CSE 599d - Quantum Computing
Quantum Entanglement and Bell's Theorem

Dave Bacon
Department of Computer Science & Engineering, University of Washington

...contemporary physicists come in two varieties. Type 1 physicists are bothered by EPR and Bell's Theorem. Type 2 (the majority) are not, but one has to distinguish two subvarieties. Type 2a physicists explain why they are not bothered. Their explanations tend either to miss the point entirely (like Born's to Einstein) or to contain physical assertions that can be shown to be false. Type 2b are not bothered and refuse to explain why. —David Mermin

Today we get to talk about one of my favorite subjects, quantum entanglement. I've been dreaming about quantum entanglement for so long now that I sometimes forget how really truly marvellous it is. I came to entanglement in the similar route that many take to the subject: it was presented as the premiere example in physics of a result which defies our common notions of how the world should work. Because entanglement challenges our common sense, it acquired a reputation among physicists as a little taboo. This was probably a tragedy, in retrospect, since we now know that quantum entanglement seems to play a central role in quantum information science. Indeed there is a real way in which quantum entanglement is the *fuel* which powers quantum computers.

I. THE GHZ GAME

We will begin our study of the strangeness of entanglement with a simple game.

Alice, Bob, and Charlie, while out looking for Dave one day, found themselves trapped at the hands of an evil Wizard (the details of how this came to be are not relevant to us.) The Wizard was evil because he liked to play games with his captives. But he wasn't so evil that he liked to play games that always resulted in the captives losing. On this day he decided to play the following game with his three captives. The three captives would be locked away in three separate rooms, without the ability to communicate with each other. The Wizard would then come around and give each of the captives a slip of paper with the letter X or Y written on the slip. At midnight, the captives are then to shout out either the value $+1$ or the value -1. The Wizard explains to the captives that he either two of them have received Y's on their slips of paper or none of them have received Y's. The captives will win the game and be released if, when they are all given slips with X on them, the product of what they shout out is $+1$, and if two of them were given Y slips, then the product of what they shout out must be -1. Or to write it all down symbolically, there are four possible combinations of the papers on the slips, $\{XXX, XYY, YXY, YYX\}$, and the products of what they shout must be $\{+1, -1, -1, -1\}$ for these corresponding slips. Now Alice, Bob, and Charlie are all told the rules to this game. They are allowed to conspire before they are locked away, but after they are locked away they are not allowed to communicate to each other. The question about this game we would like to answer is whether it is possible for Alice, Bob, and Charlie to devise a strategy to always win this game?

First let's consider protocols where Alice, Bob, and Charlie act deterministically, and don't ever conspire beforehand. In such a situation, each party can only act dependent on what slip the Wizard gives them. Thus we can specify such strategies by specifying how each party would act (what it would shout) dependent on what it receives from the Wizard. Let A_X denote what Alice will shout if the Wizard gives her slip X. Similarly let A_Y denote what Alice will shout if the Wizard gives her slip Y. Finally, we can define analogous variables for what Bob would say, B_X and B_Y, and for Charlie would say, C_X and C_Y, given that they receive a slip with X or Y respectively. Note that each of these variables is either $+1$ or -1. Now if the Wizard gives all three parties Xs then the product of what Alice, Bob, and Charlie shout will be $A_X B_X C_X$. Similarly if the Wizard gives Alice and Bob a Y and Charlie a X, then the product what they will shout is $A_Y B_Y C_X$. We can construct similar products for the remaining two cases. Now let's assume that there is a winning strategy for this game. This implies that

$$\begin{aligned} A_X B_X C_X &= +1 \\ A_Y B_Y C_X &= -1 \\ A_Y B_X C_Y &= -1 \\ A_X B_Y C_Y &= -1 \end{aligned} \tag{1}$$

But now notice that there is a contradiction! Multiply all of the left hand sides of these equations. You will obtain $A_X^2 A_Y^2 B_X^2 B_Y^2 C_X^2 C_Y^2$. But since each variable is either $+1$ or -1, this is just $+1$. But now multiply all of the right hand

sides of these equations. You get -1. So there is a contradiction! Thus there cannot exists ± 1 valued observables satisfy these equations and hence always win the game! Thus there is no way for Alice, Bob, and Charlie to always guarantee that they will win this game.

What about if they decided to use probabilities in their strategies (we still do not let them conspire beforehand about what they will do, at least not yet.) Well no consider, say Alice's strategy given that she receives slip X. She will now decide to output $+1$ and -1 with certain probabilities. Let $\langle A_X \rangle$ denote the expected value of what Alice outputs. Now the parties aren't allowed to communicate with each other, so for each variable we can be assign an independent expected value. Then, since each variable is independent of each other, the expectation values will satisfy the same equations as the ones we had above:

$$\begin{aligned} \langle A_X \rangle \langle B_X \rangle \langle C_X \rangle &= +1 \\ \langle A_Y \rangle \langle B_Y \rangle \langle C_X \rangle &= -1 \\ \langle A_Y \rangle \langle B_X \rangle \langle C_Y \rangle &= -1 \\ \langle A_X \rangle \langle B_Y \rangle \langle C_Y \rangle &= -1 \end{aligned} \tag{2}$$

And this once again leads to a contradiction. Why? Because now each of the expectations are numbers between -1 and 1, such that when we square them they are positive. This implies that the product of the left hand sides of these equations is positive. But the product of the right hand sides of these equation is -1. Which is a contradiction.

Now what about if the parties are allowed to conspire before hand and to use probabilities whenever they want. Well whatever they do before hand cannot depend on the value of the slips of paper they will be given. Suppose that they do things like flip coins and agree on strategies, and such. Then everything they do can be written in terms of conditions on some extra variables, lets just call the h. Now we can allow probabilities here as well. In particular we can let these extra variables occur with probability $p(h)$. Let $A_X(h)$ denote the output of Alice given that she received slip X and the extra variables the parties used had value h. Define similar variables for the other parties and other slips they could receive. Notice that everything that is probabilistic about a strategy can always be moved to the very beginning of the protocol, even procedures which the parties do independent of each other. Thus what we are considering now is the most general setting these parties can consider. Now in order for the parties to always win the game, it must be true that

$$\begin{aligned} \sum_h p(h) A_X(h) B_X(h) C_X(h) &= +1 \\ \sum_h p(h) A_Y(h) B_Y(h) C_X(h) &= -1 \\ \sum_h p(h) A_Y(h) B_X(h) C_Y(h) &= -1 \\ \sum_h p(h) A_X(h) B_Y(h) C_Y(h) &= -1 \end{aligned} \tag{3}$$

Now since the $p(h)$s are probabilities, in order for the parties to always win it must be true that for a particular variable h, these equations must be satisfied. Thus

$$\begin{aligned} A_X(h) B_X(h) C_X(h) &= +1 \\ A_Y(h) B_Y(h) C_X(h) &= -1 \\ A_Y(h) B_X(h) C_Y(h) &= -1 \\ A_X(h) B_Y(h) C_Y(h) &= -1 \end{aligned} \tag{4}$$

But this again leads to a contradiction (or to lots of them!)

Thus we see that there is no possible way for Alice, Bob, and Charlie to always win this game. Poor them. But wait? What we've discussed so far was only within the confines of our classical world. So we had probabilities for different variables and such. But what if we move to the quantum world? Then the variables we share might have amplitudes instead of probabilities. Surely this should change anything, should it? Well looking at our impossibility proof for the most general case we considered, we might get a little uncomfortable.

And indeed, we would be right to feel discomfort. There is a way for Alice, Bob, and Charlie to win this game if, when they get together to conspire a strategy, they distribute an entangled quantum system between them and use this entangled quantum system in the game.

Let's see how this works. Suppose that Alice, Bob, and Charlie each share one part of the tripartite quantum state

$$|\Upsilon\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{5}$$

This state is called the GHZ state after Greenberger, Horne, and Zeilinger, who must famously noted its strange properties. Now Alice, Bob, and Charlie share this state and go back to their cells. The Wizard comes along and gives them a slip with X or Y on it. What the parties do now is that if they are given an X, they measure their part of the GHZ in the $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ basis (the eigenstates of the Pauli X operator) and if they get outcome $|+\rangle$, then they say $+1$ and if they get outcome $|-\rangle$, then they say -1. Similarly if they are given an Y, they measure their part of the GHZ in the $|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$, $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$ basis (the eigenstates of the Pauli Y operator) and if they get outcome $|+i\rangle$, then they say $+1$ and if they get outcome $|-i\rangle$, then they say -1. (Okay it was a setup, the Wizard was telling them what basis to measure in!) Now what happens. Well let's calculate the probabilities!

Well start calculating away. First note that

$$\begin{aligned}(\langle +| \otimes \langle +| \otimes \langle +|)|\Upsilon\rangle &= \frac{1}{2} \\ (\langle +| \otimes \langle +| \otimes \langle -|)|\Upsilon\rangle &= 0\end{aligned} \tag{6}$$

The first of these can be seen by notating that $|+\rangle$ contains an equal superposition of bitstrings all with equal amplitudes. The second of these can be seen by noting that the presence of $|-\rangle$ means that there will be a cancelation. In fact it is not hard to convince yourself that

$$(\langle +| \otimes \langle +| \otimes \langle +|)|\Upsilon\rangle = (\langle +| \otimes \langle -| \otimes \langle -|)|\Upsilon\rangle = (\langle -| \otimes \langle +| \otimes \langle -|)|\Upsilon\rangle = (\langle +| \otimes \langle -| \otimes \langle -|)|\Upsilon\rangle = \frac{1}{2} \tag{7}$$

By similar calculations, we can calculate that

$$(\langle -| \otimes \langle -| \otimes \langle -|)|\Upsilon\rangle = (\langle +| \otimes \langle +| \otimes \langle -|)|\Upsilon\rangle = (\langle +| \otimes \langle -| \otimes \langle +|)|\Upsilon\rangle = (\langle -| \otimes \langle +| \otimes \langle +|)|\Upsilon\rangle = \frac{1}{2} \tag{8}$$

Thus we see that when all three parties measure in the X basis, and they follow the protocol, then the product of their outputs will always be $+1$. Why? Because the amplitudes for the measurement outcomes corresponding to an odd number of $|-\rangle$ states are all zero.

Now what happens if Alice and Bob measure in the $|\pm i\rangle$ basis, and Charlie measures in the $|\pm 1\rangle$ basis? In this case, Well start calculating away. First note that

$$|+i\rangle \otimes |+i\rangle \otimes |+1\rangle = \frac{1}{2\sqrt{2}}(|0\rangle + i|1\rangle) \otimes (|0\rangle + i|1\rangle)(|0\rangle + |1\rangle) \tag{9}$$

From which we can calculate that

$$(\langle +i| \otimes \langle +i| \otimes \langle +|)|\Upsilon\rangle = 0 \tag{10}$$

Now we see that the all $+1$ output for this case never occurs. Similar calculations yield

$$(\langle +i| \otimes \langle +i| \otimes \langle +|)|\Upsilon\rangle = (\langle +i| \otimes \langle -i| \otimes \langle -|)|\Upsilon\rangle = (\langle -i| \otimes \langle +i| \otimes \langle -|)|\Upsilon\rangle = (\langle +i| \otimes \langle -i| \otimes \langle -|)|\Upsilon\rangle = 0 \tag{11}$$

and

$$(\langle -i| \otimes \langle -i| \otimes \langle -|)|\Upsilon\rangle = (\langle +i| \otimes \langle +i| \otimes \langle -|)|\Upsilon\rangle = (\langle +i| \otimes \langle -i| \otimes \langle +|)|\Upsilon\rangle = (\langle -i| \otimes \langle +i| \otimes \langle +|)|\Upsilon\rangle = \frac{1}{2} \tag{12}$$

Thus we see that in this case the products of all the parties outputs will be -1. The GHZ state is symmetric under exchange of the parties, so this means that the other cases where two parties measure in the Y basis will result in the product of their outputs being -1.

So we see that by using an entangled quantum state, namely the GHZ state, the three parties can always beat the evil Wizard (who did not know quantum theory when he was setting up the game and is thus foiled: always know quantum mechanics before you play a game.)

Now this is rather strange. Why? Because we have allowed the parties to plan, classically before hand. And these plans can involve things like distributing random numbers and establishing, what we might call classical correlations. Thus it seems strange that we can allow all sorts of classical protocols, just as long as there isn't any talking after the parties are given their slips of paper, and not win the game, but if we allow them to share these quantum entangled states, then they can win the game. In fact, as we shall now discuss, this means that quantum theory cannot be equivalent to a certain type of classical theory. And for quantum computing this means that quantum devices cannot be simulated by certain classical devices.

II. THE EINSTEIN, PODOLSKY, AND ROSEN ARGUMENT

Those who are not shocked when they first come across quantum mechanics cannot possibly have understood it. - Niels Bohr

It's best, actually, to start our story with Einstein and Bohr. Both Einstein and Bohr were essential to the early development of quantum theory. However, they later had very differing views on quantum theory. The debate that Einstein and Bohr had, beginning with the 1927 Solvay conference, is one of the legendary debates of the early history of quantum theory. On the one side was Neils Bohr, and his complementary principle which asserts that quantum theory predicts different behaviors depending on the way in which we observe the system and that there was a simple consistent way to talk about quantum theory, which is today known under the moniker of the Copenhagen interpretation of quantum theory. On the other side was Albert Einstein, who position was not that quantum theory was wrong, but that there must exist a deeper theory, a more complete theory, which could explain quantum theory and which did not suffer from the strange behaviors that occur when we try to interpret quantum theory in a classical manner.

Important for us in this debate was the 1935 paper of Einstein, Podolsky, and Rosen (EPR). In this paper, EPR put forth what they considered a very strong argument that quantum theory was incomplete. Here we'll review the original EPR argument, mostly for the culture.

EPR were concerned with two propositions

1. Quantum theory is complete.

2. Incompatible observables cannot be simultaneous elements of reality.

The first of these propositions is the question of whether there is a deeper (classical) theory or whether quantum theory will be the final say on such question (the later would mean that quantum theory is complete.) The second of these propositions is whether, when we measure a quantity, we are actually revealing the value of some basic real data about the system. EPR begin their argument by showing that only one of these two propositions can hold. This is rather straightforward: if quantum theory is complete, then it must be possible to make measurements which reveal all of this complete theory and there can be no incompatible observables. Similarly if incompatible observables cannot have simultaneous reality, then there are elements of reality not described by quantum theory and thus quantum theory must be incomplete.

The second part of the EPR argument is more interesting (at this point EPR have just made a few, fairly obvious assertions.) We won't follow EPRs original argument, but instead us a similar argument using qubits. Let's examine the singlet state where Alice has one of the qubits and Bob has the other qubit,

$$|\psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{13}$$

Now suppose that Alice measures here qubit in the $|0\rangle$, $|1\rangle$ basis. Then we know that if Bob measures his qubit in the same basis, given Alice's outcome, we will be able to predict Bob's measurement outcome. Thus we might assert that there is an element of reality corresponding to measurement in this basis. But now suppose that Bob, instead of measuring in the $|0\rangle$, $|1\rangle$ basis, instead decides to measure in the $|+\rangle$ and $|-\rangle$ basis. He will get either state with 50 percent probability. But nonetheless a measurement in this basis will let us determine an element of reality corresponding to $|+\rangle$ and $|-\rangle$. Thus it seems that there must be two elements of reality revealed in this experiment. One corresponding to measurement in the $|0\rangle$, $|1\rangle$ basis, and other corresponding to the $|+\rangle$, $|-\rangle$ basis. But we know that the these measurements, on a single qubit system, cannot ever be simultaneously measured (because the measurement operators do not commute.) So it seems that this contradicts 2. Thus 1 must be true.

So what should we think about this argument. Well the first thing we should check about are the assumptions that went into this argument. The first of these is that at the time that Alice makes a measurement, Bob's system has a reality independent of Alice's system. This is an assumption of the separability of the idea of elements of reality. The second assumption is that of locality, that nothing changes about Bob's system when Alice makes his measurement. In particular we are not talking about Bob's system changing in way of it's measurements outcomes, but in terms of what it's elements of reality are. Both of these assumptions can (and have) been challenged in EPRs argument.

So, while EPR raised an interesting argument for whether quantum theory was complete or not, their argument was not so convincing given the assumptions which lead up to it.

III. BELL'S THEOREM AND THE CHSH INEQUALITY

The next person to step onto the stage, is John Bell. John Bell was fascinated by the EPR experiment and felt that Einstein was indeed onto something in his argument. After the EPR paper, various lines of argument, most famously due to von Neumann, were put for to show that quantum theory must be a complete theory and that there could be no deeper description of quantum theory. However, in 1952, David Bohm produced a theory which had many of the properties which von Neumann's proof asserted could not exist. This state of affairs led John Bell to consider the question taken up in the EPR paper anew, and to make a startling discovery in 1964.

Bell considered the following situation. Suppose that Alice and Bob were together at some point in the past, interacted, and produced a singlet state $|\psi_-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Alice now takes one of these qubits back to her lab, where she can make measurements on it and bob takes the other qubit and takes it back to his lab, where he can make measurements on it. Alice and Bob have lots of patience, so they will do this multiple times, and can obtain sufficient statistics for different measurements on this state $|\psi_-\rangle$.

Now suppose that we wanted to find a more complete theory explaining these quantum experiments (which we haven't described completely, but we'll get to that.) How could we do it. Well we might assume that there are some variables, which are hidden, which describe the quantum systems. Now we won't make any assumptions, like EPR, that these variables correspond to something as lofty as "reality." We will just assume that such variable might be useful in explaining our experiments. Now we will make a crucial assumption. Instead of allowing for our hidden variables to just be variables whose existence is all that matters, we are going to associate our hidden variables with the quantum systems we are moving around willy and nilly. Thus in our singlet experiment we associate the hidden variables with one qubit and some other hidden variables with the other qubit. Now since these two qubits have interacted, we can assume that these hidden variables are related to each other. Without loss of generality, if we assume that the hidden variables are associated with local quantum systems, then if two different local quantum systems interact, we can assume that these systems both consist of all of the hidden variables of each systems (at the time of such interaction.) What we are considering generally goes under the name of local hidden variable models.

Now what Bell asked was the following question. Is it possible to explain the measurements made on our two qubit system by a local hidden variable model. Well now we're going to have to define what those quantum measurement are. Okay, so we have a singlet shared between two parties. Consider now an experiment in which Alice measures with measurement operators $A_\pm = \frac{1}{2}(I \pm Z)$ and Bob measures with the measurement operator $B_\pm = \frac{1}{2}(I \pm \frac{1}{\sqrt{2}}(X+Z))$. Then the probability of the four different outcomes can be calculated:

$$\begin{aligned}
\langle\psi_-|A_+ \otimes B_+|\psi_-\rangle &= \frac{1}{4}(1 - \frac{1}{\sqrt{2}}) \\
\langle\psi_-|A_+ \otimes B_-|\psi_-\rangle &= \frac{1}{4}(1 + \frac{1}{\sqrt{2}}) \\
\langle\psi_-|A_- \otimes B_+|\psi_-\rangle &= \frac{1}{4}(1 + \frac{1}{\sqrt{2}}) \\
\langle\psi_-|A_- \otimes B_-|\psi_-\rangle &= \frac{1}{4}(1 - \frac{1}{\sqrt{2}})
\end{aligned} \tag{14}$$

One aid in performing such calculation is to note that $\langle\psi_-|\hat{n}\cdot\sigma \otimes I|\psi_-\rangle = 0$. Suppose we define the first and last outcome as $+1$ and the second and third outcome as -1 and call this variable AB. Then the expectation variable of AB is

$$\langle AB\rangle = -\frac{1}{\sqrt{2}} \tag{15}$$

Now define four other experiments. Define the measurement operators

$$\begin{aligned}
A'_\pm &= \frac{1}{2}(I \pm X) \\
B'_\pm &= \frac{1}{2}(I \pm \frac{1}{\sqrt{2}}(X - Z))
\end{aligned} \tag{16}$$

Now define the four experiments (one already done above) with these measurement outcomes, and again define the $+1$ and -1 outcomes of AB, $A'B$, AB', and $A'B'$. Then calculation of the quantum mechanical properties for these

variables yields

$$\begin{aligned} AB &= -\frac{1}{\sqrt{2}} \\ AB' &= -\frac{1}{\sqrt{2}} \\ A'B &= -\frac{1}{\sqrt{2}} \\ A'B' &= +\frac{1}{\sqrt{2}} \end{aligned} \tag{17}$$

Now lets consider this situation from the perspective of local hidden variable models. Let λ denote the hidden variables. Now these hidden variables may have probabilities associated with them, $p(\lambda)$. In this way we are considering local hidden variable theories which are non-deterministic. Let $A(\lambda)$ denote the outcome predicted by our local hidden variable theory given the hidden variable λ and given that we were measuring the $A_{\pm}$ observable. Similarly let $B(\lambda)$ denote the outcome predicted by our local hidden variable theory given the hidden variable λ and given that we were measuring the $B_{\pm}$ observable. Similarly define $A'(\lambda)$ and $B'(\lambda)$. Now lets examine a sum involving the four experiments we have described above. In particular consider

$$A(\lambda)B(\lambda) + A'(\lambda)B(\lambda) + A(\lambda)B'(\lambda) - A'(\lambda)B'(\lambda) \tag{18}$$

Integrating this over all hidden variable probabilities yields

$$\int p(\lambda) \left[A(\lambda)B(\lambda) + A'(\lambda)B(\lambda) + A(\lambda)B'(\lambda) - A'(\lambda)B'(\lambda)\right] d\lambda \tag{19}$$

We can factor this as

$$\int p(\lambda) \left[A(\lambda)(B(\lambda) + B'(\lambda)) + A'(\lambda)(B(\lambda) - B'(\lambda))\right] d\lambda \tag{20}$$

But now we can bound this integral. Why? Because each of the variables in this sum is either $+1$ or -1 for a given λ. Thus when $B(\lambda) - B'(\lambda) = 2$, $B(\lambda) + B'(\lambda) = 0$. Using this idea, we see that

$$\left| \int p(\lambda) \left[A(\lambda)(B(\lambda) + B'(\lambda)) + A'(\lambda)(B(\lambda) - B'(\lambda))\right] d\lambda \right| \leq 2 \tag{21}$$

This inequality is called the CHSH inequality (after Clauser, Horne, Shimony and Holt) and is an example of a Bell inequality.

But now look at what happens in the quantum theory for the four different experiments we discussed above

$$\langle AB \rangle + \langle A'B \rangle + \langle AB' \rangle - \langle A'B' \rangle = -2\sqrt{2} \tag{22}$$

Thus quantum theory predicts results that will violate the bound we have derived for the local hidden variable theories. This is Bell's theorem: certain statistics of quantum experiments cannot be explained by a local hidden variable theory. What this means is that if we set up computers to classically mimic the Bell experiments we have described above, if these computers are isolate from each other when they are told which of the different experiments they are going to emulate, then these computers cannot simulate the quantum experiment! Bell's theorem, in many ways, is really the beginning of quantum information science: a proof that quantum machines can do things that classical machines could never do in similar settings.

Now there are certain things that worry people when they first see Bell inequalites. The first is that they worry that these results mean that some sort of classical communication occurs between the two parties involved in this protocol for the quantum experiment. But we've already seen that when we calculate the reduced density matrix for an entangled quantum state, that it won't change if the other party performs a measurement on their state. Thus the correlations produced in quantum theory are not correlations which can be used to signal from one party to another. However the correlations are correlations which, if we wanted to explain them classically, we would need communication in order to establish the correlations. Notice that this is where most people misinterpret Bell inequalities: certainly in our local hidden variable theories we can establish correlations, we can flip a coin and put the result of that coin in two boxes and give each box to the two parties. Then the classical systems are surely correlated. But the point of Bell inequalities is that quantum correlations cannot be produced in a similar model.

So, given Bell inequalities, what do we do? One thing to do is to rejoice! Because, as we shall see, quantum entanglement is a very useful resource and the fact that there is no local hidden variable model of quantum correlations implies that quantum computers will be able to use resources in a different manner than classical computers. This is what we do today in quantum information science: we stopped worrying about quantum theory and learned to love it (shades of Dr. Strangelove in that sentence: we are after quantum computers that can read your email, after all!)

The second thing to do is to get really worried about Bell inequalities. Why? Because they seem to imply that either (1) our world is described by a nonlocal hidden variable model, or (2) we cannot describe the world by hidden variable models. (1) is very scary to physicists because they know that nonlocal physical models are often hard to reconcile with quantum theory. Thus most physicists belong to the second camp. Often those in this second camp even postulate some other way we should think about the universe.

IV. THE N-PARTY GHZ EXPERIMENT

Now let's return to the GHZ experiment. One way to interpret the GHZ experiment is just as a Bell inequality experiment. We have shown, in our argument about the GHZ experiment, that there is no what to reproduce quantum theory using just local hidden variables. In fact, in the GHZ experiment there is something else strange going on, because in our quantum experiment, you can check that the condition that the product of our outcomes is $+1$ and -1, were always one hundred percent (compare this to the CHSH inequality described above.) Sometimes this results in people saying silly things like the GHZ experiment allows one to violate local hidden variable theories in a single experiment. People who say this have obviously never done a single experiment nor have they considered what the word proved means in science. There is, however, a way in which the GHZ experiment differs from the Bell inequality experiment. This is that it shows that there cannot be a local non-contextual hidden variable model for the GHZ experiment. We won't go into this now, but it is very interesting and leads to a discussion of what is called the Kochen-Specker theorem.

But the GHZ experiment is interesting for another reason. Suppose that we now have 4 parties who share an 4 party GHZ state $\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$. Now suppose that the evil Warden plays a game with these four parties where he distributes slips of paper with either X or Y on them to the four parties, and he guarantees that these slips of paper are either all X or two of the six are Y (and the other two are X.) Again the parties play a game where the product of their ± 1 outputs must be $+1$ if each parties was given an X and -1 if two of the parties were given a Y. But now suppose that in addition to the normal rules of the game, where the parties cannot communicate, the warden allows us to decide to allow two of the parties to communicate after they have been given their slips of paper. Can we win this game without using quantum theory?

Well suppose that it is the first two parties who are allowed to communicate. Then consider the four cases $XXXX$, $XXYY$, $XYXY$, $XYYX$. Now if the first two parties are allowed to communicate, they can arrange their answer in an arbitrary manner. Now define $P = XX$ and $Q = XY$. Then the four cases can be written as PXX, PYY, QXY, and QYX. Now again we can go through our arguments about the GHZ experiments. Certainly P and Q are just like our old X and Y variables, they are ± 1 valued observables. And again the desired outcomes obey $PXX = +1$, $PYY = QXY = QYX = -1$, which gives rise to a contradiction. Thus we have seen that no four parties can win this four party GHZ game (without using quantum theory) even if two of the parties are allowed to communicate with each other! But if they are allowed to share a four party GHZ state $\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$, then they can beat this game with no communication (again by simply measuring along the specified directions.) Thus we see that quantum theory cannot be explained by a local hidden variable theory, plus communication between 2 of the parties. Similarly it is possible to extend this argument to n parties and an n partite GHZ state $\frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$ and show that quantum correlations cannot be explained by local hidden variable theories plus communication among $n-2$ of these parties.

Notice now that what we are doing is bounding even tighter the types of hidden variable theories which can and cannot be used to reproduce quantum theory. And what is interesting from the perspective of computer science, is that we are bounding the resources that the parties use to simulate quantum theory. We know, by using the above argument that a high degree of communication among parties is necessary to simulate multipartite quantum correlations. Quantum information science focuses our question about local hidden variable theories, no longer is it as important to show that there is no local hidden variable theory reproducing quantum theory, but instead we become interested in nonlocal hidden variable theories with certain restrictions on communication between differing parties. This is a fundamental shift in how we think about Bell inequalities, and, I think, an important on for understanding the power of entangled quantum states.

V. ENTANGLEMENT AND QUANTUM SPEEDUPS

We've seen that entangled quantum states cannot be simulated by certain classical local hidden variable theories. In this section I want to discuss why entanglement is important for the speedups offered by quantum algorithms. We have already noted that if we have n qubits then a general pure state of these n qubits requires us to specify 2^n complex numbers. Thus as a function of the number of qubits, we can't even efficiently write down a description of the quantum state. As we noted, however, a similar statement can be made about a probabilistic information processing machine. To write down a description of n probabilistic bits, we would need 2^n real numbers. So we can't really use this sort of argument to argue why quantum computers are powerful. But we can turn this argument around and use it in the other direction. Suppose that we find that in a particular situation where instead of needing 2^n complex numbers we need only a polynomial number of complex numbers. Then we can efficiently represent these states, given that we are working with a fixed precision. And if when we perform evolutions on these states, and we stay within the manifold of efficiently representable states, then we could possibly simulate this quantum computation.

So are there situations where we have only need a polynomial number of complex numbers to specify our quantum state? Well, there is one particular case that we think of right off the top of our head. Suppose that our n qubits are in a completely separable state between all n qubits: $|\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$. Then we only need $2n$ complex numbers to specify this state. Further, call a state p-blocked if we can express it as a separable state with blocks of size at most p qubits. Then, even though the qubits within a block may be entangled, we need only 2^p complex numbers to specify the state within a block. For fixed p, as n increases, the number of complex numbers we will need to specify our state will be bounded by $2^p \frac{n}{p}$. Thus, at least for the level of description we can say that if a state is p-blocked we can efficiently describe this state to a fixed precision.

What about if this state evolves via a quantum gate or there is a measurement of the state? Well if the state continues to be p-blocked throughout these evolutions, then the we can efficiently simulate these evolutions. Why? Well suppose our gates are of fixed size as we normally assume. Then these will act within or between a fixed number of p gates. We can simply perform this explicit unitary transform on our p-blocked system. Since the gates are of fixed size, we can't every have manipulations which are exponentially growing matrix multiplications. Similar arguments hold for the measurement. So, if a state can be p-blocked at all times for a quantum circuit family, then we should be able to efficiently simulate this circuit.

Now there is one problem with the above argument. Well we haven't done a very good analysis of the precision of our representations and gate sets. One way to deal with this is to use rational approximations of these gates. But now something bad can happen: a state which was p-blocked for the exact quantum algorithm we are implementing, with the rational approximation to these gates may not be p-blocked. The way to deal with this is to deal with states which are very near p-blocked states. Then if you use the rational approximations to the gates and the states are close to p-blocked states, then you will be fine. But I won't prove this (although you might be able to see the outlines of how such a proof would go.) For details about how to prove this, see "On the role of entanglement in quantum computational speed-up" by Noah Linden and Richard Jozsa (`http://arxiv.org/abs/quant-ph/0201143`).

So what have we learned? We've learned that if there is little entanglement in the different possible states involved in a quantum algorithm, then this quantum algorithm can be efficiently simulated. What is interesting about this construction is that, unlike the case where we showed the controlled-NOTs could not be used to construct universal classical computation, in this case classical computation is contained within the efficiently simulatable situations in this model. Further notice that the principle of being p-blocked is a rather crude proxy for noticing that some quantum states have efficient descriptions. Indeed, there is a very beautiful story, which is now emerging, in the simulation of quantum systems which is motivated by this observation. In particular it has been realized that if a system does not have much entanglement (a rather loose set of words for a tricky concept) then it is possible to efficiently describe this system and often to then simulate it. Oftentimes, in the low energy sector of many-body quantum systems, this is exactly the case. These two observations together are lead to new numerical algorithms for simulating such quantum systems.