# Lecture 6



The story so far!

Unlike classical bit which can take 0 or 1 at a time, in case of quantum bit it can take a linear superposition of 0 and 1. Infact this is why what provides quantum computing enormous parallel computing capabilities.

Let us now extend this concept to multiple qubits.

## A two qubit system

classical 2 bits are : 00, 01, 10, 11

Quantum 2 qubit state is a linear superposition:

$$\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle \quad \rightarrow (1)$$

which is normalized,

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \quad \rightarrow (2)$$

Please note:

$$|00\rangle = |0\rangle \otimes |0\rangle$$

$$|01\rangle = |0\rangle \otimes |1\rangle, \text{ and so on.}$$

There is an important catch in the case of 2-qubit system. Here, one can make measurement either in the first 1st qubit or in the 2nd qubit.

For example, if we make a measurement on the 1st qubit and get $|0\rangle$, then it means that the state of the 2-qubit is either $|00\rangle$ with ~~so~~ probability amplitude $\alpha_{00}$ or $|01\rangle$ with prob. amplitude $\alpha_{01}$, because these are the only two states with $|0\rangle$ in the first position.

Probability of measuring 0 in the 1st qubit is $|\alpha_{00}|^2 + |\alpha_{01}|^2$. The past measurement state is : $\dfrac{\alpha_{00}|00\rangle + \alpha_{01}|01\rangle}{\sqrt{|\alpha_{00}|^2 + |\alpha_{01}|^2}}$

Now depending on the values of the constants $\alpha_{ij}$, ~~$\alpha_{ij}$'s~~ which in general are complex, we can obtain different types of states. For example,

$$|\psi_+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

This state is different from the corresponding single qubit state. Suppose we make a measurement on qubit - 1, then we have the following possibilities: either we will get $|0\rangle$ or $|1\rangle$, each with probability $\frac{1}{2}$.

Note however, that ~~we~~ when we measure the state $|0\rangle$, the state of the second qubit (qubit - 2) is automatically determined.

If 1st qubit $= 1$

Then, $\Rightarrow$ 2nd qubit $= 0$

This is peculiar, as we have not measured the 2nd qubit, we simply measured the 1st qubit only!

$\longrightarrow$ This is what is known as Entanglement.

Not all 2-qubit states can be written as a product of two single qubit states. Bell states are examples of such states:

$$\boxed{\begin{aligned} |\psi_+\rangle &= \frac{|01\rangle + |10\rangle}{\sqrt{2}}, \quad & |\psi_-\rangle &= \frac{|01\rangle - |10\rangle}{\sqrt{2}} \\ |\phi_+\rangle &= \frac{|00\rangle + |11\rangle}{\sqrt{2}}, \quad & |\phi_-\rangle &= \frac{|00\rangle - |11\rangle}{\sqrt{2}} \end{aligned}}$$

BELL STATES

## Matrix basis for two qubits



Basis for single qubit was

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Now, basis for 2 - Qubits

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|01\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|11\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

This provides us a basis, $\left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \right\}$

Question How much information is there ?

If we have one qubit, we need 2 complex co-efficients

for two qubits, we need $2^2$ complex coefficients

for $n$ qubits, we need to have $2^n$ complex coefficients.

So for a $n$-qubit system there are $2^n$ possibilies of getting either 0 or 1. However most of such information remain hidden.

When we make a measurement we will get only $n$-bits of information.

## Process of measurement

Earlier we learnt, in a computational basis (CB) a single qubit is represented as:

$$\alpha|0\rangle + \beta|1\rangle$$

While making a measurement in CB, we get to know $\alpha$ and $\beta$. But not the relative phase. However infer some information about the relative phase could be obtained ~~ix~~ if measurement is made in the diagonal basis.

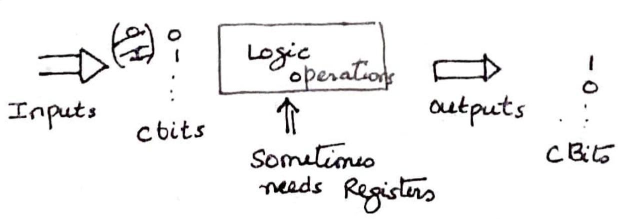
In Quantum computing, measurement process is made by something called quantum gates. Let us first talk about single qubit gates.

Quantum gates are analogous to classical logic gates, except that they must be ~~impletem~~ implemented unitarily (and thereby reversibly).

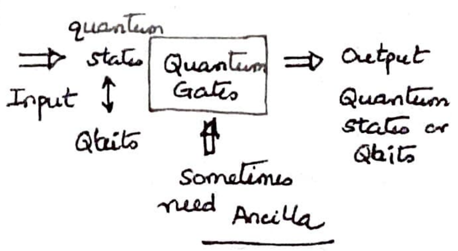
( In the case of classical computing, the only single bit gate is a NOT gate $0 \longrightarrow 1$, which is reversible.)

As, quantum states evolve unitarily, the operator which act on a single qubit state has to be unitary $U^{\dagger}U = I$, which preserves norm.

classical computing:




Quantum computing:



## Operation on CBITS

In quantum computation, almost all operations on Qbits are reversible.

An example of an irreversible operation is Erase:

$|0\rangle \rightarrow |0\rangle \quad , \quad |1\rangle \longrightarrow |0\rangle$

It is irreversible because one cannot reconstruct the input from the output: it has no inverse.

There are just two reversible operations on a single cbit:

(i) Do nothing

$$I\,|0\rangle = |0\rangle \quad , \quad I\,|1\rangle = |1\rangle \qquad (I: \text{identity operator})$$

(ii) Flip it

$$X\,|0\rangle = |1\rangle \quad , \quad X\,|1\rangle = |0\rangle \qquad \left(\begin{array}{l}\text{Flip operator } X \\ \text{QM}: \ \sigma_x\end{array}\right)$$

Less trivial reversible operations are available on two cbits. One can, for example, exchange the values of the bits they represent (swap operator $S$):

$$S\,|xy\rangle \equiv |yx\rangle$$

In manipulating such multi-cbit operations, it is useful to have a compact notion for the action on a many cbit state of operations that act on only a single one of the cbits. One labels the cbits by integers $0, 1, 2, \dots$ associated with the power of 2 that each cbit represents.

Thus if $x$ has a binary expansion $\cancel{x = 8x}$

$x = 8x_3 + 4x_2 + 2x_1 + x_0$ , then

$$|x\rangle_4 = |x_3 x_2 x_1 x_0\rangle = |x_3\rangle |x_2\rangle |x_1\rangle |x_0\rangle$$
$$= |x_3\rangle \otimes |x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle$$

An operation that acts only on cbit no. 2 is

$$X_2 = 1 \otimes X \otimes 1 \otimes 1$$

Clearly the form with a subscript indicates which of the four cbits is subject to the flip operation $X$ is more transparent than the explicit form of the operator tensor product on the right.

$$X_2 \left[ |x_3\rangle \otimes |x_2\rangle \otimes |x_1\rangle \otimes |x_0\rangle \right] = |x_3\rangle \otimes \left[ X|x_2\rangle \right] \otimes |x_1\rangle \otimes |x_0\rangle$$

Consider the following c-bit operation on one cbit:

$$Z|0\rangle = |0\rangle \qquad (\sigma_z)$$
$$Z|1\rangle = -|1\rangle$$

In the context of cbits, this operation is meaningless! Only the two vectors $|0\rangle$ and $|1\rangle$ have meaning as the two distinguishable states of cbit used to represent 0 and 1.

Meaningless $\longrightarrow$ meaningful !

Consider the 2 cbit operation : $\frac{1}{2}(I + Z_1 Z_0)$.

It acts as ~~the~~ the identity on the 2 cbit states $|0\rangle|0\rangle$ and $|1\rangle|1\rangle$, while giving 0 when acting on $|0\rangle|1\rangle$ or $|1\rangle|0\rangle$.

On the other hand, the operation $\frac{1}{2}(I - Z_1 Z_0)$ acts as the identity on $|0\rangle|1\rangle$ and $|1\rangle|0\rangle$ while giving 0 on $|0\rangle|0\rangle$ and $|1\rangle|1\rangle$.

Now, note the operations

$$S_{10}|1\,0\rangle = |0\,1\rangle$$
$$S_{10}|0\,1\rangle = |1\,0\rangle$$
$$S_{10}|0\,0\rangle = |0\,0\rangle$$
$$S_{10}|1\,1\rangle = |1\,1\rangle$$
$$X_1 X_0 |0\,1\rangle = |1\,0\rangle$$
$$X_1 X_0 |1\,0\rangle = |0\,1\rangle$$
$$\frac{1}{2}(I + Z_1 Z_0)|0\,0\rangle = |0\,0\rangle$$
$$\frac{1}{2}(I + Z_1 Z_0)|1\,1\rangle = |1\,1\rangle$$
$$\frac{1}{2}(I - Z_1 Z_0)|0\,1\rangle = |0\,1\rangle$$
$$\frac{1}{2}(I - Z_1 Z_0)|1\,0\rangle = |1\,0\rangle$$

Thus we may represent $S_{10}$ as follows:

$$S_{10} = \frac{1}{2}(I + Z_1 Z_0) + X_1 X_0 \frac{1}{2}(1 - Z_1 Z_0)$$

or

$$S_{10} = \frac{1}{2}(I + Z_1 Z_0 + X_1 X_0 - Y_1 Y_0)$$

where $Y = XZ$ $\quad (-i\sigma_y$ in QM$)$

Another important example of a 2-cbit operation is the <u>controlled - NOT</u> or reversible XOR :

$$C_{10} |x\rangle |y\rangle = (X_0)^x |x\rangle |y\rangle = |x\rangle |y \oplus x\rangle$$

where $\oplus$ denotes <u>addition modulo 2</u>.

$C_{10}$ flips cbit 0 (the target bit) if and only if cbit 1 (the control cbit) has the value 1.

We can build this operation out of ~~1-Q~~ 1-cbit projections,

$$C_{10} = \frac{1}{2}(1 + Z_1) + X_0 \frac{1}{2}(1 - Z_1)$$

$$= \frac{1}{2}(1 + Z_1 + X_0 - X_0 Z_1)$$

One can see that, interchanging the operations X and Z has the effect of exchanging the roles of target and control cbit, converting $C_{10}$ to $C_{01}$.

$$C_{10} |00\rangle = |00\rangle$$
$$C_{10} |10\rangle = |11\rangle$$
$$C_{10} |11\rangle = |10\rangle$$
$$\cancel{C_{10} |10\rangle =}$$
$$C_{10} |01\rangle = |01\rangle$$

# The Hadamard transform

$$H = \frac{1}{\sqrt{2}}\left(X + Z\right) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

This transform takes the cbit states $|0\rangle$ and $|1\rangle$ into two classically meaningless linear combinations $\frac{1}{\sqrt{2}}\left(|0\rangle \pm |1\rangle\right)$!

Because:

$$X^2 = Z^2 = I$$
$$XZ = -ZX$$

it follows that:

$$H^2 = \frac{1}{2}\left(X+Z\right)^2 = I$$
$$HX = \frac{1}{\sqrt{2}}(X+Z)X = \frac{1}{\sqrt{2}}\left(I + ZX\right)$$
$$= \frac{1}{\sqrt{2}} Z(X+Z) = ZH$$

$$\Rightarrow \quad HX = ZH$$

and therefore:

$$HXH = Z$$
$$HZH = X$$

Consequently, we can use four classically meaningless operations H to achieve a classically meaningful task: interchanging the role of target and control bits:

$$\boxed{C_{01} = \left(H_1 H_0\right) C_{10} \left(H_1 H_0\right)}$$

Note:

$$C_{10}\, |x\rangle |y\rangle = |x\rangle |y \oplus x\rangle$$
$$C_{01}\, |x\rangle |y\rangle = |x \oplus y\rangle |y\rangle$$