01/02/2022

Quantum Cryptology & Security

End-Sem Exam

Matta Uma Maheswara Reddy
CRS 2019

(Q5) (a) Matrix representation of gate corresponding to QFT ⇒

$$f_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \cdots & \omega_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix}$$

where $\omega_N = e^{i2\pi/N} \Rightarrow \therefore \omega_N^k = e^{i2\pi k/N}$, $k \in \{0, 1, \cdots, N-1\}$

↙

N^{th} root of unity $\quad (\omega_N)^N = 1$

Let the ~~n-bit~~ n-qubit state be written as

$$|X\rangle = \sum_{x \in \{0,1\}^n} \alpha_x |x\rangle \equiv \sum_{k=0}^{N-1} \alpha_k |K\rangle$$

where $|K\rangle$ represents states $|x\rangle$ (just in numbers)

like $|0\rangle = |x_1\rangle$, $|1\rangle = |x_2\rangle$ .... etc.

$|2\rangle = |x_3\rangle$ ...

$$(F_N) \times (|X\rangle)$$

$$= \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \cdots & \omega_N^{N-1} \\ 1 & \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix}$$

The $\underline{k^{th}}$ row of the matrix will be :

$$\frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \alpha_n \omega_N^{kn} . \qquad (K \in \{0, 1, 2, \cdots, N-1\})$$

(b) Shor's factoring Algorithm Statement

↳ Given a large integer N, we need to find a factor p such that p divides N (N is of the form $N = pq$).

In a classical setting, finding p from N takes exponential time. Using a quantum computer and with the help of Shor's Algorithm, we can find p in polynomial time.

(c) The foundation of RSA is build on the classical property that it is hard to factor a large N ($N = pq$, p and q are primes). If one knows p, q, they can decrypt messages as they can easily deduce the secret key from p, q.

Public key 'd' is constructed from secret key 'e'. $e \cdot d \equiv 1 \mod (p-1)(q-1)$

If one knows p, q, then they can find $(p-1)(q-1)$. And since 'd' is known to everyone, we can find 'e' from the above equation, thereby allowing us to decrypt all information sent using these keys.

(d) Shor's Algorithm for prime product factoring ⇒ involves two parts: Classical & Quantum

Classical: ① Given N, pick a random number 'a' ⇒ $1 < a \leq N$.

② Compute $K = \gcd(a, N)$. If $K \neq 1$, then you found one of the factor of N. We are done.

③ If $x=1$,

Let's define the period 'r' of the following function: $f(x) = a^x \bmod N$.

$(a^r \bmod N \equiv 1)$. r is the order of a in $\mathbb{Z}_N^*$ group $\Rightarrow$ r divides $\varphi(N)$ — Euler's Totient function.

$\Rightarrow f(x+r) = f(x)$.

④ If r = odd, start again from step ① with a new 'a'.

⑤ If $a^{r/2} \equiv -1 \bmod N$, we restart this again from ① with another 'a'.

⑥ Else, both $\gcd(a^{r/2}+1, N)$ & $\gcd(a^{r/2}-1, N)$ are both the factors of N.

↳ Basically we find p, q.

We need to find 'r'. How? Comes the Quantum part.

We use Quantum Fourier Transform (QFT) for this. for a given f_N (representing QFT in a matrix form), take a state $|X\rangle = \sum_{k=0}^{N-1} \alpha_k |k\rangle$, QFT of $|X\rangle$ ⇒

$(f_N) \times (|X\rangle) =$

$$\frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & w_N & w_N^2 & \cdots & w_N^{N-1} \\ 1 & w_N^2 & & & \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & w_N^{N-1} & \cdots & & w_N^{(N-1)(N-1)} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix}$$

(f_N) — $|X\rangle$ part

Output matrix k^{th} row would look like

$$\frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \alpha_n w_N^{kn}.$$

Say $f_N(|x\rangle) = |y\rangle$, $|y\rangle = \sum_{k=0}^{N-1} \beta_k |k\rangle$

$$\beta_k = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \alpha_n \, e^{2\pi i \frac{kn}{N}}$$

Now find $Q = 2^q$ such that Q lies between $N^2, 2N^2 \Rightarrow N^2 \leq Q \leq 2N^2$

This implies $\frac{Q}{r} > N$, so that for each $f(x)$, we can find atleast N many x's which outputs the same value.

Now, initialise all the q many qubits from the first register to $|0\rangle$ and apply Hadamard gate to each of the qubits. Initialise all the qubits from second register to $|0\rangle$.

$$|\psi_0\rangle = |0^q\rangle |0^q\rangle \xrightarrow{H^{\otimes q} \otimes I_q} \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |0^q\rangle = |\psi_1\rangle$$

Construct $f(x)$ as a quantum function and apply it to the above state i.e.

$$U_f |x\rangle |y\rangle = |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$$

We get $|\psi_2\rangle = \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle |f(x)\rangle$

Apply QFT on the first register

$$|\psi_3\rangle = \frac{1}{Q} \sum_{x=0}^{Q-1} \sum_{y=0}^{Q-1} e^{\frac{2\pi i}{Q} xy} |y\rangle |f(x)\rangle$$

Now say $f(x+r) = f(x) = z$ and $f(x+s) \neq f(x)$ $s < r$. Let x_0 be the smallest x s.t. $f(x) = z$ (Remember we have atleast N such values).

$\Rightarrow \therefore$ If $f(x) = z \Rightarrow x = x_0 + k \cdot r$

$k \in \{0, 1, \ldots, \lfloor \frac{Q - x_0 - 1}{r} \rfloor\}$

$$\therefore |\psi_3\rangle = \frac{1}{Q} \sum_{z:f(x)=z,}^{\left\lfloor \frac{Q-x_0-1}{r} \right\rfloor} \sum_{k=0}^{Q-1} \sum_{y=0}^{Q-1} e^{\frac{2\pi i}{Q}(x_0+k\cdot r)y} |y\rangle|z\rangle$$

From $|\psi_3\rangle$, probability of getting a state $|y\rangle|z\rangle$ is $\Rightarrow$

$$P(y) = \left| \frac{1}{Q} \sum_{k=0}^{\left\lfloor \frac{Q-x_0-1}{r} \right\rfloor} e^{\frac{2\pi i}{Q}(x_0+k\cdot r)y} \right|^2$$

$$= \frac{1}{Q^2} \left| \omega^{x_0 y} \right|^2 \cdot \left| \sum_{k=0}^{\left\lfloor \frac{Q-x_0-1}{r} \right\rfloor} e^{\frac{2\pi i}{Q} rky} \right|^2$$

$$= \frac{1}{Q^2} \left| \sum_{k=0}^{\left\lfloor \frac{Q-x_0-1}{r} \right\rfloor} e^{\frac{2\pi i}{Q} rky} \right|^2$$

$$P(y) = \frac{1}{Q^2} \left| \sum_{k=0} \right|^2$$

The probability is higher when $\frac{ry}{Q}$ is closer to an integer.

Say $\frac{ry}{q}$ [redacted] is closer to $m \to$

$$ry = mq \Rightarrow \frac{y}{q} \geq \frac{m}{r}$$

Turn $\frac{y}{q}$ into an irreducible fraction and then extract the denominator r' using the method of continued fraction. This r' is our candidate for period of f.

Check if $f(x+r') = f(x)$ $\Rightarrow$ If not, then find another state y and check again.

Q1 (a) NO CLONING THEOREM

We cannot make two perfect copies of a given state.

There exists NO quantum copying machine that can make two perfect copies of non-orthogonal states.

Proof: Let us assume such a machine exists. That means we have a unitary matrix U s.t.

$U(|\psi\rangle|x\rangle) = e^{i\theta}|\psi\rangle|\psi\rangle$ where $|x\rangle$ is a normalised state, θ = phase.

Take two non-orthogonal states $|\psi\rangle$, $|\phi\rangle$ and lets use this machine $\Rightarrow$

$U(|\psi\rangle|x\rangle) = e^{i\alpha}|\psi\rangle|\psi\rangle$

$U(|\phi\rangle|x\rangle) = e^{i\beta}|\phi\rangle|\phi\rangle$

Using $UU^\dagger = I = U^\dagger U$

$\Rightarrow U(|\psi\rangle|x\rangle) = e^{i\alpha}|\psi\rangle|\psi\rangle$

$\langle\psi|\langle x|U^\dagger U|\psi\rangle|x\rangle = 1$

$\Rightarrow \therefore \langle\psi|\langle x|U^\dagger = e^{-i\alpha}|\psi|\langle\psi|$

Let's try this $\Rightarrow$

$\langle\psi|\langle x|U^\dagger U|\phi\rangle|x\rangle = e^{-i\alpha}\langle\psi|\langle\psi|e^{i\beta}|\phi\rangle|\phi\rangle$

$\Rightarrow |\langle\psi|\phi\rangle\langle x|x\rangle| = |e^{i(\beta-\alpha)}\langle\psi|\phi\rangle\langle\psi|\phi\rangle|$

$\Rightarrow |\langle\psi|\phi\rangle| = |\langle\psi|\phi\rangle|^2$

either $|\langle\psi|\phi\rangle| = 0 \Rightarrow$ $|\psi\rangle, |\phi\rangle$ are orthogonal. But we assumed non-orthogonal.

$|\langle\psi|\phi\rangle| = 1 \Rightarrow |\psi\rangle, |\phi\rangle$ same states (or θ, phase difference).

∴ No cloning is possible.

(b) Quantum Teleportation ⇒ Moving quantum states even in absence of a quantum communication channel b/w sender and receiver.

Say Alice, Bob live far away but share one qubit each of an EPR pair they generated. Now Alice wants to send $|\psi\rangle$ qubit to Bob. She doesn't know the state of the qubit and can only send classical information to Bob.

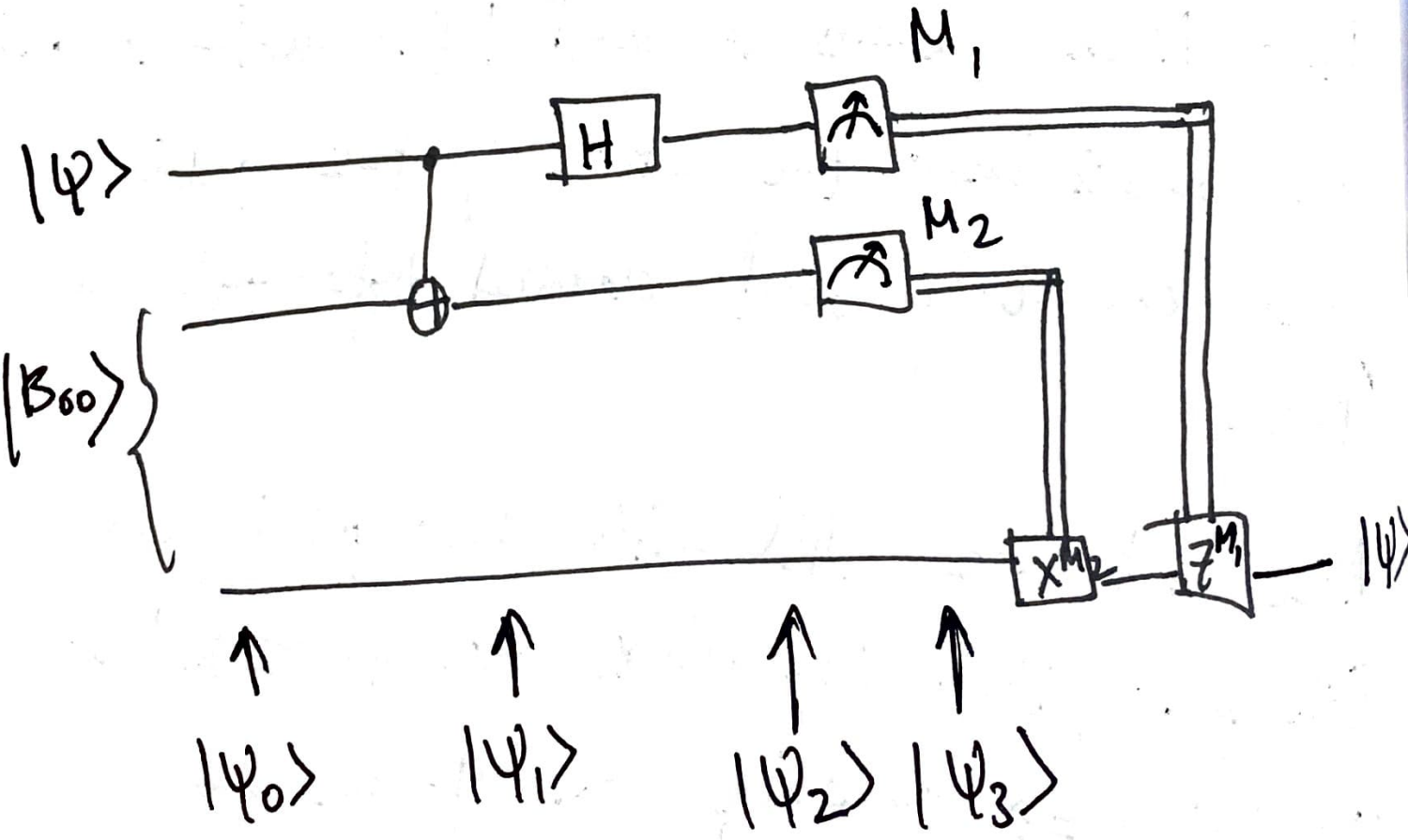
Alice interacts $|\psi\rangle$ with her qubit from EPR pair, then measures two qubits in her possession ⇒ obtaining one of the four 00, 01, 10, 11. She sends this to Bob.

Depending on Alice's message, Bob performs one of the four operations on his qubit from EPR pair.

Say $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, α, β are unknown

State input into the circuit $|\psi_0\rangle$ is

$$|\psi_0\rangle = |\psi\rangle |\beta_{00}\rangle$$



$$\Rightarrow |\psi_0\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|00\rangle+|11\rangle\Big]$$

We say $|\psi\rangle$, first qubit of $|B_{00}\rangle$ belongs to Alice and second qubit of $|B_{00}\rangle$ to Bob.

Alice sends her qubits through C_{NOT} $\Rightarrow$

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\Big[\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|10\rangle+|01\rangle)\Big]$$

Then sends the first qubit through a Hadamard gate

$$|\psi_2\rangle = \frac{1}{2}\Big[\alpha(|0\rangle+|1\rangle)(|00\rangle+|11\rangle) + \beta(|0\rangle-|1\rangle)(|10\rangle+|01\rangle)\Big]$$

$$\Rightarrow \frac{1}{2}\Big[|00\rangle(\alpha|0\rangle+\beta|1\rangle) + |01\rangle(\alpha|1\rangle+\beta|0\rangle) + |10\rangle(\alpha|0\rangle-\beta|1\rangle) + |11\rangle(\alpha|1\rangle-\beta|0\rangle)\Big]$$

So when she measures ⇒

$00 \rightarrow |\psi_3(00)\rangle \equiv [\alpha|0\rangle + \beta|1\rangle]$

$01 \rightarrow |\psi_3(01)\rangle \equiv [\alpha|1\rangle + \beta|0\rangle]$

$10 \rightarrow |\psi_3(10)\rangle \equiv [\alpha|0\rangle - \beta|1\rangle]$

$11 \rightarrow |\psi_3(11)\rangle \equiv [\alpha|1\rangle - \beta|0\rangle]$

Based on the output Bob receives, he'd apply the appropriate gate to recover $|\psi\rangle$.

If 00 → Nothing to do

If 10 → Apply Z gate

If 01 → Apply X gate

If 11 → Apply Z gate, then X gate

© Given that $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = \begin{bmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{bmatrix}$

Density matrix corresponding to $|\psi\rangle$ is

$$\rho_{|\psi\rangle} = |\psi\rangle\langle\psi| = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$$

$$= \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$$

Density matrix for $|0\rangle$, $|1\rangle$

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

Given a mixed ~~state~~ state $|\phi\rangle$ where $|0\rangle$, $|1\rangle$ are in equal superposition.

$$\Rightarrow \rho_{|\phi\rangle} = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix} = \frac{1}{2} I_2$$

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

↳ Can be written as $|\psi\rangle = \cos\theta/2\,|0\rangle + e^{i\phi} \sin\theta/2\,|1\rangle$

Equating coefficients ⇒

$\cos \theta/2 = 1/\sqrt{2}$ $(\because \sin \theta/2 = 1/\sqrt{2})$ $e^{i\phi_1} \sin \theta/2 = 1/\sqrt{2}$

$\Rightarrow \theta/2 = \pi/4 \Rightarrow \theta = \pi/2$

$\Rightarrow \because e^{i\phi_1} = 1 \Rightarrow \phi_1 = 0$

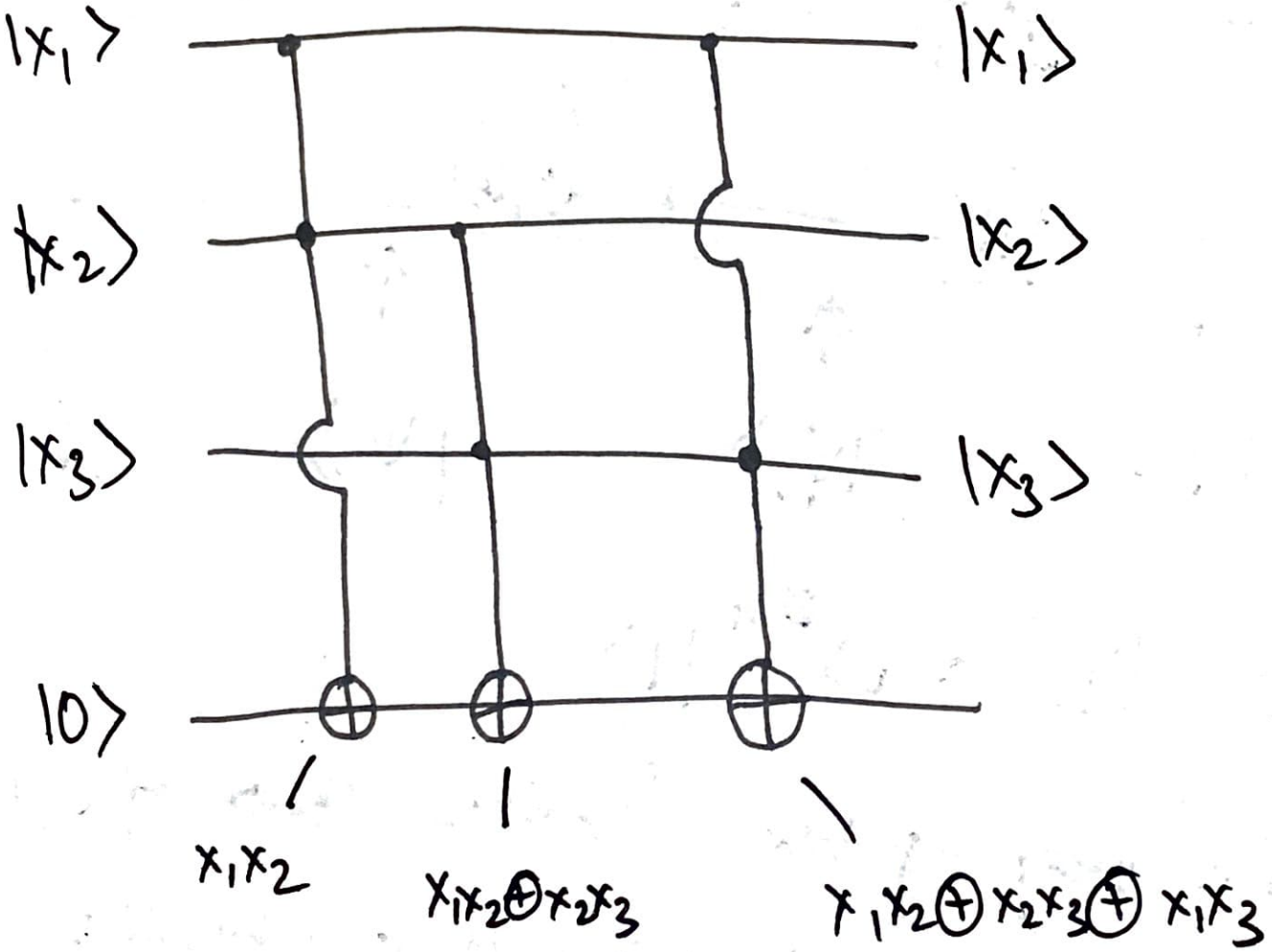
$\therefore \theta = \pi/2, \phi_1 = 0$ be the Block sphere representation of $|\psi\rangle$ ... $|\psi\rangle$ would be a point on the equator of the Block sphere in a direction $\phi_1 = 0$.

As $|\phi\rangle$ is a mixed state represented by $\frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ in Block Sphere representation

⇒ The state can take any point inside the sphere Coatisfying $\rho\phi\rangle = \begin{pmatrix} 1/2 & 0 \\ 0 & 1/2 \end{pmatrix}$

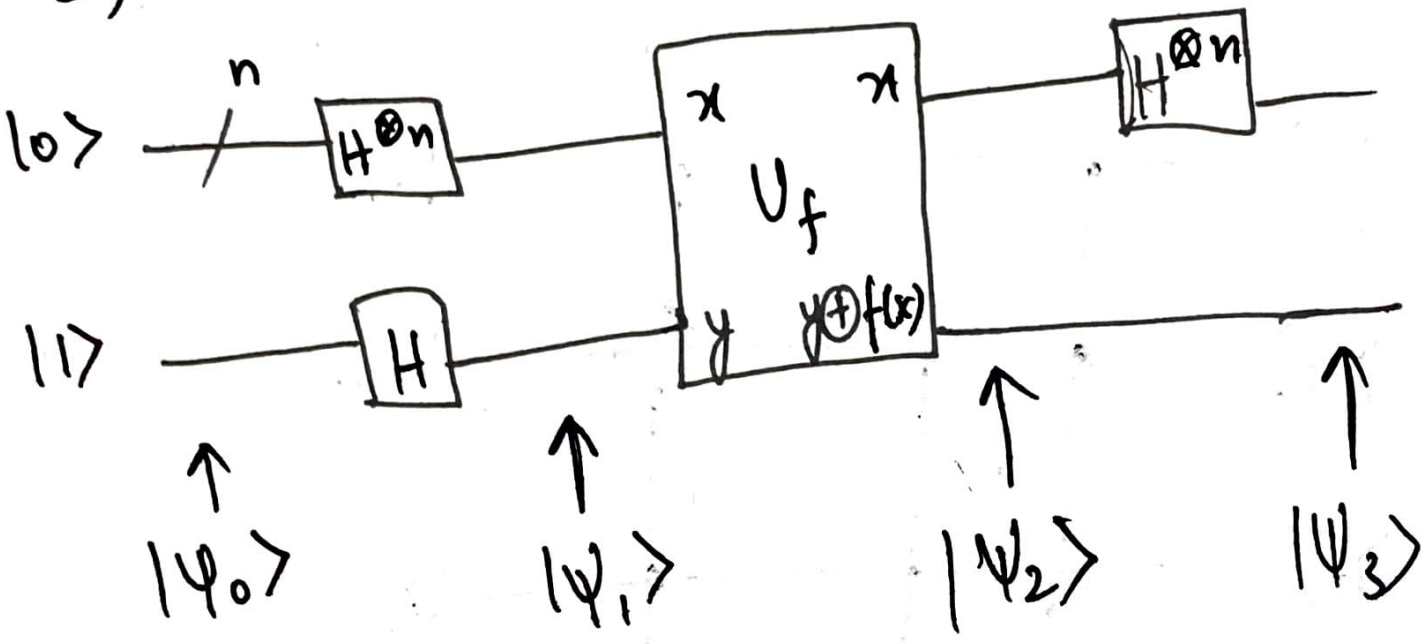
Q2 (a) Boolean function $f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3x_1$

Oracle U_f $\Rightarrow$



(6) Quantum circuit to implement Deutsch-Jozsa

⇒



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

The query register describes state of n qubits all prepared in $|0\rangle$ state. After respective Hadamard transforms ⇒

$$|\psi_1\rangle = \sum_{x \in \{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right]$$

$$|\psi_2\rangle = \sum_x \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

↳ going through U_f.

Again now all these into Hadamard ⇒

$$|\psi_3\rangle = \sum_z \sum_x \frac{(-1)^{x\cdot z + f(x)}}{2^n}|z\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

[redacted] ⟶ This is the state before measurement.

Walsh Transform of a Boolean function g is $W_g(w) = \sum_{x\in\{0,1\}^n} (-1)^{g(x)+x\cdot w}$

↳ looks same as the term in $|\psi_3\rangle$

∴ We can rewrite $|\psi_3\rangle$

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{z \in \{0,1\}^n} \left[\sum_{x \in \{0,1\}^n} (-1)^{f(x)+x\cdot z} \right] |z\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

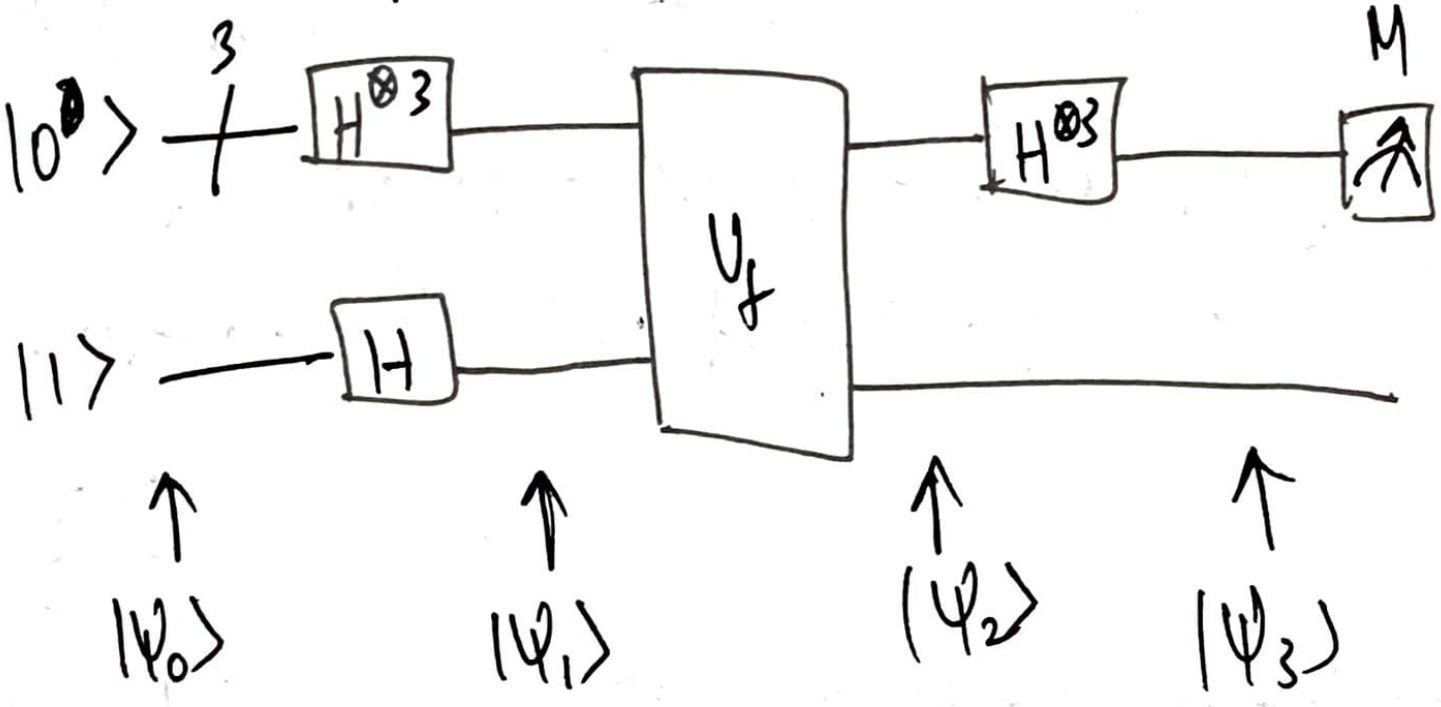
As oracle is g ⇒ Just replace $f(x)$ with $g(x)$

$$\Rightarrow |\psi_3\rangle = \frac{1}{2^n} \sum_{z \in \{0,1\}^n} W_g(z) |z\rangle \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

This is the connection.

(c) Given function is $h(x_1, x_2, x_3) = x_1 x_2 x_3$

Let's use U_f here (DJ) $\Rightarrow$



$$|\psi_0\rangle = |0\rangle^{\otimes 3} \; |1\rangle$$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^3}} \sum_{x \in \{0,1\}^3} |x\rangle \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$|\psi_2\rangle = \frac{1}{\sqrt{2^3}} \sum_{x \in \{0,1\}^3} (-1)^{h(x)} \; |x\rangle$$

$$|\psi_3\rangle = \frac{1}{8} \sum_{z \in \{0,1\}^3} \sum_{x \in \{0,1\}^3} (-1)^{h(x) + x \cdot z} \; |z\rangle \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right)$$

$$\Rightarrow \frac{1}{8} \sum_{z \in \{0,1\}^3} \left((-1)^{000 \cdot z} |z\rangle + (-1)^{001 \cdot z} |z\rangle - - - \right.$$
$$\left. - - + (-1)^{111 \cdot z} |z\rangle \right) \left(\frac{|0\rangle + |1\rangle}{\sqrt{2}} \right)$$

$$\Rightarrow \frac{1}{8} \Big[6|000\rangle + 2|001\rangle + 2|010\rangle - 2|011\rangle$$
$$+ 2|100\rangle - 2|101\rangle - 2|110\rangle + 2|111\rangle \Big]$$
$$\left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$\Rightarrow$ After measurement, we see that $P(|000\rangle) = \frac{9}{16}$ has the highest probability.

$\Rightarrow$ $|000\rangle$.

(16) (a) BB84 is a quantum key distribution scheme where two parties want to share a secret key.

Alice wants to send a private key to Bob. For this Alice chooses $(4+\delta)$ n-bit $= (b)$ random string which she uses to encode $|0\rangle$, $|+\rangle$ according to 0's, 1's in b.

Alice again chooses another $(4+\delta)$ n-bit random string c; in which she measures the above chosen qubit in $\{|0\rangle, |1\rangle\}$ basis if bit is 0 in c or in $\{|+\rangle, |-\rangle\}$ basis if bit is 1 in c.

Now Alice sends the resulting state to Bob.

Bob chooses a random $(4+\delta)n$ bit string (b').

Measures in $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ accordingly as 0 and 1 in b'.

Alice now announces c and Bob matches b' with c. They now discard any bits where Bob measured a different basis than the ones Alice made.

there are atleast $2n$ bits left with high chance (else, abort the protocol and restart again.)

these $2n$ bits which is the raw key.

(c) If Bob keeps all received qubits without measurement and wait till they discuss about basis in a public channel, then any third party can hear this and there by easily obtain the ~~private key~~ raw key. This is because in a public channel, a third part can get the exact same copy from the measurement and the basis is also known, so they can do it surely.

(b) Purpose is to create randomness. Since, third party listening to Alice sharing the key has no idea what is the basis, they can be measuring the qubits wrong with the probability of 1/2 (for each qubit).

(d) After setting the raw key as mentioned above, we have a 2n bit. Now Alice chooses a n bit string out of this 2n bits and use it as a check bit. and publishes this n bits and their values.

Bob compares his measured bit values for the n-check bits Alice shared

And announces the bits where they disagreee. Assume there is some small error too.

Alice has n bit, Bob has n-bit.

Using error correcting code Algorithm, they encode them as d_A, d_B respectively.

If they get Hash (d_A) = Hash (d_B).

they then take this n-bit as the final private key.

Q4 (a) $f: \{0,1\}^n \to \{0,1\}^n$

for any two inputs x, y $f(x) = f(y)$

iff $x = y \oplus s$, $s \in \{0,1\}^n$.

We have to find s.

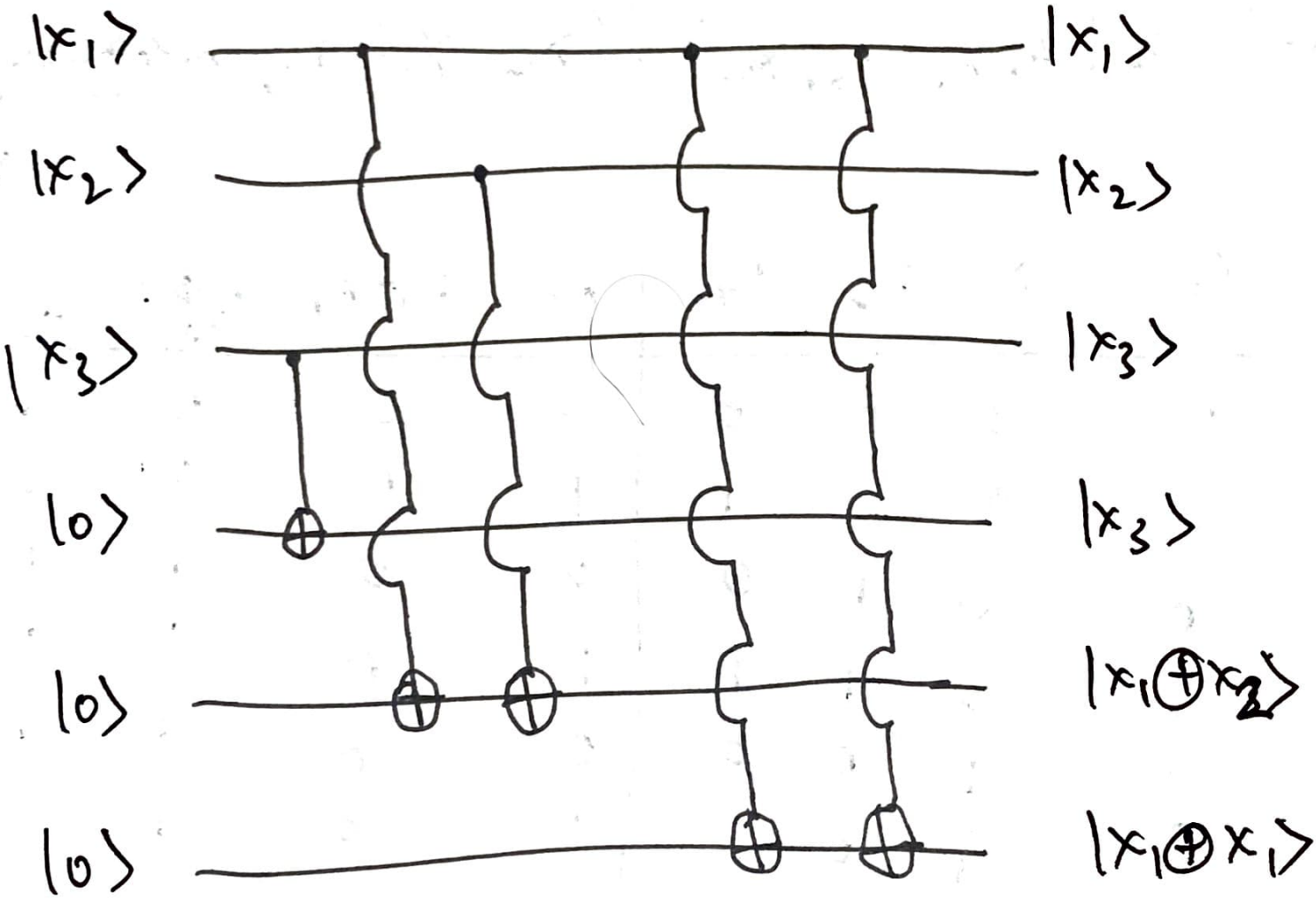
In classical, we need $2^{n-1}+1$ trails in worst case to find s.

Simon's does it in $O(n)$ in a quantum setting.

Simons says f should be one-one

or. two-one → Conditions.

(b) $f(x_1, x_2, x_3) = (x_3, x_1 \oplus x_2, x_1 \oplus x_1)$



x_1	x_2	x_3	x_3	$x_1 \oplus x_2$	$x \oplus x_1$
0	0	0	0	0	0
0	0	1	1	0	0
0	1	0	0	1	0
0	1	1	1	1	0
1	0	0	0	1	0
1	0	1	1	1	0
1	1	0	0	0	0
1	1	1	1	0	0

It's a two-one function. (Satisfies)

(c) $g(x_1, x_2, x_3, x_4) = (x_4, x_1 \oplus x_1, x_1 \oplus x_2 \oplus x_3, x_2)$

x_1	x_2	x_3	x_4	x_4	$x_1 \oplus x_1$	$x_1 \oplus x_2 \oplus x_3$	x_2
0	0	0	0	0	0	0	0
0	0	0	1	1	0	0	0
0	0	1	0	0	0	1	0
0	0	1	1	1	0	1	0
0	1	0	0	0	0	1	1
0	1	0	1	1	0	1	1
0	1	1	0	0	0	0	1
0	1	1	1	1	0	0	1
1	0	0	0	0	0	0	0
1	0	0	1	1	0	0	0
1	0	1	0	0	0	0	0
1	0	1	1	1	0	0	0
1	1	0	0	0	0	0	1
1	1	0	1	1	0	0	1
1	1	1	0	0	0	1	1
1	1	1	1	1	0	1	1

Satisfies the two - one condition ..