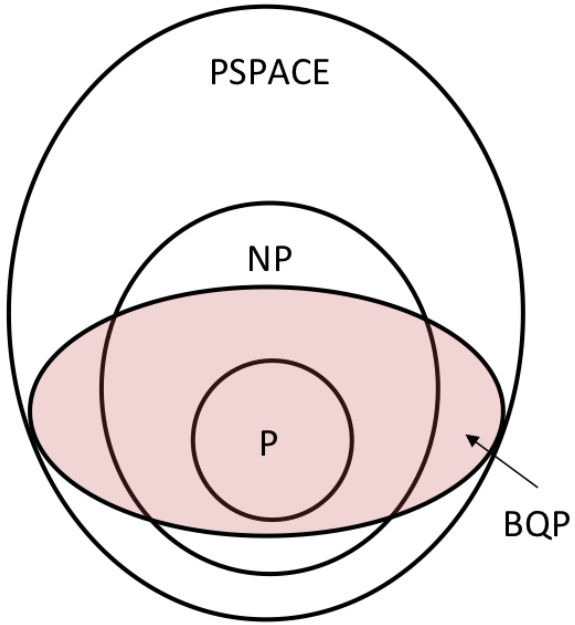
COL863: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

Introduction: Quantum Algorithms

- There are three types of Quantum Algorithms:
  - Using quantum parallelism as in the Deutsch-Jozsa algorithm.
  - Quantum search.
  - Quantum simulation.

- There are three types of Quantum Algorithms:
  - Using quantum parallelism as in the Deutsch-Jozsa algorithm.
  - Quantum search.
  - Quantum simulation.
- How powerful is quantum computation?
  - Classical computational complexity has been methodically studied. Where does quantum computation fit in the picture?

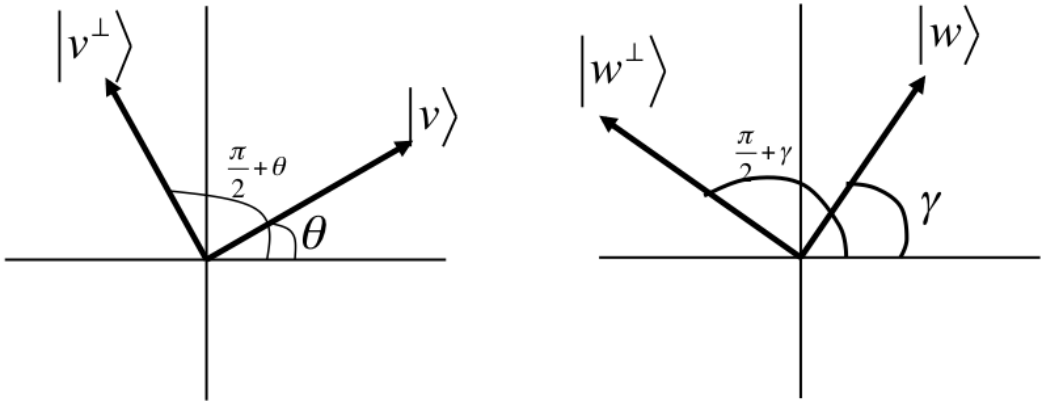


- There are a lot of subtle issues to address when developing the general area of quantum information theory. However, classical information theory provides a general outline for the questions that may be relevant.
- We may want to obtain the quantum versions of the two fundamental results of information theory:
  - Shannon's noiseless channel theorem: Quantifies the resources required to transmit information from a classical information source.
  - Shannon's noisy channel theorem: Quantifies the amount of resources needed to transmit through a channel that is noisy.
- Since quantum resource and information source are fundamentally different from a classical one, these theorems have to be revisited we should be prepared for surprises.

- Claim: It may not be possible to distinguish between the quantum states $|0\rangle, |1\rangle, |+\rangle, |-\rangle$.
- Given the above fact here is an interesting protocol for preventing counterfeiting currency.
  - Every currency note in addition to having a classical serial number also has sequence of qubits that are either $|0\rangle$ or $|+\rangle$.
- There are other interesting protocols based on similar ideas.

Introduction: Entanglement

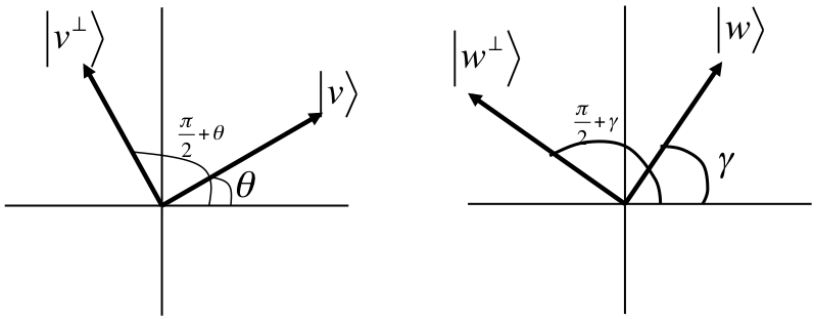
- We said that one can measure in any orthonormal basis.
- Often, we would want to measure in a basis that is rotation of the standard basis.



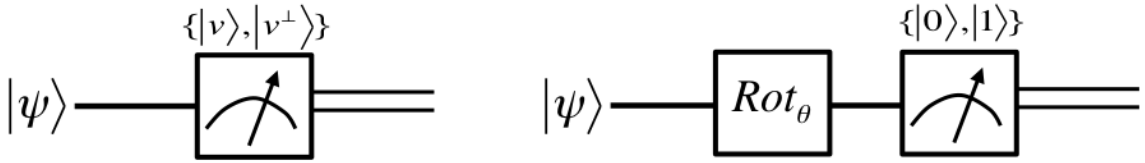
- So, $|v\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$ and $|v^\perp\rangle = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle$
- Claim: Making a measurement in the $\{|v\rangle, |v^\perp\rangle\}$ basis is the same as making a measurement in the standard basis after applying the following gate:

$$Rot_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$$

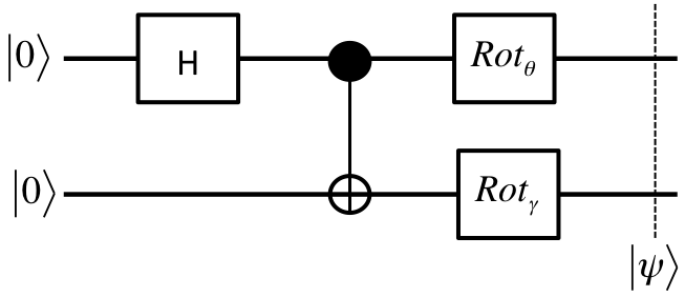
- We said that one can measure in any orthonormal basis.
- Often, we would want to measure in a basis that is rotation of the standard basis.



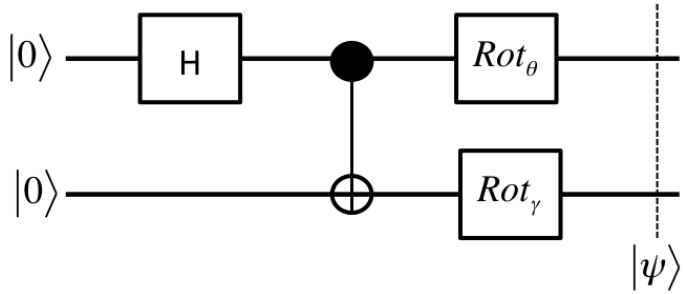
- So, $|v\rangle = \cos\theta\,|0\rangle + \sin\theta\,|1\rangle$ and $\left|v^\perp\right\rangle = -\sin\theta\,|0\rangle + \cos\theta\,|1\rangle$
- Claim: Making a measurement in the $\{|v\rangle, \left|v^\perp\right\rangle\}$ basis is the same as making a measurement in the standard basis after applying the following gate: $Rot_\theta = \begin{bmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{bmatrix}$.
- In terms of circuits, the following two circuits exhibit the same measurement results.



- Let $\Delta = \theta - \gamma$. What is output of the following circuit $|\psi\rangle$?



- Let $\Delta = \theta - \gamma$. What is output of the following circuit $|\psi\rangle$?

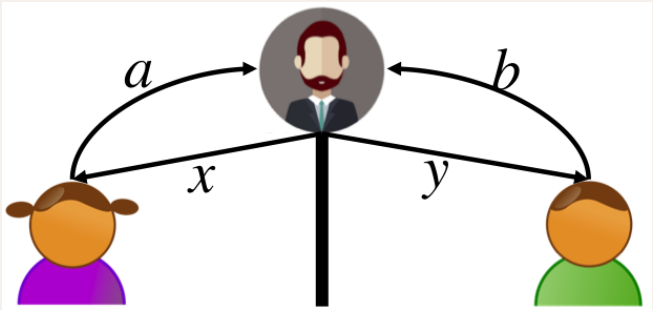


$|\psi\rangle = \frac{1}{\sqrt{2}}(\cos\Delta\,|00\rangle + \sin\Delta\,|01\rangle - \sin\Delta\,|10\rangle + \cos\Delta\,|11\rangle)$

- Corollary: Suppose Alice has the first qubit and Bob has the second qubit. Then on measurement of $|\psi\rangle$, the output is same with probability $\cos^2\Delta$ and different with probabiity $\sin^2\Delta$.

CHSH game

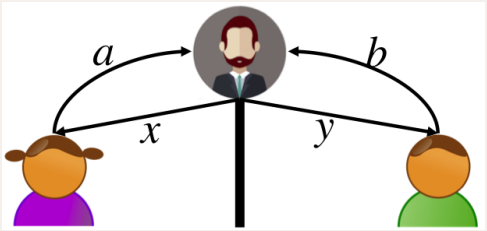
Alice and Bob receive randomly generated bits $x, y \in \{0, 1\}$ respectively from a Charlie. Their goal is to respond with bits a and b such that $a \oplus b = x \wedge y$. They are not allowed to communicate after receiving x and y.



- Lemma 1: There is no classical deterministic or randomized strategy that allows Alice and Bob to win with probability more than $3/4$.
- Lemma 2: There is a quantum strategy that allows Alice and Bob to win with probability $\cos^2 \pi/8 \approx 0.85 > 3/4$.

CHSH game

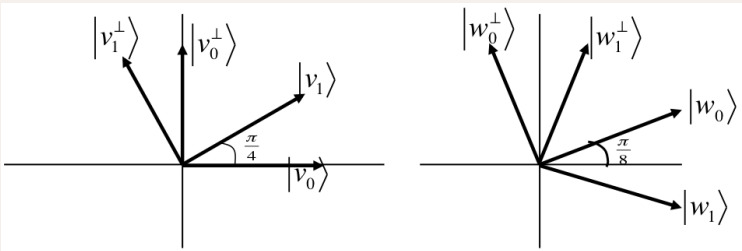
Alice and Bob receive randomly generated bits $x, y \in \{0, 1\}$ respectively from a Charlie. Their goal is to respond with bits a and b such that $a \oplus b = x \wedge y$. They are not allowed to communicate after receiving x and y.



- Lemma 2: There is a quantum strategy that allows Alice and Bob to win with probability $\cos^2 \pi/8 \approx 0.85 > 3/4$.

Quantum strategy

- Alice and Bob share an EPR pair $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$ to start with.
- Alice and Bob measure in basis $\{|v_x\rangle, |v_x^\perp\rangle\}$, $\{|w_x\rangle, |w_x^\perp\rangle\}$ respectively and they simply return their measurement outputs.



End