16) No cloning theorem :-

There is no quantum copying machine that can make two perfect copies of two nonorthogonal state.

⇒ If possible we can make a quantum circuit U, which can make two perfect copies of two nonorthogonal state.

Let $|\psi\rangle$ & $|\phi\rangle$ are two non orthogonal state, and let $|s\rangle$ is some standard pure state, Then we have —

$$U|\psi\rangle|s\rangle = |\psi\rangle|\psi\rangle$$

$$U|\phi\rangle|s\rangle = |\phi\rangle|\phi\rangle.$$

Now taking inner product we have —

$$\langle (U|\psi\rangle|s\rangle)(U|\phi\rangle|s\rangle)\rangle = \langle\psi|\langle\psi|\phi\rangle|\phi\rangle$$

$$\Rightarrow (U|\phi\rangle|s\rangle)^{\dagger} U|\psi\rangle|s\rangle = \langle\psi|\phi\rangle\langle\psi|\phi\rangle$$

$$\Rightarrow \langle s|\langle\phi| U^{\dagger}U|\psi\rangle|s\rangle = (\langle\psi|\phi\rangle)^2$$

as U is an unitary matrix so, ⟶

$$U^{\dagger}U = I_n = UU^{\dagger}$$

$$\Rightarrow \langle s|\langle\phi|\psi\rangle|s\rangle = (\langle\psi|\phi\rangle)^2$$

$$\Rightarrow \langle s|s\rangle\langle\phi|\psi\rangle = (\langle\psi|\phi\rangle)^2$$

here we choose $|s\rangle$ as unit vector —

So, $\langle S|S\rangle = 1$.

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

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

$\Rightarrow |\langle\psi|\phi\rangle| = 0$ or 1.

$\Rightarrow |\langle\psi|\phi\rangle| = 0$ or $|\langle\psi|\phi\rangle| = 1$

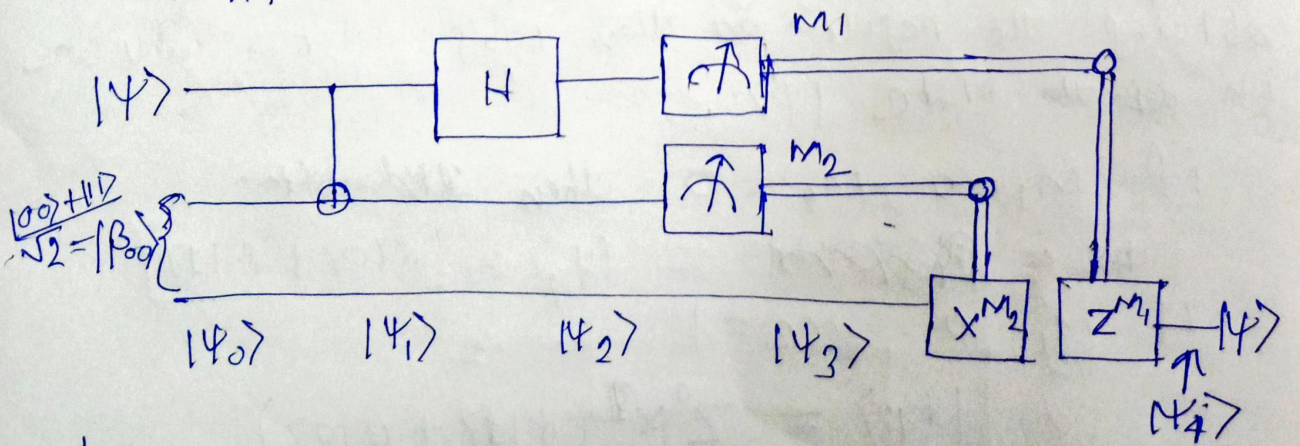
$\Rightarrow$ ~~either~~ $|\psi\rangle$ & $|\phi\rangle$ are ~~orthogonal~~ orthogonal or, $|\psi\rangle = |\phi\rangle$.

Thy cloning device can only clone States which are ~~orthogonal~~ orthogonal to one another, So, ~~cannot make a cloning~~ in general, quantum cloning is not possible.

1 (b) In quantum teleportation one can send a quantum state to a classical channel. Here we can exploited the quantum entanglement.

let if say Alice wants to send a qubit $|\psi\rangle$ to Bob, and the laws of quantum mechanics prevent her from determining the state when she only has a single copy of $|\psi\rangle$ in her possession. Alice use quantum teleportation by the help of an entangled EPR pair in order to send $|\psi\rangle$ to Bob.

Alice interacts the qubit $|\psi\rangle$ with her half EPR pair, and then measures the two qubits in her possession, obtaining one of four possible classical result 00, 01, 10, 11, she sends this information to Bob. Depending on Alice's classical message, Bob performs one of four operations on his half of the EPR pair. By this we can recover $|\psi\rangle$.



Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α, β are unknow amplitudes,

Now, $|\psi_0\rangle = |\psi\rangle|\beta_{00}\rangle$.

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle(|00\rangle+|11\rangle) + \beta|1\rangle(|00\rangle+|11\rangle)\right]$$
$$= \frac{1}{\sqrt{2}}\left[\alpha|0\rangle|\psi\rangle + \alpha|01\rangle|1\rangle + \beta|10\rangle|0\rangle + \beta|11\rangle|1\rangle\right]$$

Now, $|\psi_1\rangle = \frac{1}{\sqrt{2}}\left[\alpha|0\rangle|00\rangle\right.$

$$= \frac{1}{\sqrt{2}}\left[\alpha|00\rangle|0\rangle + \alpha|01\rangle|1\rangle + \beta|11\rangle|0\rangle + \beta|10\rangle|1\rangle\right]$$

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

She then sends the first qubit through a Hadamard gate, obtaining →

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

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

The first term has Alice's qubits in the state $|00\rangle$, and Bob's qubit in the state $\alpha|0\rangle+\beta|1\rangle$ which is the original $|\psi\rangle$ state.

If Alice performs a measurement and obtains the result 00 then Bob's system will be in the state $|\psi\rangle$.

if $M_1=0$, $M_2=0$ then $|\psi_4\rangle = [\alpha|0\rangle+\beta|1\rangle]$

If $M_1=0$, $M_2=1$

$$|\psi_4\rangle \equiv Z^0X^1(\alpha|1\rangle+\beta|0\rangle)$$
$$= X(\alpha|0\rangle+\beta|1\rangle)$$

if $M_1=1$, $M_2=0$ $|\psi_4\rangle = ZX^0(\alpha|0\rangle-\beta|1\rangle)$

$= Z(\alpha|0\rangle - \beta|1\rangle) = (\alpha|0\rangle + \beta|1\rangle)$

if $M_1 = 1, M_2 = 1$.

$$|\psi_4\rangle = ZX(\alpha|1\rangle - \beta|0\rangle)$$
$$= Z(\alpha|0\rangle - \beta|1\rangle)$$
$$= (\alpha|0\rangle + \beta|1\rangle).$$

So, $|\psi_4\rangle = |\psi\rangle$.

So, done.

1 (c) If $|\psi\rangle$ is a pure quantum state with $|0\rangle$ & $|1\rangle$

So, $|\psi\rangle = 1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle$

The density matrix corresponding to $|\psi\rangle$ is

$$\rho_1 = |\psi\rangle\langle\psi| = \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix}$$

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

In mixed state $|\phi\rangle$ containg $|0\rangle$ & $|1\rangle$ in equal proportion.

So, the density matrix of $|0\rangle$ & $|1\rangle$ are resp. $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ & $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Hence the density matrix of the mixed state $|\phi\rangle$ is $\rho_2 = 1/2\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + 1/2\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = 1/2\, I_2$.

∴ density matrix of $|\psi\rangle = 1/2\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$

" " " $|\phi\rangle = 1/2\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

Bloch-sphere reps of $|\psi\rangle$ and $|\phi\rangle$.

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

We represent $|\psi\rangle$ in the form —

$$\cos\theta/2\,|0\rangle + e^{i\phi}\sin\frac{\theta}{2}\,|1\rangle .$$

So, by comparing, $\cos\theta/2 = 1/\sqrt{2}$

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

& $e^{i\phi_1}\sin\frac{\theta}{2} = 1/\sqrt{2} \Rightarrow e^{i\phi_1} = 1$

$$\Rightarrow \phi_1 = 0.$$

So, $\theta = \pi/2$, $\phi_1 = 0$, be the Bloch sphere rep. of $|\psi\rangle = 1/\sqrt{2}|0\rangle + 1/\sqrt{2}|1\rangle$. So, $|\psi\rangle$ would be a point on the eqn of the Bloch sphere, in a direction $\phi = 0$.

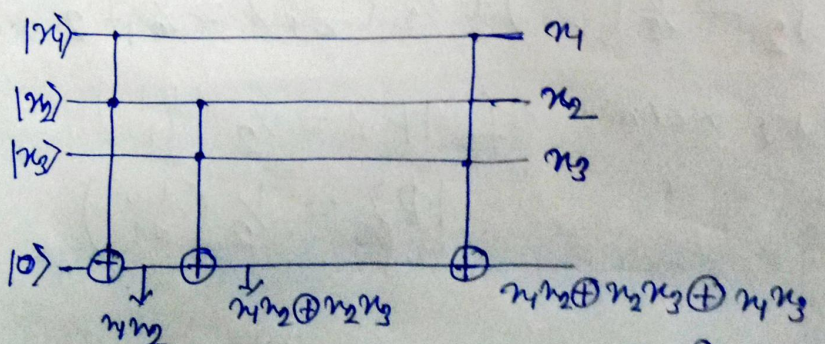
As $|\psi\rangle$ is a mixed state rep by the density matrix $\frac{1}{2}\begin{pmatrix}1&0\\0&1\end{pmatrix}$ in bloch sphere rep, the state can take any point inside the sphere.

2(a) Given boolean function —

$$f(x_1, x_2, x_3) = x_1x_2 \oplus x_2x_3 \oplus x_3x_1 .$$

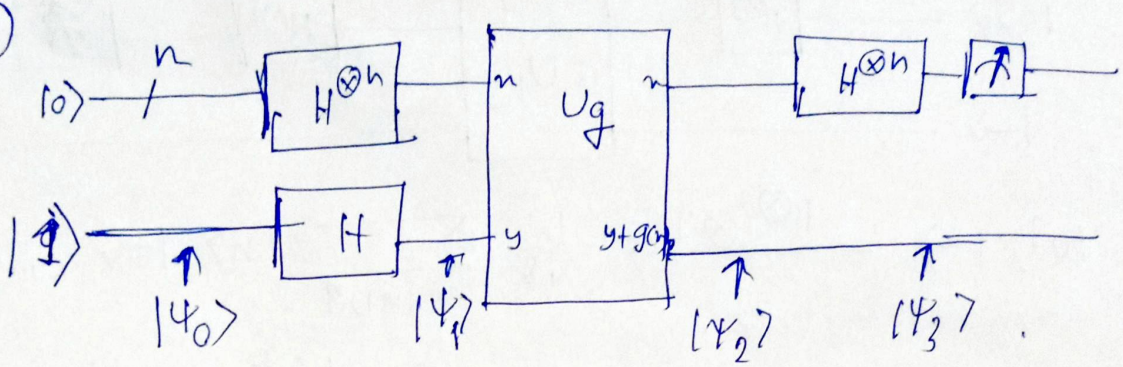
eg $U_f(|x\rangle|y\rangle) = |x\rangle|y \oplus f(x)\rangle$

oracle for U_f :-



This is the oracle for required function.

(2) (b)



$$|0^n\rangle|1\rangle \xrightarrow{H^{\otimes n}\otimes H} \frac{1}{\sqrt{2^n}}\sum_x |x\rangle|-\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2^n}}\sum_x (-1)^{f(x)}|x\rangle|-\rangle \xrightarrow{H^{\otimes n}\otimes I} \frac{1}{2^n}\sum_y\left[\sum_x (-1)^{f(x)\oplus x\cdot y}\right]|y\rangle|-\rangle .$$

where $x\cdot y$ denotes the bitwise dot product.

$$x_1y_1 \oplus x_2y_2 \oplus \cdots \oplus x_ny_n .$$

So, $$|\psi_3\rangle = \frac{1}{2^n}\sum_y \left(\sum_x (-1)^{f(x)\oplus x\cdot y}\right)|y\rangle|-\rangle .$$

This the before measurement state.

Now, we know that, walsh transform of a boolean function g is defined as—

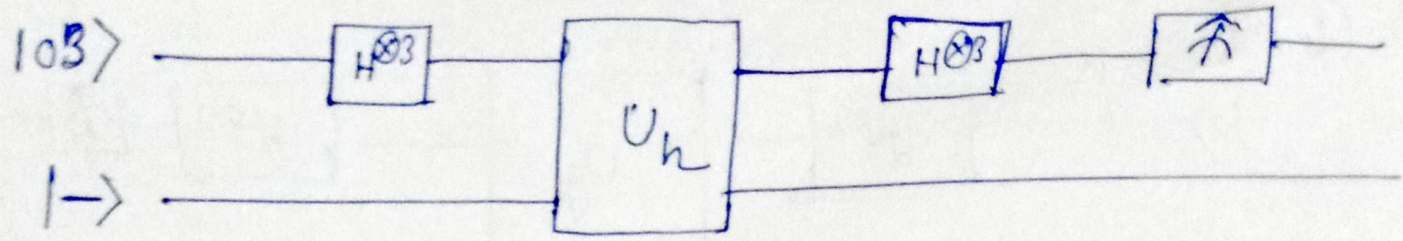
$$W_g(w) = \sum_{x\in\{0,1\}^n} (-1)^{f(x)\oplus x\cdot w} .$$

So, $$|\psi_3\rangle = \frac{1}{2^n}\sum_{y\in\{0,1\}^n} W_g(y)\,|y\rangle|-\rangle .$$

(2) (c) Given function is $h(x_1,x_2,x_3) = x_1x_2x_3$.

So, $h(x_1,x_2,x_3) = 1$ iff $x_1=x_2=x_3=1$

$= 0$ otherwise.



$$|0^3\rangle|-\rangle \xrightarrow{H^{\otimes 3}\otimes I} \frac{1}{\sqrt{8}} \sum_{n\in\{0,1\}^3} |n\rangle|-\rangle \xrightarrow{U_h} \frac{1}{\sqrt{8}} \sum_{n\in\{0,1\}^3} (-1)^{h(n)}|n\rangle|-\rangle$$

$$= \frac{1}{\sqrt{8}}\Big[|000\rangle + |001\rangle + |010\rangle + |011\rangle + |100\rangle + |101\rangle + |110\rangle - |111\rangle\Big]$$

$$\xrightarrow{H^{\otimes 3}\otimes I} \frac{1}{8} \sum_{z\in\{0,1\}^3} \sum_{n\in\{0,1\}^3} (-1)^{n\cdot z + h(n)}|z\rangle .$$

$$= \frac{1}{8}\left[\sum_{z\in\{0,1\}^3} \left((-1)^{(000)\cdot z} + (-1)^{(001)\cdot z} - (-1)^{(011)\cdot z}\right)|z\rangle\right]$$

$$= \frac{1}{8}\Big[6|000\rangle + 2|001\rangle + 2|010\rangle - 2|011\rangle + 2|100\rangle - 2|101\rangle - 2|110\rangle + 2|111\rangle\Big]$$

$$= \frac{3}{4}|000\rangle + \frac{1}{4}|001\rangle + \frac{1}{4}|010\rangle - \frac{1}{4}|011\rangle + \frac{1}{4}|100\rangle - \frac{1}{4}|101\rangle - \frac{1}{4}|110\rangle + \frac{1}{4}|111\rangle .$$

After measurement we get the $|000\rangle$ has the highest probability i.e. $pr(|000\rangle) = \frac{9}{16}$.

1@ Simon's Algorithm :-

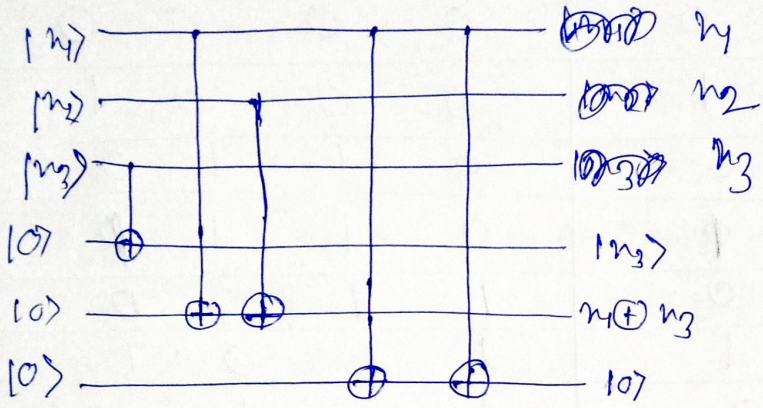
Problem statement :- Given a function $f: \{0,1\}^n \longrightarrow \{0,1\}^n$ with the promise that for some unknown $s \in \{0,1\}^n$ for all $x, y \in \{0,1\}^n$ $f(x) = f(y)$ iff $x \oplus y \in \{0^n, s\}$.

i.e. f is one to one or 2 to one.

4 (b) Given $f(x_1, x_2, x_3)$

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

Oracle for U_f



Truth table

Input x_1 x_2 x_3	Output f_1 f_2 f_3
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

So, from here f is due to one function.

So, f satisfies condition e.

4(c) Let $g : \{0,1\}^4 \to \{0,1\}^4$ s.t.

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

Now,

x_1	x_2	x_3	x_4	g_1	g_2	g_3	g_4
0	0	0	0	0	0	0	0
0	0	0	1	0	0	0	1
0	0	1	0	0	1	1	0
0	0	1	1	0	1	1	1
0	1	0	0	1	1	0	0
0	1	0	1	1	1	0	1
0	1	1	0	1	0	1	0
0	1	1	1	1	0	1	1
1	0	0	0	0	1	1	0
1	0	0	1	0	1	1	1
1	0	1	0	0	0	0	0
1	0	1	1	0	0	0	1
1	1	0	0	1	0	1	0
1	1	0	1	1	0	1	1
1	1	1	0	1	1	0	0
1	1	1	1	1	1	0	1

~~$g(0000) = g(1011) = (0000)$~~

g is a 2-to-1 function.

5 (a) Matrix rep of QFT:

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \cdots & (\omega^2)^{N-1} \\ \vdots & & & \vdots \\ 1 & \omega^{N-1} & \cdots & \omega^{(N-1)(N-1)} \end{pmatrix}$$

where ω is N^{th} root of unity, and $\omega^k = e^{\frac{2\pi i k}{N}}$

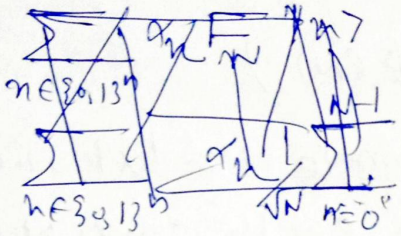
and $k \in \{0, \ldots, N-1\}$, and $i = \sqrt{-1}$

output state when QFT is applied on an n-qubit state $\sum_{n\in\{0,1\}^n} \alpha_n |n\rangle$.

So, $QFT\left(\sum_{n\in\{0,1\}^n} \alpha_n |n\rangle\right)$.

$= F_N\left(\sum_{n\in\{0,1\}^n} \alpha_n |n\rangle\right) = F_N\left(\sum_{k=0}^{N-1} \beta_k |k\rangle\right)$

k is decimal of n

$=$ 

here $N = 2^n$.

$= \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & & \omega^{N-1} \\ \vdots & & & \vdots \\ 1 & \omega^{N-1} & & \omega^{(N-1)(N-1)} \end{pmatrix} \begin{pmatrix} \beta_0 \\ \beta_1 \\ \vdots \\ \beta_{N-1} \end{pmatrix}$

any k^{th} row for $k \in \{0, \ldots N-1\}$ of the resultant matrix would look like.

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

(b) Problem statement: Shor's algorithm is a polynomial-time quantum computer algorithm algorithm for linear factorization.

So, basically Given a large N, this algo can factors p such that $p | N$ i.e, $N = p \times q$ where p, q are prime.

(c) Impact of Shor's factoring algorithm in cryptanalysis of RSA

So, basically RSA is based on the factorisation problem of some $N = pq$ where p, q are large primes.

If one knows p or q, they can easily find 'secret key from p, q.

In RSA, 'd' is a public key and e is secret key connected by

$$e \cdot d \equiv 1 \pmod{\phi(N)}$$

If one can easily factorize $N = p \times q$, i.e, he/she knows p, q so, can easily compute

$$\phi(N) = (p-1)(q-1)$$

and as d is known to everyone we can find 'e' from above eqn.

Thereby allowing us to decrypt all information using these keys.

Shor's Algorithm

Shor's algorithm is a Polynomial-time quantum computer algorithm algorithm for linear factorization.

So, basically, Given a large N, this algorithm find a factors p such that $p|N$, i.e, $N = p \times q$, where p, q are prime numbers.

period finding

(i) We start with any random integer $g < N$.

(ii) calculate $d = gcd(g, N)$. If $d \neq 1$ ——

~~d~~ & if $d = gcd(g, N) \Rightarrow d|N$

So, if N is product of two prime so, d — divides one of the prime & $1 < d \leq p$ so, d might be one of the prime, so, we are done.

So, otherwise let $d = 1$ then $gcd(g, N) = 1$ —

$\Rightarrow g \in \mathbb{Z}_N^*$, if g is unit element in multiplicative group $\mathbb{Z}_N$.

Now, we need to find $a < N$ such that —

$g^a \equiv 1 \pmod N$. & smallest such a is called order of g.

(iii) Let for any $n \in \mathbb{N}$, we have $g^n \equiv k \pmod N$

(iv) if $g^a \equiv 1 \pmod N \Rightarrow g^{n+a} \equiv k \pmod N$ for any $n \in \mathbb{N}$.

(v) Let $f(n) = g^n \pmod N$. then for all $n \in \mathbb{N}$, we have $f(n+a) = f(a)$, i.e, a is period of f.

(vi) Therefore, if we can find the period of the function f to be a, then we have —

$g^a \equiv 1 \pmod N \Rightarrow (g^{a/2})^2 \equiv 1 \pmod N$

then $N \mid (g^{a/2}-1)(g^{a/2}+1)$. and $g^{a/2} \not\equiv \pm 1 \pmod N$

and of a is the order of g in Z_N^* so, —

$g^{a/2} \not\equiv 1 \pmod N$, . . .

So, $g^{a/2} \not\equiv \pm 1 \pmod N$

$\Rightarrow N \nmid (g^{a/2}-1)$ & $N \nmid (g^{a/2}+1)$

$\Rightarrow \gcd(N, g^{a/2}-1) = d_1$ & $d_1 \neq 1$ by same logic

and $d_1 \mid N \Rightarrow d_1$ is a factors of N. and we are done.

similis $N \nmid (g^{a/2}+1)$

if $\gcd(N, g^{a/2}+1) = d_2$

$\Rightarrow d_2 \mid N \Rightarrow d_2$ is a factors of N. .

So, we are done.

Let $N = 35$ then —

(i) calculate $\gcd(g, 35)$ using Euclid's algorithm

if our $g = 5$, check $\gcd(5, 35) = 5 \neq 1$. so, we are done, as, $5 \mid 35$

So, take $g = 4$, and $\gcd(4, 35) = 1$.

ii) Now, construct a function —

$$f(n) = 4^n \pmod{35}$$

iii) Now, our goal is to find the period of the function $f(n)$ for which $f(n+a) = f(n)$

i.e, $4^{a+n} = 4^n \pmod{35} \Rightarrow 4^a \equiv 1 \pmod{35}$

our goal is to find such an 'a'.

Transforming the problem :-

So, The problem of finding the factorization of a large integer N has been converted to a problem of finding the period a of the function

$$f(x) = g^x \pmod N$$

(Quantum Fourier Transformation)

We will find the period of f using (QFT) in poly time.

We know that matrix representation of QFT :

$$F_N = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \cdots & \omega_N^{N-1} \\ \vdots & \vdots & & \vdots \\ 1 & \omega_N^{N-1} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix}$$ where

ω_N^k be the Nth root of unity. $\omega_N^k = e^{\frac{2\pi i k}{N}}$.

for a given quantum state $|x\rangle = \sum_{k=0}^{N-1} \alpha_k |k\rangle$, —

QFT$(|x\rangle)$ is given by :

$$(F_N) \times (|x\rangle) = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \cdots & \omega_N^{N-1} \\ \vdots & & & \\ 1 & \omega_N^{N-1} & \cdots & \omega_N^{(N-1)(N-1)} \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{N-1} \end{pmatrix}$$

if $F_N(|x\rangle) = |y\rangle$ where $|y\rangle = \sum_{k=0}^{N-1} \beta_k |k\rangle$, then

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

Algorithm for finding the period

(i) Find $Q = 2^q$ such that $N^2 \le Q \le 2N^2$, which implies $Q/N > N > a$

$\Rightarrow Q/a > N$.

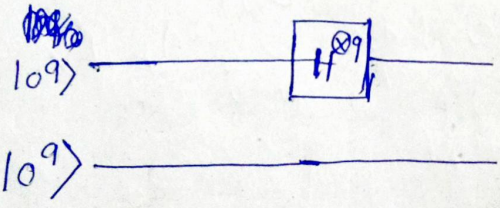
So, that for each $f(x)$, we can find at least N many x which outputs the same value.

Here $N = 35$

Thus, $35^2 \le Q = 2^q \le 2 \cdot 35^2$

$\Rightarrow Q = 2^q = 2^{11} = 2048$

(ii) Initialize all the 9 many qubits from first register to $|0\rangle$ and apply Hadamard gate to each of the qubits. Initialize all the qubits from second register to $|0\rangle$.



$$|\psi_0\rangle = |0^9\rangle|0^9\rangle \xrightarrow{H^9 \otimes I_9} \frac{1}{\sqrt{Q}} \sum_{x=0}^{Q-1} |x\rangle|0^9\rangle = |\psi_1\rangle$$

In our ex, $|\psi_0\rangle = |0^{11}\rangle|0^{11}\rangle$, $Q = 2048$.

$$|0^{11}\rangle|0^{11}\rangle \xrightarrow{H^{11} \otimes I_{11}} \frac{1}{\sqrt{2048}} \sum_{x=0}^{2047} |x\rangle|0^{11}\rangle = |\psi_1\rangle$$

(iii) construct $f(x)$ as a quantum function and apply it to the above state. That is, — $U_f|x\rangle|y\rangle = |x\rangle|y \oplus f(x)\rangle$, we get $|\psi_2\rangle$ as —

$$|\psi_2\rangle = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} |x\rangle |f(x)\rangle .$$

Applying QFT on $|x\rangle$ we get —

$$QFT(|x\rangle) = \frac{1}{\sqrt{q}} \sum_{x=0}^{q-1} \omega^{xy} |y\rangle$$ on the first register.

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

(iv) Suppose $f(x+a) = f(x) = z$ and $f(x+s) \neq f(x)$ for all $s < a$. Let x_0 is the smallest of all the x's for which $f(x) = z$, therefore if $f(x) = z$ then x is of the form $x_0 + ka$, where k varies from $\{0, 1, \ldots, \left\lfloor \frac{q-x_0-1}{a} \right\rfloor\}$. So, —

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

here z is fixed

Probability of getting a state $|y\rangle|z\rangle$ is —

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

$$= \frac{1}{q^2} \left\| \omega^{x_0 y} \right\|^2 . \left\| \sum_{k=0}^{\left\lfloor \frac{q-x_0-1}{a} \right\rfloor} e^{\frac{2\pi i}{q} aky} \right\|^2$$

$$P(y) = \frac{1}{q^2} \left\| \sum_{k=0}^{\lfloor \frac{q-r+1}{a} \rfloor} e^{\frac{2\pi i}{q} aky} \right\|^2.$$

The probability is higher when $\frac{a \cdot y}{q}$ is close an integer. let $\frac{a \cdot y}{q} = m$ an integer.

$$\Rightarrow \frac{y}{q} = \frac{m}{a}.$$

Turn y/q into an irreducible fraction and then extract the denominators a' using the method of continued fraction. This is our is period of the function f.

We need to check $f(n+a) = f(n)$, if not find another state y and check again.

For $$\frac{y}{q} = r_0 + \cfrac{1}{r_1 + \cfrac{1}{r_2 + \cfrac{1}{\ddots}}}$$

$d_0 = r_0$, $d_1 = 1 + r_0 r_1$, $d_n = r_n d_{n-1} + d_{n-2}$ and

$a_0 = 1$, $a_1 = r_1$, $a_n = r_n a_{n-1} + a_{n-2}$

Now we need to check the condition,

$$\left| \frac{y}{q} - \frac{d_i}{a_i} \right| < \frac{1}{2q}.$$

6(a) In BB84 quantum key Distribution, both the two parties Alice and Bob want to share a secret key.

For this Alice choose $(4+\delta)$ n-bit random string d_0 and which she use to encode lot of $|1\rangle$ according to 0 and 1 in d_0.

Alice again choose 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.

Now Bob choose a random $(4+\delta)$ n bit random string b' and measure in $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$ according on 0 and 1 in b'.

Now Alice announce c and Bob match b' with c. They now discard any bits where Bob measured a diff. basis than Alice prepared,

with high probability, there at least 2n bit left,

They keeps the 2n bits which is the base key.

(b)

In this protocol, we used two different basis since they can create randomness when they encoded there bits, for that they choose random bits.

(c) If Bob keeps all received qubits — unmeasured until they discuss about the choice of basis over a public channel. Then any third party can know the bit in which Alice and Bob agree. And easily get the new key

(d) After setting the new key i.e, of 2n-bit. Now Alice choose a n-bit string out of 2n bit and use as check bit, and announces this relation of n bits and their bit values.

Bob compares the bit values he measured for the n-check bits selected. Alice and announces the bits where they disagree They can take a certain percentage of errors.

Now Alice has n bit string and Bob has n bit string, they use errors correcting code when they encoded it to d_1, d_2,

If they set $hash(d_1) = hash(d_2)$

They take the n bit as final key.

They can also take the Hash of it.