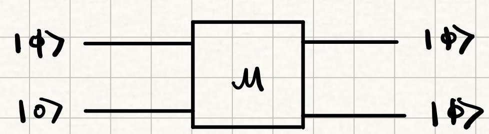
QIT Lecture #2

1. No cloning Theorem
2. Quantum Teleportation
3. Quantum Key Distribution (QKD)
4. EPR & Bell's Inequality (CHSH version)
5. The Rotating Frame
6. NMR as a quantum computer

The Quantum No-cloning Theorem:

Suppose $\mathcal{M}$ is a proposed cloning machine:



$|\phi\rangle$ = "input state"

$|0\rangle$ = "blank paper"

$|\mathcal{M}_0\rangle$ = Initial state of the machine

$$|\phi, 0, \mathcal{M}_0\rangle \xrightarrow{U} |\phi, \phi, \mathcal{M}_\phi\rangle$$

↳ Final state of the machine may depend on the arbitrary state $|\phi\rangle$.

If we consider two distict non-orthogonal states $|\phi\rangle$ & $|\phi'\rangle$ so that

$$0 < |\langle\phi|\phi'\rangle| < 1$$

Consider

$$|\phi, 0, M_0\rangle \xrightarrow{U} |\phi, \phi, M_\phi\rangle = U|\phi, 0, M_0\rangle$$

$$|\phi', 0, M_0\rangle \xrightarrow{U} |\phi', \phi', M_{\phi'}\rangle = U|\phi', 0, M_0\rangle$$

$$\langle\phi, \phi, M_\phi|\phi', \phi', M_{\phi'}\rangle = \langle\phi, 0, M_0|U^\dagger U|\phi', 0, M_0\rangle$$

$$= \langle\phi, 0, M_0|\phi', 0, M_0\rangle$$

$$\langle\phi|\phi'\rangle^2 \langle M_\phi|M_{\phi'}\rangle \stackrel{?}{=} \langle\phi, \phi'\rangle$$

Since $|\langle\phi|\phi'\rangle|^2 |\langle M_\phi|M_{\phi'}\rangle| < 1$ the above equality cannot hold. The LHS must be smaller in magnitude than the right hand side.

Thus no cloning machine can exist.

Quantum Cryptography

Suppose Alice wants to send Bob a secret message. One option that Alice has is to communicate with Bob using a private channel. But what if such a private channel is not available or they think that the security of their private channel has been compromised. Under such circumstances they must consider public channel but to keep anyone else from reading their message Alice needs to encrypt her message. She does it by using a private key. Anyone who wants to read the message must decrypt it using the same key.

Suppose the message that Alice wants to send is expressed in a string of binary digits (bits) we call this the plaintext. It consists on n bits. The plaintext is converted into a code by adding to it, modulo 2, an n-bit key:

Plain text : 0 1 1 0 1 0 0 1 1 1 0 1

Key : 1 0 1 0 0 1 1 1 0 1 1 0

Cyphertext : 1 1 0 0 1 1 1 0 1 0 1 1

The result of adding the key to the plaintext results in the cyphertext. Alice then shares the cyphertext with Bob over a public channel. Without having access to the key the cyphertext reads like complete gibrish.

Bob, when he recieves the cyphertext adds the private key to decrypt the message:

Cyphertext : 1 1 0 0 1 1 1 0 1 0 1 1

Key : 1 0 1 0 0 1 1 1 0 1 1 0

Plain text : 0 1 1 0 1 0 0 1 1 1 0 1

For large n it becomes increasingly more difficult to guess the key. For n there are 2^n possibilities. But in principle with the help of a powerful computer the evesdropper Eve can crack the code. There is also the worry that the key itself might be compromised. In the first instance Alice & Bob will have to meet up to exchange the key.

Quant cryptography offers many advantages over classical cryptography. Here we describe a protocol for quantum key distribution (QKD) known as BB 84 named after its inventors Charles Bennet & Gilles Brassard and the year (1984) in which they proposed it. BB84 is considered the beginning of the field of quantum cryptography.

In BB84 protocol Alice produces two random strings: One consists of 0s and 1s called the parent string. And the string consists of Z & X and is called the basis string. She chooses a qubit in a state given by the following chart:

Basis	Parent	Qubit state
Z	0	$\|0\rangle$
Z	1	$\|1\rangle$
X	0	$\|+\rangle$
X	1	$\|-\rangle$

Alice gives Bob a string of qubits according to this rule. Below we consider a sample:

Z	X	Z	Z	X	Z	X	X	X	Z	Alice's basis string
1	0	1	1	1	0	1	0	1	1	Alices parent string
$\|1\rangle$	$\|+\rangle$	$\|1\rangle$	$\|1\rangle$	$\|-\rangle$	$\|0\rangle$	$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	$\|1\rangle$	Qubit states

Bob doesn't know either of Alice's string. He then generates his own random basis string and measures the qubit according to those basis states:

Z	Z	X	Z	X	X	Z	X	Z	X	Bob's basis string
$\vert 1\rangle$	$\vert 0\rangle$	$\vert -\rangle$	$\vert 1\rangle$	$\vert -\rangle$	$\vert +\rangle$	$\vert 1\rangle$	$\vert +\rangle$	$\vert 0\rangle$	$\vert -\rangle$	Bob's results of measurement in the basis given by Bob's basis string.

Bob then constructs a parent string according to the same rule as Alice:

1	0	1	1	1	0	1	0	0	1	Bob's parent string.

Bob then compares his basis string with Alice's over a public channel and he throws away all the qubits and the corresponding parent bits in which he measured in the wrong basis:

Right basis	Y	N	N	Y	Y	N	N	Y	N	N
Key string	1			1	1			0		

In this way Bob and Alice generate a key.

Now what about Eve? Eve can only gather information about the basis strings used. But if she doesn't have access to parent bits corresponding to the common basis bits she has no knowlege about the key.

Since Alice uses $N=4$ states and the dimension of the Hilbert space $d=2$ we see that on each qubit Eve's probability of error is

$$P_E \geq 1 - \frac{2}{4} = \frac{1}{2}.$$

What happens if Eve intercepts the qubit sent by Alice, makes a measurement and then sends it to Bob. Since Eve will sometimes misidentify the state the state that she passes onto Bob will be in a state different from the state that Alice prepared. Thus even if Alice and Bob measures in the same basis they will obtain different parent bits.

Alice & Bob can detect Eve's meddling by choosing a random sample of their key bits and compare them over a public channel and then eliminate them from their key, since these bits are no longer useful as key bits. If even after comparing several hundred bits Alice and Bob find no discrepancy they can be confident that no one had been interfering.

<u>Comments:</u>

1. Bob gets the right parent bit about 75% of the time: prob of guessing the right basis $= \frac{1}{2}$ + Prob. of guessing the wrong basis $= \frac{1}{2} \times$ Prob of getting the right parent bit $= \frac{1}{2}$ $= \frac{1}{2} + \frac{1}{4}$ $= \frac{3}{4}$.

2. Although Bob gets the correct parent bit 75% of the time it is only when his choice of the basis bit agrees with that of Alice is when he can sure of the parent bit being the same as that of Alice. Thus Bob only keeps those (50%) of his parent bits.

The EPR Critique of Quantum Mechanics:

In 1935 Albert Einstein, Boris Podolsky, and Nathan Rosen (EPR) offered an argument that quantum mechanics is an incomplete theory. The EPR argument, if true, would imply that there must exist hidden variables which are not part of quantum mechanics. Such theories are called 'hidden variable theories.'

Here we present a version of the EPR argument that is due to John Bell who derived a testable version of the argument which led to the Bell inequalities.

Suppose we have two qubits (say, two particles with spin $\frac{1}{2}$) which are in an entangled state given by the Bell state:

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}\{|01\rangle - |10\rangle\}$$

For two spin $\frac{1}{2}$ particles in this state it can be shown that the total angular momentum operator $\vec{S} = \vec{S}_A \otimes \mathbb{1}_B + \mathbb{1}_A \otimes \vec{S}_B$ has eigenvalue given by $\vec{S}^2 = s(s+1)\hbar$ with $s=0$. This state is called a singlet state.

The nice thing about the singlet state is that it has the <u>same form</u> in any basis. So if we express it in the X basis it becomes:

$$|\beta_{11}\rangle = \frac{1}{\sqrt{2}}\left\{\frac{1}{2}[|+\rangle + |-\rangle][|+\rangle - |-\rangle] - \frac{1}{2}[|+\rangle - |-\rangle][|+\rangle + |-\rangle]\right\} = \frac{1}{\sqrt{2}}\left\{\frac{1}{2}(\cancel{|++\rangle} + |-+\rangle - |+-\rangle - \cancel{|--\rangle}) - \frac{1}{2}(\cancel{|++\rangle} - |-+\rangle + |+-\rangle - \cancel{|--\rangle})\right\} = \frac{1}{\sqrt{2}}(|-+\rangle - |+-\rangle).$$

Now suppose the particle A ends up in Alice's lab while particle B ends up in Bob's lab. Alice and Bob's labs can be far apart. EPR argued that any measurement that Alice made on her qubit must be independent of any measurement that Bob did and vice versa. We may call this assumption the locality assumption.

Now according to quantum mechanics Alice can do a bunch of incompatible measurement on her qubit. Suppose Alice has a choice of two measurements X_A or Z_A. Suppose Bob also has the same choice: X_B or Z_B. But according to QM the 'value' of these variables do not exist before Alice or Bob makes the measurement.

If Alice chooses to measure X_A then the value of Bob's qubit's X_B value is determined. On the other hand a measurement of Z_A will yield the value of Z_B. But the (apparently) reasonable assumption of locality means that Alice's choice

of measurement doesn't influence the measurement that Bob does. Thus the values of X_B & Z_B must exist even though they are not simultaneously measureable according to quantum mechanics. An aspect of a physical system which can be measured without disturbing it is called 'an element of reality.' This assumption is known as the reality assumption.

This version of local realism seems compelling since there is no known 'mechanism' by which the two particles can interact over vast distances. Furthermore Alice and Bob can even do their measurements so that the elapsed between the events of measurement shorter than the time taken for a beam of light to traverse the distance between them. In the language of special relativity the two events are space-like separated.

Criticism of the EPR argument involves:

i) It's counterfactual. So Alice can never do both X_A & Z_A measurements and so making the statement the values of both X_B & Z_B exist is not a factual statement.

ii) Niels Bohr argued that there needn't be a physical mechanism by which the two qubits can communicate with each other. He argued that the two different choices of measurements were complementary to each other in the same way the wave aspect and the particle aspect of a quantum particle are complementary. The latter is the statement of principle of complementarity which says that whether we see the particle or wave nature of a quantum particle depends on the experimental setup.

The Bell Inequalities or the Bell Theorem

In 1964, John Bell proposed a statistical experimental test of the EPR argument. Here we present a version of the argument due to John Clauser, Michael Horne, Abner Shimony, and Richarch Holt (CHSH).

Let Alice and Bob have choice of making measurements A_1 or A_2 and B_1 or B_2, respectively. Thus jointly there are four possible measurements: (A_1, B_1), (A_1, B_2), (A_2, B_1), (A_2, B_2). Suppose we choose units such that these measurements can take the values $+1$ or -1. For our case we take the state to be an entangled singlet state and so we are measuring in units of $\hbar/2$.

Note that each pair of these observables are mutually exclusive as a set but we can built us a statistics of their joint values: $A_i \cdot B_j$. This quantity takes the value either $+1$ or -1. CHSH then proposed to measure the average value of $Q = A_1(B_1 - B_2) + A_2(B_1 + B_2)$. Q then can take values between $+2$ and -2.

This means that the average value of Q lies between -2 & $+2$.

$$\Rightarrow \boxed{-2 \leq \langle A_1 B_1 \rangle - \langle A_1 B_2 \rangle + \langle A_2 B_1 \rangle + \langle A_2 B_2 \rangle \leq +2}$$

This is knows as the CHSH inequality and it is an example of a Bell inequality. It was derived assuming that A_i & B_j can take values independent of each other.

What values does quantum mechanics predict?

The values of $\langle A_i B_j \rangle$ in quantum mechanics will depend on both our choice of A_i & B_j as well as the state with respect to which we take the average.

For measurement we consider a spin measurement in the x-z plane in which the angle of the axis of measurement makes an angle θ from the z-axis. This direction is defined by the unit vector $\hat{n} = (\sin\theta, 0, \cos\theta)$ and the measurement is $W_\theta = \frac{2}{\hbar}\hat{n}\cdot\vec{S} = \sin\theta\, \mathbb{X} + \cos\theta\, \mathbb{Z}$.

We can now calculate $\langle W_{A\theta} W_{B\theta'}\rangle$ for the singlet Bell state:

We first observe:

$$\mathbb{X}|0\rangle = |1\rangle \;\;\&\;\; \mathbb{X}|1\rangle = |0\rangle$$

And so

a) $\mathbb{X}_A\mathbb{X}_B|\beta_{11}\rangle = \mathbb{X}_A\mathbb{X}_B\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) = -\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = -|\beta_{11}\rangle$

b) $\mathbb{X}_A\mathbb{Z}_B|\beta_{11}\rangle = \mathbb{X}_A\mathbb{Z}_B\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(-|11\rangle - |00\rangle) = -\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = -|\beta_{00}\rangle$

c) $\mathbb{Z}_A\mathbb{Z}_B|\beta_{11}\rangle = \mathbb{Z}_A\mathbb{Z}_B\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{-1}{\sqrt{2}}(|01\rangle - |10\rangle) = -|\beta_{11}\rangle$

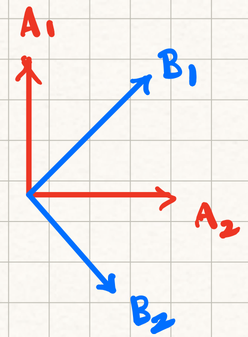
d) $\mathbb{Z}_A\mathbb{X}_B|\beta_{11}\rangle = \mathbb{Z}_A\mathbb{X}_B\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\beta_{00}\rangle$

Thus
$$\begin{aligned}\langle W_{A\theta} W_{B\theta'}\rangle &= \sin\theta\sin\theta'\langle\mathbb{X}_A\mathbb{X}_B\rangle + \sin\theta\cos\theta'\langle\mathbb{X}_A\mathbb{Z}_B\rangle \\ &\quad + \cos\theta\sin\theta'\langle\mathbb{Z}_A\mathbb{X}_B\rangle + \cos\theta\cos\theta'\langle\mathbb{Z}_A\mathbb{Z}_B\rangle. \\ &= -\sin\theta\sin\theta' + 0 + 0 - \cos\theta\cos\theta' = -\cos(\theta-\theta')\end{aligned}$$

Let us pause for a moment and see if this result makes sense. For $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ we see that $\mathbb{Z}_A$ & $\mathbb{Z}_B$ are anti-correlated. This agrees with $\theta = \theta' \Rightarrow \langle W_{A\theta}W_{B\theta}\rangle = -1$.

Now for A_i & B_j we choose

$$A_1 = W_0, \quad B_1 = W_{\frac{\pi}{4}}$$
$$A_2 = W_{\frac{\pi}{2}}, \quad B_2 = W_{\frac{3\pi}{4}}$$



And so

$$\langle Q \rangle = \langle W_0 W_{\frac{\pi}{4}} \rangle - \langle W_0 \; W_{\frac{3\pi}{4}} \rangle + \langle W_{\frac{\pi}{2}} W_{\frac{\pi}{4}} \rangle + \langle W_{\frac{\pi}{2}} W_{\frac{3\pi}{4}} \rangle$$

$$= \left(-\frac{1}{\sqrt{2}}\right) - \left(\frac{1}{\sqrt{2}}\right) + \left(-\frac{1}{\sqrt{2}}\right) + \left(-\frac{1}{\sqrt{2}}\right)$$

$$= -2\sqrt{2} < -2$$

Thus we see that in QM $\langle Q \rangle$ violates the CHSH inequality. By changing θ & θ' we can also obtain $\langle Q \rangle = 2\sqrt{2} > 2$.

Thus we see that QM violates the prediction of locally realistic hidden variable theory.

We have proved Bell's theorem.