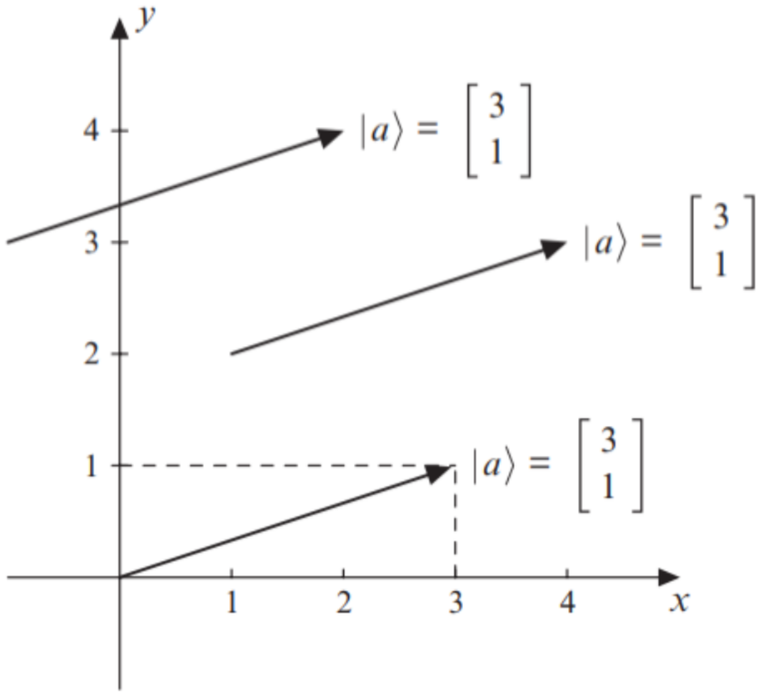
Linear Algebra

Ket : column vector ($|v\rangle$)
Bra : Row vector ($\langle v|$)

Dimension : number of elements in vector

Each element in Ket (or Bra) gives amount of change in the coordinates with respect to the initial points



Ket representation with different initial points

Length of vector $||v\rangle|$: if $|v\rangle = \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{bmatrix}$; $||v\rangle| = \sqrt{a_1^2 + a_2^2 + \ldots\ldots + a_n^2}$

or $||v\rangle| = \sqrt{\langle v|v\rangle}$

if $|v\rangle = \dfrac{|a\rangle}{||a\rangle|}$;

$||v\rangle| = 1$.

Orthogonal vectors:

From pythagorean theorem for orthogonality : $||a\rangle|^2 + ||b\rangle|^2 = ||a+b\rangle|^2$

or

$\langle a|b\rangle = 0$

Eg. of orthonormal basis : $\left\{ \begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix}, \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} \right\}$, $\left\{ \begin{bmatrix} 1/2 \\ \sqrt{3}/2 \end{bmatrix}, \begin{bmatrix} \sqrt{3}/2 \\ -1/2 \end{bmatrix} \right\}$

Standard bases : $|\uparrow\rangle = \begin{bmatrix}1\\0\end{bmatrix}$, $|\downarrow\rangle = \begin{bmatrix}0\\1\end{bmatrix}$; $|\rightarrow\rangle = \begin{bmatrix}1/\sqrt{2}\\-1/\sqrt{2}\end{bmatrix}$, $|\leftrightarrow\rangle = \begin{bmatrix}1/\sqrt{2}\\1/\sqrt{2}\end{bmatrix}$

$$|\nearrow\rangle = \begin{bmatrix}1/2\\-\sqrt{3}/2\end{bmatrix}, \quad |\swarrow\rangle = \begin{bmatrix}\sqrt{3}/2\\1/2\end{bmatrix}$$

Vectors as a linear combination of standard basis

Eg. $\begin{bmatrix}c\\d\end{bmatrix} = x_1|\rightarrow\rangle + x_2|\leftrightarrow\rangle$

$$\langle\rightarrow| \begin{bmatrix}c\\d\end{bmatrix} = x_1\langle\rightarrow|\rightarrow\rangle + x_2\langle\rightarrow|\leftrightarrow\rangle$$

$$= x_1$$

$$\begin{bmatrix}1/\sqrt{2} & -1/\sqrt{2}\end{bmatrix}\begin{bmatrix}c\\d\end{bmatrix} = x_1 \qquad \therefore x_1 = \frac{c-d}{\sqrt{2}}$$

$$\langle\leftarrow| \begin{bmatrix}c\\d\end{bmatrix} = x_1\langle\leftarrow|\rightarrow\rangle + x_2\langle\leftarrow|\leftarrow\rangle$$

$$\begin{bmatrix}1/\sqrt{2} & 1/\sqrt{2}\end{bmatrix}\begin{bmatrix}c\\d\end{bmatrix} = x_2 \qquad \therefore x_2 = \frac{c+d}{\sqrt{2}}$$

In general; if $|v\rangle = x_1|b_1\rangle + x_2|b_2\rangle + \ldots + x_n|b_n\rangle$

where $x_i = \langle b_i|v\rangle$

and all x_i's are called probability amplitudes and their squares tell us the probability of $|v\rangle$ jumping on $|b_i\rangle$ when we measure them.

Ordered basis

$(|\uparrow\rangle, |\downarrow\rangle) \neq (|\downarrow\rangle, |\uparrow\rangle)$, when we change the order, it's like flipping the entire apparatus (/magnets) by 180°.

* normal brackets used instead of curly brackets.

Matrix multiplication

if $A = \begin{bmatrix} 1 & -4 & 2 \\ 2 & 3 & 0 \end{bmatrix}$; $B = \begin{bmatrix} 1 & 2 \\ 7 & 5 \\ 6 & 1 \end{bmatrix}$

whenever we do multiplication, bra comes before kets

$\therefore A = \begin{bmatrix} \langle a_1| \\ \langle a_2| \end{bmatrix}$ where $\langle a_1| = [1 \ -4 \ 2]$; $\langle a_2| = [2 \ 3 \ 0]$

$B = [|b_1\rangle \ |b_2\rangle]$ where $|b_1\rangle = \begin{bmatrix} 1 \\ 7 \\ 6 \end{bmatrix}$; $|b_2\rangle = \begin{bmatrix} 2 \\ 5 \\ 1 \end{bmatrix}$

$AB = \begin{bmatrix} \langle a_1| \\ \langle a_2| \end{bmatrix} [|b_1\rangle \ |b_2\rangle] = \begin{bmatrix} \langle a_1|b_1\rangle & \langle a_1|b_2\rangle \\ \langle a_2|b_1\rangle & \langle a_2|b_2\rangle \end{bmatrix}$

If we want to find out if given set of kets are orthonormal or not, we can do the following:

let $A = [|b_1\rangle \ |b_2\rangle \ \dots \ |b_n\rangle]$

if $A^\dagger A = I_n$, then A is a set of orthonormal basis

And to represent a ket $|v\rangle$ in terms of linear combination of the basis vector A,

we can calculate $A^\dagger |v\rangle = \begin{bmatrix} \langle b_1| \\ \langle b_2| \\ \vdots \\ \langle b_n| \end{bmatrix} |v\rangle = \begin{bmatrix} \langle b_1|v\rangle \\ \langle b_2|v\rangle \\ \vdots \\ \langle b_n|v\rangle \end{bmatrix}$

Orthogonal matrix : $M^\dagger M = I_n$

* Quantum logic gates are orthogonal matrix

Hadamard gate: $\begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{bmatrix}$, ordered basis $(|\leftarrow\rangle, |\rightarrow\rangle)$

Spin and Qubits

Mathematics of quantum spin

- The vector space required to specify spin is 2-D irrespective of taking real or complex number

Choosing the direction of spin corresponds to choosing the orthonormal bases vectors.

Eg. If we had measured spin in vertical direction and got spin in N and now we want to find it's probability in horizontal direction

$$|\uparrow\rangle = c_1|\rightarrow\rangle + c_2|\leftarrow\rangle$$

using matrix $A = [|\rightarrow\rangle |\leftarrow\rangle] = \begin{bmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ -1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix}$

$$A^T|\uparrow\rangle = \begin{bmatrix} 1/\sqrt{2} & -1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix} = \begin{bmatrix} c_1 \\ c_2 \end{bmatrix}$$

↳ probability amplitude

If we take 4 kets: $\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle$; $-\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle$; $\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle$; $-\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle$

The first two kets are equivalent as both are just negative of the other, the case is same with the later two and their probabilities are also equal even if we measure it in some other directions.

However $\frac{1}{\sqrt{2}}|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle = |\leftarrow\rangle$ and $\frac{1}{\sqrt{2}}|\uparrow\rangle - \frac{1}{\sqrt{2}}|\downarrow\rangle = |\rightarrow\rangle$, so here if we measure in horizontal direction, we can distinguish them, so they are not equivalent.

How are the basis associated with given spin direction.

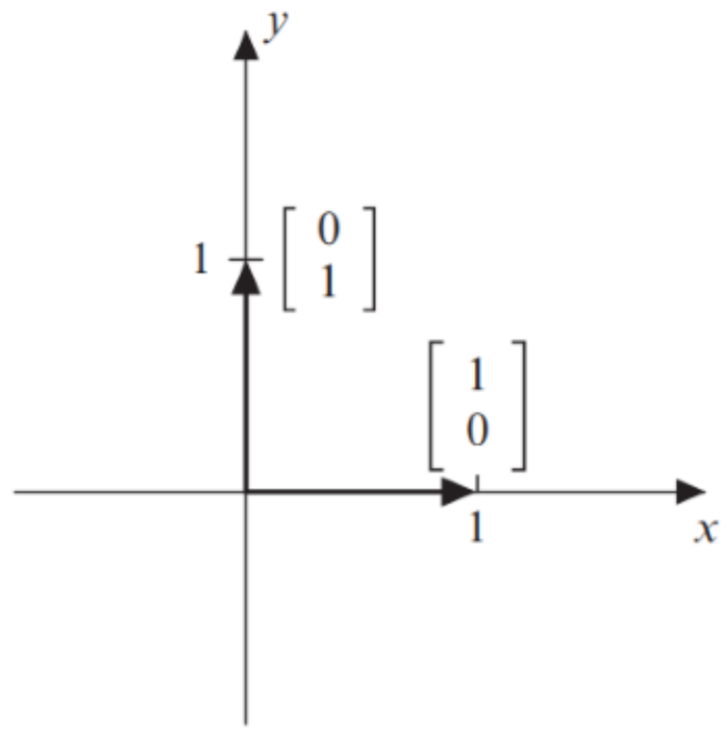


Figure 3.1
The standard basis.

we consider $(|\uparrow\rangle, |\downarrow\rangle)$ as standard basis, and

$$|\uparrow\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \; ; \; |\downarrow\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

* the kets are orthonormal

Now, we rotate the vectors by α°

so $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow \begin{bmatrix} \cos\alpha \\ -\sin\alpha \end{bmatrix}$ and

$$\begin{bmatrix} 0 \\ 1 \end{bmatrix} \rightarrow \begin{bmatrix} \sin\alpha \\ \cos\alpha \end{bmatrix}$$

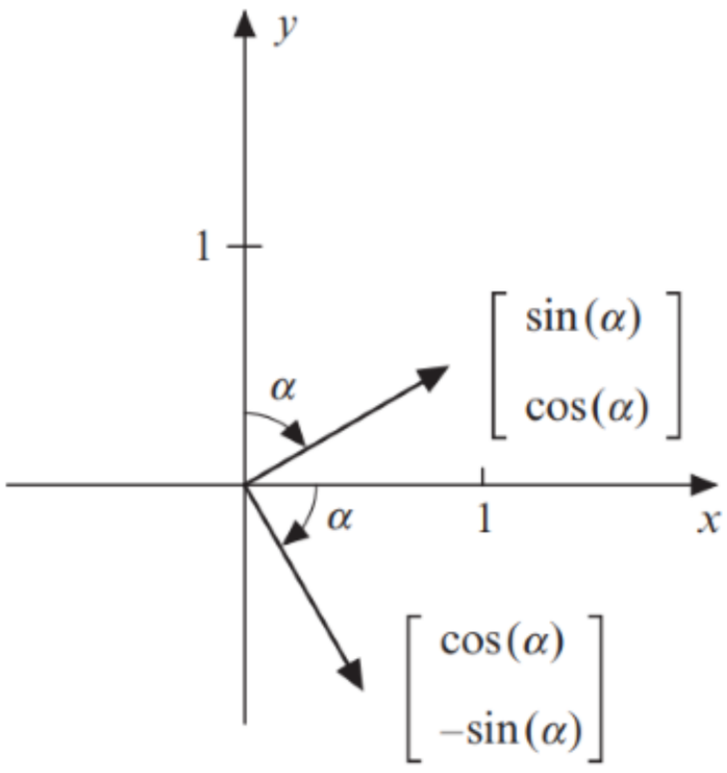


Figure 3.2
The standard basis rotated by α°.

when we reach at $\alpha = 90^\circ$,

$$\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix}\right) \rightarrow \left(\begin{bmatrix} 0 \\ -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix}\right)$$ and

we know that $\begin{bmatrix} 0 \\ -1 \end{bmatrix}$ is equivalent to $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$

so rotating through 90° brings us back to the same basis, except that the order of basis elements are interchanged.

Also, we need to rotate the apparatus by 180° only, to cover all possible directions, as an electron having N in 0° is sure to have S pole in 0°+180° direction.

* We get same measurement after rotating the apparatus by 180° or by rotating the basis vectors by 90°.

If θ° = rotation of apparatus and α° = rotation of basis vectors,

$\alpha = \theta/$

So, if we had measured spin in 0° direction and it turned out to be N, and then we rotated the apparatus by 60°, then its probability of having N in that condition is,

$$\begin{bmatrix}1\\0\end{bmatrix} = c_1\begin{bmatrix}\sqrt{3}/2\\-1/2\end{bmatrix} + c_2\begin{bmatrix}1/2\\\sqrt{3}/2\end{bmatrix}$$

$$A = \begin{bmatrix}\sqrt{3}/2 & 1/2\\-1/2 & \sqrt{3}/2\end{bmatrix}$$

$$A^T\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}\sqrt{3}/2\\1/2\end{bmatrix} = \begin{bmatrix}c_1\\c_2\end{bmatrix}$$

∴ its probability of having N would be $\left(\frac{\sqrt{3}}{2}\right)^2 = \frac{3}{4} = 75\%$

Alice, Bob and Eve

∴ Alice wants to send message to Bob, and Eve wants to eavesdrop.

Alice measures qubits in 240° and Bob plans to measure in 120°.

Standard basis of Alice : $\theta = 240°$; $\left\{\begin{bmatrix}\cos(\theta/2)\\-\sin(\theta/2)\end{bmatrix}, \begin{bmatrix}\sin(\theta/2)\\\cos(\theta/2)\end{bmatrix}\right\}$

0 1

$$= \left\{\begin{bmatrix}-1/2\\-\sqrt{3}/2\end{bmatrix}, \begin{bmatrix}-\sqrt{3}/2\\1/2\end{bmatrix}\right\}$$

we can multiply it with -1

$$= \left\{\begin{bmatrix}1/2\\\sqrt{3}/2\end{bmatrix}, \begin{bmatrix}\sqrt{3}/2\\-1/2\end{bmatrix}\right\}$$

Standard basis of Bob : $\theta = 120°$; $\left\{\begin{bmatrix}\cos(\theta/2)\\-\sin(\theta/2)\end{bmatrix}, \begin{bmatrix}\sin(\theta/2)\\\cos(\theta/2)\end{bmatrix}\right\}$

0 1

$$= \left\{\begin{bmatrix}1/2\\-\sqrt{3}/2\end{bmatrix}, \begin{bmatrix}\sqrt{3}/2\\1/2\end{bmatrix}\right\}$$

so if Alice wants to send 0, the ket sent is $\begin{bmatrix} 1/2 \\ \sqrt{3}/2 \end{bmatrix}$ and to see what Bob measures we do the following calculations

$$\begin{bmatrix} 1/2 & \sqrt{3}/2 \\ -\sqrt{3}/2 & 1/2 \end{bmatrix}^T \begin{bmatrix} 1/2 \\ \sqrt{3}/2 \end{bmatrix} = \begin{bmatrix} 1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & 1/2 \end{bmatrix} \begin{bmatrix} 1/2 \\ \sqrt{3}/2 \end{bmatrix} = \begin{bmatrix} -1/2 \\ \sqrt{3}/2 \end{bmatrix}$$

$\therefore$ Bob measures 0 with probability 1/4 and 1 with probability 3/4.

BB84 protocol (used to check if message is leaked or not)

- Assume Alice and Bob have accepted to use any of the two bases (Vertical and Horizontal) with equal probability and Alice wants to send Bob a string of length 4 N. (4N to make calc. easy)

- Now Alice, if wants to send 0 in Vertical direction, selects the basis $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ or else if in horizontal direction, selects the basis $\begin{bmatrix} 1/\sqrt{2} \\ -1/\sqrt{2} \end{bmatrix}$

- Bob will select any of the standard bases with equal probability, and thus will get the right qubit measurements half the times.

- Alice and Bob also store the record of instances when they measured qubit horizontally and vertically.

- They remove the instances of the data when they measured bit in different directions. So they are left with the string of length approximately equal to 2N.

- Now, if Eve is trying to intercept the message, he will also select any of these two bases and hence will get right reading half of the times. So the other half would be altered by probability 0.5

- So, quarter of Bob's bit will disagree with that of Alice

- Alice and Bob compare half of 2n bits over an unencrypted line, and

if they disagree on quarter of them, then they know Eve was listening.

- If they agree on all the bits, then they can use the other half of the string as a private key.

Entanglement

We use tensor product to define entanglement

Tensor product: represented as $\otimes$
is not commutative i.e. $|v\rangle \otimes |w\rangle \neq |w\rangle \otimes |v\rangle$

Assuming Alice and Bob have one qubit each and Alice uses orthonormal basis $(|a_0\rangle, |a_1\rangle)$ and Bob uses $(|b_0\rangle, |b_1\rangle)$ to measure

Let $|v\rangle = c_0|a_0\rangle + c_1|a_1\rangle$ and $|w\rangle = d_0|b_0\rangle + d_1|b_1\rangle$

so $|v\rangle \otimes |w\rangle = (c_0|a_0\rangle + c_1|a_1\rangle) \otimes (d_0|b_0\rangle + d_1|b_1\rangle)$

$= c_0d_0(|a_0\rangle \otimes |b_0\rangle) + c_0d_1(|a_0\rangle \otimes |b_1\rangle) + c_1d_0(|a_1\rangle \otimes |b_0\rangle) + c_1d_1(|a_1\rangle \otimes |b_1\rangle)$

$= c_0d_0\,|a_0\rangle|b_0\rangle + c_0d_1|a_0\rangle|b_1\rangle + c_1d_0|a_1\rangle|b_0\rangle + c_1d_1|a_1\rangle|b_1\rangle$

here $c_i d_j$ represent the probability amplitudes of Alice and Bobs qubits jumping on $|a_i\rangle$ and $|b_j\rangle$ after measuring.

let $c_0d_0 = r$, $c_0d_1 = s$, $c_1d_0 = t$, $c_1d_1 = u$

thus $|v\rangle \otimes |w\rangle = r|a_0\rangle|b_0\rangle + s|a_0\rangle|b_1\rangle + t|a_1\rangle|b_0\rangle + u|a_1\rangle|b_1\rangle$
and $r^2 + s^2 + t^2 + u^2 = 1$ as r, s, t and u are probability amplitudes

Also, $ru = st = c_0d_0c_1d_1$

Now, we stipulate the fact that $r^2+s^2+t^2+u^2=1$ and no longer insist that $ru = st$.

Thus there are two cases:

(i) $ru = st$

- This means both the qubits are not entangled

(ii) $ru \neq st$

- This means both the qubits are entangled

Eg. if Alice and Bob's qubits are given by

$$\frac{1}{2\sqrt{2}}|a_0\rangle|b_0\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|a_0\rangle|b_1\rangle + \frac{1}{2\sqrt{2}}|a_1\rangle|b_0\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|a_1\rangle|b_1\rangle$$

then their qubits are clearly unentangled.

Let us assume that Alice only make measurement.

$$\therefore \frac{1}{2\sqrt{2}}|a_0\rangle|b_0\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|a_0\rangle|b_1\rangle + \frac{1}{2\sqrt{2}}|a_1\rangle|b_0\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|a_1\rangle|b_1\rangle = |a_0\rangle\left(\frac{1}{2\sqrt{2}}|b_0\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|b_1\rangle\right) + |a_1\rangle\left(\frac{1}{2\sqrt{2}}|b_0\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|b_1\rangle\right)$$

we want the terms inside the paranthesis to be unit so we divide and multiply by their length.

$$\therefore |a_0\rangle\left(\frac{1}{2\sqrt{2}}|b_0\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|b_1\rangle\right) + |a_1\rangle\left(\frac{1}{2\sqrt{2}}|b_0\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|b_1\rangle\right) = \frac{|a_0\rangle}{\sqrt{2}}\left(\frac{|b_0\rangle}{2} + \frac{\sqrt{3}|b_1\rangle}{2}\right) + \frac{|a_1\rangle}{\sqrt{2}}\left(\frac{|b_0\rangle}{2} + \frac{\sqrt{3}|b_1\rangle}{2}\right)$$

$$= \left(\frac{|a_0\rangle}{\sqrt{2}} + \frac{|a_1\rangle}{\sqrt{2}}\right)\left(\frac{|b_0\rangle}{2} + \frac{\sqrt{3}}{2}|b_1\rangle\right)$$

* remember to keep Alice's vector to left of that of Bob's as tensor product is not commutative.

Thus we can deduce from the expression that Alice gets 0 or 1 with equal probability and it has no effect on that of Bob's as his measurement will still be $\left(\frac{1}{2}|b_0\rangle + \frac{\sqrt{3}}{2}|b_1\rangle\right)$

And niether will Bob's measurement, will influence that of Alice's.

Entangled qubit calculation

Let Alice and Bob's qubit be written as

$$\frac{1}{2}|a_0\rangle|b_0\rangle + \frac{1}{2}|a_0\rangle|b_1\rangle + \frac{1}{\sqrt{2}}|a_1\rangle|b_0\rangle + 0|a_1\rangle|b_1\rangle$$

This implies that Alice and Bob's qubits are entangled

If Alice make measurement first, we write equation in Alice's perspective.

$$\therefore \frac{1}{2}|a_0\rangle|b_0\rangle + \frac{1}{2}|a_0\rangle|b_1\rangle + \frac{1}{\sqrt{2}}|a_1\rangle|b_0\rangle + 0|a_1\rangle|b_1\rangle = |a_0\rangle\left(\frac{1}{2}|b_0\rangle + \frac{1}{2}|b_1\rangle\right) + |a_1\rangle\left(\frac{1}{\sqrt{2}}|b_0\rangle + 0|b_1\rangle\right)$$

$$= \frac{|a_0\rangle}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}|b_0\rangle + \frac{1}{\sqrt{2}}|b_1\rangle\right) + \frac{1}{\sqrt{2}}|a_1\rangle(1|b_0\rangle + 0|b_1\rangle)$$

This expression cannot be simplified further.

Now, Alice gets 0 or 1 with probability of $(1/\sqrt{2})^2 = 1/2$,
if Alice gets 0, then Bob gets 0 or 1 with probability of $1/2$

However, if Alice gets 1, then Bob gets 0 with probability 1.

Thus Alice's measurement influences that of Bob.

If Bob had made measurement first, then writing the expression in Bob's perspective will give us

$$\frac{1}{2}|a_0\rangle|b_0\rangle + \frac{1}{2}|a_0\rangle|b_1\rangle + \frac{1}{\sqrt{2}}|a_1\rangle|b_0\rangle + 0|a_1\rangle|b_1\rangle = \left(\frac{1}{2}|a_0\rangle + \frac{1}{\sqrt{2}}|a_1\rangle\right)|b_0\rangle + \left(\frac{1}{2}|a_0\rangle + 0|a_1\rangle\right)|b_1\rangle$$

$$= \left(\frac{1}{\sqrt{3}}|a_0\rangle + \frac{\sqrt{2}}{\sqrt{3}}|a_1\rangle\right)\frac{\sqrt{3}}{2}|b_0\rangle + (1|a_0\rangle + 0|a_1\rangle)\frac{1}{2}|b_1\rangle$$

Here, Bob gets 0 with probability 0.75 and 1 with probability 0.25

If Bob gets 0, Alice gets 0 with probability of $(1/\sqrt{3})^2 \approx 0.33$ and 1 with probability of $(\sqrt{2}/\sqrt{3})^2 \approx 0.67$

However, if Bob would have gotten 1, Alice would get 0 surely.

Thus Bob's measurement also influences that of Alice's

Standard Basis for Tensor product

$$\begin{bmatrix} a_0 \\ a_1 \end{bmatrix} \otimes \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} = \begin{bmatrix} a_0 \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} \\ a_1 \begin{bmatrix} b_0 \\ b_1 \end{bmatrix} \end{bmatrix} = \begin{bmatrix} a_0 b_0 \\ a_0 b_1 \\ a_1 b_0 \\ a_1 b_1 \end{bmatrix}$$

The standard Basis for $\mathbb{R}^2$ is $\left(\begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right)$

If both bases are same

$$|v\rangle \otimes |w\rangle = r \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} + s \begin{bmatrix} 1 \\ 0 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix} + t \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 1 \\ 0 \end{bmatrix} + u \begin{bmatrix} 0 \\ 1 \end{bmatrix} \otimes \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

$$= r \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} + s \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} + t \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} + u \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}$$

We use CNOT gates to entangle electrons. By entanglement of electrons, we actually mean that we entangle their vectors.
For now think of CNOT Gate as a orthogonal matrix given below

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

Lets take unentangled tensor product

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\\0\end{bmatrix}$$

when we qubits through CNOT gates they change

$$\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\1\\0\end{bmatrix}=\begin{bmatrix}1/\sqrt{2}\\0\\0\\1/\sqrt{2}\end{bmatrix}=\underbrace{\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}}$$

this vector corresponds to pair of entangled bits as the product of inner amplitudes is not equal to product of outer amplitudes Thus it can be written as:

$$\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\\0\\1\end{bmatrix}=\frac{1}{\sqrt{2}}\begin{bmatrix}1\\0\end{bmatrix}\otimes\begin{bmatrix}1\\0\end{bmatrix}+\frac{1}{\sqrt{2}}\begin{bmatrix}0\\1\end{bmatrix}\otimes\begin{bmatrix}0\\1\end{bmatrix}$$

Bell's Inequality

Copenhagen interpretation : model jumps on a specific state with some probability

The results we have seen so far can be explained using classical and quantum theory.

Classical theory assumes that their is no uncertainity and answers to the measurements are already fixed whereas the quantum theory assumes that the uncertainity is removed only after measurement.

We generate pairs of qubits which are in entangled state $\frac{1}{\sqrt{2}}|\uparrow\rangle|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle|\downarrow\rangle$

we send one from each pair to Alice and the other to Bob.
Alice and Bob choose to measure qubits in any of 0°, 120° and 240°.

Alice decides to measure first and chooses any of the three standard bases with equal probability that is 1/3 for measuring each qubit.
She only stores string of 0s and 1s.

Bob also does the same.

Now both compare their strings with each other and create a new string of A's and D's. A is added when both get similar bits and D when both get dissimilar bits

Now, we see the counts of dissimilar bit according to quantum approach and the classical approach.

The Quantum Approach

- We can neglect case when both the measurements are same.

- Case: when Alice chooses: $(|\searrow\rangle, |\nwarrow\rangle)$ and Bob chooses: $(|\swarrow\rangle, |\nearrow\rangle)$

so, $\frac{1}{\sqrt{2}}|\uparrow\rangle|\uparrow\rangle + \frac{1}{\sqrt{2}}|\downarrow\rangle|\downarrow\rangle$ can be written as $\frac{1}{\sqrt{2}}|\searrow\rangle|\searrow\rangle + \frac{1}{\sqrt{2}}|\nwarrow\rangle|\nwarrow\rangle$ in Alice's basis.
suppose that Alice gets $|\searrow\rangle|\searrow\rangle$, so Bob's qubit is $|\searrow\rangle$ and

$$|\searrow\rangle = \begin{bmatrix} 1/2 \\ -\sqrt{3}/2 \end{bmatrix} \quad ; \quad |\swarrow\rangle = \begin{bmatrix} -1/2 \\ -\sqrt{3}/2 \end{bmatrix} \quad ; \quad |\nearrow\rangle = \begin{bmatrix} \sqrt{3}/2 \\ -1/2 \end{bmatrix}$$

$$\therefore \begin{bmatrix} -1/2 & -\sqrt{3}/2 \\ \sqrt{3}/2 & -1/2 \end{bmatrix} \begin{bmatrix} 1/2 \\ -\sqrt{3}/2 \end{bmatrix} = \begin{bmatrix} 1/2 \\ \sqrt{3}/2 \end{bmatrix}$$

$$\therefore |\searrow\rangle = \frac{1}{2}|\swarrow\rangle + \frac{\sqrt{3}}{2}|\nearrow\rangle$$

This implies that Bob makes measurement, he get $|\leftarrow\rangle$ with probability $1/4$ and $|\uparrow\rangle$ with probability $3/4$.

So when Alice gets 0, Bob will also get 0 with probablity $1/4$.

This is true for each and every other case possible i.e if Alice and Bob choose different directions, they get same result $1/4^{th}$ of the time and disagree $3/4^{th}$ of the tome.

This implies:

(i) $1/3^{rd}$ of the time, they measure in same direction, and thus get same result.

How? : $P(B=0^\circ \mid A=0^\circ) = \frac{1}{9}$, similarly; $P(B=120^\circ \mid A=120^\circ) = P(B=240^\circ \mid A=240^\circ) = \frac{1}{9}$

(ii) Out of the $2/3^{rd}$ of the time, when they measure in different direction they get same readings $1/4^{th}$ of the time

$\therefore$ The proportion of A's $= \frac{1}{3} \times 1 + \frac{1}{4} \times \frac{2}{3} = \frac{1}{2}$

Now considering the classical approach.

Classical approach assumes that the directions are already fixed for each direction.

For each direction we take each possible measurement, so the possible values for each directions are 000, 001, 010, 011, ..., 111 where first bit give value in 0°, the second bit gives value for 120° and the thurd one for 240°.

Both, Alice and Bob are choosing direction with equal probability, so there are 9 possible selections each with probabilty $1/9$.

We give A when Alice and Bob get similar measurements and D when both get dissimilar measurements, so if we make a table giving all this information, it will look something like the one in the next page.

	Measurement directions								
Config.	(a,a)	(a,b)	(a,c)	(b,a)	(b,b)	(b,c)	(c,a)	(c,b)	(c,c)
000	A	A	A	A	A	A	A	A	A
001	A	A	D	A	A	D	D	D	A
010	A	D	A	D	A	D	A	D	A
011	A	D	D	D	A	A	D	A	A
100	A	D	D	D	A	A	D	A	A
101	A	D	A	D	A	D	A	D	A
110	A	A	D	A	A	D	D	D	A
111	A	A	A	A	A	A	A	A	A

Notice, that each row has atleast 5 A's.

So, the proportion of A's in the string is $\frac{1}{9} \times 5 = \frac{5}{9}$

The Ekert Protocol for Key Distribution

- When Alice and Bob try to measure using random from the standard bases, we know that they will use same bases $1/3^{rd}$ of the time, so they get same result.

- The other times when both don't use the same basis, $1/4^{th}$ of the time, they will get same measurements, but if it is somehow read by Eve, the probability jumps to $(3/8)$ (complex calculations can prove it). So, we can know that she's eavesdropping.

Classical Logic, Gates, and Circuits

Reversible gates are required for quantum computing

Common logic gates: not ($\neg$), or ($\vee$), exclusive or ($\oplus$), and ($\wedge$), nand ($\uparrow$)

Reversible gates are those gates, from which if output is known, input can be derived

Eg. AND gate is not reversible as, if output is 0 input cant be known

*Half Adder is not a reversible gate

Input		Digit	Carry
0	0	0	0
0	1	1	0
1	0	1	0
1	1	1	1

Here, we get digit 1 and Carry 0 for two possible inputs, thus we lose information during the process, hence half adder is not a reversible gate.

Landauer limit: the energy required to erase one bit of information

However, if computation can be reversed it can be proved that there is no energy lost.

Reversible Gates:

(i) Controlled Not (CNOT) Gate: $f(x, y) = (x, x \oplus y)$

The first input remains as it is, and the second input remains as it is if $x = 0$ or else it also flips.

Input		Output	
0	0	0	0
0	1	0	1
1	0	1	1
1	1	1	0

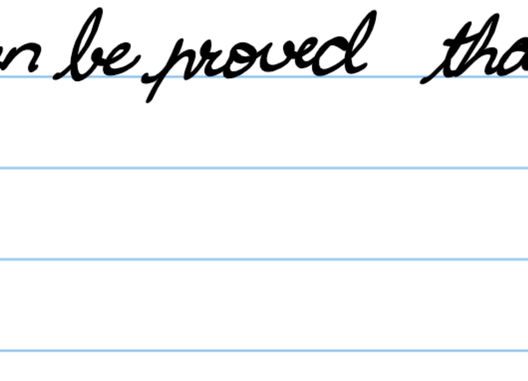


Figure 6.13
Usual representation of *CNOT* gate.

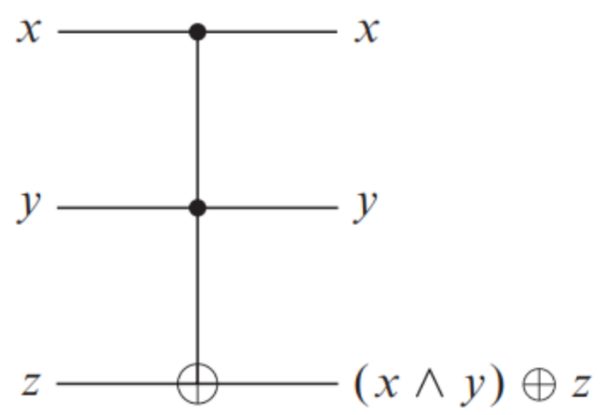
*CNOT is invertible too! ie $f(f(x,y)) = x, y$

(ii) Toffoli Gate (CCNOT) : $f(x, y, z) = (x, y, (x \wedge y) \oplus z)$

Toffoli gate

Input			Output		
x	y	z	x	y	$(x \wedge y) \oplus z)$
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

- x and y remain as it is but z flips when both x and y are 1.



Toffoli gate is universal gate as we can construct NAND and NOR from it.

(iii) Fredkin Gate : $F(x, y, z) = \begin{cases} (x, y, z) & \text{if } x = 0 \\ (x, z, y) & \text{if } x = 1 \end{cases}$

Quantum Gates and Circuits

Quantum circuits : a sequence of quantum gates that perform complex calculation on qubits

Quantum gates can be used to : spin qubit, entangle qubits or measure state of qubit

Previously, we thought choosing direction to measure qubit is like choosing an orthogonal matrix, but now we think of orthogonal matrix as a gate through which qubit passes (we also think that the measuring direction is also fixed)

Qubits

We take the standard basis to be $(|\uparrow\rangle, |\downarrow\rangle)$ where qubit jumping to $|\uparrow\rangle$ represents 0 and to $|\downarrow\rangle$ represents 1, so we let

$|0\rangle = |\uparrow\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = |\downarrow\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

as we take multiple qubits, the underlying ordered basis will be

$(|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle) \equiv (|00\rangle, |01\rangle, |10\rangle, |11\rangle)$

The CNOT Gate

$Q = r|00\rangle + s|01\rangle + t|10\rangle + u|11\rangle$

CNOT Gate:

CNOT

Input		Output	
x	Y	x	$x \oplus y$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	$\|0\rangle$
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	$\|1\rangle$
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	$\|1\rangle$
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	$\|0\rangle$

$\equiv$

CNOT

Input	Output
$\|00\rangle$	$\|00\rangle$
$\|01\rangle$	$\|01\rangle$
$\|10\rangle$	$\|11\rangle$
$\|11\rangle$	$\|10\rangle$

$\therefore Q' = r|00\rangle + s|01\rangle + u|1\,0\rangle + t|11\rangle \quad = cnot\,(Q)$

* It flips the probability of $|10\rangle$ and $|1\,1\rangle$

How CNOT Gate can be used to entangle an unentangled qubit.

Lets say we have two qubits : $q_1 = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$ and

$q_2 = 1|0\rangle + 0|1\rangle$

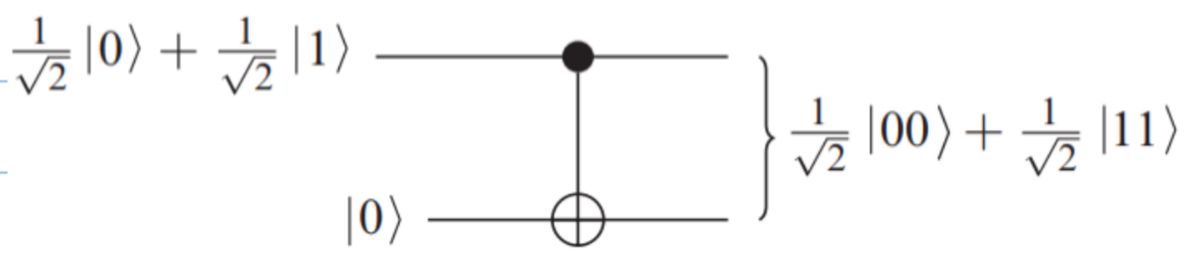
$\therefore$ The input is $\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes |0\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$

we pass it through a CNOT gate, therefore

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle \longrightarrow \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|1\,1\rangle$$

and this is an entangled state, hence we cannot assign individual state to each output.

Thus, we represent it in this form:



* CNOT gate is a permutation of the original orthogonal matrix and is therefore an orthogonal matrix, infact all the quantum gates are orthogonal matrices

Quantum Gates acting on only one Qubit

- For a single bit (not qubit) there are only two possible operations: identity and negation, however for a single qubit there are multiple possible operations.

- Pauli's Transformation: 4 gates (2 are identity and the other two are flipping)

- Gates I and X

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$ (makes no change to probability amplitudes)

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$ (makes no change to probability amplitude of $|0\rangle$ but negates that of $|1\rangle$)

if $$\psi = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$Z(\psi) = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

Note: $\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \equiv -\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$ but not equivalent to $Z(\psi)$

Z changes the relative phase of the qubit.

- Gates X and Y

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \quad ; \quad Y = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$ (usually multiplied by i)

X and Y are used to flip qubits by Y changes the relative phase of the qubit too!

* Hadamard Gate : This gate is used to put standard basis in superposition

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

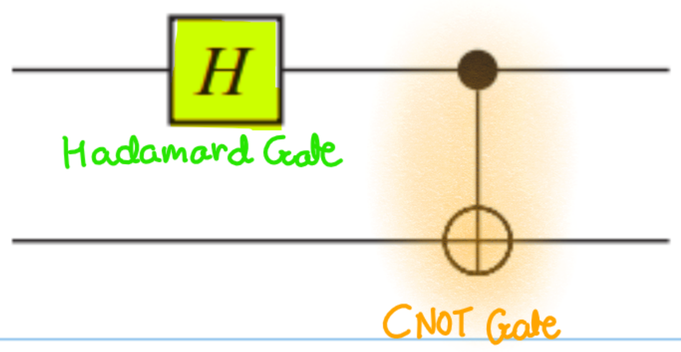
$$H(|0\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad H(|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

* There are no universal Quantum Gates

Any modifications of Von Neumann architecture cannot be used to create Quantum computer as Von Neumann architecture is based on copying bits from one part to the another. The whole purpose of Quantum computing is for fast and secure operations (as we have seen in Alice, Bob and Eve's case)

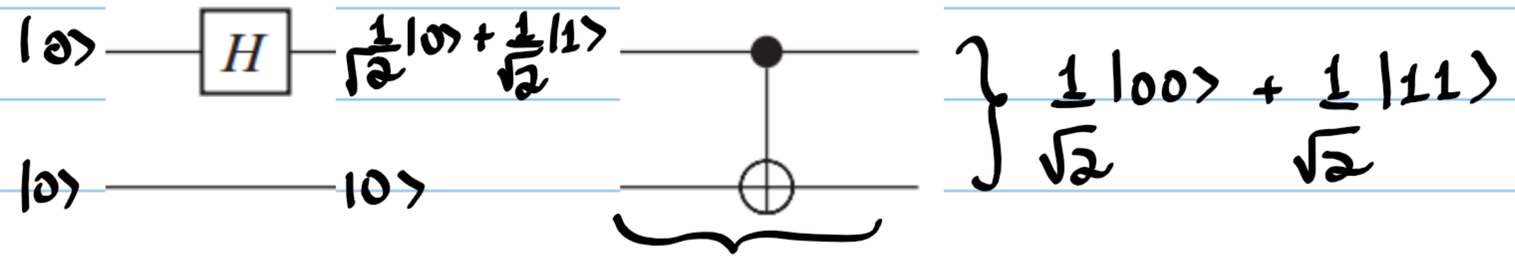
Quantum computation includes all of classical computation and is a general form of computation.

The Bell Circuit



We use it to get Bell basis from standard orthonormal basis

If we input $|00\rangle$:

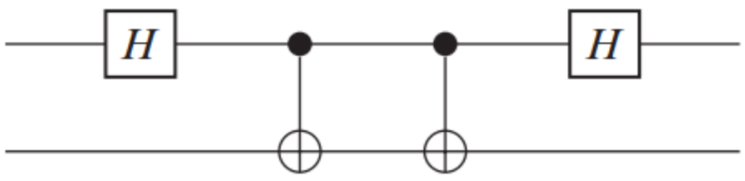


input: $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|10\rangle$

Similarly,

$$B(|01\rangle) = (1/\sqrt{2})|01\rangle + (1/\sqrt{2})|10\rangle$$
$$B(|10\rangle) = (1/\sqrt{2})|00\rangle - (1/\sqrt{2})|11\rangle$$
$$B(|11\rangle) = (1/\sqrt{2})|01\rangle - (1/\sqrt{2})|10\rangle$$

Let A represent this gate; all the gates we consider are orthogonal and symmetric, $\therefore AA^T = I$ and $\therefore AA = I$. Thus if we put two such gates consequently, we get the input back



Thus, we pass input through Hadamard and then CNOT first. Now when we apply CNOT again, we know that CNOT is it's own inverse, so we get the same output we got from Hadamard gate first. Then, we pass this result through Hadamard again to get our input back.

This property can be used for superdense coding and teleportation

Superdense coding

Suppose we have two qubits in entangled state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

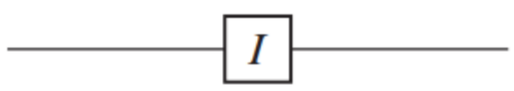
One of the qubit is with Alice and the other one is with Bob. and Alice wants to send two bit information to Bob, it can be either 00, 01, 10, or 11, but she will sending only one qubit-her electron

Alice we choose different gates to give different information, however, Bob will have to use same circuit to measure as he doesn't know what she is trying to send.

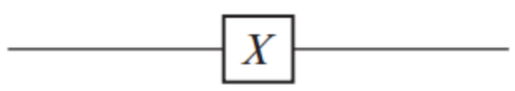
What Alice will do: act on her qubit in such a way that both the qubits will be in one of the basis vectors in the Bell bases

What Bob will do: pass the pair of qubits through reverse Bell circuit.

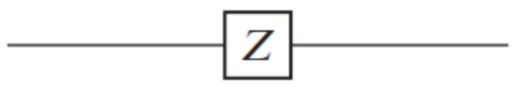
The gates Alice will use for each bit of information:



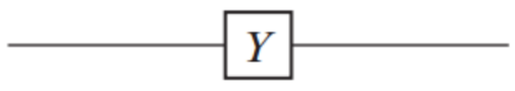
Circuit for 00



Circuit for 01



Circuit for 10



Circuit for 11

Remember: $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ $Y = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$

See what happens:

Initially, the state of qubits is in $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$

$$\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle = \frac{1}{\sqrt{2}}|0\rangle\otimes|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\otimes|1\rangle$$

If Alice wants to send 00, she uses I so no change in the state,

If she wants to send 01, she uses X, so this interchanges her bit only

$$\frac{1}{\sqrt{2}}|0\rangle\otimes|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\otimes|1\rangle \rightarrow \frac{1}{\sqrt{2}}|1\rangle\otimes|0\rangle + \frac{1}{\sqrt{2}}|0\rangle\otimes|1\rangle$$

If she wants to send 10, she uses Z, so

$$\frac{1}{\sqrt{2}}|0\rangle\otimes|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\otimes|1\rangle \rightarrow \frac{1}{\sqrt{2}}|0\rangle\otimes|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\otimes|1\rangle$$

And finally, if she wants to send 11, she uses Y, so

$$\frac{1}{2}|0\rangle\otimes|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\otimes|1\rangle \rightarrow \frac{1}{\sqrt{2}}|1\rangle\otimes|0\rangle - \frac{1}{\sqrt{2}}|0\rangle\otimes|1\rangle$$

Now, after Bob recieves Alice's qubit, he passes them through the reverse Bell circuit and hence gets the information Alice wanted to send to him.

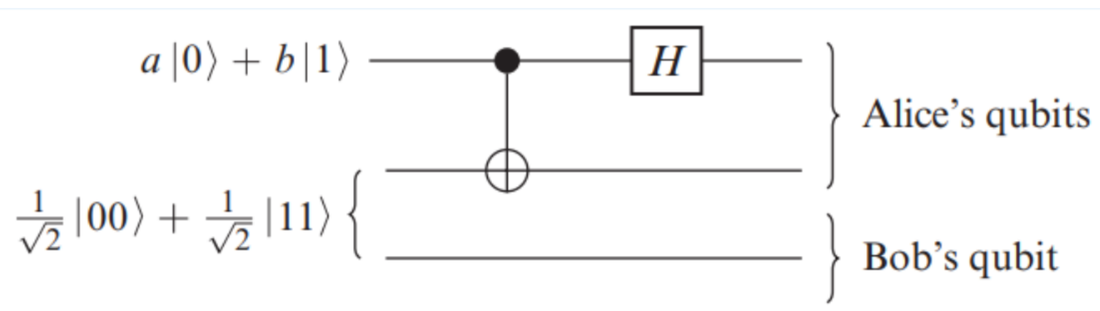
Quantum Teleportation

Alice and Bob have one electron each, which are in entangled state $(1/\sqrt{2})|00\rangle + (1/\sqrt{2})|11\rangle$ and Alice has one more electron which is in state $a|0\rangle + b|1\rangle$ but Alice doesn't know a and b. But she and Bob want to change Bob's electron so that it is in state

$a|0\rangle + b|1\rangle$. For this Alice needs to send 2 bits (Yes, we can send one of those infinite possibilities only using 2 classical bits.)

They will need to disentangle the state of both electrons for which Alice has to measure state of her qubit and she also needs to entangle both the electrons present with her.

So, first she passes both the qubit she has through CNOT and then apply Hadamard gate on the top qubit (Reverse Bell circuit)



The mathematics involved here: The initial state is:

$$(a|0\rangle + b|1\rangle) \otimes \left(\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle\right) = \frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|100\rangle + \frac{b}{\sqrt{2}}|111\rangle$$

as Alice is going to act on top 2 qubits:

$$\frac{a}{\sqrt{2}}|000\rangle + \frac{a}{\sqrt{2}}|011\rangle + \frac{b}{\sqrt{2}}|100\rangle + \frac{b}{\sqrt{2}}|111\rangle = \frac{a}{\sqrt{2}}|00\rangle\otimes|0\rangle + \frac{a}{\sqrt{2}}|01\rangle\otimes|1\rangle + \frac{b}{\sqrt{2}}|10\rangle\otimes|0\rangle + \frac{b}{\sqrt{2}}|11\rangle\otimes|1\rangle$$

now applying CNOT Gate gives us

$$\text{CNOT}\left(\frac{a}{\sqrt{2}}|00\rangle\otimes|0\rangle + \frac{a}{\sqrt{2}}|01\rangle\otimes|1\rangle + \frac{b}{\sqrt{2}}|10\rangle\otimes|0\rangle + \frac{b}{\sqrt{2}}|11\rangle\otimes|1\rangle\right)$$

$$= \frac{a}{\sqrt{2}}|00\rangle\otimes|0\rangle + \frac{a}{\sqrt{2}}|01\rangle\otimes|1\rangle + \frac{b}{\sqrt{2}}|11\rangle\otimes|0\rangle + \frac{b}{\sqrt{2}}|10\rangle\otimes|1\rangle$$

Alice will be now performing actions on first qubit only, so we can write the present state as

$$\frac{a}{\sqrt{2}}|0\rangle\otimes|0\rangle\otimes|0\rangle + \frac{a}{\sqrt{2}}|0\rangle\otimes|1\rangle\otimes|1\rangle + \frac{b}{\sqrt{2}}|1\rangle\otimes|1\rangle\otimes|0\rangle + \frac{b}{\sqrt{2}}|1\rangle\otimes|0\rangle\otimes|1\rangle$$

now as Alice will apply Hadamard on first qubit only, we will get

$$H\left(\frac{a}{\sqrt{2}}|0\rangle\otimes|0\rangle\otimes|0\rangle + \frac{a}{\sqrt{2}}|0\rangle\otimes|1\rangle\otimes|1\rangle + \frac{b}{\sqrt{2}}|1\rangle\otimes|1\rangle\otimes|0\rangle + \frac{b}{\sqrt{2}}|1\rangle\otimes|0\rangle\otimes|1\rangle\right)$$

$$= \frac{a}{2}|0\rangle\otimes|0\rangle\otimes|0\rangle + \frac{a}{2}|1\rangle\otimes|0\rangle\otimes|0\rangle + \frac{a}{2}|0\rangle\otimes|1\rangle\otimes|1\rangle + \frac{a}{2}|1\rangle\otimes|1\rangle\otimes|1\rangle + \frac{b}{2}|0\rangle\otimes|1\rangle\otimes|0\rangle$$

$$-\frac{b}{2}|1\rangle\otimes|1\rangle\otimes|0\rangle + \frac{b}{2}|0\rangle\otimes|0\rangle\otimes|1\rangle - \frac{b}{2}|1\rangle\otimes|0\rangle\otimes|1\rangle$$

$$= \frac{1}{2}|00\rangle\otimes(a|0\rangle + b|1\rangle) + \frac{1}{2}|01\rangle\otimes(a|1\rangle + b|0\rangle) + \frac{1}{2}|10\rangle\otimes(a|0\rangle - b|1\rangle) +$$

$$\frac{1}{2}|11\rangle\otimes(a|1\rangle - b|0\rangle)$$

Now, Alice measures the two qubits she has and sends those bits to Bob.

if Bob gets 00, there is no change to be done,
if Bob gets 10, it means his bit is in state $a|0\rangle - b|1\rangle$ so he uses Z gate
if Bob gets 01, it means his bit is in state $a|1\rangle + b|0\rangle$ so he uses X gate
if Bob gets 11, it means his bit is in state $a|1\rangle - b|0\rangle$ so he uses Y gate.

Problem: how to measure it?
↳ sol^n: using parity test

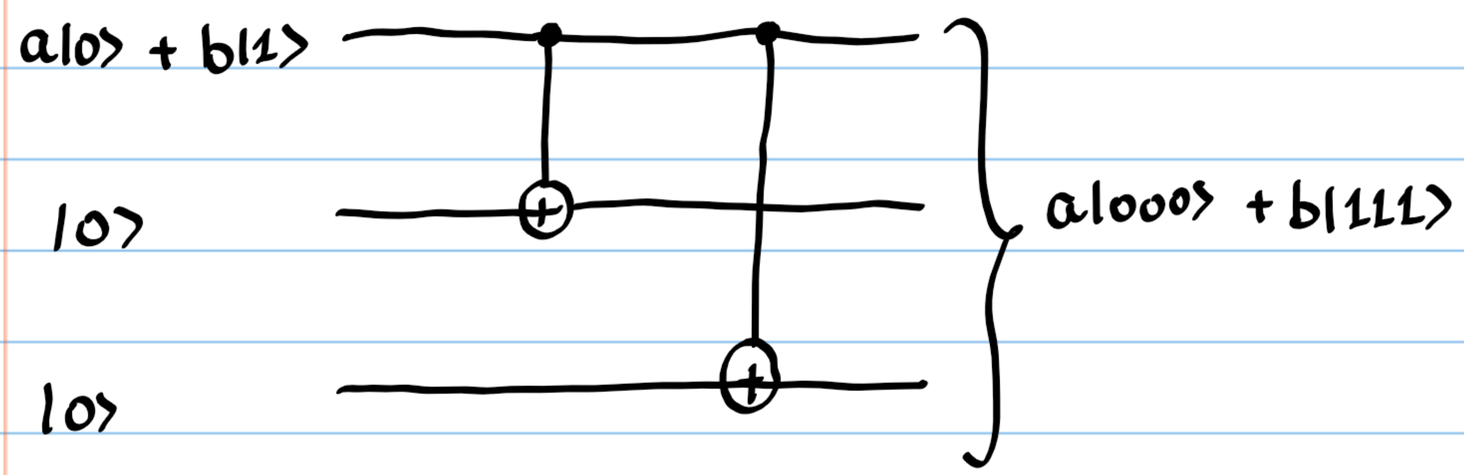
Suppose Bob recieves $b_0 b_1 b_2$
now, Bob does parity test i.e. $b_0 \oplus b_1$ and $b_0 \oplus b_2$.
if he gets 00, no change required
01, b_2 needs to be flipped
10, b_1 needs to be flipped
11, b_0 needs to be flipped.

* This method tells us which bit is to be flipped but doesnt tell whether we are flipping 0 or 1.

Quantum bit-flip correction

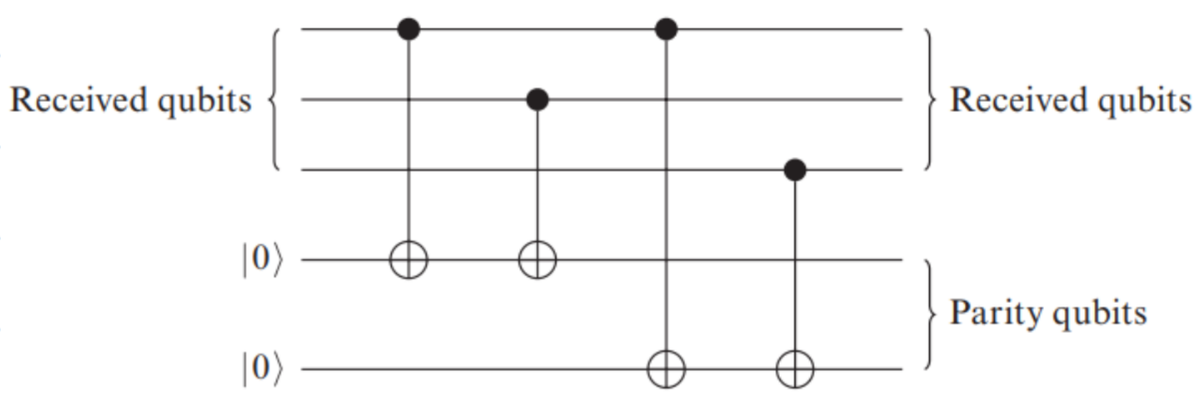
Asume, Alice wants to send $a|0\rangle + b|1\rangle$, but there can be chances that her qubit can flip to $a|1\rangle + b|0\rangle$. Alice cant send three qubits due to no cloning theorem, so she can use fan-out method.

She can start with three qubits ($a|0\rangle + b|1\rangle$, $|0\rangle$ and $|0\rangle$)



Bob can recive either the right bit, or $a|100\rangle + b|011\rangle$ or $a|010\rangle + b|101\rangle$ or $a|001\rangle + b|110\rangle$

Now, if he wants to measure them too, he can use the below circuit.



The circuit seems to entangle all the five bits, but this isn't true. Only the top three qubits are entangled

Suppose, Bob recieves qubit $a|c_0c_1c_2\rangle + b|d_0d_1d_2\rangle$

*Observation: if there is an error, it will be seen in both $c_0c_1c_2$ and $d_0d_1d_2$ and at the same place

Ignoring the 5th wire, we get

$$(a|c_0c_1c_2\rangle + b|d_0d_1d_2\rangle)\,|0\rangle = a|c_0c_1c_2\rangle|0\rangle + b|d_0d_1d_2\rangle|0\rangle$$

The two CNOT gates attached perform the parity check on first two qubits

if $c_0 \oplus c_1 = d_0 \oplus d_1 = 0$, they will be in state $(a|c_0c_1c_2\rangle + b|d_0d_1d_2\rangle)\,|0\rangle$

if $c_0 \oplus c_1 = d_0 \oplus d_1 = 1$, they will be in state $(a|c_0c_1c_2\rangle + b|d_0d_1d_2\rangle)\,|1\rangle$

This same argument can be applied for the 5th wire with first and third qubit and we can prove that both of them aren't entangled

Hence, Bob can measure bottom two qubits without disturbing the top 3 qubits

If he gets 00 : no change
01 : use X gate to flip third bit
10 : use X gate to flip second bit and .
11 : use X gate to flip first bit

This way, the bits are corrected and are now in the state Alice had sent

Quantum Algorithms

Not every classical algorithm is susceptible to quantum speed up These algorithms dont work by brute force method, but these exploit the underlying pattern that can be seen in quantum approach.

P and NP class problems

Concept of complexity : if $T(n) \leq kn^p$ for some $k, p \geq 0$, we say its complexity if polynomial

if $T(n) \leq kc^n$ for some $k, c > 0$, we say it is exponential

* Most polynomial time problems have smaller degree, so if not now, the problem can be solved in the near future, whereas if it is exponential, after certain 'n' it will be unsolvable

P class problems : those problems which can be solved in polynomial time

NP class problems : those problems whose solutions are given to you, and checking if those solutions are right takes polynomial time

As checking if any answer is correct or not is easier than searching for it, every problem belonging to class P also belongs to class NP i.e.
$P \subseteq NP$

No one has been able to prove if $P = NP$ or not.

Checking if the product of two given prime numbers equal to the third number is an NP problem but finding those two prime numbers is not a class P problem.

Shor's algorithm is used factoring the product of Two primes.

Query Complexity

Query complexity deals with the number of times we are evaluating the function. The function is called as a Black Box or an oracle as we don't have to calculate the number of steps the function takes to evaluate the input.

* We just keep track of number of questions asked

Deutsch Algorithm

- David Deutsch

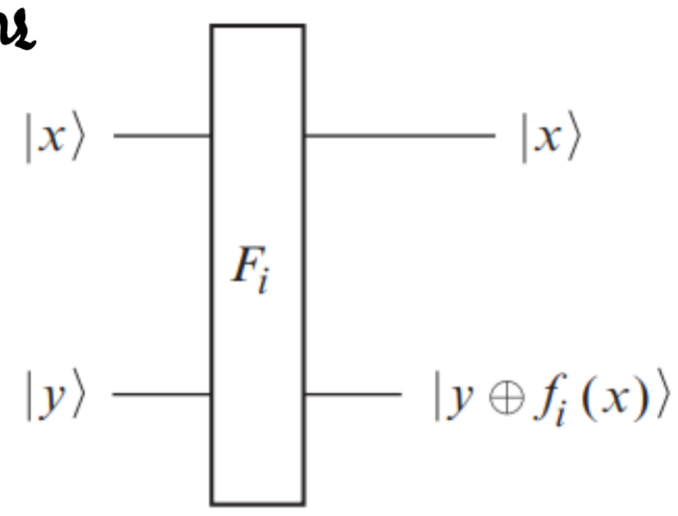
- You are given four functions f_0, f_1, f_2 and f_3
  - f_0 maps both, 0 and 1 to 0
  - f_1 maps 0 to 0 and 1 to 1.
  - f_2 maps 0 to 1 and 1 To 0
  - f_3 maps both, 0 and 1 to 1.

f_0 and f_3 : constant function
f_1 and f_2 : balanced function (function sends half of its input to 0 and other half to 1)

Question posed: Given one of these functions at random, how many function evaluations needed to know if the function is constant or balanced.

In classical approach, we need to evaluate the function twice once by 0 and then by 1

In quantum approach, we first create gates that correspond to four functions



$|0\rangle \otimes |0\rangle \rightarrow |0\rangle \otimes |0 \oplus f_i(0)\rangle = |0\rangle \otimes |f_i(0)\rangle$

$|0\rangle \otimes |1\rangle \rightarrow |0\rangle \otimes |1 \oplus f_i(0)\rangle$

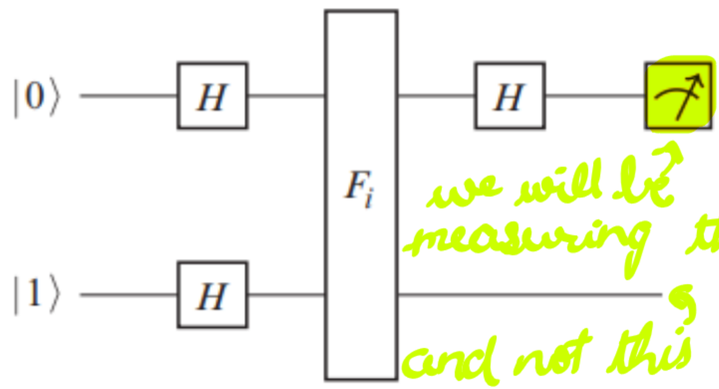
$|1\rangle \otimes |0\rangle \rightarrow |1\rangle \otimes |0 \oplus f_i(1)\rangle = |1\rangle \otimes |f_i(1)\rangle$

$|1\rangle \otimes |1\rangle \rightarrow |1\rangle \otimes |1 \oplus f_i(1)\rangle$

Here i can take any of 0, 1, 2 and 3.

Deutsch showed that if we only enter $|0\rangle$ and $|1\rangle$ corresponding to classical bit, we have to evaluate the function twice but if we input qubits in superposition of $|0\rangle$ and $|1\rangle$, we have to evaluate it only once.

Following circuit is used



The qubits $|0\rangle \otimes |1\rangle$ is the input.

After passing those through hadamard, we get

$$H(|0\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle)$$

These then go through F_i and then the state becomes

$$\frac{1}{2}(|0\rangle \otimes |f_i(0)\rangle - |0\rangle \otimes |f_i(0) \oplus 1\rangle + |1\rangle \otimes |f_i(1)\rangle - |1\rangle \otimes |f_i(1) \oplus 1\rangle)$$

we can rearrange these to get

$$\frac{1}{2}(|0\rangle \otimes (|f_i(0)\rangle - |f_i(0) \oplus 1\rangle) + |1\rangle \otimes (|f_i(1)\rangle - |f_i(1) \oplus 1\rangle)$$

* $|f_i(0)\rangle - |f_i(0) \oplus 1\rangle$ is either $|0\rangle - |1\rangle$ or $|1\rangle - |0\rangle$ depending on $f_i(0)$ is 0 or 1 but we can write this as

$$|f_i(0)\rangle - |f_i(0) \oplus 1\rangle = (-1)^{f_i(0)}(|0\rangle - |1\rangle)$$

similarly, $|f_i(1)\rangle - |f_i(1) \oplus 1\rangle = (-1)^{f_i(1)}(|0\rangle - |1\rangle)$

therefore we can also write the equation in form:

$$\frac{1}{2}\left[|0\rangle \otimes (-1)^{f_i(0)}(|0\rangle - |1\rangle) + |1\rangle \otimes (-1)^{f_i(1)}(|0\rangle - |1\rangle)\right]$$

$$= \frac{1}{2}\left[(-1)^{f_i(0)}|0\rangle \otimes (|0\rangle - |1\rangle) + (-1)^{f_i(1)}|1\rangle \otimes (|0\rangle - |1\rangle)\right]$$

$$= \frac{1}{2}\left[(-1)^{f_i(0)}|0\rangle + (-1)^{f_i(1)}|1\rangle\right] \otimes (|0\rangle - |1\rangle)$$

$$= \frac{1}{\sqrt{2}}\left[(-1)^{f_i(0)}|0\rangle + (-1)^{f_i(1)}|1\rangle\right] \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

This shows that the outputs are not entangled. We send the top qubit through Hadamard gate

if $i=0$; $f_i(0)=0$ & $f_i(1)=0$ so qubit is $\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]$

Hadamard gate: $H\left(\frac{1}{\sqrt{2}}[|0\rangle + |1\rangle]\right) = |0\rangle$

if $i=1$; $f_i(0)=0$ & $f_i(1)=1$ so qubit is $\frac{1}{\sqrt{2}}[|0\rangle - |1\rangle]$

Hadamard gate: $H\left(\frac{1}{\sqrt{2}}[|0\rangle - |1\rangle]\right) = |1\rangle$

if $i=2$; $f_i(0)=1$ & $f_i(1)=0$ so qubit is $\frac{1}{\sqrt{2}}[-|0\rangle + |1\rangle]$

Hadamard gate: $H\left(\frac{1}{\sqrt{2}}[-|0\rangle + |1\rangle]\right) = -|1\rangle$ and

if $i=3$; $f_i(0)=1$ & $f_i(1)=1$ so qubit is $\frac{1}{\sqrt{2}}[-|0\rangle - |1\rangle]$

Hadamard gate: $H\left(\frac{1}{\sqrt{2}}[-|0\rangle - |1\rangle]\right) = -|0\rangle$

∴ we get $|0\rangle$ if $i=0$ or 3 when f_i is constant function and we get $|1\rangle$ if $i=1$ or 2 when f_i is balanced function

Thus, we can say that there are quantum algorithms which are faster than classical ones

The Kronecker Product of Hadamard matrix

Hadamard matrix, $H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

$$H(|0\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$H(|1\rangle) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}\begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

If we take two qubits and send them through Hadamard, we get

$|0\rangle \otimes |0\rangle$ goes to $\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$

$|0\rangle \otimes |1\rangle$ goes to $\left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$

$|1\rangle \otimes |0\rangle$ goes to $\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle - \frac{1}{2}|11\rangle$ and

$|1\rangle \otimes |1\rangle$ goes to $\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) \otimes \left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle - \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle$

Therefore we can say that

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \to \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}; \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} \to \frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ 1 \\ -1 \end{bmatrix}; \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} \to \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ -1 \\ -1 \end{bmatrix}; \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} \to \frac{1}{2}\begin{bmatrix} 1 \\ -1 \\ -1 \\ 1 \end{bmatrix}$$

Writing this in another form

$$H^{\otimes 2} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} & \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \\ \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} & \frac{1}{\sqrt{2}}\begin{bmatrix} -1 & -1 \\ -1 & 1 \end{bmatrix} \end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix} H & H \\ H & -H \end{bmatrix}$$

In general, $H^{\otimes n} = \frac{1}{\sqrt{2}} \begin{bmatrix} H^{\otimes n-1} & H^{\otimes n-1} \\ H^{\otimes n-1} & -H^{\otimes n-1} \end{bmatrix}$.

These are called Kronecker Products

The Deutsch-Jozsa Algorithm

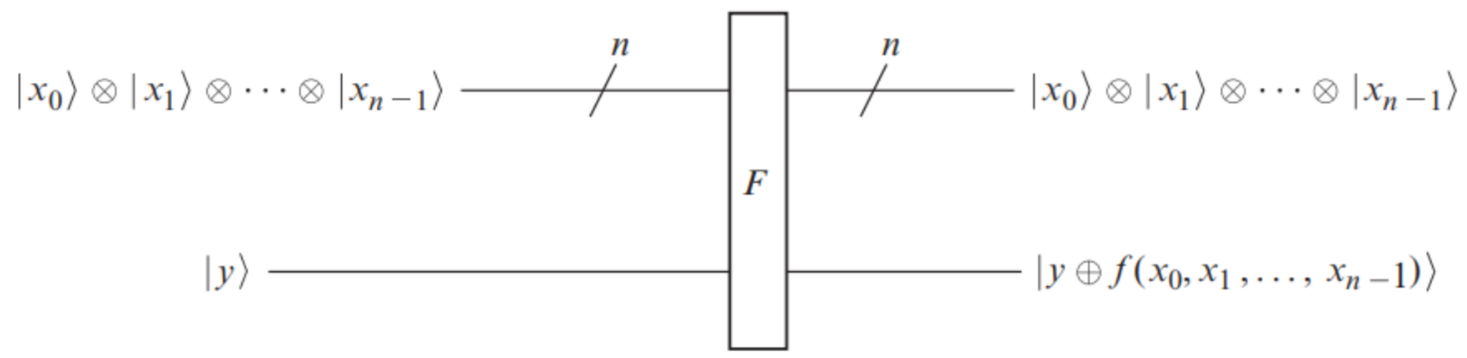
- It is generalization of Deutsch algorithm

- For example, if there are 3 bits, there are 8 possible inputs and we need to check the function atleast 5 times and in the worst case we need to ask the oracle $2^{n-1}+1$ times

- But, this quantum algorithm needs to ask question only 1 time, so it gives an exponential leap.

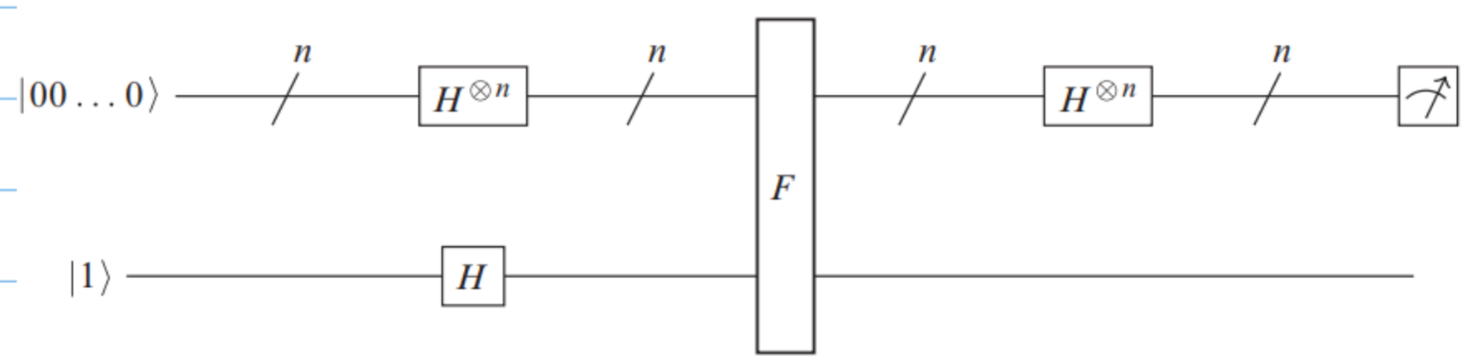
- We construct an orthogonal matrix representing the function.

- We construct a gate F.



input consists of n+1 kets, which include the n inputs and 1 output and output consists n+1 kets too, n inputs and $f(x_0,x_1,\ldots,x_{n-1})$ if $y=0$ or some other boolean value if $y=1$.

As usual, we use Hadamard gates to pass qubits on either side of F gate.



we use n=2 for explanation...

If the top qubits is $|0\rangle$ i.e. $|00\rangle$, we get

$$H^{\otimes 2} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)$$

* for any value of n, we get superposition of all possible states with equal probability amplitudes ($= 1/\sqrt{2^n}$)

If the bottom qubit is $|1\rangle$, and after passing it through Hadamard gate, we get $\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$. So our three qubit input is

$\frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle) \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ which we can rewrite as

$\frac{1}{2\sqrt{2}}|00\rangle\otimes(|0\rangle-|1\rangle) + \frac{1}{2\sqrt{2}}|01\rangle\otimes(|0\rangle-|1\rangle) + \frac{1}{2\sqrt{2}}|10\rangle\otimes(|0\rangle-|1\rangle) + \frac{1}{2\sqrt{2}}|11\rangle\otimes(|0\rangle-|1\rangle)$

Then, the qubits pass through F gate and we get,

$$\frac{1}{2\sqrt{2}}|00\rangle\otimes(|f(0,0)\rangle - |f(0,0)\oplus 1\rangle) + \frac{1}{2\sqrt{2}}|01\rangle\otimes(|f(0,1)\rangle - |f(0,1)\oplus 1\rangle)$$

$$+ \frac{1}{2\sqrt{2}}|10\rangle\otimes(|f(1,0)\rangle - |f(1,0)\oplus 1\rangle) + \frac{1}{2\sqrt{2}}|11\rangle\otimes(|f(1,1)\rangle - |f(1,1)\oplus 1\rangle)$$

* $|a\rangle - |a\oplus 1\rangle = (-1)^a(|0\rangle - |1\rangle)$

so, we get : $\frac{(-1)^{f(0,0)}}{2\sqrt{2}}|00\rangle\otimes(|0\rangle-|1\rangle) + \frac{(-1)^{f(0,1)}}{2\sqrt{2}}|01\rangle\otimes(|0\rangle-|1\rangle)$

$$+ \frac{(-1)^{f(1,0)}}{2\sqrt{2}}|10\rangle\otimes(|0\rangle-|1\rangle) + \frac{(-1)^{f(1,1)}}{2\sqrt{2}}|11\rangle\otimes(|0\rangle-|1\rangle)$$

as the top two and the bottom qubits aren't entangled, we get

$$\frac{1}{2}\left[(-1)^{f(0,0)}|00\rangle + (-1)^{f(0,1)}|01\rangle + (-1)^{f(1,0)}|10\rangle + (-1)^{f(1,1)}|11\rangle\right] \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

now, we measure the top 2 qubits only.

we multiply by appropriate Kronecker product

$$\frac{1}{4}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix} \begin{bmatrix} (-1)^{f(0,0)} \\ (-1)^{f(0,1)} \\ (-1)^{f(1,0)} \\ (-1)^{f(1,1)} \end{bmatrix}$$

we only calculate only the products with the top row, which gives the probability amplitude for $|00\rangle$

if f is constant function and equals to 0, the probability amplitude is 1 and if f equals to 1, we get probability amplitude of -1.

if f is a balanced function, the probability amplitude is 0.

So, if we measure the qubits and get $|00\rangle$ (if probability is 1), we are sure that function is constant, or if we dont get $|00\rangle$ (if probability is 0), we can assure that the function is balanced.

It means, we need to ask our oracle only 1 question irrespective of number of possible inputs.