Roll No- CRS1908 Asim Manna

1

(a) n- qubit state examples!

(i) $\begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \Big\}$ 2^n length.

$= 1 \cdot \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + 0 \cdot \begin{bmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{bmatrix} + \cdots + 0 \cdot \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{bmatrix}$

~~where $|\alpha_0|^2 = 1$ with~~

(ii) $\begin{bmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \\ \vdots \\ 0 \end{bmatrix} \Big\}$ 2^n length.

(b) (i)

Consider $A = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & & & \vdots \\ & 0 & 0 & 0 & \cdots & 1 \\ 0 & & & & & \end{pmatrix}_{2^n \times 2^n}$

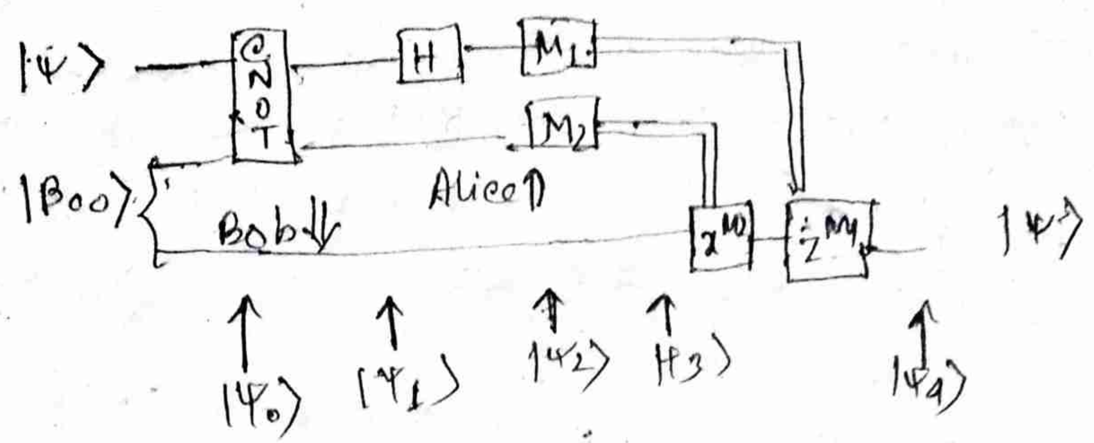
Here A is unitary matrix and input is $\begin{pmatrix} a_1 \\ \vdots \\ a_{2^n} \end{pmatrix}$ Then output will be $\begin{pmatrix} a_{2^n} \\ \vdots \\ a_1 \end{pmatrix}$ $\begin{pmatrix} a_1 \\ \vdots \\ a_{2^n} \end{pmatrix}$

(ii) $\begin{pmatrix} 0 & 0 & \cdots & & 1 \\ 0 & 0 & \cdots & 1 & 0 \\ & & & & \\ 1 & 0 & \cdots & 0 & 0 \end{pmatrix}_{2^n \times 2^n} = B$ (say) then

B is an unitary matrix is input $\begin{pmatrix} a_1 \\ \vdots \\ a^{2^n} \end{pmatrix}$

and output is $\begin{pmatrix} a^{2^n} \\ \vdots \\ a_1 \end{pmatrix}$

② Teleporation!



Here, $|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle = (\alpha|0\rangle + \beta|1\rangle)\dfrac{(|00\rangle + |11\rangle)}{\sqrt{2}}$

and $|\psi_1\rangle = \alpha|0\rangle \dfrac{(|00\rangle + |11\rangle)}{\sqrt{2}} + \beta|1\rangle \dfrac{(|10\rangle + |01\rangle)}{\sqrt{2}}$

$$|\psi_2\rangle = \alpha\left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)\left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right) + \beta\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)\left(\frac{|10\rangle + |01\rangle}{\sqrt{2}}\right).$$

$= \frac{1}{2}|00\rangle(\alpha|0\rangle + \beta|1\rangle)$ (Nothing to do)

$+\frac{1}{2}|01\rangle(\beta|0\rangle + \alpha|1\rangle)$ (Apply x gate)

$+\frac{1}{2}|10\rangle(\alpha|0\rangle - \beta|1\rangle)$ (Apply Z gate)

$-\frac{1}{2}|11\rangle(\beta|0\rangle - \alpha|1\rangle)$ (Apply both X and Z gates)

Now, ① if Bob get 00, then he will do nothing.

(ii) if Bob get 01 the ~~n~~ he ~~use~~ apply x- gate

(iii) if Bob ~~apply~~ get 10 then Bob apply Z- gate

(iv) if Bob get 11 then Bob will apply X and Z both. then back $|\psi\rangle$.

(3)

(a) Given a classical circuit f there is a quantum circuit of comparable efficiency which computes the transformation U_f ~~to~~ that takes input $|x,y\rangle$ & produces output $|x, y \oplus f(x)\rangle$.

- let f be either constant or blanced. Consider f as an oracle

In Deterministic classical ~~d~~ algorithim in the worst case might have to check more than half the values i.e $2^{n-1}+1$ quires might be in the worst case

In probabilistic classical algorithms a constant k many quires can generate the answer with failing prob. $\leq \frac{1}{2^k}$

At last we can conclude that the result deterministically with just a single query to the oracle

(b) <u>Deutch - Jozsa Algorithim</u>:

At first two quantum registers, the first one is an n- ~~bit~~ qubit quantum register with all the qubits are intialized to $|0\rangle$. and the 2nd one is a 1 qubit register, intialized to $|1\rangle$.

$|\psi_0\rangle = |0\rangle^{\otimes n} |1\rangle$.

Then apply Hadamard gate to each qubit.

$$|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} |x\rangle (|0\rangle - |1\rangle).$$

Apply the quantum oracle $U_f : |x\rangle|y\rangle \to |x\rangle|y \oplus f(x)\rangle$ on $|\psi_1\rangle$:

$$|\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} |x\rangle (|0 \oplus f(x)\rangle - |1 \oplus f(x)\rangle)$$

$$\Rightarrow |\psi_2\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle (|0\rangle - |1\rangle)$$

Igonore the last qubit from the 2nd register and apply Hadamard gate to all n qubits from the last register

$$H^{\otimes n} \left(\frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} |x\rangle \right)$$

$$\Rightarrow \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} (-1)^{f(x)} \left[\frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} (-1)^{x \cdot y} |y\rangle \right]$$

$$= \frac{1}{\sqrt{2^n}} \sum_{y \in \{0,1\}^n} \left[\sum_{x \in \{0,1\}^n} (-1)^{f(x)} (-1)^{x \cdot y} \right] |y\rangle.$$

Then measure all the n qubits from the first register:
if f(x) is constant, then check that the above prob is 1 & if f(x) is balanced the probablity is 0.

Hence after measurement if we get $|0\rangle^{\otimes n}$ we can conclude that f(x) is constant function then f(x) is blanced.

③ ⓒ In deterministic classical algorithm we might have to check the wrost case we might have to check $2^{n-1}+1$ quires is required in the wrost case, and in probabistic classical algo a constent is many quires can generate the answer with failing prob. $\leq \frac{1}{2^k}$. But Deuth-Jozsa algo can conclude the result deterministically with just a single query.

③ ⓐ

Given boolean function

$f(x_1, x_2, x_3) = x_1 x_2 x_3$

Now, $|\psi_0\rangle = |000\rangle \otimes |1\rangle$

Then

$$|\psi_1\rangle = \frac{1}{2\sqrt{2}} \{ |000\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle + |111\rangle \} \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$\Rightarrow |\psi_2\rangle = \frac{1}{2\sqrt{2}} \{ (-1)^0 |000\rangle + (-1)^0 |001\rangle + (-1)^0 |010\rangle + (-1)^0 |011\rangle + (-1)^0 |100\rangle + (-1)^0 |101\rangle + (-1)^0 |110\rangle + (-1) |111\rangle \} \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

$$= \frac{1}{2\sqrt{2}} \{ |000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle - |111\rangle \} \otimes \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle)$$

Now we ignore the last q-bit form the 2nd register

$$|\psi_2\rangle = \frac{1}{2\sqrt{2}} \{ |000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle - |111\rangle \}$$

Now, $|\psi_3\rangle = H^{\otimes 3} (|\psi_2\rangle)$.

Finally we calculate the prob. of getting $|0\rangle^{\otimes n}$

is $\frac{1}{2^6} \left[\sum_{x \in \{0,1\}^3} (-1)^{f(x)} \right]^2$

Here $f(1,1,1) = 1$ & for all other cases of outputs 0 Have ; the probablity of getting $|0\rangle^{\otimes n}$

is $\frac{1}{2^6} \left[(-1)^0 + (-1)^0 + (-1)^0 + (-1)^0 + (-1)^0 + (-1)^0 + (-1)^0 + (-1) \right]^2$

$$= \frac{1}{2^6} \{ 1+1+1+1+1+1+1-1 \}^2$$

$$= \frac{1}{2^6} \cdot 6^2 = \frac{36}{64} = 0.5625$$

Hence for DJ algo, as f is assumed to be either balance or constant. The given output 1 in one case and 0 in others. Hence f is neither ~~const~~ balanced nor constant. So executing ~~the given algo~~, we cannot get any information

(4) (a)

Given a function $f:\{0,1\}^n \to \{0,1\}$.
The goal is to find $x \in \{0,1\}^n$, such that $f(x)=1$ or to conclude that no such x exists i.e $f=0$, a constant function

lets,
$$A = \{x \in \{0,1\}^n : f(x)=1\}$$
$$B = \{x \in \{0,1\}^n : f(x)=0\}$$

Also let $|A|=a$, $|B|=b$, then $N=2^n$, $a+b=N$.

Begin with a state: $|\psi_0\rangle = |0\rangle^{\otimes n}$

Matrix Representation $|\psi_0\rangle = \begin{pmatrix}1\\0\end{pmatrix}^{\otimes n}$

· Apply the Hadamard gate to each of these qubits
$$|\psi_1\rangle = (H|0\rangle)^{\otimes n}$$
$$|\psi_1\rangle = \left(\frac{1}{\sqrt2}\begin{pmatrix}1&1\\1&-1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}\right)^{\otimes n} = \begin{pmatrix}\frac{1}{\sqrt2}\\ \frac{1}{\sqrt2}\end{pmatrix}^{\otimes n}$$
$$= \frac{1}{\sqrt{2^n}} \cdot \sum_{x \in \{0,1\}^n} |x\rangle = \frac{1}{\sqrt N} \cdot \sum_{x \in \{0,1\}^n} |x\rangle$$

consider the states: $|A\rangle = \frac{1}{\sqrt a} \sum_{x \in A} |x\rangle$ & $|B\rangle = \frac{1}{\sqrt b} \sum_{x \in B} |x\rangle$

Note that $|A\rangle$ & $|B\rangle$ are orthogonal. Consider the space spanned by $|A\rangle$ & $|B\rangle$.

Then
$$|\psi_1\rangle = \frac{1}{\sqrt N} \sum_{x \in \{0,1\}^n} |x\rangle = \frac{1}{\sqrt N}\left(\sum_{x \in A} |x\rangle + \sum_{x \in B} |x\rangle\right)$$
$$= \frac{1}{\sqrt N}\left(\sqrt a \times \frac{1}{\sqrt a} \sum_{x \in A} |x\rangle + \sqrt b \times \frac{1}{\sqrt b} \sum_{x \in B} |x\rangle\right)$$
$$\Rightarrow |\psi_1\rangle = \sqrt{\frac{a}{N}}|A\rangle + \sqrt{\frac{b}{N}}|B\rangle$$

· $|\psi_1\rangle = \sqrt{\frac{a}{N}}|A\rangle + \sqrt{\frac{b}{N}}|B\rangle$

Assuming $\sqrt{\frac{a}{N}} = \sin\theta$ & $\sqrt{\frac{b}{N}} = \cos\theta$ geometry we can think of $|\psi_1\rangle$ is making an angle θ with the state $|B\rangle$. This implies $\theta = \sin^{-1}\sqrt{\frac{a}{N}}$.

$Z_f|x\rangle = (-1)^{f(x)}|x\rangle$, Then $Z_0|x\rangle = \begin{cases} -|x\rangle & \text{if } x = 0^n \\ |x\rangle & \text{if } x \neq 0^n \end{cases}$

Matrix Represent, $Z_0 = I - 2|0^n\rangle\langle 0^n|$

for $n=2$, $Z_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} - 2\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}(1\,0\,0\,0)$

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

Define the unitary operator $G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$

$$H^{\otimes n} Z_0 H^{\otimes n} = H^{\otimes n}(I - 2|0^n\rangle\langle 0^n|)H^{\otimes n}$$
$$= (H^{\otimes n} - 2H^{\otimes n}|0^n\rangle\langle 0^n|)H^{\otimes n}$$
$$= I - 2H^{\otimes n}|0^n\rangle\langle 0^n|H^{\otimes n}$$
$$= I - 2|\psi_1\rangle\langle\psi_1|$$

Thus $G = (I - 2|\psi_1\rangle\langle\psi_1|)(-Z_f)$

Same derivation for $n=2$

$H^{\otimes n} Z_0 H^{\otimes n}$

$$= \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$$

Similar $I - 2|\psi_1\rangle\langle\psi_1|$

$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} - 2\cdot\frac{1}{2}\begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}\frac{1}{2}(1\,1\,1\,1)$$

$$= \frac{1}{2}\begin{pmatrix} 1 & -1 & -1 & -1 \\ -1 & 1 & -1 & -1 \\ -1 & -1 & 1 & -1 \\ -1 & -1 & -1 & 1 \end{pmatrix}$$

Hence $H^{\otimes n} Z_0 H^{\otimes n} = I - 2|\psi_1\rangle\langle\psi_1|$

that

Note that $G|A\rangle = [I - 2|\psi_1\rangle\langle\psi_1|](-I)|A\rangle$

$$= [I - 2|\psi_1\rangle\langle\psi_1|]\cdot|A\rangle$$

$$= |A\rangle - 2\langle\psi_1|A\rangle|\psi_1\rangle$$

$$= |A\rangle - 2\sqrt{\frac{a}{N}}\left(\sqrt{\frac{a}{N}}|A\rangle + \sqrt{\frac{b}{N}}|B\rangle\right)$$

$$= \left(1 - \frac{2a}{N}\right)|A\rangle - \frac{2\sqrt{ab}}{N}|B\rangle$$

Similarly $G|B\rangle = \frac{2\sqrt{ab}}{N}|A\rangle - \left(1 - \frac{2b}{N}\right)|B\rangle$

Thus G can be considered as a matrix

$$\begin{pmatrix} -\left(1-\frac{2b}{N}\right) & -\frac{2\sqrt{ab}}{N} \\ \frac{2\sqrt{ab}}{N} & \left(1-\frac{2b}{N}\right) \end{pmatrix}$$

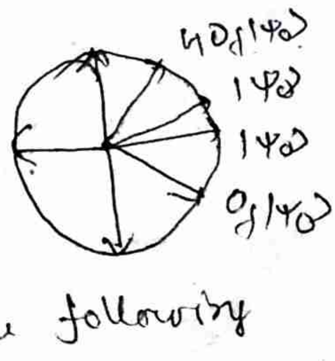
Now using $N = a+b$, we get:

$$\begin{pmatrix} \frac{b-a}{N} & -\frac{2\sqrt{ab}}{N} \\ \frac{2\sqrt{ab}}{N} & \frac{b-a}{N} \end{pmatrix} = \begin{pmatrix} \sqrt{\frac{b}{N}} & -\sqrt{\frac{a}{N}} \\ \sqrt{\frac{a}{N}} & \sqrt{\frac{b}{N}} \end{pmatrix}^2$$

$$= \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}^2$$

Thus G can be considered as a rotation matrix which on application to a state increase its angle by 2θ, & our goal is to increase the prob. of getting $|A\rangle$ i.e. $\sin^2\theta \approx 1$

Each application of G of $G\theta_f$ amplifies the angle from θ to 3θ.



After k applications of amplitude amplification operator $G\theta_f$ the resulting state is of the following form $|\psi_k\rangle = \sin(2k+1)\theta|x_0\rangle + \cos(2k+1)\theta|\phi_0\rangle$

prob. of observing x_0 from $|\psi_k\rangle$ is
$$\sin^2(2k+1)\theta$$

calculating the number of intera $\theta \to 0$

The success prob. is $\sin^2(2k+1)\theta$

To make the success prob. $\frac{1}{2}$ we need

$\sin^2(2k+1)\theta = \frac{1}{2}$

$\Rightarrow (2k+1)\theta = \arcsin\frac{1}{\sqrt{2}}$

$\Rightarrow (2k+1)\theta = \frac{\pi}{4} \Rightarrow k \simeq \frac{\pi}{8\theta}$

$= \frac{\pi}{8}\sqrt{2^n}$

: prepare the intial state.

$|\varphi_0\rangle = \frac{1}{\sqrt{2^n}} \sum_{x \in \{0,1\}^n} |x\rangle$

Apply $G = -H^{\otimes n} Z_0 H^{\otimes n} Z_f$

$= (1 - 2|\psi_1\rangle\langle\psi_1|)(-Z_f)$ on the

state $|\varphi_0\rangle$ for approx $\frac{\pi\sqrt{N}}{4}$ many time

Measure the state in computation basis.

check $|x'\rangle \xrightarrow{Z_f} (-1)^{f(x')}|x'\rangle = -|x'\rangle$ or not.

If yes the we got the correct resuelt

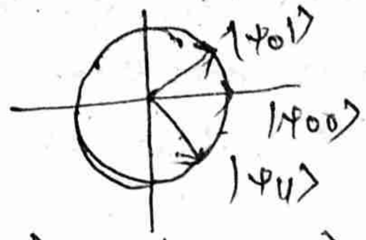
otherewise incorrect

(4) (b) Grover algorithm performs a search over an unordered set of $N = 2^m$ items to find an unique element that satisfy some condition. while the best classical algo for a ~~sear~~ searchs over ~~query~~ unordered data requires $O(N)$ times quantum computers is only $O(\sqrt{N})$ ~~of~~ operation an quadratic speed up.

⑤ ⓐ Alice randomly guarantees two strings of bits $x, y \in \{0,1\}^n$

Define $|\psi_{00}\rangle = |0\rangle$, $|\psi_{10}\rangle = |1\rangle$, $|\psi_{01}\rangle = |+\rangle$ & $|\psi_{11}\rangle = |-\rangle$

We have these 4 states as



Alice prepares m qbits in the state $|\psi_{x,y}\rangle = |\psi_{x_1y_1}\rangle \dots |\psi_{x_my_m}\rangle$.

and Sends these m q-bits over quantum channel to Bob. Bob receives m q-bits, although they may not longer is a stable $|\psi_{xy}\rangle$ because Eve may have tampered with them or possibly the channel is noisy.

Bob randomly choses $y' \in \{0,1\}^m$ & measures each q-bit reached from Alice to follows.

- If $y_i' = 0$, Bob measures qubit i.
- if $y_i' =$ Bob performs a Hadamard transform to q bit i, then measures it with respect to the standard basis

Let $x' \in \{0,1\}^m$ be the string corresponding to the results of Bobs measurements. The important thing to note at this point is that if $y_i = y_i'$ for some i & there was no noise or evesdropping than it is certain $x_i = x_i'$

Finally, Alice & Bob publicly compare y and y'

They discard bits x_i & x_i' for which $y_i \neq y_i'$

The reaming bits of x & x' represent a 'semi private'. key that will go into the next stange of the protocol

2nd Stage of protocol:

Alice & Bob now need to estimate how much Eve might know about x and x'. They do this by some of bits x and x'. comparing these bits publicly they can estimate the error rate with high accuracy and if it is too large they about.. The maximum error rate can be tolerated is about 11%. If they have acceptable error rate Alice & Bob will have two strings x and x' that agree in a high percentange of positions with high prob. They have some bound on the amount of information. Eve posses about the given strings.