e.g. $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ → entangled state example

Q Is the state

$$|\phi\rangle = \frac{1}{\sqrt{2}}[|00\rangle - i|01\rangle + |10\rangle + i|11\rangle]$$

a product state or an entagled state?

* Basis for $V \otimes V$:-

$|00\rangle, |01\rangle, |10\rangle, |11\rangle$ → Basis vectors for 2-qubit system

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}[|00\rangle + |11\rangle]$$

$$|\phi^-\rangle = \frac{1}{\sqrt{2}}[|00\rangle - |11\rangle]$$

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}[|01\rangle + |10\rangle]$$

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}[|01\rangle - |10\rangle]$$

} Bell states

* Choice of basis :-

for 2-qubit vector space

- Computational basis → $|00\rangle, |01\rangle, |10\rangle, |11\rangle$
- Bell states formbasis → $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle$

Note:- Entanglement is a property which is independent of the choice of basis for the tensor product space.

Consider the state

$$|\psi\rangle = \frac{1}{2}\left[|0000\rangle + |0101\rangle + |1010\rangle + |1111\rangle\right]$$

↓

Factorize it w.r.t. individual qubit (standard decomposition)

$$= \frac{1}{2}\left[|0\rangle^{(3)} |0\rangle^{(2)} |0\rangle^{(1)} |0\rangle^{(0)} + |0\rangle^{(3)} |1\rangle^{(2)} |0\rangle^{(1)} |1\rangle^{(0)} + |1\rangle^{(3)} |0\rangle^{(2)} |1\rangle^{(1)} |0\rangle^{(0)} + |1\rangle^{(3)} |1\rangle^{(2)} |1\rangle^{(1)} |1\rangle^{(0)} \right]$$

Entangled

Now, consider decomposition in the space of 1st & 3rd qubits and 0th & 2nd qubits.

$$|\psi\rangle = \frac{1}{2}\left[|0\rangle^{(3)} |0\rangle^{(1)} \{ |0\rangle^{(2)} |0\rangle^{(0)} + |1\rangle^{(2)} |1\rangle^{(0)} \} + |1\rangle^{(3)} |1\rangle^{(1)} \{ |0\rangle^{(2)} |0\rangle^{(0)} + |1\rangle^{(2)} |1\rangle^{(0)} \} \right]$$

↓

That means, state is not entangled w.r.t this new decomposition.

Note :- Entanglement → decomposition dependent
→ But basis independent

Q) Is $|\psi\rangle$ entagled w.r.t. decomposition into a subsystem consisting of 0^{th} & 1^{st} qubits and 2^{nd} & 3^{rd} Qubits ?

* Operators on Tensor product spaces :-

Consider the space $V \otimes W$

Let $\hat{A} : V \to V$

$\hat{B} : W \to W$

be arbitary linear operators,

then - $\hat{A} \otimes \hat{B} : V \otimes \omega \rightarrow V \otimes \omega$ is a linear operators on $V \otimes \omega$ such that if

$|v\rangle \in V$ & $|\omega\rangle \in \omega$

then - $(\hat{A} \otimes \hat{B})(|v\rangle \otimes |\omega\rangle) = (\hat{A}|v\rangle) \otimes (\hat{B}|\omega\rangle)$

→ If $\hat{C}$ & $\hat{D}$ are operators on V & ω respectively then -

$$(\hat{A} \otimes \hat{B})(\hat{C} \otimes \hat{D}) = (\hat{A}\hat{C}) \otimes (\hat{B}\hat{D})$$

→ Linearity ⇒

$$(\hat{A} \otimes \hat{B}) \left(\sum_i a_i |v_i\rangle \otimes |\omega_i\rangle \right)$$

$$= \sum_i a_i (A|v_i\rangle) \otimes (B|\omega_i\rangle)$$

Q Given that $|\psi\rangle = \frac{|0\rangle|0\rangle - |1\rangle|1\rangle}{\sqrt{2}}$ → entangled state

$(\hat{x} \otimes \hat{z})|\psi\rangle = ?$

Ans $(\hat{x} \otimes \hat{z}) \left(\frac{|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle}{\sqrt{2}} \right)$

$$= \frac{1}{\sqrt{2}} \left[(\hat{x}|0\rangle) \otimes (\hat{z}|0\rangle) - (\hat{x}|1\rangle) \otimes (\hat{z}|1\rangle) \right]$$

$$= \frac{1}{\sqrt{2}} \left[|1\rangle|0\rangle + |0\rangle|1\rangle \right]$$

→ entangled state

Q Let $A = |0\rangle\langle 0|$, $B = |1\rangle\langle 1|$

& $|\chi\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$ → entangled state

what is $(A \otimes B)\,|\chi\rangle = ?$

Ans

$$\left(|0\rangle\langle 0| \otimes |1\rangle\langle 1|\right)\left(\frac{|01\rangle + |10\rangle}{\sqrt{2}}\right)$$

$$= \frac{1}{\sqrt{2}}\Big[(|0\rangle\langle 0|)|0\rangle \otimes (|1\rangle\langle 1|)(|1\rangle) + |0\rangle\langle 0|(|1\rangle) \otimes |0\rangle\langle 1|(|0\rangle)\Big]$$

$$= \frac{1}{\sqrt{2}}\left[|0\rangle|1\rangle\right]$$ → entangled product state

Note :- (i) $|v\rangle \otimes |\omega\rangle = |v\rangle|\omega\rangle$ or $|v\omega\rangle$

But $\hat{A} \otimes \hat{B} \neq \hat{A}\hat{B}$

(ii) $(\hat{A} \otimes \hat{B})^{+} = A^{+} \otimes B^{+}$

* Matrix representation of states & operators on tensor product spaces :-

Consider the state space of 2 qubits

First of all, we need basis -

Basis → $|00\rangle, |01\rangle, |10\rangle, |11\rangle$

If $|\phi\rangle = v \otimes v$

$\{ v \Rightarrow \mathbb{C}^2 \}$

then -

$$|\phi\rangle \equiv \begin{pmatrix} \langle 00|\phi\rangle \\ \langle 01|\phi\rangle \\ \langle 10|\phi\rangle \\ \langle 11|\phi\rangle \end{pmatrix}$$

4×1 column vector

→ If $|\phi\rangle$ is product state

say $|\phi\rangle = |a\rangle \otimes |b\rangle$

so that $|a\rangle \equiv \begin{pmatrix} \langle 0|a\rangle \\ \langle 1|a\rangle \end{pmatrix} = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$

& $|b\rangle = \begin{pmatrix} b_0 \\ b_1 \end{pmatrix}$

then- $|\phi\rangle = |a\rangle \otimes |b\rangle$

$$= \begin{pmatrix} \langle 00|ab\rangle \\ \langle 01|ab\rangle \\ \langle 10|ab\rangle \\ \langle 11|ab\rangle \end{pmatrix} = \begin{pmatrix} \langle 0|a\rangle\langle 0|b\rangle \\ \langle 0|a\rangle\langle 1|b\rangle \\ \langle 1|a\rangle\langle 0|b\rangle \\ \langle 1|a\rangle\langle 1|b\rangle \end{pmatrix}$$

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

Q $|a\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ & $|b\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} \sqrt{2} \\ 1 \end{pmatrix}$

Find $|a\rangle \otimes |b\rangle$

→ If $\hat{O}$ is an operator on $V \otimes V$

$$\hat{O} \equiv \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} \langle 00|\hat{O}|00\rangle & \langle 00|\hat{O}|01\rangle & \cdots & \cdots \\ \langle 01|\hat{O}|00\rangle & \langle 01|\hat{O}|01\rangle & & \\ \langle 10|\hat{O}|00\rangle & & & \\ \langle 11|\hat{O}|00\rangle & \cdots & \cdots & \langle 11|\hat{O}|11\rangle \end{pmatrix} \end{array}$$

So, if $\hat{O} = \hat{A} \otimes \hat{B}$

then -

$$\hat{A} \times \hat{B} \equiv \begin{pmatrix} \langle 0|A|0\rangle\langle 0|B|0\rangle & \cdots & \cdots \\ \langle 0|A|0\rangle\langle 1|B|0\rangle & \cdots & \cdots \\ \langle 1|A|0\rangle\langle 0|B|0\rangle & \cdots & \cdots \\ \langle 1|A|0\rangle\langle 1|B|0\rangle & \cdots & \cdots \end{pmatrix}$$

$$\equiv \left(\begin{array}{cc|cc} A_{00}B_{00} & A_{00}B_{01} & A_{01}B_{00} & A_{01}B_{01} \\ A_{00}B_{10} & A_{00}B_{11} & A_{01}B_{10} & A_{01}B_{11} \\ \hline A_{10}B_{00} & A_{10}B_{01} & A_{11}B_{00} & A_{11}B_{01} \\ A_{10}B_{10} & A_{10}B_{11} & A_{11}B_{10} & A_{11}B_{11} \end{array}\right)$$

Q Find the matrix representation of $\hat{X} \otimes \hat{Y}$.

Q $\hat{Z}$, $\hat{Z} \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

↓

outer product representation $\equiv |0\rangle\langle 0| - |1\rangle\langle 1|$

$\hat{Y}$, $\hat{Y} \equiv \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}$

↓

outer product rep. $\equiv i\,|1\rangle\langle 0| - i\,|0\rangle\langle 1|$

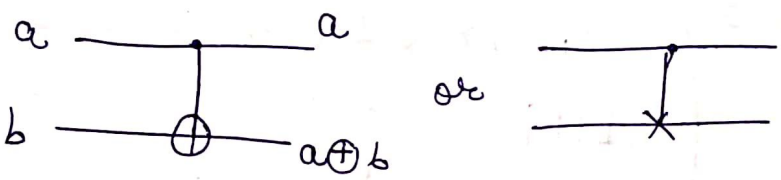
Find the matrix rep. & outer product rep. of $\hat{x} \otimes \hat{y}$.

Ans $(|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes (i|1\rangle\langle 0| - i|0\rangle\langle 1|)$

* Quantum gates with multiple inputs & outputs :-

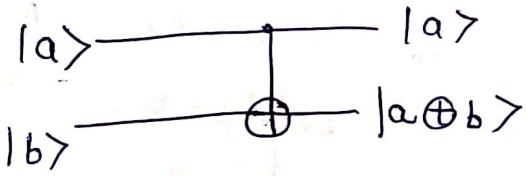
$$UU^\dagger = I$$
$$\Rightarrow U^\dagger = U^{-1}$$

(i) CNOT gate →



↓

quantum version of it



Suppose, $|a\rangle = a_0|0\rangle + a_1|1\rangle$

$|b\rangle = b_0|0\rangle + b_1|1\rangle$

Note :- Inputs of CNOT gate / gates with multiple inputs & outputs is in tensor product space

$\therefore$ $|00\rangle \xrightarrow{\text{CNOT}} |00\rangle$

$|01\rangle \xrightarrow{\text{CNOT}} |01\rangle$

$|10\rangle \xrightarrow{\text{CNOT}} |11\rangle$

$|11\rangle \xrightarrow{CNOT} |10\rangle$

Representation of CNOT gate →

$$CNOT \equiv \begin{array}{c} \\ |00\rangle \\ |01\rangle \\ |10\rangle \\ |11\rangle \end{array} \begin{array}{c} \begin{array}{cccc} |00\rangle & |01\rangle & |10\rangle & |11\rangle \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \end{array}$$

Inputs

Outputs

$$\equiv |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes X$$

$\mathbb{I}$ → Identity $(|0\rangle\langle 0| + |1\rangle\langle 1|)$

X → X gate $(|0\rangle\langle 1| + |1\rangle\langle 0|)$

$$C_{NOT} : |a, b\rangle \longrightarrow |a, a \oplus b\rangle$$

e.g. Let $|a\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$

$|b\rangle = |0\rangle$

$|ab\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle$ → Product state

$CNOT(|ab\rangle) = \frac{CNOT(|00\rangle) + CNOT(|10\rangle)}{\sqrt{2}}$

$= \frac{|0\rangle|0\rangle + |1\rangle|1\rangle}{\sqrt{2}}$ → Entangled state

— (2)

Note:- Output of CNOT may not be product state even if input is in product state

Q Write the column vector corresponding to the mixed input state in the previous eg. & act with the matrix representation of CNOT to find the output in (2)

Ans Let $|a\rangle = a_0|0\rangle + a_1|1\rangle$

$|b\rangle = b_0|0\rangle + b_1|1\rangle$

What is $CNOT:|ab\rangle = ?$

Q What is C_{NOT}^{+} ?

$$C^{+}_{not} = [|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X]^{+}$$

$$= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

$$= C_{NOT}$$

Q Is C_{NOT} unitary?

Or,

Is $C_{NOT} \cdot C^{+}_{NOT} = C_{NOT} \cdot C_{NOT} = I$?

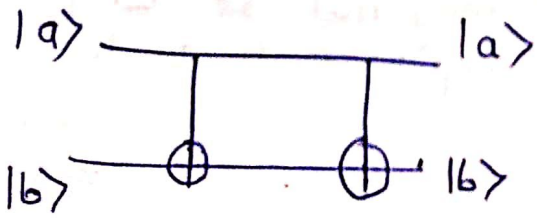
Ans $C_{NOT}\, C_{NOT} = [|0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X]^2$

$$= |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes I$$

$$= (|0\rangle\langle 0| + |1\rangle\langle 1|) \otimes I$$

$$= I^{(1)} \otimes I^{(0)}$$

↓ least significant bit

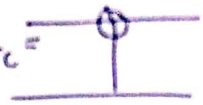


* C_{NOT} with control & target qubits interchanged.

C_{CT} → for conventional C_{NOT}

C_{TC} → for inverted C_{NOT}

C_{CT} = 

C_{TC} = 

Representation of C_{TC} →

outer product representation = $I \otimes |0\rangle\langle 0| + X \otimes |1\rangle\langle 1|$

Check that: $C_{TC} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$

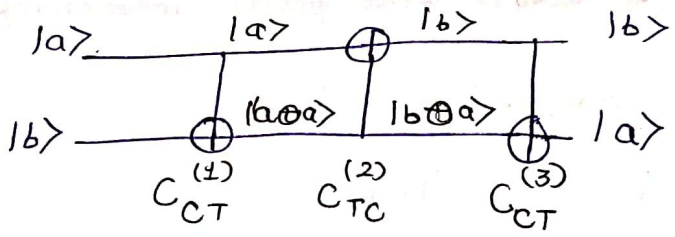
* Cross-over or Swap gate :-

$|ab\rangle \xrightarrow{\text{swap}} |ba\rangle$

Matrix rep. ⇒ $\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

Note:-

* Swap gate can be constructed using 3 CNOTs

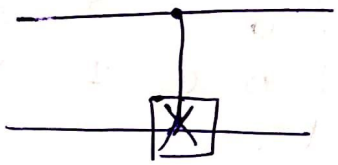


$$C_{CT}^{(3)}\ C_{TC}^{(2)}\ C_{CT}^{(1)}\ |ab\rangle = |ba\rangle$$

Q Check through matrix multiplication:

$$C_{CT}\, C_{TC}\, C_{CT} = \text{Swap}$$

* Generic 2-qubit controlled gate :-

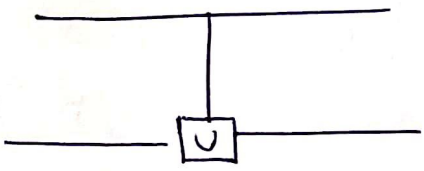


C NOT is controlled X gate

$$C_{NOT} = \begin{pmatrix} I_{2\times2} & 0 \\ 0 & X_{2\times2} \end{pmatrix}$$

(i) Controlled U gate →

All these gates can take product state to entangled state.



This can be represented as-

$$\begin{pmatrix} I_{2\times2} & 0 \\ 0 & U_{2\times2} \end{pmatrix}$$

e.g. Controlled phase shift gate

Here U ~~= phase shift gate~~

$$= \begin{pmatrix} e^{i\theta} & 0 \\ 0 & e^{i\theta} \end{pmatrix} = e^{i\theta} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Note:- This 'U' is not the phase shift gate we defined earlier

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\theta} & 0 \\ 0 & 0 & 0 & e^{i\theta} \end{pmatrix}$$

$\Rightarrow$
$$|00\rangle \longrightarrow |00\rangle$$
$$|01\rangle \longrightarrow |01\rangle$$
$$|10\rangle \longrightarrow e^{i\theta}|10\rangle$$
$$|11\rangle \longrightarrow e^{i\theta}|11\rangle$$

→ If I/P is $\frac{|00\rangle + |11\rangle}{\sqrt{2}}$, say, then O/P is $\frac{|00\rangle + e^{i\theta}|11\rangle}{\sqrt{2}}$ which is very different from i/p

→ Even though single q-bit (global) phase shift is trivial operator, controlled phase shift is non-trivial.

Note:- Notion of control qubit is basis dependent

↓

Why? (see below example)

Q Verify that the action of C_{NOT} on the Hadamard basis is as below :-

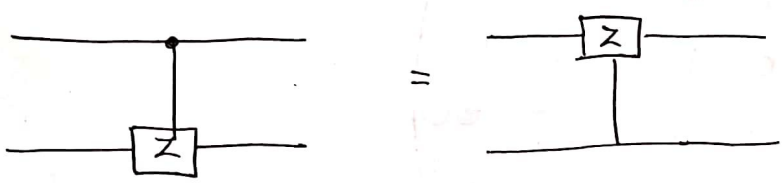
C_{NOT} : $|++\rangle \longrightarrow |++\rangle$

$|+-\rangle \rightarrow |--\rangle$

$|-+\rangle \rightarrow |-+\rangle$

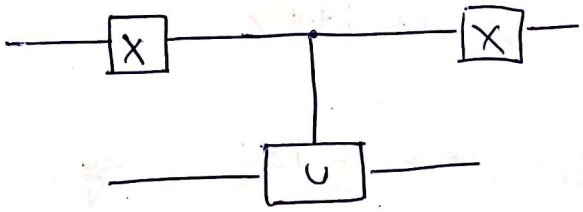
$|--\rangle \rightarrow |+-\rangle$

Q Check that



i.e. $C_{CT}^{Z} = C_{TC}^{Z}$

* Controlled U op. with $|0\rangle$ on the control line



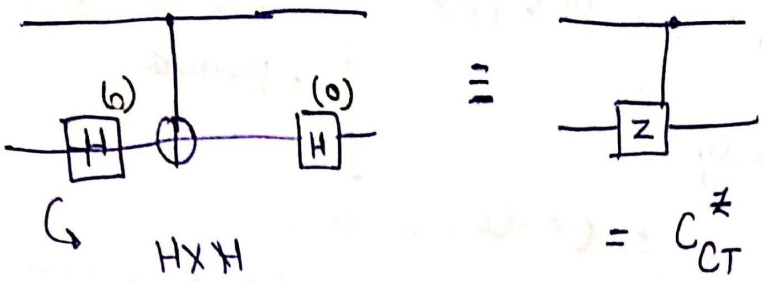
* Converting C_{CT} to C_{TC} using Hadamard gate :-

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

$$H^2 = \mathbb{1}$$

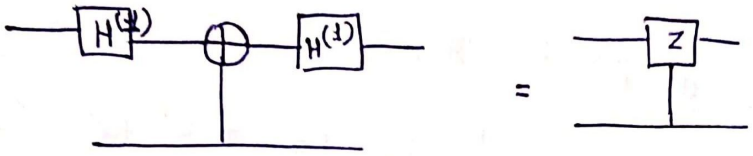
And, $HXH = Z$, $HZH = X$

Also, $C_{CT}^{Z} = C_{TC}^{Z}$



↳ H⊗H

$= C_{CT}^{\neq}$



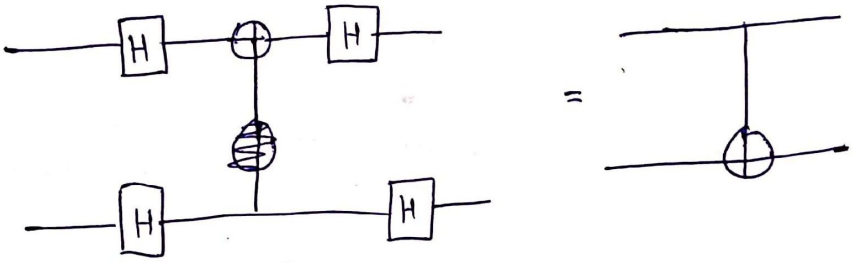
$= C_{TC}^{\neq}$

$$\Rightarrow H^{(0)} C_{CT} H^{(0)} = H^{(1)} C_{TC} H^{(1)}$$

$$\Rightarrow H^{(1)} H^{(0)} C_{CT} H^{(0)} H^{(1)} = C_{TC}$$

{Multiplying $H^{(1)}(\ )H^{(1)}$ on both sides}

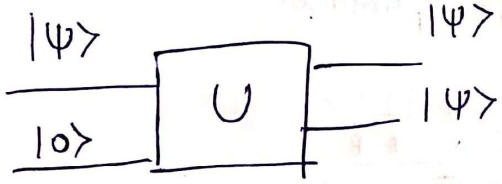
$\Rightarrow$



* No cloning Theorem :-

Linearity of quantum systems ⇒ One can not create a copy of a Qbit in an unknown state.

Let



$\Rightarrow U|\psi\rangle|0\rangle = |\psi\rangle|\psi\rangle$ } Assumed

& similarly

$U|\chi\rangle|0\rangle = |\chi\rangle|\chi\rangle$

we know, linear superposition of two states is also state.

$$|\lambda\rangle = a|\psi\rangle + b|\chi\rangle$$

$$\Rightarrow U(|\lambda\rangle|0\rangle) = U[a|\psi\rangle|0\rangle + b|\chi\rangle|0\rangle]$$

$$RHS = a|\psi\rangle|\psi\rangle + b|\chi\rangle|\chi\rangle \quad \text{— (1)}$$

$$LHS = |\lambda\rangle|\lambda\rangle$$

$$= a^2|\psi\rangle|\psi\rangle + ab|\psi\rangle|\chi\rangle + ba|\chi\rangle|\psi\rangle + b^2|\chi\rangle|\chi\rangle \quad \text{— (2)}$$

It is clear that (1) = (2) only if one of a & b is zero & other is one.

⇓

even then we obtain $|\psi\rangle, |\chi\rangle$ which we assumed to be able to have their clones.

* Applications of multiple-qubit system :-

(i) Quantum Key distribution :-
(using quantum entanglement)

Eckert's protocol

$$|\psi\rangle = \frac{|00\rangle_{AB} + |11\rangle_{AB}}{\sqrt{2}}$$

Info of first qubit is with Alice & second qubit info is with Bob.

Alice chooses randomly b/w the computational basis ($|0\rangle, |1\rangle$) & the Hadomard basis ($|+\rangle, |-\rangle$) to make measurements on the qubit with her.

→ If Alice chooses 'C' basis, result would be either $|0\rangle$ or $|1\rangle$

Suppose it is $|0\rangle$ ⇒ entanglement state $|\psi\rangle$ becomes $|0_A 0_B\rangle$

→ If Bob now chooses the 'C' basis then with certainity he gets result $|0\rangle$

→ If however, B chooses the H basis to make measurement

$$|0_A\rangle \left(\frac{|+\rangle + |-\rangle}{\sqrt{2}} \right)$$

⇒ 50% chances of measuring $|+\rangle$
50% " $|-\rangle$

Possible encoding

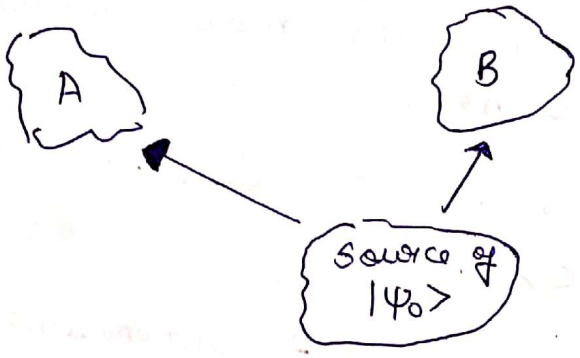
$1 \rightarrow |0\rangle$ or $|+\rangle$

$0 \rightarrow |1\rangle$ or $|-\rangle$

* Rest part is same as BB-84 protocol we studied earlier

(ii) Dense coding :-

$$|\psi_0\rangle = \frac{|0_A\, 0_B\rangle + |1_A\, 1_B\rangle}{\sqrt{2}}$$



Alice wants to transmit 2 bits words of info by sending only 1 qubit to Bob

$$Q_A \otimes I_B$$

$$I_A \otimes Q_B$$

	Values to be xmitted	Xformation applied by A	New state
00	0	$I_A \otimes I_B$	$\frac{\|0_A 0_B\rangle + \|1_A 1_B\rangle}{\sqrt{2}}$
01	1	$X_A \otimes I_B$	$\frac{\|1_A 0_B\rangle + \|0_A 1_B\rangle}{\sqrt{2}}$
10	2	$Z_A \otimes I_B$	$\frac{\|0_A 0_B\rangle - \|1_A 1_B\rangle}{\sqrt{2}}$
11	3	$Y_A \otimes I_B$	$\frac{i}{\sqrt{2}}[\|1_A 0_B\rangle - \|0_A 1_B\rangle]$

A now transmits her qubit to B who now has both the qubits.

Since he now has both the qubits, he can apply product space gate like CNOT

At his end, B, applies the Cnot gate to the entangled pair using A's qubits as control qubit

New state $\xrightarrow{CNOT}$

$$\frac{|0_A 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}} \rightarrow \frac{(|0_A\rangle + |1_A\rangle)\,|0_B\rangle}{\sqrt{2}}$$

$$\rightarrow (|1_A\rangle + |0_A\rangle)\,|1_B\rangle$$

$$\rightarrow \frac{(|0_A\rangle - |1_A\rangle)\,|0_B\rangle}{\sqrt{2}}$$

$$\rightarrow \frac{i}{\sqrt{2}}\,[|1_A\rangle - |0_A\rangle]\,|1_B\rangle$$

each state is now a product state

State of qubits after application of CNOT gate is -

$|+\rangle_A\,|0\rangle_B \xrightarrow{H\otimes I} |0\rangle|0\rangle$

$|+\rangle_A\,|1\rangle_B \xrightarrow{H\otimes I} |0\rangle|1\rangle$

$|-\rangle_A\,|0\rangle_B \xrightarrow{H\otimes I} |1\rangle|0\rangle$

$-i|-\rangle_A\,|1\rangle_B \xrightarrow{H\otimes I} i|1\rangle|1\rangle$

2 bits of info transfered by Alice just sharing her bit.

(iii) Quantum Teleportation :- By sending only a finite no. of bits, the unknown state of a qubit can be communicated.

$$|\phi_0\rangle_A = a|0\rangle_A + b|1\rangle_{BA}$$

$$|\psi_0\rangle_B = \frac{|0_A\, 0_B\rangle + |1_A\, 1_B\rangle}{\sqrt{2}}$$

$$|\phi\rangle_A \otimes |\psi_0\rangle = (a|0\rangle_A + b|1\rangle_A) \otimes \left(\frac{|0_A\, 0_B\rangle + |1_A 1_B\rangle}{\sqrt{2}}\right)$$

$$= \frac{a}{\sqrt{2}} |0_A\, 0_A\rangle |0_B\rangle + \frac{a}{\sqrt{2}} |0_A 1_A\rangle |1\rangle_B$$

$$+ \frac{b}{\sqrt{2}} |1_A\, 0_A\rangle |0_B\rangle + \frac{b}{2} |1_A\, 1_A\rangle |1\rangle_B$$

→ Quantum teleportation is in a sense opposite of dense coding. Alice starts by applying $C_{not} \otimes I_B$ (since she has info of two bits now) followed by $H_A \otimes I_A \otimes I_B$ to the qubits with her.

$$(C_{not} \otimes I_B)(|\phi_A\rangle_A \otimes |\psi_0\rangle)$$

$$= \frac{a}{\sqrt{2}} |0_A\, 0_A\, 0_B\rangle + \frac{a}{\sqrt{2}} |0_A\, 1_A\, 1_B\rangle$$

$$+ \frac{b}{\sqrt{2}} |1_A\, 1_A\, 0_B\rangle + \frac{b}{\sqrt{2}} |1_A\, 0_A\, 1_B\rangle$$

$$H \otimes I \otimes I \,(C_{NOT} \otimes I_B)\,(|\phi_A\rangle \otimes |\psi_0\rangle)$$

$$= \frac{1}{2}\Big[|0_A 0_A\rangle (a|0_B\rangle + b|1_B\rangle)$$
$$+ |0_A 1_A\rangle (a|1\rangle_B + b|0\rangle_B)$$
$$+ |1_A 0_A\rangle (a|0\rangle_B - b|1\rangle_B)$$
$$+ |1_A 1_A\rangle (a|1\rangle_B - b|0\rangle_B)\Big]$$

Note Bob now has info regarding $|\phi\rangle$

Alice now ~~measures~~ makes measurement on her qubits using computational basis & sends the result (0, 1, 2 or 3) to B over classical channels

$0 \rightarrow I$
$1 \rightarrow X$
$2 \rightarrow Z$
$3 \rightarrow Y$

Q Will dense coding of teleportation work with the entangled state $\frac{|0 1\rangle + |1 0\rangle}{\sqrt{2}}$ instead of $\frac{|0 0\rangle + |1 1\rangle}{\sqrt{2}}$? If yes, complete the analysis. If no, why ?

Ans Answer is 'yes'

Q How would error correction happen if cloning of bit is not possible?

Quiz 2 :
23rd Oct, 2019
& Wednesday ?
4:00 - 4:45 PM

* Multi-qubit measurement & generalized Born rule →

For single qubit system →

$$|\psi\rangle = a|0\rangle + b|1\rangle$$

Probability: $|a|^2$ $|b|^2$ → Born rule

In multiple qubit system

$$|\Psi\rangle_n = \sum_{x=1}^{2^n-1} |\alpha_x|^2 |x\rangle_n$$

$$|\Psi\rangle_n \xrightarrow{\text{Measure}} |\alpha_x|^2 \rightarrow \text{Probability of } |x\rangle_n$$

So, In 2-qubit system

Let $|\Psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$

Respective probabilities of	$\|a_{00}\|^2$	$\|a_{01}\|^2$	$\|a_{10}\|^2$	$\|a_{11}\|^2$
	$\|00\rangle$	$\|01\rangle$	$\|10\rangle$	$\|11\rangle$

In normalized state → $\sum_{x=0}^{2^n-1} |\alpha_x|^2 = 1$

Q Let $|\Psi\rangle = 2|00\rangle + 3|01\rangle + |10\rangle$ be a 2-qubit state. Is it normalized? If not, what is the corresponding normalized state? With what probability is $|\Psi\rangle$ measured to be in $|00\rangle$, $|10\rangle$ & $|01\rangle$?

→ If one of the qubits is measured w.r.t. the Hadamard basis & the other w.r.t. the computational basis.

then-

$$|\Psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

↓

use $$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}$$

$$|1\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}}$$

to express $|\Psi\rangle$ as-

$$|\Psi\rangle = a_{+0}|+0\rangle + a_{+1}|+1\rangle + a_{-0}|-0\rangle + a_{-1}|-1\rangle$$

→ More interesting is the case where we make measurement only on one of the qubits of multiple-qubit system.

$$|\Psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

We want to make measurement only on the left qubit, say -

$$|\Psi\rangle = |0\rangle\left(a_{00}|0\rangle + a_{01}|1\rangle\right) + |1\rangle\left(a_{10}|0\rangle + a_{11}|1\rangle\right)$$

$$|\Psi\rangle = \underbrace{\sqrt{|a_{00}|^2 + |a_{01}|^2}}_{\alpha_0}\ |0\rangle\ \frac{\left(a_{00}|0\rangle + a_{01}|1\rangle\right)}{\sqrt{|a_{00}|^2 + |a_{01}|^2}}$$

$$+ \underbrace{\sqrt{|a_{10}|^2 + |a_{11}|^2}}_{\alpha_1}\ |1\rangle\ \frac{\left(a_{10}|0\rangle + a_{11}|1\rangle\right)}{\sqrt{|a_{10}|^2 + |a_{11}|^2}}$$

$$\Rightarrow |\Psi\rangle = \alpha_0|0\rangle|\phi_0\rangle + \alpha_1|1\rangle|\phi_1\rangle$$

where, $\alpha_i = \sqrt{|a_{i0}|^2 + |a_{i1}|^2}$

$$|\phi_i\rangle = \frac{1}{\alpha_i}(a_{i0}|0\rangle + a_{i1}|1\rangle)$$

$\Rightarrow$ 1 st qubit measured in state $|0\rangle$ with probability $|\alpha_0|^2$ & the state of 2 qubits immediately after measurement is $|0\rangle|\phi_0\rangle$

Similarly, $|\alpha_1|^2$ is the probability of measuring $|1\rangle$ & state of 2 qubits after measurement is $|1\rangle|\phi_1\rangle$

→ For multiple qubits (let's say 5)
if we want to measure just 2nd qubit

$$a|\underset{4}{0}\ \underset{3}{1}\ \underset{2}{0}\ \underset{1}{0}\ \underset{0}{1}\rangle + b|\underset{4}{1}\ \underset{3}{0}\ \underset{2}{0}\ \underset{1}{0}\ \underset{0}{1}\rangle$$

$$\Rightarrow |\underset{2}{0}\rangle\left(a|\underset{4}{0}\ \underset{3}{1}\ \underset{1}{0}\ \underset{0}{1}\rangle + b|\underset{4}{1}\ \underset{3}{0}\ \underset{1}{0}\ \underset{0}{1}\rangle\right)$$

Q) For the 2-qubit state:

$$|\Psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$$

Find the probability for measuring $|10\rangle$.

Q) For the above state we measure the left qubit in the Hadamard basis with what probability does the measurement result in $|+\rangle$ state & what is the state of the 2-qubit system immediately after measurement?

* State preparation :-

$|0000\ldots00\rangle_n$

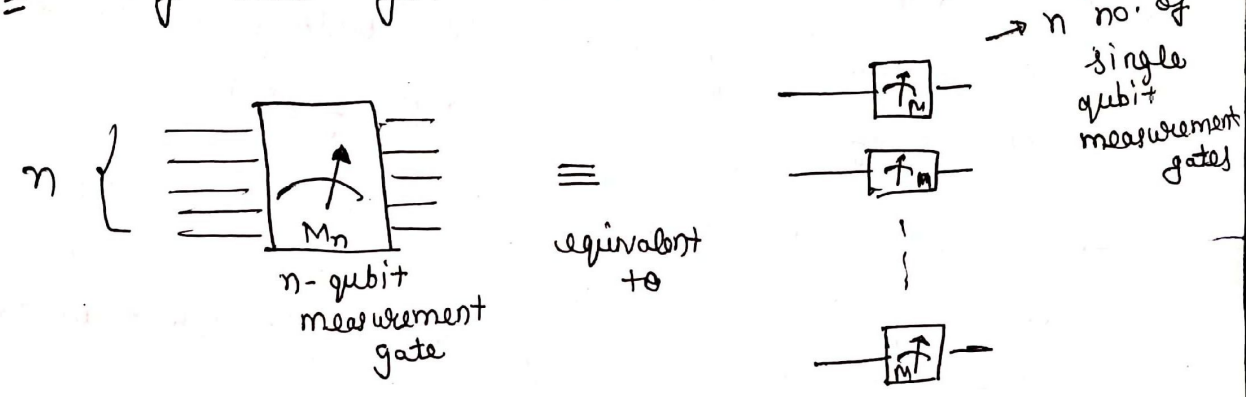
How to obtain above state?

Mathematically, or Theoretically → Apply measurement gate (for each photons)
↳ if it measures $|1\rangle$ apply 'not' X gate (not gate)

E=1 ——— 1st excited state
} ΔE
E=0 ——— Ground state

when $\Delta E > K_B T$ ↳ Temp.
↳ All the e^- → In ground state

Q Using the generalized Born Rule show that :



* Use of single Qbit unitaries & the Cnot in constructing 1 & 2-qubit states :-

1-qubit case is simple. If $|0\rangle$ is the starting state, then for an appropriate unitary U we have -

$U|0\rangle = |\psi\rangle$, where $|\psi\rangle$ is the desired state (arbitary)
$= a|0\rangle + b|1\rangle$

$U|1\rangle = |\phi\rangle$

∵ U is Unitary & $|0\rangle$ & $|1\rangle$ are orthogonal.

∴ $|\phi\rangle$ & $|\psi\rangle$ are orthogonal.

How to prepare arbitrary 2-qubit state :

$|\psi\rangle = a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle$

starting with the state $|00\rangle$ & using only single qubit unitaries & C-not gate?

→ $|\psi\rangle = |0\rangle \otimes |\chi\rangle + |1\rangle \otimes |\phi\rangle$

where $|\chi\rangle = a_{00}|0\rangle + a_{01}|1\rangle$

$|\phi\rangle = a_{10}|0\rangle + a_{11}|1\rangle$

} not orthogonal in general

∴ Our aim is to make the state appearing in the position of $|\chi\rangle$ & $|\phi\rangle$ orthogonal to each other (if they are not already so)

→ we will do this by using a single qubit unitary & we first need to know what is the general state of a single Qbit unitary.

$$U = \begin{pmatrix} A & -B^* \\ B & A^* \end{pmatrix}$$ → This is generic form of single qubit unitary with $|A|^2 + |B|^2 = 1$

$$U^\dagger = \begin{pmatrix} A^* & B^* \\ -B & A \end{pmatrix}$$

$$UU^\dagger = I$$

Going reverse,

Let $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be unitary

$$\Rightarrow UU^\dagger = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a^* & c^* \\ b^* & d^* \end{pmatrix}$$

$$= \begin{pmatrix} |a|^2+|b|^2 & ac^* + bd^* \\ a^*c + b^*d & |c|^2+|d|^2 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

↓ For U to be unitary operator

$\Rightarrow |a|^2 = |d|^2 \Rightarrow$ ~~$a = d e^{i\alpha}$~~

$\& \; |b|^2 = |c|^2$

Why do we want to have $|\chi\rangle$ & $|\phi\rangle$ orthogonal?

Because when they are orthogonal

$\hat{T}|\phi\rangle = |a\rangle$ } both orthogonals

Same gate needed $\hat{T}|\chi\rangle = |b\rangle$ }

But when they are not orthogonal? Two separate gates will give orthogonal vectors.

We know, $|a|^2 = |d|^2$ if $a \rightarrow$ real (assuming)

$d = a e^{i\alpha}$ — (1)

& ~~$ac^* + bd$~~

$ac^* + bd^* = a^* c + b^* d = 0$

$\Rightarrow c = -\frac{b^* d}{a^*}$ ($a \rightarrow$ real)

$$\therefore U = \begin{pmatrix} a & b \\ -b^* e^{i\alpha} & a e^{i\alpha} \end{pmatrix} = e^{i\frac{\alpha}{2}} \begin{pmatrix} a e^{-i\frac{\alpha}{2}} & b e^{-i\alpha/2} \\ -b^* e^{i\alpha/2} & a e^{i\alpha/2} \end{pmatrix}$$

$$= e^{i\alpha/2} \begin{pmatrix} A & -B^* \\ B & A^* \end{pmatrix}$$ — H.P.

& $|A|^2 + |B|^2 = 1$

Quantum Computation & quantum Information (3rd part)

We Know,

Special unitary → $U = \begin{pmatrix} a & -b^* \\ b & a^* \end{pmatrix}$

$$U|0\rangle = \begin{pmatrix} a & -b^* \\ b & a^* \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = a|0\rangle + b|1\rangle$$

$$U|1\rangle = \begin{pmatrix} a & -b^* \\ b & a^* \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -b^* \\ a^* \end{pmatrix} = -b^*|0\rangle + a^*|1\rangle$$

$$\hat{U} \otimes \mathbb{I}_0 |\Psi\rangle = (a|0\rangle + b|1\rangle)|\chi\rangle + (-b^*|0\rangle + a^*|1\rangle)|\phi\rangle$$

$$= |0\rangle|\chi'\rangle + |1\rangle|\phi'\rangle$$

where,

$$|\chi'\rangle = a|\chi\rangle - b^*|\phi\rangle$$

$$|\phi'\rangle = b|\chi\rangle + a^*|\phi\rangle$$

& we want $\langle \phi'|\chi'\rangle = 0$

$$\Rightarrow b^* a\langle\chi|\chi\rangle - b^{*2}\langle\chi|\phi\rangle + a^2\langle\phi|\chi\rangle - a b^*\langle\phi|\phi\rangle = 0$$

L.H.S. is a quadratic in $\frac{a}{b^*}$ which along with $|a|^2 + |b|^2 = 1$ fixes a & b.

↳ [a & b → for a particular $\hat{U}_1$ which makes $|\phi'\rangle$ & $|\chi'\rangle$ orthogonal]

Again

$\hat{u}_1 \otimes \mathbb{I}_0 |\Psi\rangle = |0\rangle|x'\rangle + |1\rangle|\phi'\rangle$

& $\langle\phi'|x'\rangle = 0$

$\therefore$ $|\phi'\rangle$ & $|x'\rangle$ are not normalized, we can normalize them.

$$|x''\rangle = \frac{|x'\rangle}{\lambda}$$

$$|\phi''\rangle = \frac{|\phi'\rangle}{\mu}$$

$$\hat{u}_1 \otimes \mathbb{I}_0 |\Psi\rangle = \lambda|0\rangle|x''\rangle + \mu|1\rangle|\phi''\rangle$$

$$\Rightarrow |\Psi\rangle = \hat{u}_1^{+} \left[\lambda|0\rangle|x''\rangle + \mu|1\rangle|\phi''\rangle\right]$$

$|x''\rangle$ & $|\phi''\rangle \rightarrow$ orthogonal

$\therefore$ $\hat{v}_0|0\rangle = |x''\rangle$

$\hat{v}_0|1\rangle = |\phi''\rangle$

$$= \hat{u}_1^{+} \otimes \hat{v}_0 \left[\lambda|0\rangle|0\rangle + \mu|1\rangle|1\rangle\right]$$

$$= \hat{u}_1^{+} \otimes \hat{v}_0 \, C_{CT} \left[\lambda|0\rangle + \mu|1\rangle\right]|0\rangle$$

↳ Single qubit system

$$= \hat{u}_1^{+} \hat{v}_0 \, C_{CT} \, \hat{\omega}_1 |00\rangle$$

* Universal Quantum gates :-

(i) A unitary operator on a d-dimension vector space can be decomposed into a product of unitary operator acting on 2-dimension subspace

i.e. if $U \rightarrow$ $d \times d$ unitary matrix,
then we can express U as a product of unitary matrices which act only on 2 dimension sub spaces

$\therefore$ have only 4 non-trivial entries

e.g. $U = \begin{pmatrix} a & d & g \\ b & e & h \\ c & f & i \end{pmatrix}$

Aim is to find unitary matrices $U_1, U_2 \&$ U_3 such that -

$$U_3 U_2 U_1 U = \mathbb{1}$$

$$\Rightarrow U = U_1^{+} U_2^{+} U_3^{+}$$

where each U_i acts non-trivially only on a 2-d sub space. (2-level matrix) (unitaries)

e.g. $\begin{pmatrix} 1 & 0 & 0 \\ 0 & x & z \\ 0 & y & w \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}$

2-level unitary matrix $\rightarrow$ affects only $Y \& Z$.

Choose $U_1 = \begin{pmatrix} A & -B^{*} & 0 \\ B & A^{*} & 0 \\ 0 & 0 & 1 \end{pmatrix} \rightarrow$ 2-level unitary

$|A|^2 + |B|^2 = 1$

$$\Rightarrow U_1 U = \begin{pmatrix} Aa - B^{*}b & Ad - B^{*}e & Ag - B^{*}h \\ Ba + A^{*}b & Bd + A^{*}e & Bg + A^{*}h \\ c & f & i \end{pmatrix}$$

$$Ba + A^* b = 0 \Rightarrow B = \frac{-A^* b}{a}$$

$$U_2 = \begin{pmatrix} A' & 0 & -C^* \\ 0 & 1 & 0 \\ C' & 0 & A'^* \end{pmatrix} \qquad |A|^2 + |C|^2 = 1$$

↓

A', C' can be determined by imposing condition

$$U_2 U_1 U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & g'' \end{pmatrix}$$

↓

This has to be true for calculation of A' & C' in above case

$$\Rightarrow U_3 = (U_2 U_1 U)^+$$

$\therefore$ All U_i's are 2-level matrices

$$(d-1) + (d-2) + \cdots 1 = \frac{d(d-1)}{2}$$

$$= {}^{d}C_2 \geq K$$

is the max. no. of 2-level matrices such that (for 'd' dimension unitary)

$$U = U_1^+ U_2^+ U_3^+ \cdots U_K^+$$

Note:- n-qubit system $\longrightarrow 2^n$ dimension

$$\therefore d = 2^n$$

So, $k \leq \frac{2^n(2^n-1)}{2} = 2^{n-1}(2^n-1)$

We have seen,

$U_{dxd} = U_1^+ U_2^+ \cdots\cdots U_k^+$

$U_i \rightarrow$ 2-level unitary

Now the question comes....

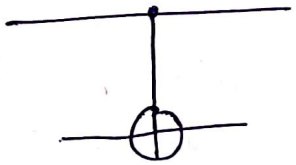
Q How to implement a 2-level unitary?

Ans A 2-level unitary can be implemented using multiply controlled NOT & multiply controlled single qubit unitary

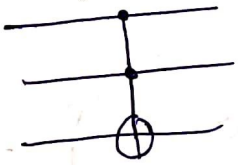
Make-up class:
Nov-1 (Friday)
1:30 PM - 3:00 PM

Quiz - 2:
Nov-2 (Sat)
11:00 AM - 11:45 AM

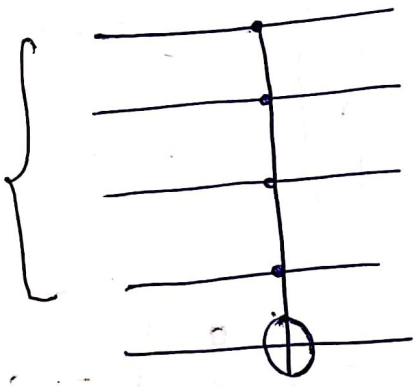
Multiply controlled NOT → A generalization of CNOT & CCNOT.



CNOT



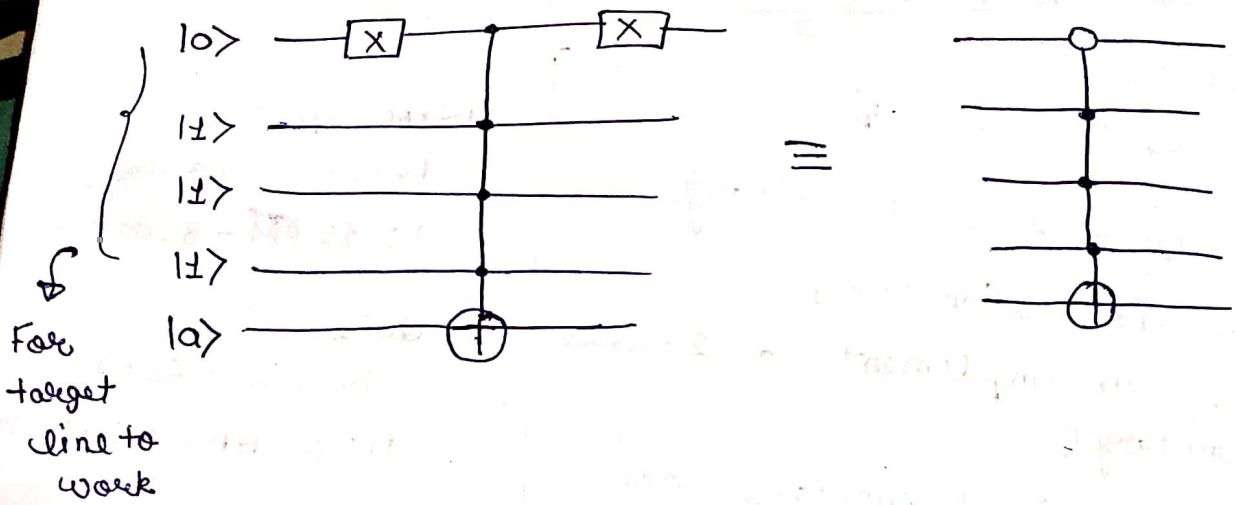
CCNOT



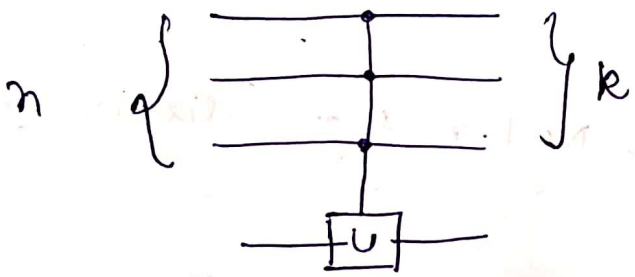
(n-1) qubits

→ generalized version (multiply controlled NOT)

We will want to activate the multiply controlled NOT when some of the control lines are in state $|0\rangle$



So, Multiply controlled Unitary looks like -



$\tilde{U}_2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ → 2-level unitary acting on single qubit

$U_4 = \begin{pmatrix} a & 0 & 0 & b \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ c & 0 & 0 & d \end{pmatrix}$ → 2-level unitary acting on 2-qubits.

$U(|00\rangle) = U\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ 0 \\ 0 \\ c \end{pmatrix} = a|00\rangle + c|11\rangle$

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

Similarly,

$U(|10\rangle) = |10\rangle$

& $U(|11\rangle) = b|00\rangle + d|11\rangle$

2-level unitary U connects $|00\rangle$ & $|11\rangle$ here.

e.g. $|s\rangle = |101001\rangle$, $|t\rangle = |110011\rangle$ Suppose our 2-level unitary connects only $|s\rangle$ & $|t\rangle$

First construct gray code →

$|s\rangle = |101001\rangle$
→ $|101011\rangle$
→ $|100011\rangle$
$|t\rangle \rightarrow |110011\rangle$

} gray code

⇒ Consider a 3-qubit system & a particular 2-level unitary.

$$U_2 = \begin{pmatrix} a & 0 & \cdots & 0 & c \\ 0 & 1 & & & 0 \\ 0 & & \ddots & & \\ 0 & & & 1 & \\ b & 0 & \cdots & & d \end{pmatrix}$$

$$\tilde{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \begin{pmatrix}a\\b\end{pmatrix} = a|0\rangle + b|1\rangle$$

Suppose $|000\rangle$ & $|111\rangle$ are the states connected by U_2.

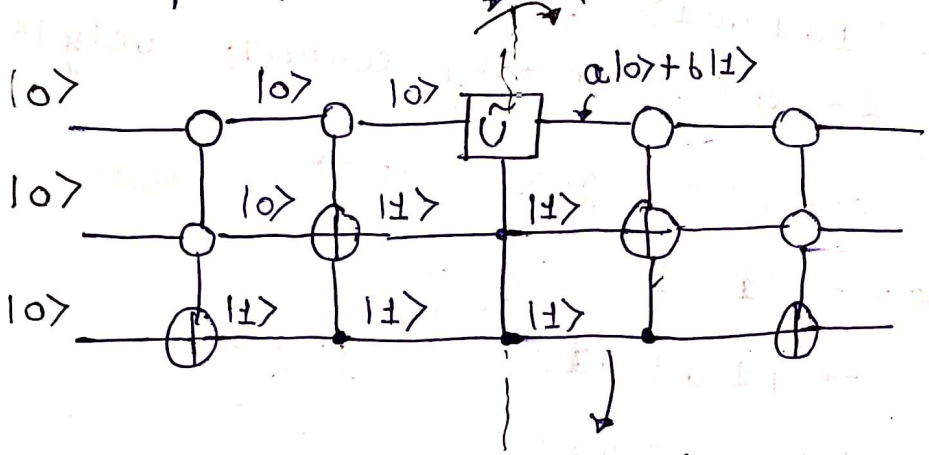
$|000\rangle$

$|001\rangle$

$|010\rangle$

$|011\rangle$

To implement this → mirror image



At this stage

$$(a|0\rangle + b|1\rangle)|1\rangle|1\rangle$$

$$= a|0\rangle|1\rangle|1\rangle + b|1\rangle|1\rangle|1\rangle$$

$$\hookrightarrow a|0\rangle|0\rangle|1\rangle + b|1\rangle|1\rangle|1\rangle$$

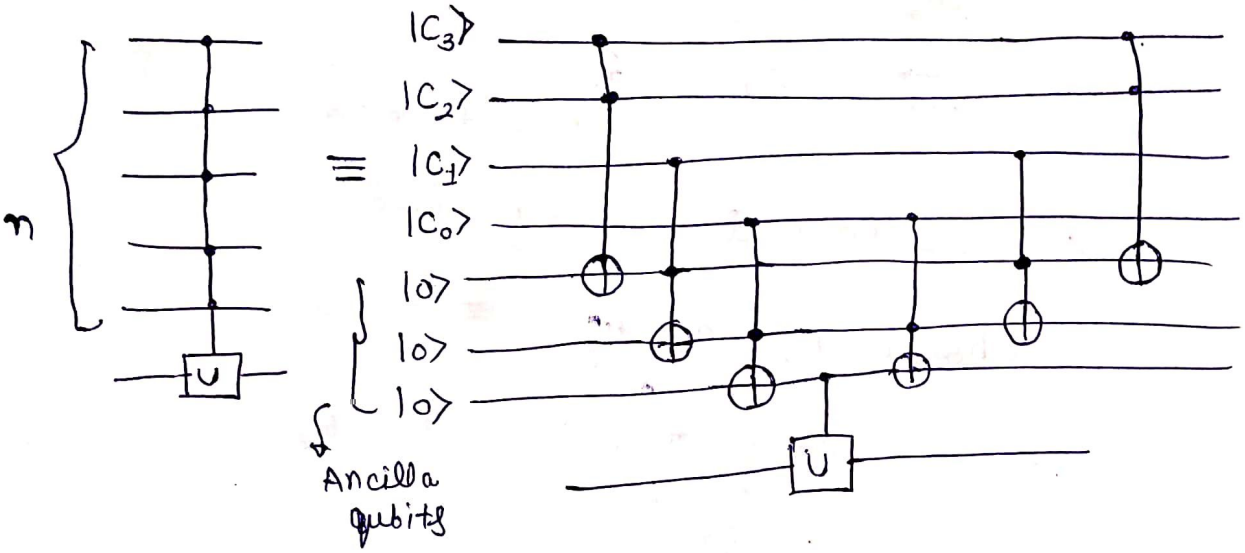
$$\hookrightarrow a|000\rangle + b|111\rangle$$

* In general, for a n-qubit system a 2-level unitary will be implemented (in the worst case) by (n-1) qubit controlled NOTs & on the input side we will require (n-1) of these (n-1) qubit controlled NOT.

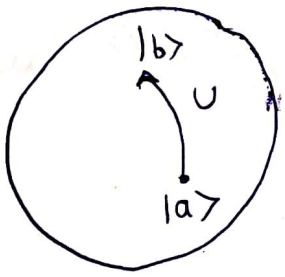
Similarly (n-1) controlled NOTs on the output side ⇒ total of 2(n-1) NOTs controlled by (n-1) qbits of 1 single qubit unitary controlled by (n-1) qubits.

→ A multiply controlled unitary can be constructed using CC NOTs.

* n- Qbit controlled NOT constructed using 2(n-1) CCNOTs & (n-1) work qubits (Ancillas) :-



* Implementing single qubit unitaries :-



Single qubit unitary

$$U = \begin{pmatrix} a & -b^* \\ b & a^* \end{pmatrix}$$

$$a_R^2 + a_I^2 + b_R^2 + b_I^2 = 1 \quad \Rightarrow \quad \begin{pmatrix} a_R + i a_I & -b_R + i b_I \\ b_R + i b_I & a_R - i a_I \end{pmatrix}$$

$$U = a_R I + i a_I Z + i b_I X + i b_R Y$$

Let $X = \sigma_x$, $Y = \sigma_y$, $Z = \sigma_z$

Renaming $a_R, a_I, \ldots$ etc.

$$U = u_0 I + u_x i\sigma_x + i u_y \sigma_y + i u_z \sigma_z$$

$$= u_0 I + i \vec{u} \cdot \vec{\sigma}$$

with $u_0^2 + u_x^2 + u_y^2 + u_z^2 = 1$

We choose,

$$u_0 = \cos\frac{\gamma}{2} \qquad \hat{n} \equiv (n_x, n_y, n_z)$$

$$\vec{u} = \sin\left(\frac{\gamma}{2}\right) \hat{n} \quad \hookrightarrow \text{unit vector}$$

$$\therefore U = \cos\frac{\gamma}{2} I + i \sin\frac{\gamma}{2} \hat{n} \cdot \vec{\sigma}$$

Choose $n_x = 0 = n_y$, $\Rightarrow n_z = 1$

$$\Rightarrow U = \cos\frac{\gamma}{2} I + i \sin\frac{\gamma}{2} \sigma_z$$

$$R_z(\gamma) = \begin{pmatrix} e^{i\frac{\gamma}{2}} & 0 \\ 0 & e^{-i\gamma/2} \end{pmatrix}$$

Q Show that $R_z(\gamma) = e^{i\sigma_z \gamma/2}$ using Taylor series expansion.

Similarly, if $n_z = 1$, $n_y = 0 = n_x$,

$$R_x(\gamma) = \begin{pmatrix} \cos\gamma/2 & i\sin\gamma/2 \\ i\sin\gamma/2 & \cos\gamma/2 \end{pmatrix}$$

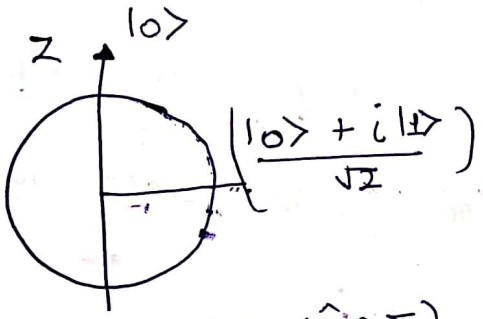
& for $n_y = 1$, $n_x = 0 = n_z$

$$R_y(\gamma) = \begin{pmatrix} \cos\frac{\gamma}{2} & \sin\gamma/2 \\ -\sin\alpha/2 & \cos\gamma/2 \end{pmatrix}$$

Q Show that $e^{i\gamma\sigma_x/2} = R_x(\gamma)$

(in matrix terms) Using power series expansion $e^{i\gamma\sigma_y/2} = R_y(\gamma)$

Q Action of $R_x(\gamma = \pi/2)$ on the state $|0\rangle$.



In general, $U = e^{i\gamma/2\,(\hat{n}\cdot\vec{\sigma})}$ Make Sir Remember to mention it in next class

$\Rightarrow R_{\hat{n}}(\gamma) = e^{i\gamma/2\,(\hat{n}\cdot\vec{\sigma})}$

That corresponds to a rotation by an angle γ about the axis $\hat{n}$ of the Bloch sphere.

$\Rightarrow$ A general single Qbit unitary will be -

$$U = e^{i\alpha\omega} R_n(\gamma)$$

$\omega \rightarrow$ Phase ~~vector~~ angle

Q What are $\alpha, \gamma \& \hat{n}$ for the Hadamard gate

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

→ It is a fact that any rotation by an arbitary $\angle \gamma$ about an arbitary axis $\hat{n}$ can be written as a sequence of 3 rotation. - a rotation about the z-axis followed by a rotation about y-axis followed by a rotation about z axis.

$$R_{\hat{n}}(\gamma) = R_z(\alpha) R_y(\beta) R_z(\delta)$$

where $\alpha, \beta \& \delta$ depend on $\gamma \& \hat{n}$

Q Confirm the last equality

This result ⇒ That for implementing an arbitrary single Qbit unitary we need to consider only rotation about y & z- axis of the Bloch sphere.

~~Implementing singly~~ Cont^d

* Implementing singly controlled qubit unitaries in terms of single Qbit unitaries & CNOT :-

Let A, B, C → single qubit unitary such that -

$$ABC = I$$

An arbitrary single Qbit unitary can be written as -

$$U = e^{i\omega} A X B X C$$

What are A, B & C ?

Choose, $A = R_z(\alpha) R_y(+\beta/2)$

$$B = R_y(-\beta/2)\, R_z\left(-\frac{\delta-\alpha}{2}\right)$$

$$C = R_z\left(\frac{\delta-\alpha}{2}\right)$$

$$ABC = R_z(\alpha)\, R_y\left(-\frac{\beta}{2}+\frac{\beta}{2}\right) R_z\left(-\frac{\delta-\alpha}{2}+\frac{\delta-\alpha}{2}\right)$$

$$= R_z(0)\; R_y(0) = \mathbb{I} \quad \checkmark$$

Now,
To show that - $U = e^{i\omega} AXBXC$

we use the fact that $XY = -YX$

$$\Rightarrow \boxed{XYX = -Y}$$

Q Use the above result to prove

$$X R_y(\theta) X = R_y(-\theta)$$

↳ Similarly, this result holds for R_z

We have,

$$XBX = X R_y(-\beta/2) R_z\left(-\frac{\delta-\alpha}{2}\right) X$$

$$= X R_y(-\beta/2) \underbrace{XX}_{\mathbb{I}} R_z\left(-\frac{\delta-\alpha}{2}\right) X$$

$$= R_y(+\beta/2) R_z\left(\frac{\delta+\alpha}{2}\right)$$

$$A \times B \times C = R_z(\alpha)\, R_y\left(\tfrac{\beta}{2}\right) R_y\left(\tfrac{\beta}{2}\right) R_z\left(\tfrac{\delta+\alpha}{2}\right) R_z\left(\tfrac{\delta-\alpha}{2}\right)$$

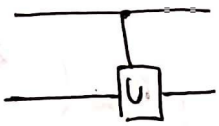
$$= R_z(\alpha)\, R_y(\beta)\, R_z(\delta) = R_n(\gamma)$$

We know,

$$U = e^{i\omega} R_n(\gamma)$$

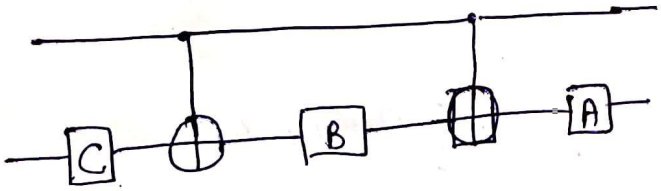
$$\Rightarrow U = e^{i\omega} A \times B \times C$$ — Hence proved

So,



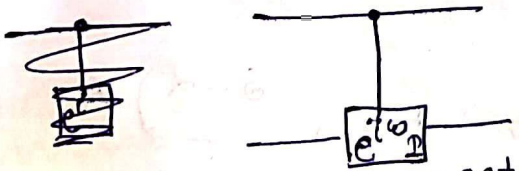
$= ?$

The controlled version of $A \times B \times C$ is -



Next, we need to complete implementing the controlled version of U we need to include the $e^{i\omega}$ factor (as a controlled operation)

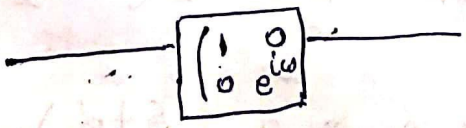
$$e^{i\omega} I = \begin{pmatrix} e^{i\omega} & 0 \\ 0 & e^{i\omega} \end{pmatrix}$$



$\Rightarrow$

$$\begin{cases} |00\rangle \rightarrow |00\rangle \\ |01\rangle \rightarrow |01\rangle \\ |10\rangle \rightarrow e^{i\omega}|10\rangle \\ |11\rangle \rightarrow e^{i\omega}|11\rangle \end{cases}$$

$\equiv$

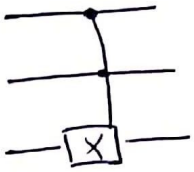


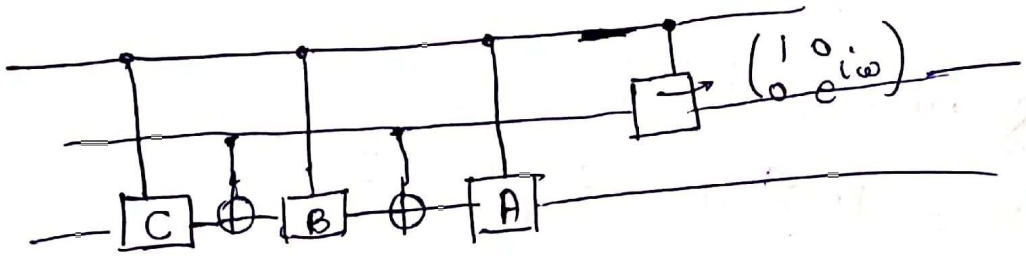
Singly controlled single qubit U requires 4 single Qbit unitaries & 2 CNOTS.

→ The only remaining task is to implement the CCNOT which has 2 control Qbits.

Let us implement

instead of





↳ only when upper two line are $|11\rangle$

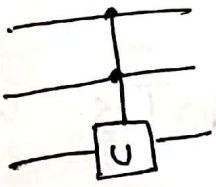
↓

This will act

$U = e^{i\omega} A \times B \times C$

Q. If upper line is in state $|1\rangle$ then $P = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\omega} \end{pmatrix}$ gate is also active.

However, if the middle line is in state $|0\rangle$, it does not matter. Why?

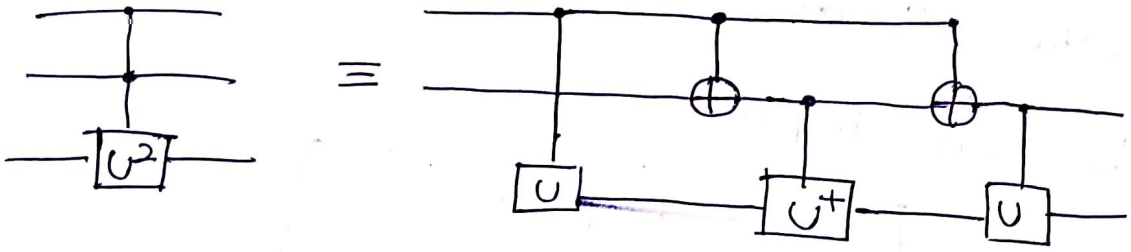
Q. 

requires how many single Qbit unitaries & CNOTS.

16, 10 (How?)

Note:- Not that if U is unitary, then U^2 is also unitary.

Q Check this.



For CCNOT, $U^2 = X$

$\Rightarrow U = \sqrt{X}$

Q What is $\sqrt{X}$?

$X = H Z H$ & $H^2 = I$

$\Rightarrow \sqrt{X} = H\sqrt{Z}\,H$

$\{ \because \sqrt{X}\sqrt{X} = H\sqrt{Z}\,H\,H\sqrt{Z}\,H$

$= H Z H \}$

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

$\therefore \sqrt{X} = H\sqrt{Z}\,H \rightarrow$ Find out?

For n-qubit system

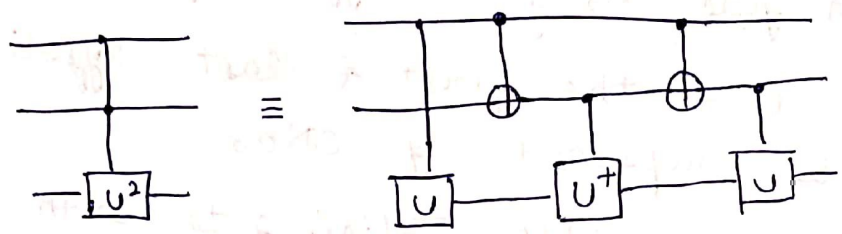
$\Rightarrow U_{2^n \times 2^n}$

2(n-1) Controlled NOTs with (n-1) control qubits

each controlled NOT with (n-1) control

Qbit requires $2(n-2)$ CCNOTs & each CCNOT implemented using $\Theta(c)$ CNOTs & single Qbit unitary.

We saw,



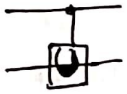
Q How many single Qbit unitaries & how many CNOTs does the above implementation requires.

Ans 8 single Qbit unitaries
& CNOT's

each singly controlled unitary requires 4 single q-bit unitaries for its implementation.

But, In above case
Single qbit unitaries $\neq 3 \times 4$
(why?)

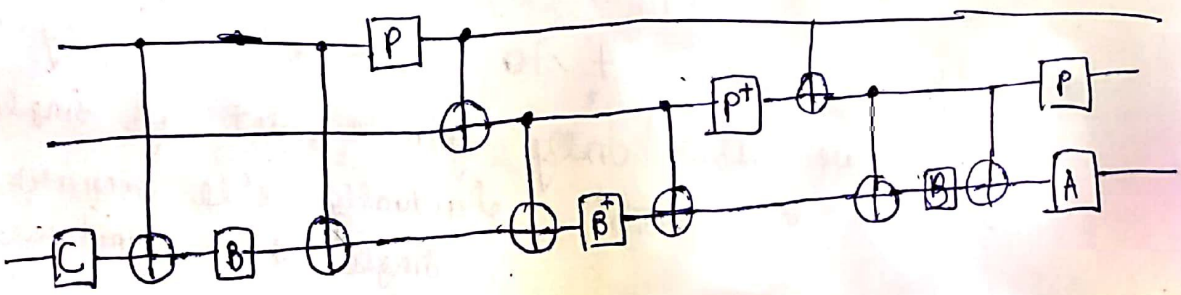
Q Let $C(\overset{U}{\bullet})$ be the notation for the controlled version of U i.e.



$\equiv C(U)$.

Substitute for $C(U)$ & $C(U^\dagger)$ in the previous circuit in terms of A, B, C, P & the CNOT to find the circuit.

Ans



Q Recall the construction of the SWAP gate using CNOT's. Also recall the Fredkin gate is controlled SWAP.

(i) Modify the circuit of SWAP to implement a Fredkin gate using 3 Toffoli gates.

(ii) Check that the first & last Toffoli gates can be replaced by CNOTs.

(iii) Replace the middle Toffoli gate with its circuit in terms of $\sqrt{X}$ & CNOT to obtain Fredkin gate which uses single qubit unitaries & CNOT's.

Q What quantum circuit using Toffoli gates of a single Qbit gate $\hat{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ will implement

$$U = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & a & 0 & 0 & 0 & 0 & c \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & b & 0 & 0 & 0 & 0 & d \end{pmatrix}$$

Assuming that a Toffoli gate can be implemented using 8 CNOT's, find the no. of CNOT's & single Q bit unitaries required.

→ Suppose we want to implement unitary U (arbitrary) And, we use only finite set of single Qbit unitaries & CNOTs (actually we'll require 3 different single Q bit unitaries as we'll see)

then we will not be implementing U but some operation $V \Rightarrow$ There will be an error

Error → quantified $E(U,V) = \max_{|\psi\rangle} \|(U-V)|\psi\rangle\|$

Universal gates :- Hadamard + $\frac{\pi}{8}$ + CNOT + (Phase shift) + Only used for error correction

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

$$T = e^{i\pi/8} \begin{pmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{pmatrix}$$

Upto a global phase, T is a rotation about z-axis of Bloch sphere.

$$R_z(\theta) = \begin{pmatrix} e^{+i\theta/2} & 0 \\ 0 & e^{-i\theta/2} \end{pmatrix}$$

$$\therefore \quad T = e^{i\pi/8} R_z(-\pi/4)$$

Q Check that :-

$$HTH = e^{i\pi/8} R_x(-\pi/4)$$

Earlier we studied that about an arbitrary axis $\hat{n}$

$$R_{\hat{n}}(\theta) = R_z(\alpha) R_y(\beta) R_z(\delta)$$

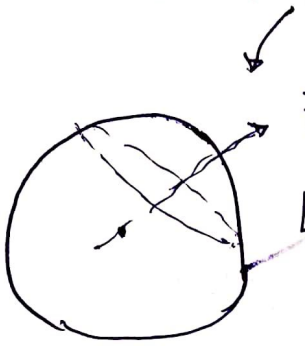
or

$$R_{\hat{n}'}(\theta) = R_z(\alpha') R_z(\beta') R_z(\delta')$$

If α', β', γ' are fixed $\Rightarrow$ n $\rightarrow$ fixed (not arbitrary anymore)

If $\alpha', \beta', \gamma' = \pi/4$

$\frac{2\pi}{\pi/4} = 8 \rightarrow$ In 8 steps you can reach again where you started.

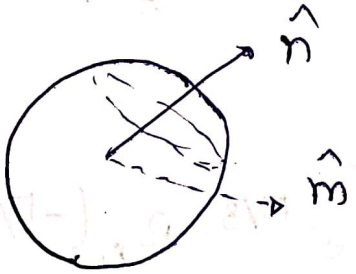


$\Rightarrow$ Rational rotation

But to denote any single qubit on Bloch sphere, we need both rational & irrational rotations.

$$H\, R_{\hat{n}}(\theta)\, H = R_{\hat{m}}(\theta)$$

It is noted that if we have $R_{\hat{n}}(\theta)$ & $R_{\hat{m}}(\theta)$ both operating simultaneously, we'll have an irrational rotation.



* Efficiency of construction :-

Q How many gates from the discrete set are required to approx. an arbitrary single qubit unitary to an accuracy ϵ?

$\Theta\left[\log^c(1/\epsilon)\right]$; $c \simeq 2$

↳ Solvay Kitaev Theorem

→ To approximate a circuit containing 'm gate' {single Qbit}

$$\Theta\left(m \log^c\left(\frac{1}{\epsilon/m}\right)\right)$$

$\Theta(n^2 4^n)$ → is the upper bound on the no. of single Qbit unitaries & CNOT's required to implement an arbitrary n-Qbit unitary.

∴ The no. of gates from our discrete set needed to implement $U_{2^n \times 2^n}$ will be bounded by -

Upper bound → $\Theta\left(n^2 4^n \log^c\left(\frac{n^2 4^n}{\epsilon}\right)\right)$

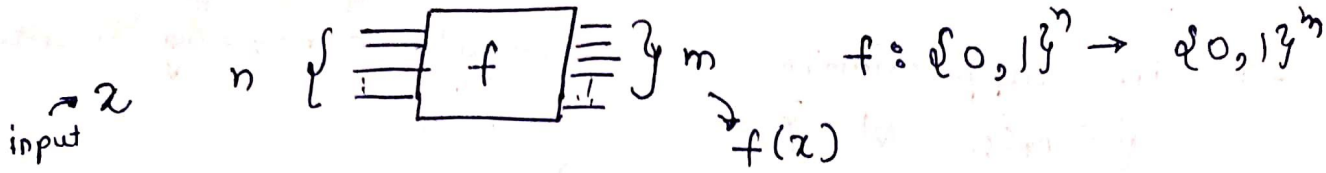
{ Lower bound → $\Omega\left(2^n \frac{\log(1/\epsilon)}{\log(n)}\right)$

But as we increase Qbits, Compexity increases exponential {Hence, not very useful result}

↓

~~How can we~~ we want to figure out something useful

→ Suppose a classical circuit performs an operator 'f' on an n-bit I/p & gives m-bit output.

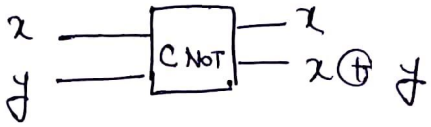


Conditions for reversibility →

(i) No. of inputs = No. of outputs

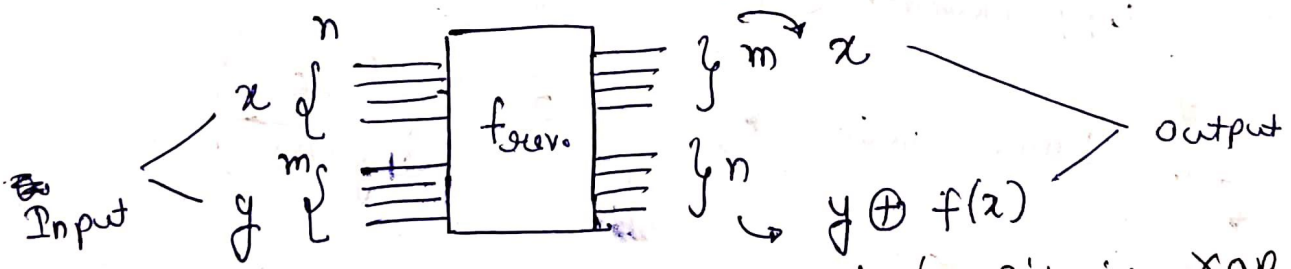
(ii) For unique input / comb. of input → Unique output / comb. of output

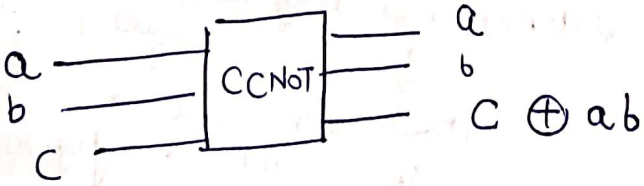
Not reversible



Reversible

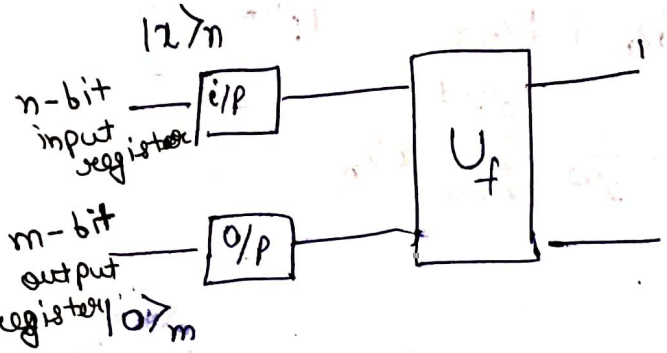
To make f reversible?





In quantum ckt case →

As long as inputs are in base states & not in superposition of the base states, quantum ckt works same as



$|0 \oplus f(x)\rangle_m$

$= |f(x)\rangle_m$

* Quantum Algorithms :-

Quantum Parallelism :→

$$U_f(|x\rangle_n |y\rangle_m) = |x\rangle_n |y \oplus f(x)\rangle_m$$

In particular, if $|y\rangle_m = |0\rangle_m$

$$U_f(|x\rangle_n |0\rangle_m) = |x\rangle |f(x)\rangle_m$$

Now, $H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ → equally weighted superposition of base states

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

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

$$= \frac{1}{(\sqrt{2})^2}\left[|0\rangle_2 + |1\rangle_2 + |2\rangle_2 + |3\rangle_2\right]$$

For n-qubits →

$$(H \otimes H \otimes \cdots \otimes H)\{|0\rangle|0\rangle \cdots |0\rangle)$$

(n-factors)

$$= \frac{1}{2^{n/2}}\left[|0\rangle_n + |1\rangle_n + |2\rangle_n + \cdots |2^n - 1\rangle_n\right]$$

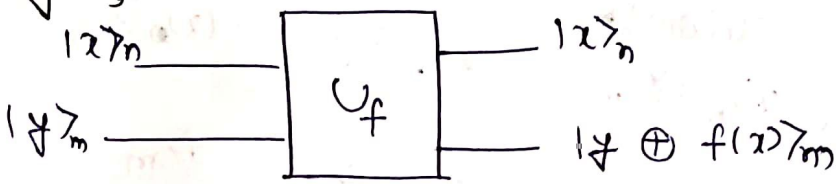
$\Rightarrow H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}}\left[|0\rangle_n + |1\rangle_n + \ldots + |2^n-1\rangle_n\right]$

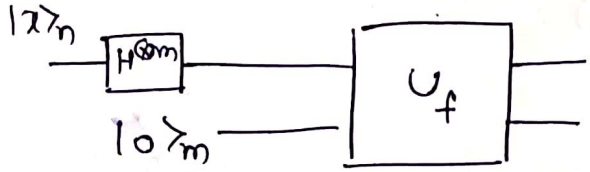
or $H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n$

Q Confirm this.

Note:- Hadamard-Walsh Transformation $\rightarrow \omega = H \otimes H \otimes H \otimes \ldots \otimes H$ (n-factor)

Again,





We know that,

$$U_f\left(|x\rangle_n |y\rangle_m\right) = |x\rangle |y \oplus f|x\rangle\rangle$$

& $H^{\otimes n}|0\rangle_n = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n$

$$\Rightarrow U_f\left(H^{\otimes n} \otimes I_m\right)|0\rangle_n |0\rangle_m$$

$$= U_f\left[\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle|0\rangle\right]$$

$$= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle|f(x)\rangle$$

i.e.

$$U_f\left(H^{\otimes n} \otimes I\right)\left(|0\rangle_n |0\rangle_m\right)$$

$$= \frac{1}{2^{n/2}} \left[|0\rangle_n |f(0)\rangle_m + |1\rangle_n |f(1)\rangle_m + |2\rangle_n |f(2)\rangle_m + \cdots + |2^n - 1\rangle_n |f(2^n-1)\rangle_m \right]$$

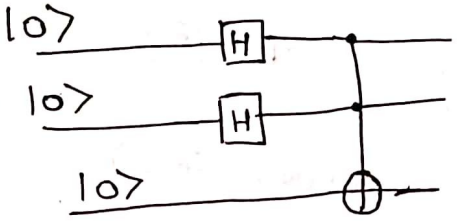
To make sense of this - we make measurement

For 1000 qubit Input registers

dimension $= 2^{1000} \sim 10^{300}$ (More than 10^{80} atoms in this universe)

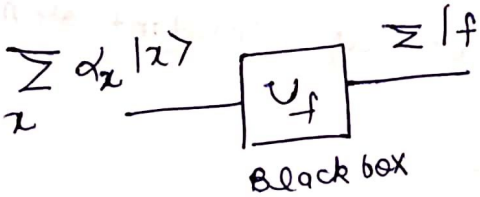
= Base states in superposition after above operation

Q



$$\text{Output} = \frac{1}{2}\left[|000\rangle + |01\rangle + |100\rangle + |111\rangle\right]$$

* Query Complexity :-



To solve a particular problem, no. of times a black box is called is given by Query Complexity

Black box (or oracle) Problem

↓

Those that are theoretically solved & we do not bother its implementation

1. Deutsch Algorithm :-

Given a Boolean function $f: B \to B$ determine whether f is constant or not.

$B = \{0, 1\}$

Q How many n-bit Boolean functions are possible?

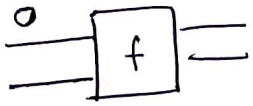
For 1-bit operations, no. of such functions = 4

$f_0 : B \to 0$ (constant fn 0)

f_1 : takes 0 to 0, 1 to 1 (Identity fn)

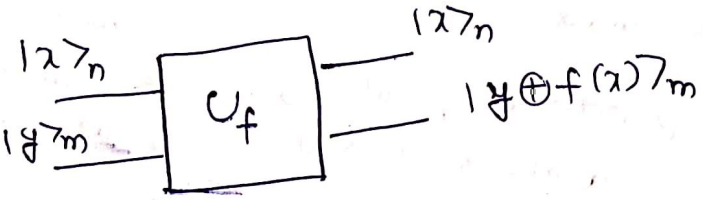
f_2 : takes 0 to 1, 1 to 0 (Not fn)

$f_3 : B \to 1$ (constant fn 1)



Q Confirm that calling the oracle only once reduces the options from 4 to 2, but does classically, not tell whether it is constant or not.

Let's do it quantum-mechanically



If $|x\rangle_n = |+\rangle$

$|y_m\rangle = |-\rangle$

then - $U_f(|+\rangle|-\rangle) = U_f\left(\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right)\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\right)$

$= U_f\left(\frac{|00\rangle}{2} - \frac{|01\rangle}{2} + \frac{|10\rangle}{2} - \frac{|11\rangle}{2}\right)$

$= \frac{1}{2}\left[|0\rangle|0+f(0)\rangle - |0\rangle|1\oplus f(0)\rangle + |1\rangle|0\oplus f(1)\rangle - |1\rangle|1\oplus f(1)\rangle\right]$

$0 \oplus f(x) = f(x)$

$1 \oplus f(x) = \overline{f(x)}$

$\therefore \quad U_f(|+\rangle|-\rangle) = \frac{1}{2}[|0\rangle|f(0)\rangle - |0\rangle|\overline{f(0)}\rangle + |1\rangle|f(1)\rangle - |1\rangle|\overline{f(1)}\rangle]$ — (1)

Case I – $f = f_0 \Rightarrow f_0(0) = 0, f(1) = 0$

$U_{f_0}(|+\rangle|-\rangle) = \frac{1}{2}[|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|0\rangle - |1\rangle)]$

$= |+\rangle|-\rangle \xrightarrow{H \otimes H} |0\rangle|1\rangle$

Case II – $f = f_1 \Rightarrow f_1(0) = 0, f_1(1) = 1$

$U_{f_1}(|+\rangle|-\rangle) = \frac{1}{2}[|0\rangle(|0\rangle - |1\rangle) + |1\rangle(|1\rangle - |0\rangle)]$

$= |-\rangle|-\rangle \xrightarrow{H \otimes H} |1\rangle|1\rangle$

Case III – $f = f_2$

$U_{f_2}(|+\rangle|-\rangle) = -|-\rangle|-\rangle \xrightarrow{H \otimes H} -|1\rangle|1\rangle$

Case IV – $f = f_3$

$U_{f_3}(|+\rangle|-\rangle) = -|+\rangle|-\rangle \xrightarrow{H \otimes H} -|0\rangle|1\rangle$

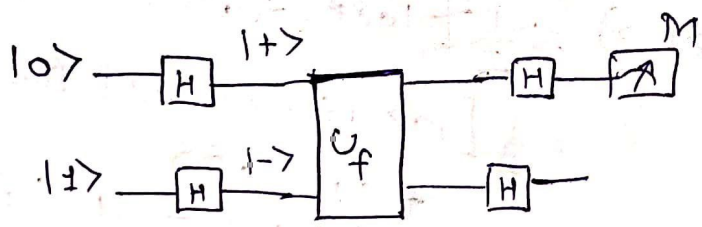
For constant functions → output same

For non-constant $f^{n}s$ → output same

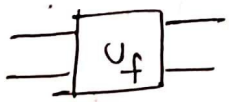
~~Again,~~ ~~$U_f(|+\rangle|-\rangle) = \frac{1}{2}$~~

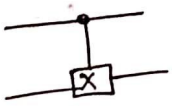
That can directly be seen from eq. (1)

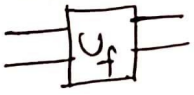
Notably, after converting output to base states, we see output is $|x\rangle|-\rangle$ i.e. ~~second qubit~~ independent of 2nd qubit.

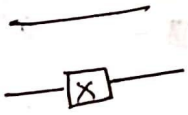


Q Show that the quantum circuit for the black box U_f that implements the 4 possible function f_0, f_1, f_2 & f_3 are -

f_0 :  ≡ 

f_1 :  ≡ 

f_2 :  = ?

f_3 :  = 

2. Deutsch-Jozse Algorithm :→ Multi-qubit generalization of the Deutsch algorithm.

f — Constant
f — Balanced → Balanced functions are those for which for half of the inputs result is 0, for other half, result is 1.

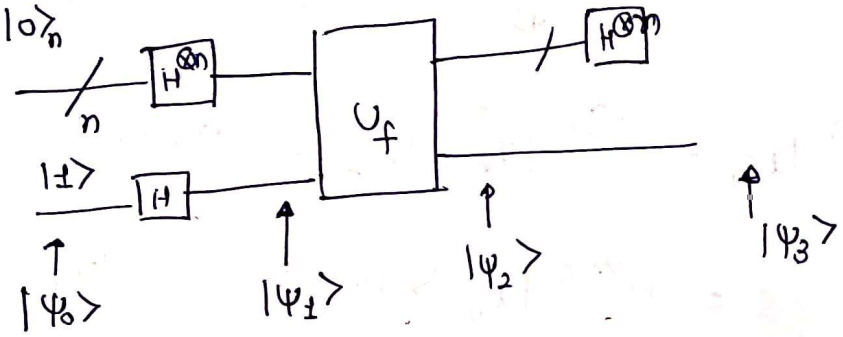
Let's say we know, for a n-qubit system, we know for sure that the function taking these n-qubits as input is either, constant or balanced.

Then,

classically $\frac{2^n}{2} + 1$ or $2^{n-1}+2$ queries we'll need to make to know nature of function.

{exponential in size}

Quantam mechanically, just '1' query



$$|\psi_0\rangle = |0\rangle_n |1\rangle$$

$$|\psi_1\rangle = (H^{\otimes n} \otimes H)|\psi_0\rangle = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

$$|\psi_2\rangle = U_f |\psi_1\rangle$$

$$= U_f \left[\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \right]$$

$$= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n \frac{(|f(x)\rangle - |\overline{f(x)}\rangle)}{\sqrt{2}}$$

$$\left\{ \because \frac{|f(x)\rangle - |\overline{f(x)}\rangle}{\sqrt{2}} = (-1)^{f(x)} \frac{(|0\rangle - |1\rangle)}{\sqrt{2}} \right\}$$

$$= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n (-1)^{f(x)} \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

$$|\psi_3\rangle = (H^{\otimes n} \otimes I)\,|\psi_2\rangle$$

$$= (H^{\otimes n} \otimes I)\,\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} (-1)^{f(x)} |x\rangle_n \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right) \quad \text{— (1)}$$

But, what is $H^{\otimes n}|x\rangle_n = ?$

Again,

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

$$H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$\Rightarrow H|x\rangle = \sum_{z=0}^{1} (-1)^{xz} \frac{|z\rangle}{\sqrt{2}}$$

$$\therefore H^{\otimes n}|x\rangle_n = H^{\otimes n}|x_{n-1}\, x_{n-2} \cdots x_1\, x_0\rangle$$

$$= H^{\otimes n}\,|x_{n-1}\rangle\,|x_{n-2}\rangle \cdots |x_1\rangle\,|x_0\rangle$$

$$= H|x_{n-1}\rangle \otimes H|x_{n-2}\rangle \cdots \otimes H|x_0\rangle$$

$$= \sum_{z_{n-1}, z_{n-2} \cdots z_1, z_0 = 0}^{1} (-1)^{x_{n-1}z_{n-1} + x_{n-2}z_{n-2} + \cdots} \frac{|z_{n-1} \cdots z_0\rangle}{2^{n/2}}$$

or even compactly,

$$H^{\otimes n}|x\rangle_n = \sum_{z=0}^{2^n-1} (-1)^{x \cdot z} |z\rangle_n$$

where,

$$x \cdot z = x_{n-1} z_{n-1} \oplus x_{n-2} z_{n-2} \oplus \cdots \oplus x_1 z_1 \oplus x_0 z_0$$

the modulo-2 dot product of x & z.

$$|\psi_3\rangle = \sum_{x=0}^{2^n-1} \sum_{z=0}^{2^n-1} (-1)^{x\cdot z + f(x)} |z\rangle_n \frac{(|0\rangle - |1\rangle)}{2^n} \quad \text{---} \ (2)$$

Now, $f(x)$ is either 0 or 1.

→ If $f(x) \rightarrow$ constant function then $(-1)^{f(x)}$ term in (2) can be pulled out

$$- |\psi_3\rangle = (-1)^{f(x)} \sum_{x=0}^{2^n-1} \sum_{z=0}^{2^n-1} (-1)^{x\cdot z} |z\rangle_n \left(\frac{|0\rangle - |1\rangle}{2^n}\right)$$

The amplitude for the input register to be in the state $|0\rangle_n$ is -

$$\left[\frac{\langle 0| - |1| \langle 0|}{\sqrt{2}}\right] |\psi_3\rangle = 1$$

↓ why?

$z = 0 \Rightarrow z_1 = z_2 = z_3 = \ldots = 0$

↓ for output register

If 'f' is constant with certainity, the input register is $|0\rangle_n$ state.

→ If on the other hand, $f(x)$ is balanced then for half of the terms $|\psi_3\rangle$ there will be factor $(-1)^{x\cdot z + f(x)} = -1$ & for remaining $(-1)^{x\cdot z + f(x)} = +1$ if $|z\rangle_n = 0$

$$\Rightarrow \left[\frac{\langle 0| - |1| \langle 0|}{\sqrt{2}}\right] |\psi_3\rangle = 0 \quad \text{in this case}$$

with certainity, input register is not in $|0\rangle_n$ state.

↓

Hence query complexity = 1

③ Bernstein - Vazirani Problem :-

Given an unknown 'n-bit' binary "a" & a subroutine (black box) which evaluates

$$f(x) = x \cdot a .$$

Find a?

Classically,

$$a = a_{n-1}\, a_{n-2} \cdots a_1\, a_0$$

$$f(x) = x \cdot a = x_{n-1}\, a_{n-1} \oplus x_{n-2}\, a_{n-2} \oplus \cdots \oplus x_0\, a_0$$

We've $x \rightarrow$ in our control

So, let's say $x = 000\cdots01$

$\downarrow$

f will give a_0

Similary, $x = 000\cdots10$

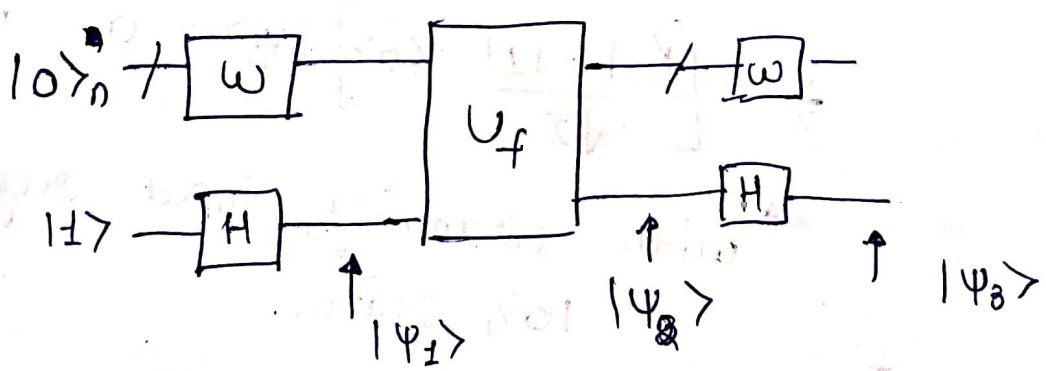
$\downarrow$

a_1

!

Such queries needed to figure out 'a' $= n$

Quantum Mechanically,



Here $\omega \cong H^{\otimes n}$

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} |x\rangle_n \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$|\psi_2\rangle = U_f |\psi_1\rangle = \sum_{x=0}^{2^n-1} (-1)^{f(x)} \frac{|x\rangle_n}{\sqrt{2^n}} \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}} \right)$$

$$|\psi_3\rangle = (H^{\otimes n} \otimes H) |\psi_2\rangle$$

$$= \frac{1}{2^n} \sum_{x=0}^{2^n-1} \sum_{z=0}^{2^n-1} (-1)^{f(x)+z\cdot x} |z\rangle_n |1\rangle$$

But $f(x) = a \cdot x$

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{x} \sum_{z} (-1)^{x\cdot(a \oplus z)} |z\rangle_n |1\rangle$$

— (A)

Now,

$$\sum_{x=0}^{2^n-1} (-1)^{(z+a)\cdot x}$$

$$= (-1)^{(z_{n-1}+a_{n-1})x_{n-1}} \cdot (-1)^{(z_{n-2}+a_{n-2})x_{n-2}}$$

$$(-1)^{(z_0+a_0)x_0}$$

$$= \prod_{i=0}^{n-1} \sum_{x_i=0}^{1} (-1)^{(a_i \oplus z_i)x_i}$$

$$= \prod_{i=0}^{n-1} \left(1 + (-1)^{(a_i \oplus z_i)} \right)$$

(a) If $a_i \neq z_i \Rightarrow a_i \oplus z_i = 1$

$$\Rightarrow (-1)^{a_i \oplus z_i} = -1$$

(b) If $a_i = z_i$, $a_i \oplus z_i = 0$

$\Rightarrow (-1)^{a_i \oplus z_i} = 1$

In ③

$$|\psi_3\rangle = \frac{1}{2^n} \sum_{z_i=0}^{1} \prod_{i=0}^{n-1} \left(|+\rangle + (-1)^{(a_i + z_i)} |z\rangle_n |1\rangle\right) \quad \text{— ④}$$

$$= |a\rangle_n |1\rangle$$

↓

How ?

If $a_i = z_0 \rightarrow \langle 0|\psi_3\rangle = 1$

& $a_i \neq z_0 \rightarrow \langle 1|1\rangle \langle 1|\psi_3\rangle = 0$ (for output register)

↓ Amplitude for input register

↓

So just make measurement on $|\psi_3\rangle$ in ④ & whatever it measures is $|a\rangle$.

④ Simon's Problem :-

Given a two to one function $B^n \rightarrow B^{n-1}$ satisfying $f(x \oplus a) = f(x)$ i.e. $f(x)$ is a periodic function.

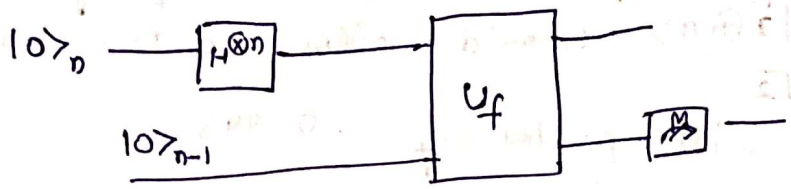
Find the n-bit no. 'a'.

$$f(y) = f(x)$$

$$y = x \oplus a$$

i.e. $f(x)$ periodic under modulo 2 addition & we want to find period 'a'.

The quantum solution gives exponential speed-up compared to the classical solution.



$$U_f \left(H^{\otimes n} \otimes I \right) |0\rangle_n |0\rangle_{n-1}$$

$$= U_f \left(\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |0\rangle_{n-1} \right)$$

$$= \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle_n |f(x)\rangle_{n-1}$$

$$= \frac{1}{2^{n/2}} \left[|0\rangle_n |f(0)\rangle_{n-1} + |1\rangle_n |f(1)\rangle_{n-1} + \cdots + |2^n-1\rangle_n |f(2^n-1)\rangle_{n-1} \right]$$

If we make a measurement on the output register, we get - say, $|f(x_0)\rangle$

$\Rightarrow$ Complete state after measurement is -

$$\frac{(|\tilde{x}_0\rangle + |\tilde{x}_0 \oplus a\rangle)}{\sqrt{2}} |f(\tilde{x}_0)\rangle$$

↳ By generalized Born rule.

∵ we know, $f(\tilde{x}) = f(\tilde{x} \oplus a)$

↓

If we want to figure out 'a'?

we can make measurement on this state. which will give either $|\tilde{x}\rangle$ or $|\tilde{x} \oplus a\rangle$

But we don't get access to a.

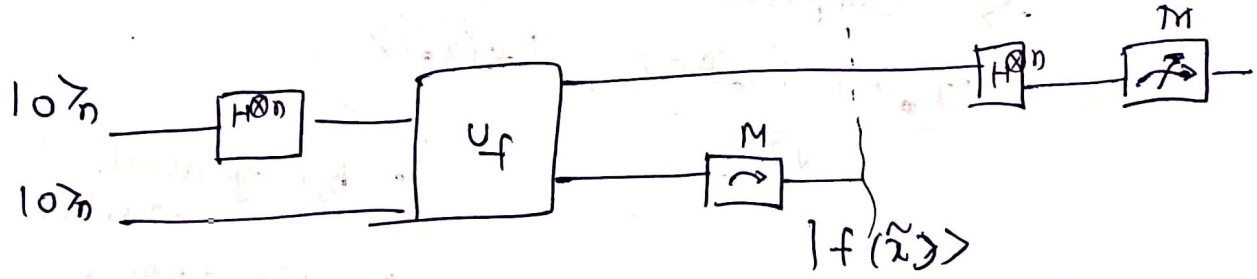
Secondly, if we could clone this stage & make measurement on each copy, we get $|\tilde{x}\rangle$ & $|\tilde{x} \oplus a\rangle$ with equal probability. But we can't clone.

Q Show that if quantum cloning was possible then preparing a mere 10 copies of the given state of the input or query register $\frac{|\tilde{x}\rangle + |\tilde{x} \oplus a\rangle}{\sqrt{2}}$ would allow determination of "a" with probability 0.998.

Again, we need to work with the input register from here and we apply the Hadamard - Walsh transformation to the input register.

$$H^{\otimes} |x\rangle = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n - 1} (-1)^{x \cdot y} |y\rangle$$

$$\therefore H^{\otimes n}\left(\frac{|\tilde{x}\rangle + |\tilde{x} \oplus a\rangle}{\sqrt{2}} \right] = \frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n - 1} \left[(-1)^{\tilde{x} \cdot y} + (-1)^{(\tilde{x} \oplus a) \cdot y} \right] |y\rangle$$



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

Now, $1 + (-1)^{a \cdot y} = 0$ if $a \cdot y = 1$

& $1 + (-1)^{a \cdot y} = 2$ if $a \cdot y = 0$

$$\Rightarrow \frac{H^{\otimes n}(|\tilde{x}\rangle + |(\tilde{x} \oplus a)\rangle)}{\sqrt{2}}$$

$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{a \cdot y = 0} (-1)^{\tilde{x} \cdot y} |y\rangle$$

Now, $a \cdot y = 0$ is

$$a_{n-1} y_{n-1} \oplus a_{n-2} y_{n-2} \oplus \cdots \oplus a_0 y_0 = 0$$

If we make a measurement on query required now, we will get one of states $|y\rangle$ satisfying $a \cdot y = 0$.

Run the procedure $\Theta(n)$ times to obtain 'n' equations for 'a'.

→ Probability of obtaining the same y when running the procedure multiple times is small & one finds that -

$$P(a) > 1 - \frac{2}{2^{n+1}}$$

when U_f is invoked $(n+1)$ times.

Number theory Recap →

∃ N ∈ Z

$x = kN + r$

$x \equiv r \bmod N$

For Inverse of x

→ $x x^{-1} = 1 \bmod N$

And inverse exists i.e. $x^{-1} \bmod N$ exists iff x & N are coprime.

Euclidean Theorem → For GCD calculation

Theorem :- Suppose p is a prime & k is an integer such that $1 \le k \le p-1$, then p divides $\binom{p}{k} = {}^{p}C_{k}$

Proof → $\binom{p}{k} = \dfrac{p(p-1)\cdots[p-(k-1)]}{k(k-1)\cdots 2\cdot 1}$

$\Rightarrow p(p-1)\cdots[p-(k-1)] = \binom{p}{k} k(k-1)\cdots 2\cdot 1$

$\because k \ge 1 \Rightarrow$ L.H.S. (i.e. RHS) is divisible by p.

On the R.H.S., the factor $k(k-1)\cdots 2\cdot 1$ is not divisible by p $\{\because k \le p-1\}$

$\Rightarrow \binom{p}{k}$ is divisible by p.

* Fermat's little theorem :-

Suppose p is a prime & "a" is any +ve integer, then - $a^p = a \bmod p$

& if "a" is not divisible by p then $a^{p-1} = 1 \bmod p$

Proof :- Second part of the theorem follows from the first part.

If "a" is not divisible by p then a^{-1} modulo mod p exists.

$\Rightarrow a^{p-1} = a^p \cdot a^{-1} = a\,a^{-1} \bmod p$ (from the first part)

$= 1 \bmod p$

To prove the first part, we need mathematical induction

→ If $a = 1$ then $a^p = 1^p = 1 \bmod p$

$= a \bmod p$

→ let $a^p = a \bmod$ holds for "a"

→ Now, consider the case for $(a+1)$

$$(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k$$

we know, for $1 \le k \le p-1$, $\binom{p}{k}$ is divisible by p i.e. $\binom{p}{k} = 0 \bmod p$ for $1 \le k \le p-1$

$$\Rightarrow (a+1)^p = \left(\underbrace{1}_{\text{for } k=0} + \underbrace{a^p}_{\text{for } k=p}\right) \bmod p$$

But $a^p = a \bmod p$ by Induction hypothesis

$\Rightarrow (a+1)^p = (1+a) \bmod p$

e.g. I Let $p = 3$, $k = 1 \Rightarrow \binom{p}{k} = 3 = 0 \bmod 3$

$k = 2 \Rightarrow \binom{p}{k} = 3 = 0 \bmod 3$

II Let $p = 3$ & $a = 2 \Rightarrow a^p = 2^3 = 8 = 2 \times 3 + 2$

$= 2 \bmod 3$

$\Leftarrow a^{p-1} = 2^{3-1} = 4 = 1\times 3 + 1 = 1 \bmod 3$

If $a = q \Rightarrow a^{p-1} = q^{3-1} = 81 = 27\times 3$
$= 0 \bmod 3$

→ For the purpose of RSA one applies Fermat's little theorem to 2 distinct primes p & q.

Let 'a' be coprime to p as well as q.

$\Rightarrow a^{q-1}$ is not divisible by p.

By Fermat's little theorem →

$$(a^{q-1})^{p-1} = 1 \bmod p$$

i.e. $a^{(q-1)(p-1)} - 1$ is a multiple of p. — (1)

By same reasoning,

$$(a^{p-1})^{q-1} = 1 \bmod q$$

$\therefore$ $a^{(p-1)(q-1)} - 1$ is multiple of q. — (2)

From (1) & (2) and also for the fact that p & q are distinct,

we say, $a^{(p-1)(q-1)} - 1$ is a multiple of $N = pq$.

$\Rightarrow$ $\boxed{a^{(p-1)(q-1)} = 1 \bmod pq}$

e.g. Let $p = 2$, $q = 3$ $\Rightarrow p-1 = 1$; $q-1 = 2$

$pq = 6$

Let $a = 5$ $\Rightarrow$ $a^{(p-1)(q-1)} = 5^{1\cdot 2} = 25$

$= 4\times 6 + 1$

$= 1 \bmod 6$

Now,

$\because a^{1(p-1)(q-1)} = 1 \bmod pq$

$\Rightarrow a^{s(p-1)(q-1)} = 1 \bmod pq \quad (s \in z)$

$\Rightarrow a \cdot a^{s(p-1)(q-1)} = a \bmod pq$

$\Rightarrow \boxed{a^{1+s(p-1)(q-1)} = a \bmod pq} \quad \text{--- (3)}$

Interestingly, this result is true even when 'a' is divisby by p & or q.

→ Let 'e' be an integer coprime to $(p-1)(q-1)$ $\Rightarrow$ Inverse of e modulo $(p-1)(q-1)$ exists.

call this inverse as 'd'.

{ e → encryption
d → decryption }

$\Rightarrow ed = 1 \bmod (p-1)(q-1)$

i.e. $ed = 1 + s(p-1)(q-1)$ — (4)

for some integer 's'.

From eq. (3) & (4)

$a^{ed} = a \bmod pq$

If we call $a^e = b$ then

$b^d = a \bmod pq$

RSA :- Alice wants to receive messages. She generates 2 large prime numbers p & q (~ 200 digits)

so that $N = pq$ (~ 400 digits)

She also finds 'e' which is coprime to $(p-1)(q-1)$ & d which is inverse to e modulo $(p-1)(q-1)$.

$\Rightarrow$ (N, e) is "public key"

(N, d) is the "primary key"

Bob wants to send message to Alice. Bob knows (N, e). He breaks his message in blocks of length $< \log_2 N$ (so that the corresponding binary string when converted to decimal will represent a no. $M < N$)

[M message]

& Bob encodes it to

$$E(M) = M^e \bmod N$$

& sends it to Alice

~~let 'e' be an integer coprime to $(p-1)(q-1)$~~

~~$\Rightarrow$ Inverse~~

→ Alice receives $E(M)$ & simply performs the operation.

$$[E(M)]^d = M^{ed} = M \bmod (pq = N)$$

↓

Alice receives & reads message.

* Primality & Factorization :→

Let $N \sim 10^{308} \sim 2^{1024}$

$\Rightarrow p \& q \sim 10^{154}$

One way to check whether N is prime or not is ~~Kaf~~ Keep dividing N by all primes from 1 to $\sqrt{N}$.

→ Now, the no. of primes less than or equal to x is given by -

$$\pi(x) \sim \frac{x}{\ln x}$$

If $x \sim 10^{154}$ $\quad x = \sqrt{N}$

$$\Rightarrow \pi(10^{154}) = \frac{10^{154}}{\ln 10^{154}} \sim 10^{151}$$

Let there are no. of supercomputers equal to population of world (7×10^9) computing for 10^{40} primes per sec.

$\therefore$ $7 \times 10^9 \times 10^{40} \sim 10^{50}$

$\Rightarrow$ To check all 10^{151} primes requires $\sim \frac{10^{151}}{10^{50}}$ sec

$\sim 10^{101}$ sec.

Age of universe $\sim 10^{17}$ sec.

$\therefore$ In entire age of universe, we'll complete $\frac{10^{17}}{10^{101}} \sim 10^{-84}$ % of task only.

→ We can use Fermat's little theorem

e.g. $n = 15144781$, $a = 2$

$$2^{n-1} = 2^{15144780} = 178993 \bmod n$$
$$\neq 1$$

For any number 'n'.... $a = 2, 3, 4, 5, 6, 7$ & every time one finds

$$a^{n-1} = 1 \bmod n$$

$\Rightarrow$ very high probability 'n' is prime.