits on average. While we won't prove it in class, Shannon's channel capacity theorem shows that this in turn would let you send classical information faster than the speed of light using just entanglement, which we assume is impossible from Einstein's theory of relativity.