

## Lecture 2

Tuesday, September 16, 2014  
10:29 AM

History: 2 clouds hanging over physics (late 1800's)

- Ether

- Ultraviolet catastrophe

Planck, 1900  
Einstein, 1905

Schrodinger, 1926:

We won't be at any specific system, "abstract"

We don't focus on natural progression, energy, Feynman diagrams, etc.

Want to know what can be done within the QM limitations. Engineer.

---

QM Properties:

1.) Indeterminism:

- We never fully know the state.

- Measurements are inherently non-deterministic.  
"randomness is free"

2.) Interference:

- Even one particle experiences interference (2-slit experiment)

3.) Uncertainty:

Position / momentum  
BB84 quantum key agreement.

4.) Superposition:

Two level systems "qubits"

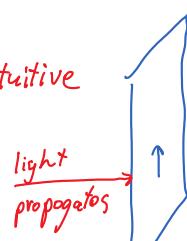
- spin of electron

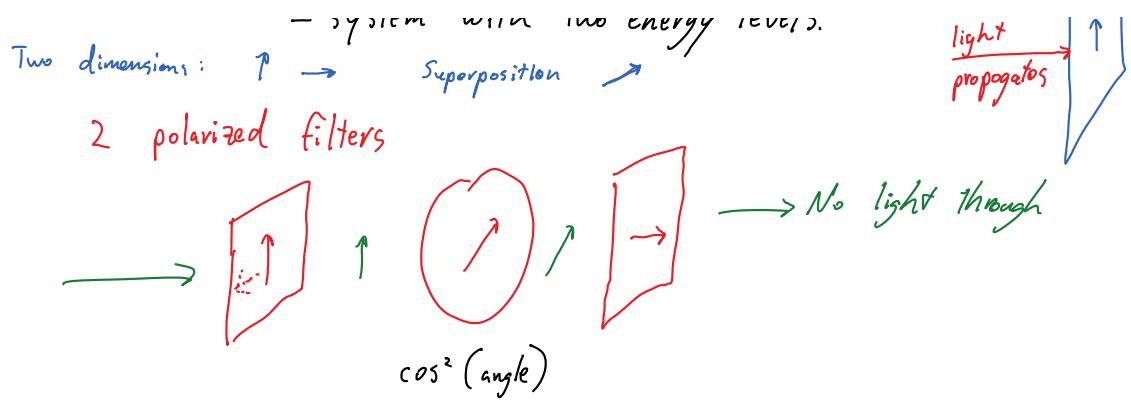
- polarization of photon

- system with two energy levels.

Two dimensions:  $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \rightarrow \text{Superposition} \rightarrow \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

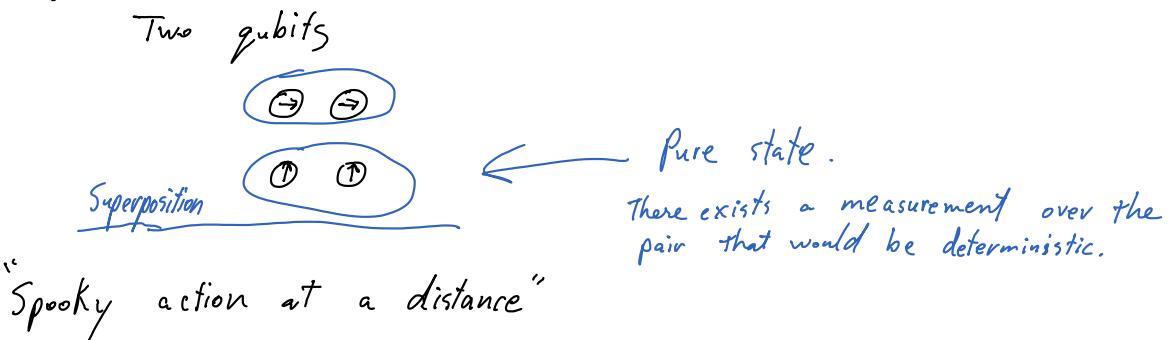
intuitive





- Superposition is a consequence of the linearity of QM.
- Maintaining an arbitrary superposition is key to quantum computing.

## 5.) Entanglement



Einstein, Podolsky, Rosen : "local hidden-variable theory"

Bell's Theorem: (1964)

Entanglement cannot be explained by local hidden variables.

Start with a perfectly entangled state between two qubits.

Measure each at angle  $\theta$  and  $\phi$ .



Let  $m(p_x, \theta)$  be the outcome of first measurement  $\leftarrow$  binary  
 $m(p_y, \phi)$

Notation :  $X_\theta = m(p_x, \theta)$ ,  $Y_\phi = m(p_y, \phi)$

$$\text{QM: } P(X_\theta \neq Y_\phi) = 1 - P(X_\theta = Y_\phi) = 1 - \cos^2(\theta - \phi) \\ = \sin^2(\theta - \phi)$$

L HV:  $\{X_\theta, Y_\phi\}_{\theta, \phi}$  are R.V.'s

$$P(X_\Delta \neq Y_{-\Delta}) \leq P(X_\Delta \neq Y_0) + \cancel{P(X_0 \neq Y_0)} + P(X_0 \neq Y_{-\Delta}) \\ \sin^2(2\Delta) \leq 2 \sin^2(\Delta) \quad \begin{matrix} \rightarrow \\ \text{union bound} \\ \text{Contradiction.} \end{matrix}$$

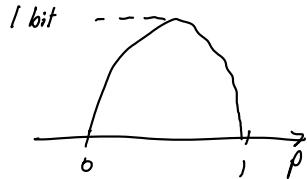
Classical:

"Bit": Physical  
Binary unit in memory (switch on or off)

Information: What is the result of a coin flip?

Biased coin with prob.  $p$ .

$$h(p) = p \log_2 \frac{1}{p} + (1-p) \log_2 \frac{1}{1-p}$$



Quantum bit ("qubit")

Physical: Two-dimensional state  
(level)

Information:

Example: A specific pure state is prepared

↑ No entropy.

Measure  $+$ , always get  $\uparrow$ . Deterministic.

However, measure  $\times$ , get random binary output.

Random state preparation:

$$\uparrow \text{w.p. } \frac{1}{2} p \rightarrow \text{w.p. } \frac{1}{2} (1-p)$$

$$\text{Entropy} = \cancel{1 \text{ bit}} h(p)$$

Measure +, get uniform binary  $\text{Bern}(p)$   
 Measure X, get uniform binary

Quantum (von Neumann) entropy is probabilistic (Shannon) entropy of best rank 1 measurement  
 (the one that minimizes entropy)

Random state preparation:

$$\uparrow \text{w.p. } \frac{1}{2} \rightarrow \text{w.p. } \frac{1}{2}$$

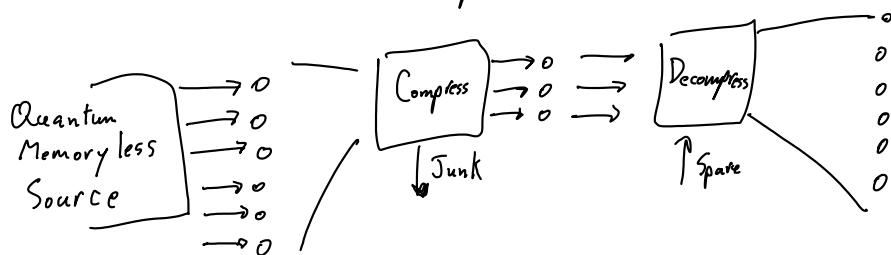
Measure +, outcome is  $\text{Bern}\left(\frac{3}{4}\right)$ ,  $h\left(\frac{3}{4}\right) \approx 0.81$  bits

Measure X,

Measure  ~~$\sqrt[4]{35^\circ}$~~ ,  $\text{Bern}\left(\sin^2\left(\frac{\pi}{8}\right)\right)$ ,  $h \approx 0.6$  bits

Is there a notion of compression related to this definition of entropy?  
 Yes

Schumacher compression:



Quantum extensions to classical information theory tools:

- method of types
- typical set  $\rightarrow$  typical subspace
- total variation  $\rightarrow$  trace distance
- mutual information:  $I(X;Y) = H(X) + H(Y) - H(X,Y)$

- mutual information :

$$\begin{aligned} I(X;Y) &= H(X) + H(Y) - H(X,Y) \\ &= H(X) - H(X|Y) \end{aligned}$$

QIT

Difficult to define

Quantum extensions of operational tasks:

- Capacities (quantum and classical)
  - Compression
  - Privacy Coding
    - Quantum noise is equivalent to entanglement with environment.
- environment "learns" about system

Tradeoffs between resources:

Example : Teleportation :

