# CS290A, Spring 2005:

# Quantum Information & Quantum Computation

**Wim van Dam**

**Engineering 1, Room 5109**
**vandam@cs**

**http://www.cs.ucsb.edu/~vandam/teaching/CS290/**

# Administrative

- The Final Examination will be:
  Monday June 6, 12:00–15:00, PHELPS 1401

- New Exercises are posted
  Try to answer Question 2 before Thursday.

# Last Week / This Week

- Last week we looked at quantum money and quantum cryptography, which uses the qubit states 0,1,+,–.

- This week we will extend this idea to describe "quantum fingerprinting".

- Also this week: superdense quantum coding and quantum teleportation of quantum states.

# Fingerprinting

Assume two parties A and B that each have data in the form of a (long) string x and $y \in \{0,1\}^N$.

A and B want to check if they have the same data, without revealing a priori to the other their strings.

They do this by sending (publicly) information about their strings (x and y) to a trusted third party C, who decides.

Sending the whole strings is not allowed because the strings are too long / risk of eavesdropping.

A and B want to have a way of *fingerprinting* their strings.

# Quantum Fingerprinting

"Quantum Fingerprinting" refers to a way of mapping the strings $x,y \in \{0,1\}^N$ to quantum states $|\varphi_x\rangle$ and $|\varphi_y\rangle$, that live in a 'much smaller than $2^N$'-dimensional Hilbert space, such that from $\psi$ and $\varphi$ we can tell decide whether $x=y$.

The set $\{ |\varphi_x\rangle : x \in \{0,1\}^N \}$ cannot be mutually orthogonal. Instead we will have to work with near orthogonal states.

Central Idea: Encode $x \in \{0,1\}^N$ into m qubit state $|\varphi_x\rangle$ (with m much smaller than N).
Do this in a way such that $|\langle\varphi_x|\varphi_y\rangle|^2 \leq ½$ if $x \neq y$.
Third party decides if $|\varphi_x\rangle = |\varphi_y\rangle$ or not.

# Simple Example

Let x and y be from a set of 6 possibilities.
Let $|\varphi_x\rangle$ and $|\varphi_y\rangle$ be qubits from the set of 6 states
$\{|0\rangle, |1\rangle, (|0\rangle+|1\rangle)/\sqrt{2}, (|0\rangle-|1\rangle)/\sqrt{2}, (|0\rangle+i|1\rangle)/\sqrt{2}, (|0\rangle-i|1\rangle)/\sqrt{2}\}$

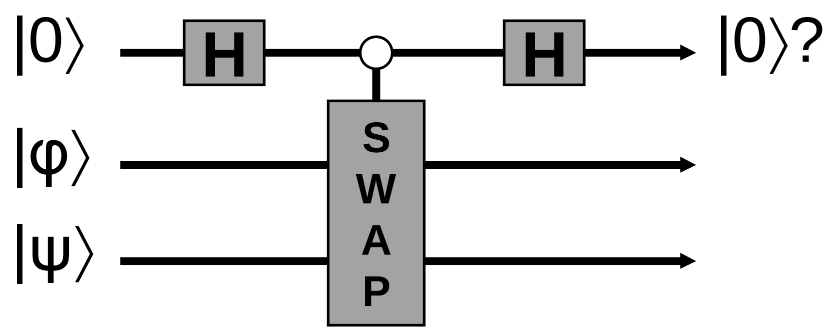
For all qubit states with $x \neq y$ we have $|\langle\varphi_x|\varphi_y\rangle|^2 \leq ½$.
The third party receives two unknown states $|\varphi_x\rangle$ and $|\varphi_y\rangle$ that are either the same or very different.

How to distinguish between these two possibilities?

A Quantum State Equality Tester for unknown states can be implemented with a Controlled Swap Test…

# Controlled Swap Test

- Given two unknown quantum states $|\psi\rangle$ and $|\varphi\rangle$, are they the same or not?
- You can test this using the Controlled Swap Test”
  C-SWAP:$|0,x,y\rangle \mapsto |0,x,y\rangle$
  C-SWAP:$|1,x,y\rangle \mapsto |1,y,x\rangle$
  in the circuit…………….

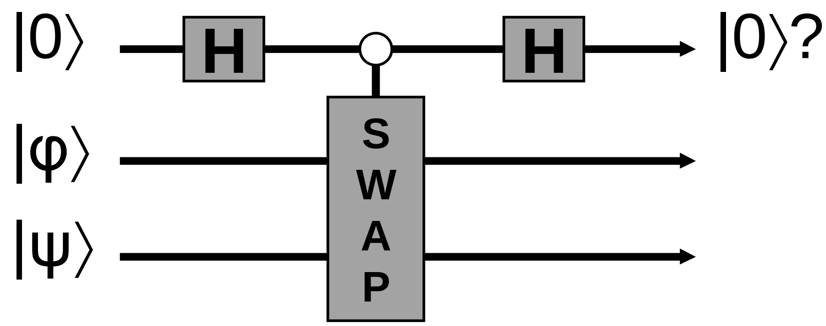



- Observing a “0” indicates that $|\psi\rangle$ and $|\varphi\rangle$ are close to each other, observing a “1” that they are far apart.

- What are the exact probabilities?

# Probabilities of C-SWAP

- The evolution of the system is




$$\left|0,\varphi,\psi\right\rangle \mapsto \tfrac{1}{\sqrt{2}}\left(\left|0,\varphi,\psi\right\rangle + \left|1,\varphi,\psi\right\rangle\right)$$

$$\mapsto \tfrac{1}{\sqrt{2}}\left(\left|0,\varphi,\psi\right\rangle + \left|1,\psi,\varphi\right\rangle\right)$$

$$\mapsto \tfrac{1}{2}\left(\left|0,\varphi,\psi\right\rangle + \left|1,\varphi,\psi\right\rangle + \left|0,\psi,\varphi\right\rangle - \left|1,\psi,\varphi\right\rangle\right)$$

$$= \left|0\right\rangle \otimes \tfrac{1}{2}\left(\left|\varphi,\psi\right\rangle + \left|\psi,\varphi\right\rangle\right) + \left|1\right\rangle \otimes \tfrac{1}{2}\left(\left|\varphi,\psi\right\rangle - \left|\psi,\varphi\right\rangle\right)$$

The probability of observing a “0” is therefore

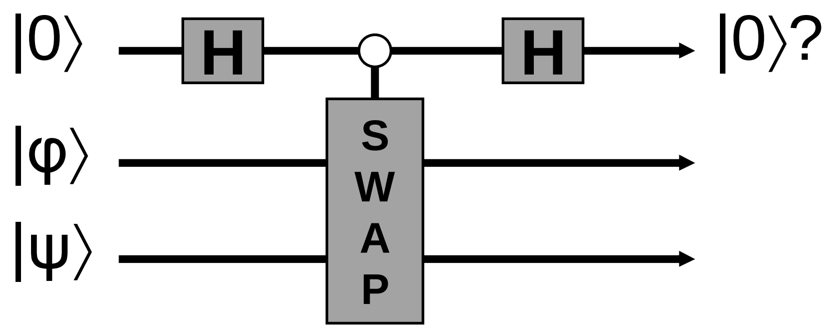
$$\text{Prob("0")} = \tfrac{1}{4}\left(\left\langle\varphi,\psi\right| + \left\langle\psi,\varphi\right|\right)\left(\left|\varphi,\psi\right\rangle + \left|\psi,\varphi\right\rangle\right)$$

$$= \tfrac{1}{4}\left(2 + \left\langle\psi,\varphi\middle|\varphi,\psi\right\rangle + \left\langle\varphi,\psi\middle|\psi,\varphi\right\rangle\right)$$

$$= \tfrac{1}{2} + \tfrac{1}{2}\left|\left\langle\psi\middle|\varphi\right\rangle\right|^2$$

# Equality Testing

- The previous calculations show that if $|\langle \varphi,\psi\rangle|^2 \approx 1$, then the probability of observing a "0" is $\approx 1$.




- If $|\langle \varphi,\psi\rangle|^2 \approx 0$, then the probability of "0" is $\approx$ ½.

- By repeating the experiment a number of times (using fresh copies of $|\psi\rangle$ and $|\varphi\rangle$), we can –with near certainty– distinguish between the cases $|\psi\rangle = |\varphi\rangle$ and $|\langle \varphi,\psi\rangle|^2 \leq$ ½.

# More on Q-Fingerprinting


Using methods from error correction it is possible to encode N bits of information into $M \approx c \log N$ qubits such that $|\langle\varphi_x|\varphi_y\rangle|^2 \leq ½$ if $x \neq y$.

Even if we have to send many copies of the the fingerprint, it will still be more efficient than sending the N classical bits of the original strings x and y.

Added advantage: because we send such a highly compressed quantum state, it is impossible to infer the string x from the fingerprint $|\varphi_x\rangle$.

# Communication & Entanglement

- Holevo's bound tells us that we can encode only one bit of information into one qubit.
  This bound assumes that the qubit is unentangled.

- Things change if we allow the communication of qubits that are entangled with qubits of the receiver.

- **What happens if A and B share a prior entangled pair of qubits $|EPR\rangle = (|0_A,0_B\rangle+|1_A,1_B\rangle)/\sqrt{2}$ before Alice is to send (quantum) information to Bob?**

# Superdense Quantum Coding

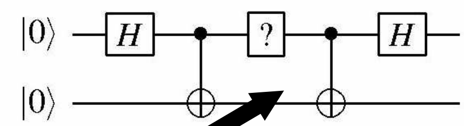
- Let A and B share an EPR pair of qubits.
  Alice wants to transmit classical information to Bob.

- Using Superdense coding, A can send two bits of information to B, using only one qubit.

- Approach: Depending on A's input {1,2,3,4} she applies to her side of the EPR pair, one of 4 transformations { I, X, Y, Z}, and sends her EPR qubit to Bob.
- From the changed EPR pair, Bob decodes which transformation A has applied. This can be done reliably and will transfer 2 bits of information from A to B.

# How to Do It?

**Question 1.** (The Effect of Pauli Gates). Consider the following 2 qubit circuit:




where the ?-gate can be one of the Pauli matrices $\{I,X,Y,Z\}$. Calculate what the output of this quantum circuit will be depending on the choice for the ?-gate.

**Question 2.** (Creating Correlated Quantum States). Describe

- Look back at Question 1, Exercises 2 (Week 3)

- The four transformations give us four entangled states that are mutually orthogonal…

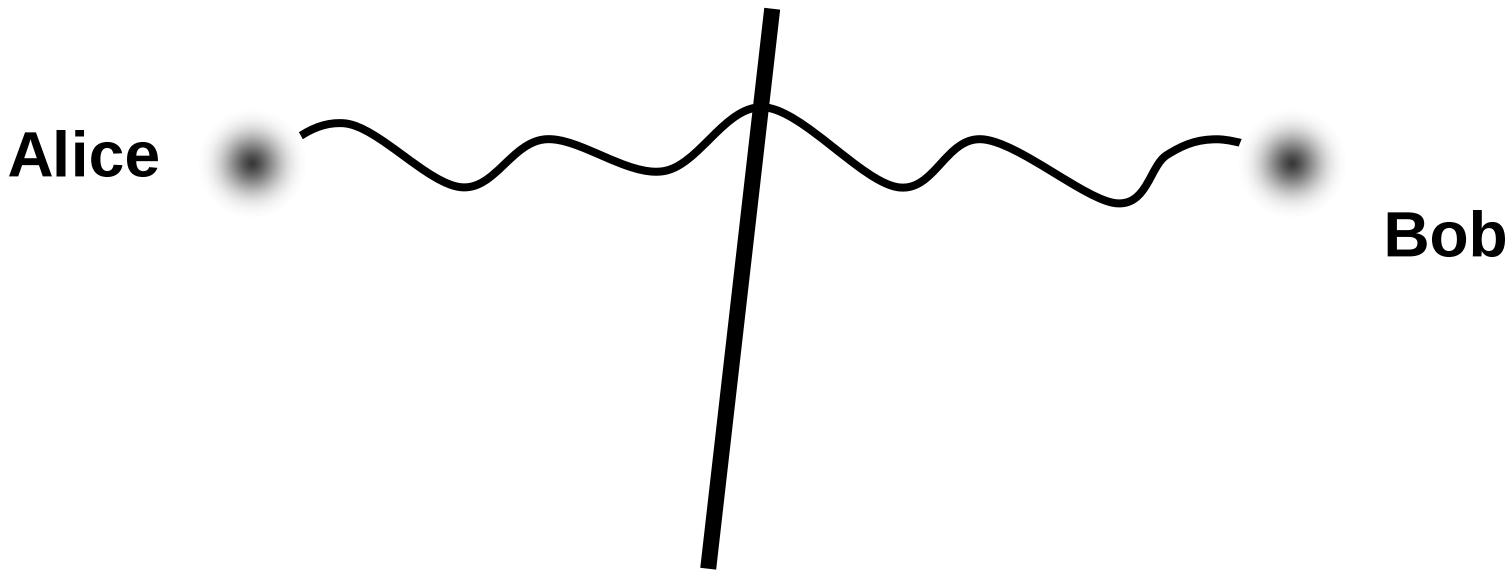
$$(\mathrm{I}) \mapsto \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$
$$(\mathrm{X}) \mapsto \tfrac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$$
$$(\mathrm{Y}) \mapsto \tfrac{1}{\sqrt{2}}(\mathrm{i}|10\rangle - \mathrm{i}|01\rangle)$$
$$(\mathrm{Z}) \mapsto \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

- With a CNOT and a Hadamard, Bob can map those states to the outputs |00⟩, |01⟩, –i|11⟩ |and |10⟩.

# More on Superdense Coding

- One can prove that the 2 bits / 1 qubit ratio is optimal: it is not possible to send (say) 3 bits of information using 1 qubit and lots of entanglement.
- Superdense coding is not possible classically.
- Experimental implementation of superdense coding: [Zeilinger et al.,1996, Innsbruck, Austria]
- Can we do the inverse: Send quantum information using classical communication between A and B?

# What is Teleportation?




*Alice wants to send her unknown quantum information to Bob.*

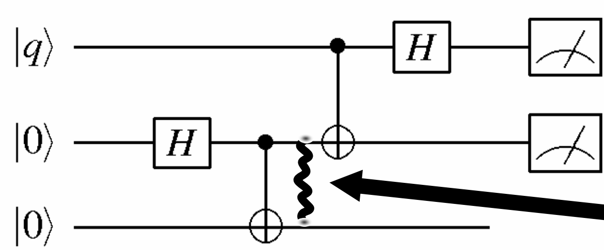
A and B do not have a quantum channel:
only classical communication is allowed.

Alice cannot tell Bob what the values $\alpha$,$\beta$ are,
nor can she measure $|q\rangle$ to see what they are.

**Solution: Use an entangled EPR pair**

# Towards Teleportation

**Question 2.** (Towards Teleportation) (See Handout III if you have problems answering this question.) Consider the following three qubit circuit that has as input an unknown qubit $|q\rangle$ and two zero states:




**(a)** With $|q\rangle = \alpha|0\rangle + \beta|1\rangle$, what is the output state before the measurements?

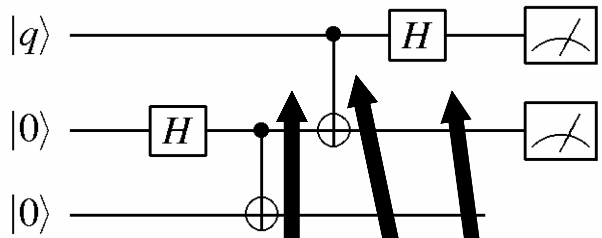
The first two qubits are on Alice's side
The 3$^{rd}$ one is Bob's

After H/CNOT, they share an EPR pair.

Alice performs a CNOT and a Hadamard to her 2 qubits and measures them in the 0/1 basis.

What can she expect to observe?

# Output?




**(a)** With $|q\rangle = \alpha|0\rangle + \beta|1\rangle$, what is the output state before the measurements?

$$\begin{aligned}
|q\rangle \otimes |EPR\rangle &= (\alpha|0\rangle + \beta|1\rangle) \otimes \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
&= \tfrac{1}{\sqrt{2}}(\alpha|0{,}00\rangle + \alpha|0{,}11\rangle + \beta|1{,}00\rangle + \beta|1{,}11\rangle) \\
&\mapsto \tfrac{1}{\sqrt{2}}(\alpha|0{,}00\rangle + \alpha|0{,}11\rangle + \beta|1{,}10\rangle + \beta|1{,}01\rangle) \\
&\mapsto \tfrac{1}{2}(\alpha|0{,}00\rangle + \alpha|1{,}00\rangle + \alpha|0{,}11\rangle + \alpha|1{,}11\rangle + \\
&\qquad \beta|0{,}10\rangle - \beta|1{,}10\rangle + \beta|0{,}01\rangle - \beta|1{,}01\rangle)
\end{aligned}$$

$$\begin{aligned}
&= \tfrac{1}{2}|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + \\
&\quad \tfrac{1}{2}|01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) + \\
&\quad \tfrac{1}{2}|10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + \\
&\quad \tfrac{1}{2}|11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle)
\end{aligned}$$

Regardless of the values α,β the probability of measuring {00,01,10,11} is one-quarter.

# Effect of A's Measurement

$$
\begin{aligned}
&= \tfrac{1}{2}|00\rangle \otimes (\alpha|0\rangle + \beta|1\rangle) + \\
&\quad \tfrac{1}{2}|01\rangle \otimes (\alpha|1\rangle + \beta|0\rangle) + \\
&\quad \tfrac{1}{2}|10\rangle \otimes (\alpha|0\rangle - \beta|1\rangle) + \\
&\quad \tfrac{1}{2}|11\rangle \otimes (\alpha|1\rangle - \beta|0\rangle)
\end{aligned}
$$

Depending on the two leftmost qubits (A's side), the third qubit (B's side) is 1-out of-4 permutations of the original qubit $|q\rangle$.

When A measures the two bits $\in\{00,01,10,11\}$ the qubit of B collapses to 1 of the 4 versions of q.

Outcome "00": $\rightarrow \alpha|0\rangle+\beta|1\rangle$
Outcome "01": $\rightarrow \alpha|1\rangle+\beta|0\rangle$
Outcome "10": $\rightarrow \alpha|0\rangle-\beta|1\rangle$
Outcome "11": $\rightarrow \alpha|1\rangle-\beta|0\rangle$

When A tells B which one of the 4 outcomes she has observed, Bob knows what to do to correct his qubit to the original $|q\rangle$.

# Bob's Correction

| |
|---|
| "00": $\rightarrow \alpha|0\rangle+\beta|1\rangle$ |
| "01": $\rightarrow \alpha|1\rangle+\beta|0\rangle$ |
| "10": $\rightarrow \alpha|0\rangle-\beta|1\rangle$ |
| "11": $\rightarrow \alpha|1\rangle-\beta|0\rangle$ |

When A tells B which one of the 4 outcomes she has observed, Bob knows what to do to correct his qubit to the original $|q\rangle$…

If first bit is a "1", Bob applies a Z gate $|b\rangle \mapsto (-1)^b|b\rangle$.
If 2nd bit is a "1", Bob applies a NOT $|b\rangle \mapsto |b\oplus 1\rangle$

The outcome will always be $\alpha|0\rangle+\beta|1\rangle = |q\rangle$

Bob has (re)created the unknown qubit q that was on Alice's side. During the process Alice has 'lost' her copy of the qubit (otherwise we would have copied q).

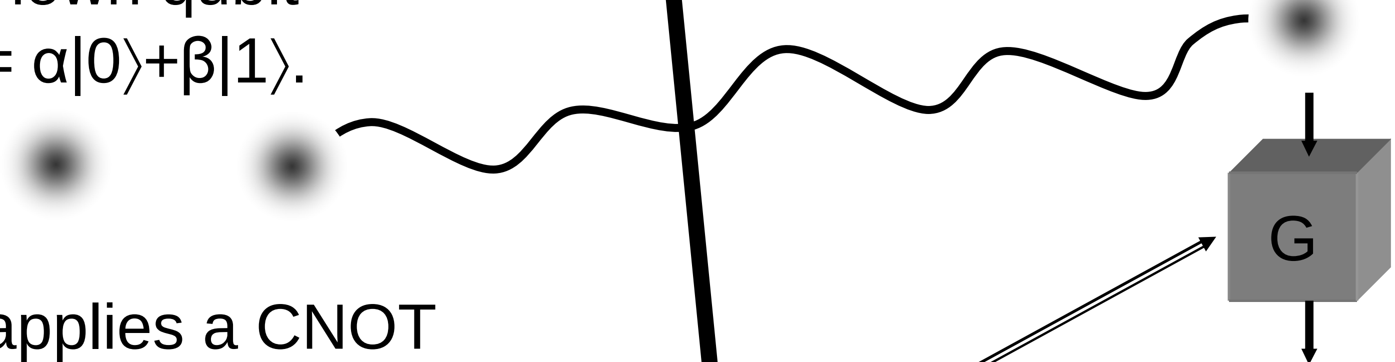
# Teleportation

**Alice**

**Shared EPR pair**

**Bob**

unknown qubit
$|q\rangle = \alpha|0\rangle+\beta|1\rangle$.




Alice applies a CNOT and a Hadamard to q and her EPR half.

She measures the bits in the 0/1 basis and sends the information to Bob.

Bob receives the two bits and acts on his side of the EPR, in a way that recreates the unknown qubit $|q\rangle = \alpha|0\rangle+\beta|1\rangle$.

# What Just Happened?

- Teleportation requires one EPR pair and two classical bits to transfer one qubit from A to B.
- Superdense coding requires one EPR pair and one quantum bit to transfer two classical bits of information.

- The qubit did not get copied: Alice's measurement destroyed it on her side.

- The outcome of Alice's measurement is completely random and independent of the $\alpha,\beta$ values of $|q\rangle$.
  A and B learn nothing about the unknown qubit.

# Alice’s Measurement

- Initially, Bob’s part of the EPR pair has nothing to do with the qubit q on Alice’s side.
- After she has performed her measurement, this appears to have changed: Now Bob’s EPR-half is (almost) identical to q (except for some ‘corrections’).
- Does Alice’s measurement instantaneously change B’s qubit in a way that can be used for communication?

- Answer: No (of course). Until Bob has received the two bits of information from Alice, his qubit remains as random as it was before the measurement.

# So What does Happen?

- What exactly happens when one half of an EPR pair gets measured is a deep question in physics.

- Example, take $|EPR\rangle=(|00\rangle+|11\rangle)/\sqrt{2}$ between A and B.
- If B measures his part, he will see 0/1 with 50%/50%. We say that this is caused by of the unavoidable randomness of quantum physics.
- But if A has measured her qubit beforehand, then she knows with 100% that Bob will observe the same value.

- *When is the outcome of a measurement determined?*

# Classical Correlations

- Compare a classically correlated state:
  Two distributed bits with are promised to be equal, but are otherwise random (“00” or “11”)

- Again, Bob does not know what value he will see.
  But when Alice knows her value, she can predict Bob’s value with 100% accuracy.
- In this situation we would say that the randomness on Bob’s side is due to his **ignorance**: The outcome is predetermined, but he is just unaware of it.

- In quantum mechanics, on the other hand, the outcome does not seem to be predetermined…

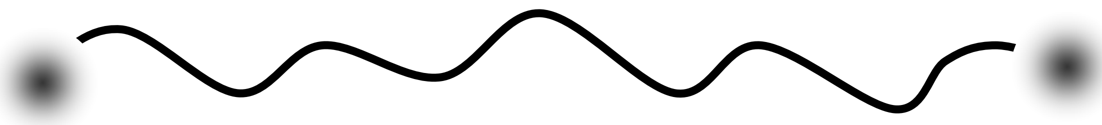
# Complete Description?

- The question is: When we say that two qubits are in the state $|EPR\rangle=(|00\rangle+|11\rangle)/\sqrt{2}$, is that all there is to know?
- From it, we cannot predict what the outcomes of our measurements will be, so some information seems to be missing in our description (ignorance).

- Are there “hidden variables” that we could include in our description of the quantum state that would predict the outcomes of (future) measurements?

- **Answer: This is not the case.**

# Hidden Variables



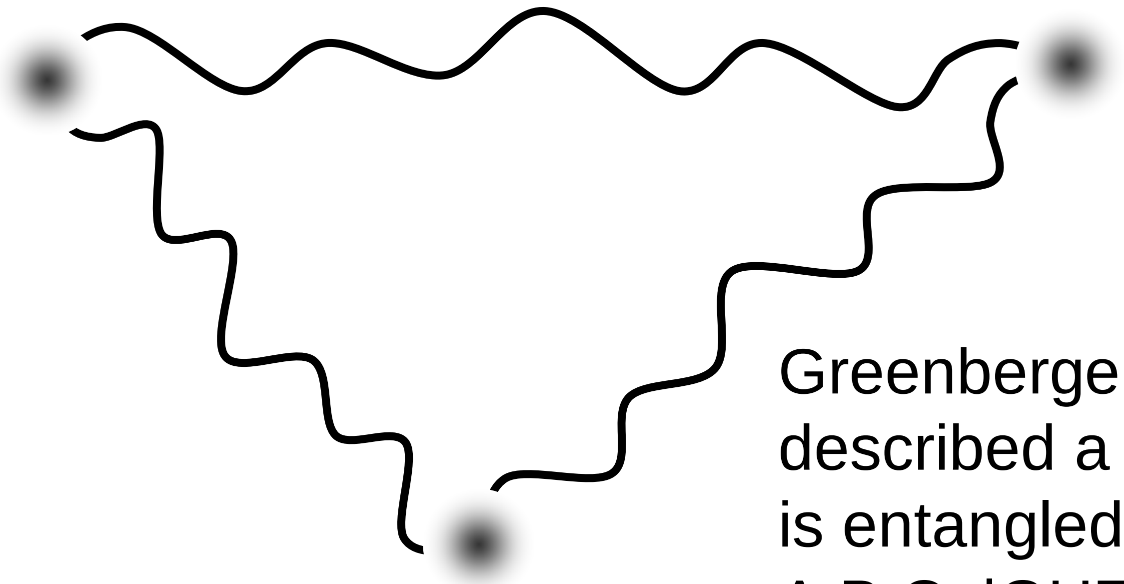
In a hidden variable theory, the particles A and B have determined beforehand what the outcomes will be when (later on) they are measured.

Several kinds of measurements are possible so each particle would have a list of answers for the various kinds of measurements:

| <u>Measurement</u>: | <u>Outcome</u>: |
|---|---|
| “0”? | “Yes” |
| “+”? | “No” |

Such lists cannot mimic the statistics of quantum mechanics that we see in the laboratory.

# Three Party Entanglement



Greenberger, Horne and Zeilinger described a three qubit state that is entangled over three parties A,B,C: $|GHZ\rangle = (|000\rangle + |111\rangle)/\sqrt{2}$

Party A will change the phase of her qubit according to $|0\rangle \mapsto |0\rangle$ and $|1\rangle \mapsto e^{i\alpha}|1\rangle$. Same for B,C with angles β,γ. After that they perform a Hadamard gate and measure their qubits in the standard 0/1 basis…

# Midterm Flashback

- What happens was the last question on the Midterm.
- If the sum $\alpha+\beta+\gamma = 0 \bmod 2\pi$ then the parity of the outcome bits will be even. If $\alpha+\beta+\gamma = \pi \bmod 2\pi$, then the parity of the three bits will be odd.
- You can use this to implement a distributed even/odd deciding algorithm that minimizes the communication between the three parties A,B and C.
- **It is impossible to implement this algorithm using a “hidden variables technique”…**