Quantum Information

Lecture #2

What is quantum information? This is a deep question whose general answer we won't attempt here.

In the context of classical digital computing information is a string of 0s and 1s. Thus if we have a byte it maybe something like 01101011. When we move to quantum computation the analogous information is the specification of the state in the computational basis $|01101011\rangle$.

In quantum computing we represent each bit by a two-level quantum system whose basis states are $|0\rangle$ & $|1\rangle$. This is the qubit.
States that require more information require multiple qubits. The state $|01101011\rangle$ require 8 qubits.

In a classical computer a single register can only have a finite number of states. 2^8 states for a register that is 1 byte long. In quantum information theory one can have an arbitrary linear combination of the computational basis. A quantum register can take on an infinite number of states.

The fact that one can have superposition of states mean that a quantum circuit (which is just a bunch of linear unitary operators) can act on many inputs simultaneously. However, this doesn't mean we can get <u>all</u> the answers simultaneously since observing the result will collapse the superposition of all the results into only one result. Thus to take advantage of quantum aspects of computing we shall need to perform the right kind of observations.

Entanglement is another aspect of quantum states that is not available to classical computers. By using entanglement as resources we can move quantum states around in a quantum computer in a non-local way.

Entanglement also allows us to be able to send classical information in high density known as super dense coding.

The Qubit

The simplest unit of quantum information is a two-level quantum mechanical system known as the qubit.
Physically a qubit can be realized in many different ways: a spin $\frac{1}{2}$ particle, the low lying states of an atom, an interferometer with two paths for photons each labelled 0 and 1. etc.

The Hilbert space of a qubit is $\mathbb{C}^2$. We denote by $|0\rangle$ and $|1\rangle$ the orthonormal basis of $\mathbb{C}^2$ which are the eigenkets of Z:

$$Z|0\rangle = |0\rangle$$

$$Z|1\rangle = -|1\rangle$$

An arbitrary state of a qubit is $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ with $|\alpha|^2 + |\beta|^2 = 1$.

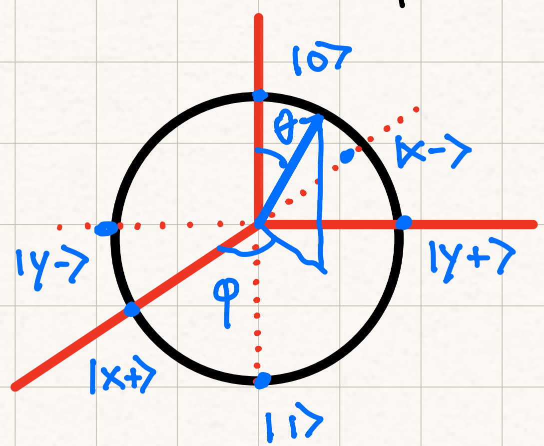
Taking into account the freedom $|\psi\rangle \sim \lambda|\psi\rangle$ we can write:

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$ [show]

where $0 < \varphi \leq 2\pi$ and $0 \leq \theta \leq \pi$.

As is obvious from this parametrization the pure states of a qubit are in 1-to-1 correspondence with the points of a sphere known as the

Bloch sphere:



Comment:

Each point on the surface of a Bloch sphere is a unique pure state.

The Density Matrix of a Qubit:

A density matrix is a Hermitian positive semi-definite matrix with unit trace. This means for a qubit ρ must have the form:

$$\rho = \frac{1}{2}(\mathbb{I}_2 + \bar{a}\cdot\bar{\sigma})$$

where $\bar{\sigma} = (X, Y, Z)$ are the Pauli operators. $\bar{a} = (a_x, a_y, a_z)$ is a real 3-vector. Paulis satisfy

$$\left.\begin{aligned} [\sigma_i, \sigma_j] &= 2i\,\epsilon_{ijk}\,\sigma_k \\ \{\sigma_i, \sigma_j\} &= 2\,\delta_{ij}\,\mathbb{I}_2 \end{aligned}\right\} \quad \sigma_i\sigma_j = i\,\epsilon_{ijk}\sigma_k + \delta_{ij}$$

i) $\vec{a} \Rightarrow$ Bloch vector. When $|\bar{a}| = 1 \Rightarrow$ The state is on the surface of the Bloch sphere and thus the state is pure.

ii) $|\bar{a}| < 1 \Rightarrow$ The states are inside the Bloch sphere. ρ then represents mixed states:

$$\mathrm{Tr}\,\rho^2 = \mathrm{Tr}\left[\tfrac{1}{2}(\mathbb{I} + \bar{a}\cdot\bar{\sigma})\right]^2 = \mathrm{Tr}\left[\tfrac{1}{4}\left\{\mathbb{I} + (\bar{a}\cdot\bar{\sigma})(\bar{a}\cdot\bar{\sigma}) + 2\,\bar{a}\cdot\bar{\sigma}\right\}\right]$$

$$= \frac{2}{4} + \frac{a_i a_j}{4}\,\mathrm{Tr}(\sigma_i\sigma_j) + 0$$

$$= \frac{1}{2} + \frac{a_i a_j}{4}\,2\delta_{ij} = \frac{1}{2} + \frac{|\bar{a}|^2}{2} = \frac{1}{2}(1 + |\bar{a}|^2)$$

Thus $|\bar{a}|^2 < 1 \Rightarrow \mathrm{Tr}\,\rho^2 < 1$.

Innerproduct between two mixed states:

$\mathrm{Tr}(\rho_1\rho_2) = \frac{1}{2}(1 + \bar{a}_1\cdot\bar{a}_2)$ For pure states $\mathrm{Tr}(\rho_1\rho_2) = |\langle\psi_1|\psi_2\rangle|^2$

The state $\vec{a} = 0$ corresponds to the maximally mixed state:

$$\rho = \tfrac{1}{2}|0\rangle\langle 0| + \tfrac{1}{2}|1\rangle\langle 1|.$$

Ambiguity of Mixtures:

Any <u>convex</u> linear combination of Bloch vectors:

$$\vec{a} = p_1 \bar{a}_1 + p_2 \bar{a}_2 + \cdots + p_n \bar{a}_n \quad \text{s.t.} \quad p_1 + p_2 + \cdots + p_n = 1$$

is also a valid Bloch vector.

Proof: $p_1 \bar{a}_1 + p_2 \bar{a}_2$

$$\begin{aligned} \rho &= p_1 \rho_1 + p_2 \rho_2 \\ &= \frac{p_1}{2} (\mathbb{I} + \bar{a}_1 \cdot \bar{\sigma}) + \frac{p_2}{2} (\mathbb{I} + \bar{a}_2 \cdot \bar{\sigma}) \\ &= \frac{(p_1 + p_2)}{2} \mathbb{I} + \frac{1}{2} (p_1 \bar{a}_1 + p_2 \bar{a}_2) \cdot \bar{\sigma} \\ &= \frac{1}{2} \mathbb{I} + \frac{1}{2} \vec{a} \cdot \bar{\sigma} \end{aligned}$$

This implies that any mixed state can be written as a convex linear combination of an arbitrary number of valid density matrices. This is known as the ambiguity of mixtures.

Measurements in Quantum Mechanics:

The measurement postulate stated in the last lecture is what is known as a von Neumann measurement or a projective measurement. But quantum mechanics allows for a more generalized measurement postulate:

Generalized Measurements:

Quantum measurements are described by a collection $\{M_m\}$ of measurement operators. These are operators which act on the state space of the system that is being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the system is $|\psi\rangle$ immediately before the measurement then the probability that the result m occurs is given by

$$p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$$

and the state of the system after the measurement is

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$$

The measurement operators satisfy the completeness condition

$$\sum_m M_m^\dagger M_m = \mathbb{I}$$

which follow from $\sum_m p(m) = 1$.

<u>Exercise:</u> Show that a projective measurement is a type of generalized measurement.

POVM Measurements

In the generalized measurement postulates there are two parts. 1st it gives a way to compute the probabilities of each outcome and then end it gives us the state of the system after the measurement. However in many applications we are not interested in the state of the system after the measurement. For example there are experiments where we measure the system only once at the conclusion of the experiment. In such cases we use a variation of the generalized measurement known as POVM.

Suppose a generalized measurement is described by the operators M_m, and the state of the system is $|\psi\rangle$. Then $p(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle$. Suppose we define $E_m = M_m^\dagger M_m$ then from the postulate

$$\sum_m E_m = \mathbb{1}$$

And from linear algebra E_m is a positive operator. E_m then are known as POVM elements and $p(m) = \langle\psi|E_m|\psi\rangle$.

An Example: Suppose Alice prepares two states $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$. Alice gives Bob one of these states. Since $|\psi_1\rangle$ and $|\psi_2\rangle$ are not orthogonal Bob can not determine whether he had been given $|\psi_1\rangle$ or $|\psi_2\rangle$ with perfect reliability. But Bob can make a POVM measurement which distinguishes the state some of the time but he never makes an error of mis-identification. The POVM contains:

$$E_1 = \frac{\sqrt{2}}{1+\sqrt{2}} |1\rangle\langle 1|$$

$$E_2 = \frac{\sqrt{2}}{1+\sqrt{2}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{\langle 0| - \langle 1|}{\sqrt{2}}\right)$$

$$E_3 = 1 - E_1 - E_2 .$$