U_1, U_2, U_3

U_1, U_2, U_3 all are 2 Level Matrice

PAGE NO.:
DATE: / /

$$U_1 = \begin{pmatrix} A & B^* & 0 \\ B & A^* & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad |A|^2 + |B|^2 = 1$$

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

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

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

$$U_2 U_1 U = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e'' & h'' \\ 0 & f'' & j'' \end{pmatrix}$$ (But it is a unitary so inverse is $(U_3 U_1 U)^\dagger$)

Known $U_3 \underbrace{(U_2 U_1 U)}_{U_3^{-1}} = I$

$$\therefore U_3 = (U_3 U_1 U)^\dagger = \begin{pmatrix} 1 & 0 & 0 \\ 0 & e''^* & f''^* \\ 0 & h''^* & j''^* \end{pmatrix}$$

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

is the max. no. of 2-Level unitaries such that

$$U = U_1^\dagger U_2^\dagger \dots U_k^\dagger$$

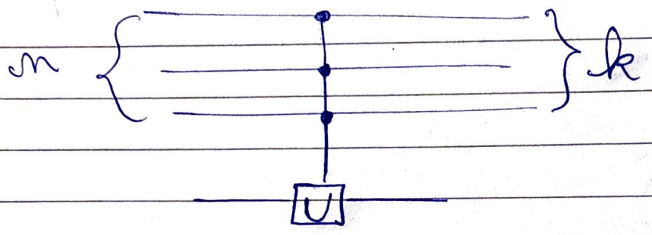
For n-qu

PAGE NO. :
DATE : / /

For n-qubit system, the number of dimension is 2^n dim
Vector Space

PAGE NO. :
DATE : / /

Universal Quantum gates :



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

Base states :

$|00\rangle$ $|01\rangle$ $|10\rangle$ $|00\rangle$

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

$$\begin{pmatrix} a \\ 0 \\ 0 \\ c \end{pmatrix} \quad \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} \quad \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} \quad \begin{pmatrix} b \\ 0 \\ 0 \\ d \end{pmatrix}$$

$a|00\rangle + c|11\rangle$ $\quad |01\rangle \quad$ $|10\rangle \quad$ $b|00\rangle + d|11\rangle$

PAGE NO. :
DATE : / /

Suppose:

$|S\rangle = |1010001\rangle$ $\quad$ $|t\rangle = |1100111\rangle$

→ Suppose our 2-Level Unitary
First convert only $|s\rangle$ & $|t\rangle$
Next construct a gray code

$|s\rangle = |1010001\rangle$
$\rightarrow |1010011\rangle$
$\rightarrow |1000011\rangle$
$|t\rangle = |1100111\rangle$

} Gray Code

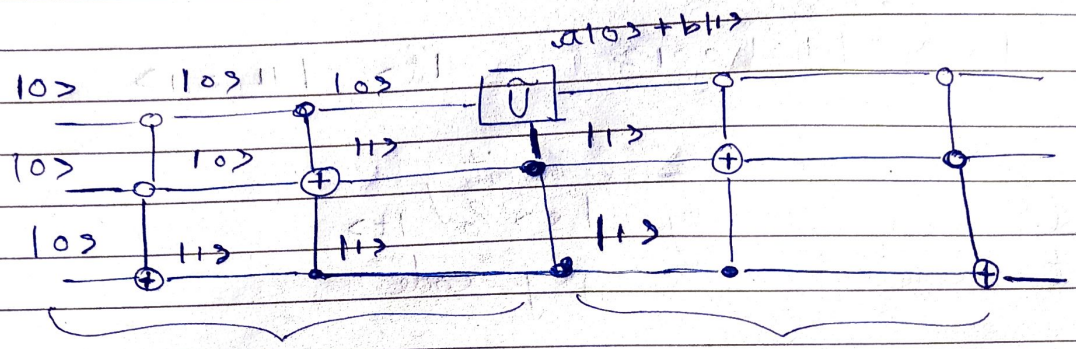
Eg: Consider a 3-Qubit System of a particular 2-Level Unitary

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

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

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

$|000\rangle$
$|001\rangle$
$|011\rangle$
$|111\rangle$



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

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

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

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

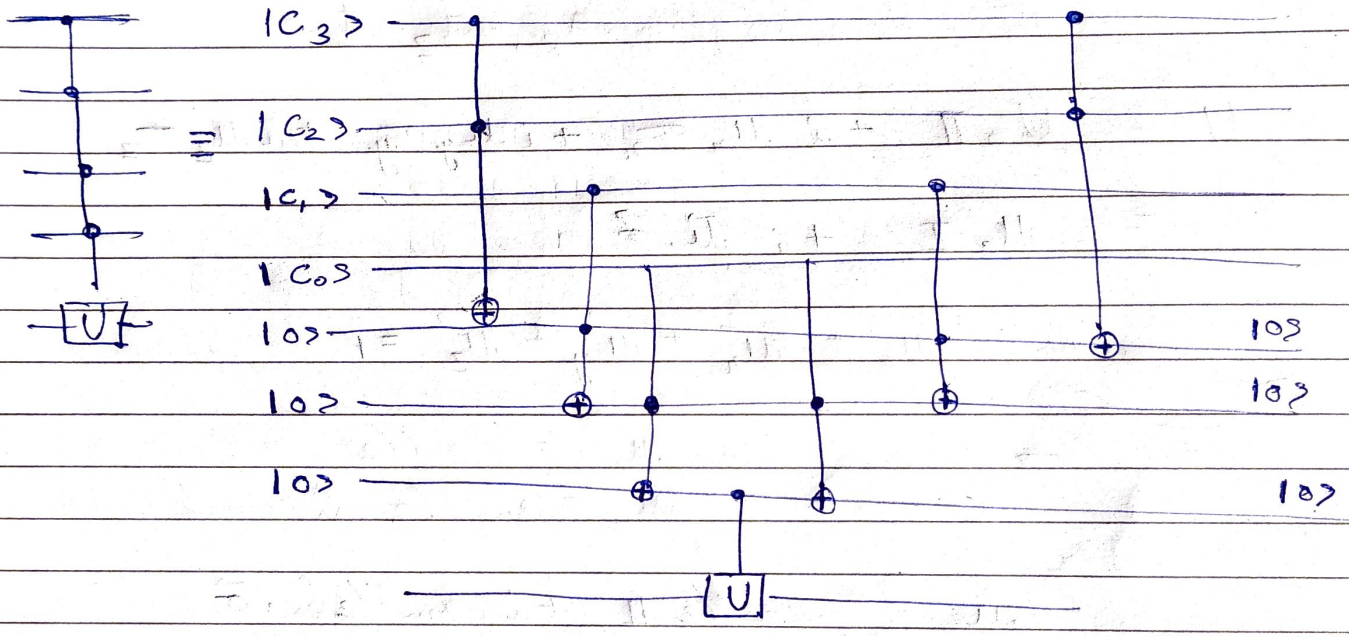
→ In general for a n-qubit system a 2-Level Unitary will be implemented (in the worst case) by (n-1) qubit controlled NOTs. & on the i/ps side we will require (n-1) of these (n-1) qbit controlled NOT. Similarly (n-1) controlled NOTs on the o/p side

=> in total of 2(n-1) NOTs Controlled by (n-1) qbits & 1 single qubit Unitary controlled bit (n-1) qbits.

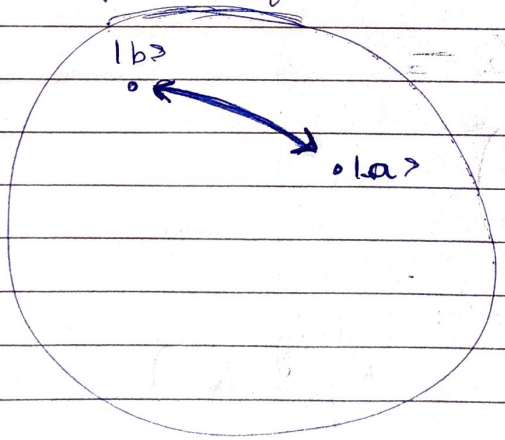
PAGE NO. :
DATE : / /

A multiply controlled unitary can be constructed using CCNOTs.

n-bit controlled NOT constructed using $2(n-1)$ CCNOTs & $(n-1)$ work qubits (or ancillas)



☆ Implementing Single Qubit Unitaries :



Mathematically :

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

$$\begin{pmatrix} a_R + i a_I & -b_R + i b_I \\ b_R + i b_I & a_R - i a_R \end{pmatrix}$$

$$\det = 1 \quad a_R^2 + a_I^2 + b_R^2 + b_I^2 = 1$$

3 Unknowns which are independent

& Rotation Requires 3 Parameters.

PAGE NO. :
DATE : / /

$$U = a_R \mathbb{I} + i a_I Z + i b_I X + i b_R Y$$

$X = \sigma_x$, $Y = \sigma_y$, $Z = \sigma_z$ {Pauli Matrices}

Renaming a_R, a_z etc.

$$U = U_0 \mathbb{I} + i u_x \sigma_x + i u_y \sigma_y + i u_z \sigma_z$$

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

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

we choose $u_0 = \cos \gamma/2$

$\vec{u} = \sin \gamma/2 \, \hat{n}$ → unit Vector

$$u = \cos \gamma/2 \, \mathbb{I} + i \sin \gamma/2 \, \hat{n} \cdot \vec{\sigma}$$

choose $n_x = 0 = n_y$, $n_z = 1$

$$u = \cos \gamma/2 \, \mathbb{I} + i \sin \gamma/2 \, \sigma_z$$

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

Ex: Show that $R_z(\gamma) = e^{i \sigma_z \gamma/2}$ (Using Taylor Series Expansion)

PAGE NO. :
DATE : / /

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

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

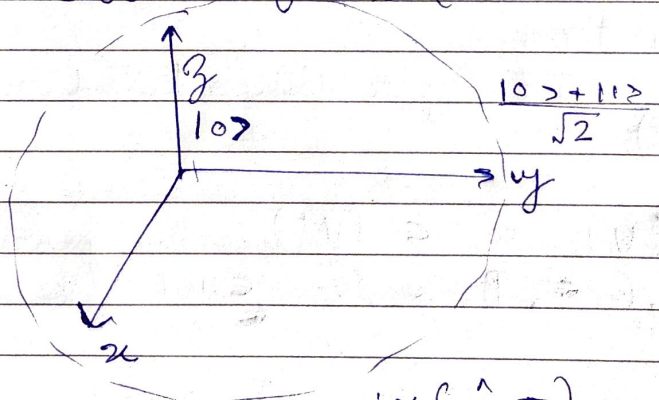
& for $n_y = 1, n_x = 0 = n_z$

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

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

$$e^{i\gamma\sigma_y/2} = R_y(\gamma)$$

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



$$U = e^{\frac{i\gamma(\hat{n}\cdot\sigma)}{2}}$$

PAGE NO.:
DATE: / /

Universal Quantum Gates:

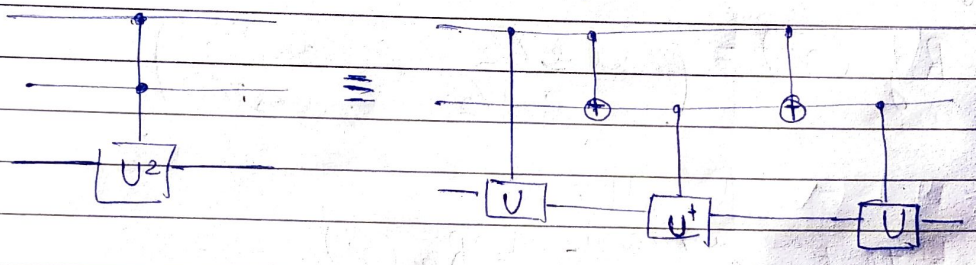
CCNOT - $\Theta(C)$

$O(n^2)$

$O(4^n)$ → is the upper bound on the no. of single Qbit unitaries & CNOTs reqd. to implement an arbitary n-Qbit unitary.

Circuit Complexity $O(n^2 4^n)$

Not Very Efficient.

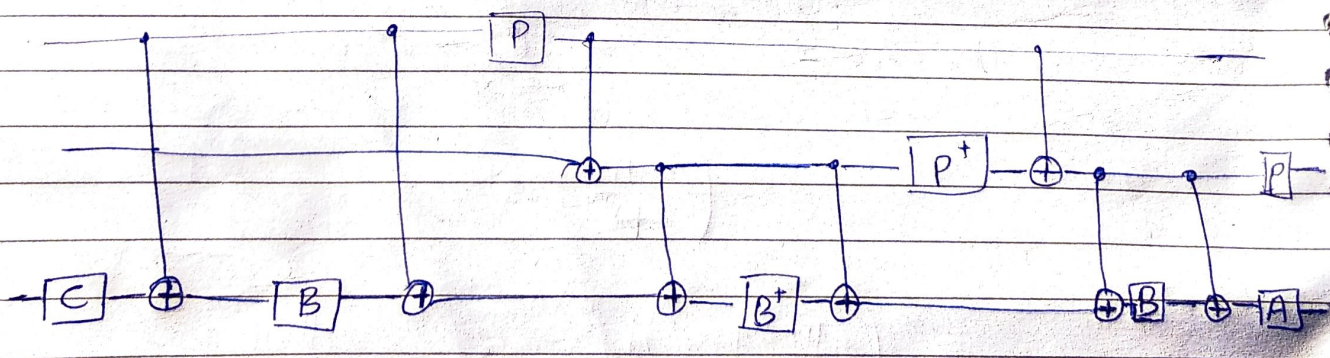


Ex: How many single Qbit Unitaries & how many CNOTs does the above implementation require?

Soln: 8 Single Qbit unitaries
8 CNOTs

Ex: Let $c(U)$ be the notation for the controlled version of U — ● — [U] — ≡ $c(U)$

Substitute for $c(U)$ & $c(U^+)$ in the prev ckt in terms of A, B, C, P & the CNOT to find the circuit.



Now check for U^2.

Ex: Re
recall
(i) Mod
Gate
(ii) Che
(iii) Repla
terms
which
Ex: U
Qbit
Ũ
V =
As
use
sin

PAGE NO.:
DATE: / /

Ex: Recall the construction of SWAP gate using CNOTs. Also recall that 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 & the 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 the Fredkin gate which uses only single qubit unitaries & CNOTs.

Ex: What quantum circuit using Toffoli gate & a single qubit gate

$\tilde{U} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$ will implement

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

Assume that a Toffoli gate can be implemented using 8 CNOTs, find the no. of CNOTs & single qubit unitaries required.

PAGE NO. :
DATE : / /

* Suppose we want to implement unitary U.

And suppose we use only finite set of single Qbit unitaries & CNOTs

(actually only 3 diff single Qbit unitaries as we will see)

then we will not be implementing U but some op. V => there will be an error

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

Hadamard + $\pi/8$ + CNOT (+ Phase Shift) gates are universal (in the above case)

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

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

Upto a global phase, T is a rotation about the 2-axis of Block Sphere

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

$$\Rightarrow T = e^{i\pi/8} R_z\left(\frac{-\pi}{4}\right)$$

Ex : Check that

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

PAGE NO. :
DATE : / /

→ Rational Rotation

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

$R_{\hat{n}}(\theta)$: Arbitary

$R_z(\alpha)$: (T)

$R_x(\beta)$: (HTH)

$R_z(\delta)$: (T)

$R_z(\beta) \simeq R_x(\beta)$

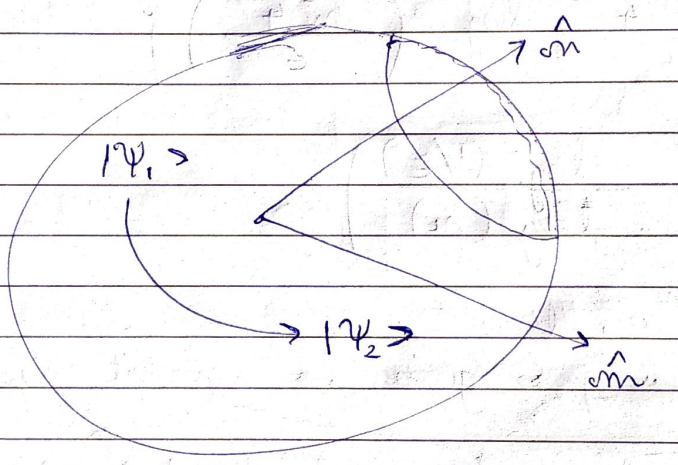
to some fixed Axis (can be changed to any arbitary axis by use combination of $R_z(\alpha)\, R_x(\beta)\, R_z(\delta)$

Need two things to implement arbitary unitary :

① Change the axis of Rotation.

② Rotation about $\hat{n}$ & $\hat{m}$, together implement irrational rotation.

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



Efficiency of Construction :

How many gates from the discrete set are required to approximate an arbitary single Qbit unitary to an accuracy ϵ ?

Solovay - Kitaev theorem

$$O\left[\log^c(1/\epsilon)\right]$$

$c \simeq 2$

H, π/8, Phase-Shift, C NOT

Classical :
Need 3 Bit Gate
for Reversible

In Quantum :
1 Qubit & 2 - Qubit Gate } Reversible

PAGE NO. :
DATE : / /

=> to approximate a circuit containing m gates (single qubit)

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

↓

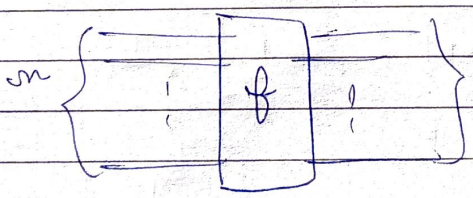
Accuracy of Individual Gates is ϵ/m & total is ϵ.

=> the no. of gates from one discrete set needed to implement $U_{2^n \times 2^n}$ will be bounded by

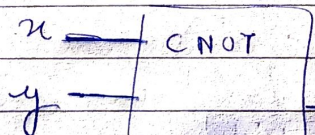
$$O\left(n^2 4^n \log^c\left(\frac{n^2 4^n}{\epsilon}\right)\right) \quad \text{(Upper Bound)}$$

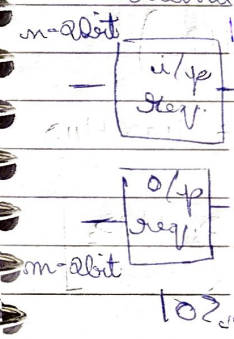
$$\Omega\left(2^n \frac{\log(1/\epsilon)}{\log(n)}\right)$$

Suppose a classical ckt performs an op. f on an n-bit i/p & gives a m-bit o/p.



$$f : \{0,1\}^n \to \{0,1\}^m$$

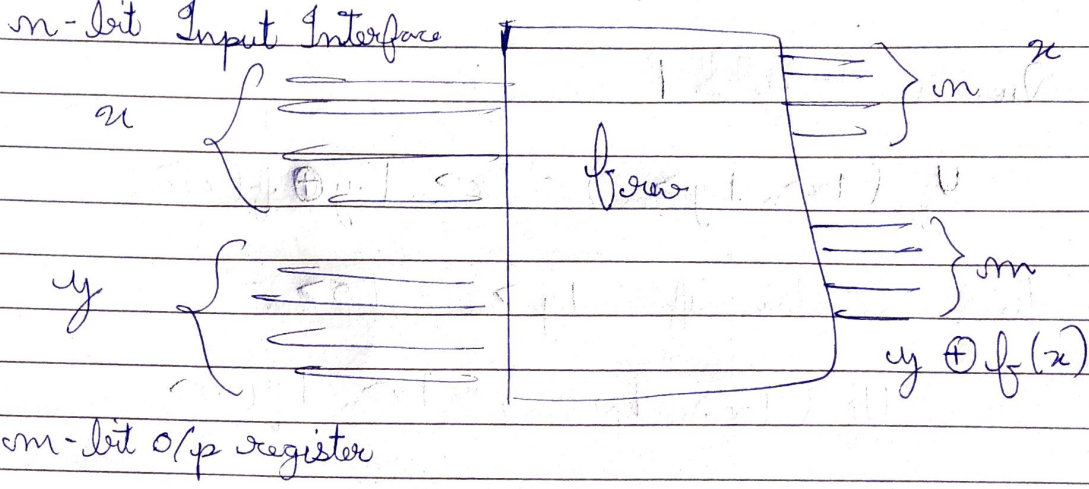




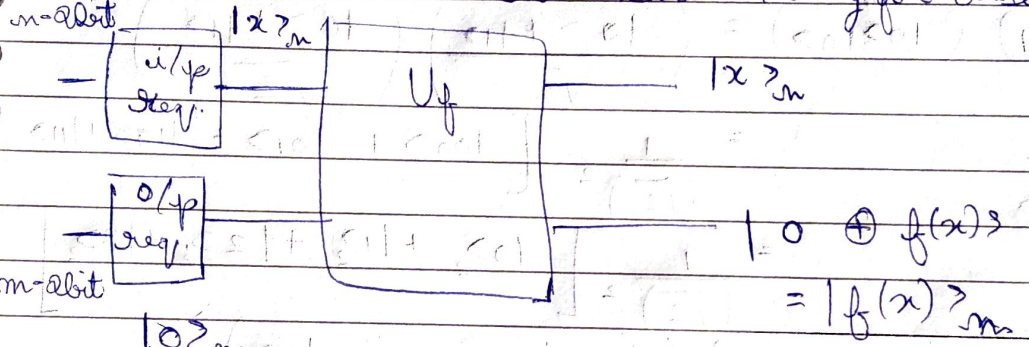
Any Permutation is a Unitary

PAGE NO. :
DATE : / /

$\{0,1\}^n \rightarrow \{0,1\}^m$



Quantum Reversible ckt: {Only for base states}



$|0\rangle_m$ → m-qubit

PAGE NO.:
DATE: / /

Quantum Algorithms:

Quantum ~~Parallelism~~ Parallelism:

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

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

$$U_f\left(|x\rangle_m |0\rangle_m\right) = |x\rangle_m |f(x)\rangle_m$$

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

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

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

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

$$(H \otimes H \otimes \cdots \otimes H)\underbrace{(|0\rangle|0\rangle \cdots |0\rangle)}_{m\text{-factors}}$$

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

$$H^{\otimes m}|0\rangle_m = \frac{1}{2^{m/2}}\left[|0\rangle_m + |1\rangle_m + \cdots + |2^m - 1\rangle_m\right]$$

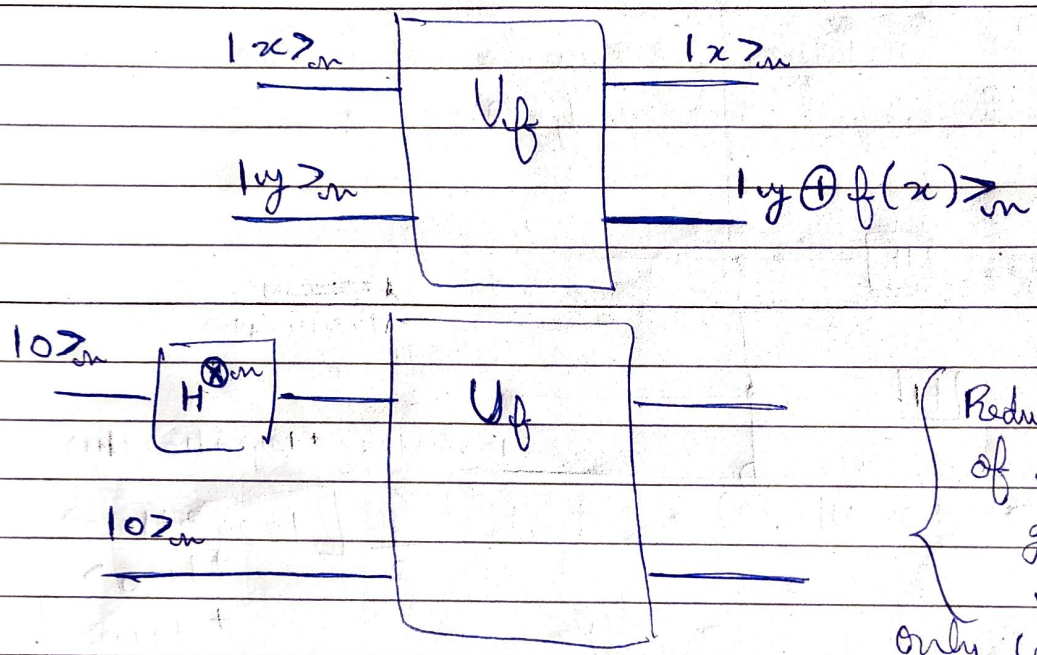
or $$H^{\otimes m}|0\rangle_m = \frac{1}{2^{m/2}}\sum_{x=0}^{2^m - 1}|x\rangle_m$$

Exe: Confirm This.

PAGE NO. :
DATE : / /

$$W = H \otimes H \otimes \cdots \otimes H = H^{\otimes n}$$

Hadamard-Walsh Transform



{ Reduces the number of inputs to one to get output for all base states }

only apparent for measurements

We know that

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

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

$$\Rightarrow U_f \left(H^{\otimes n} \otimes \underbrace{I_n}_{\text{Identity}} \right) |0\rangle_n |0\rangle_n$$

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

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

Eg: for 1000 qubit i/p register

$2^{1000} \sim 10^{30}$ & ~~Size of~~ No. of Atoms in Universe $\approx 10^{80}$

PAGE NO.:
DATE: / /

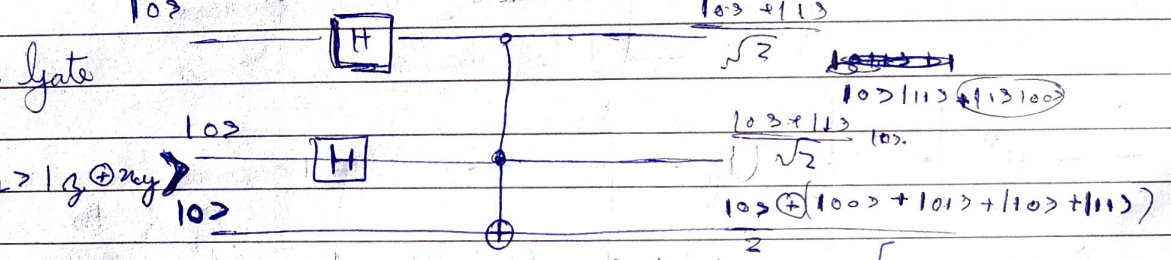
ie. $U_f \left(H^{\otimes m} \otimes \mathbb{I} \right) \left(|0\rangle_m |0\rangle_n \right)$

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

But need to measure, so in the end know only one state with equal probability.

Ex:

Toffelis gate



Output: $\frac{1}{2}\left[|000\rangle + |010\rangle + |100\rangle + |111\rangle \right]$

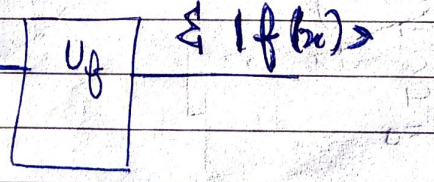
② Verify Output?

③ Optimise number of measurement?

Comparison of Complexity of Classical or Quantum:

① Bounded Quantum Probability

② Query Complexity: Black Box (no need to look at practicality) or Oracle Box.



(0,0) (0,1) (1,0) (1,1)

$2^m \times 2^m$

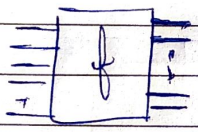
PAGE NO.:
DATE: / /

✡ Deutsch Algorithm :

Given a Boolean Function $f : \mathbb{B} \to \mathbb{B}$ determine whether f is constant or not.

$$\mathbb{B} = \{0, 1\}$$

Ex : How many n bit Boolean function are possible ?



① What are ~~bob~~ Boolean function ?

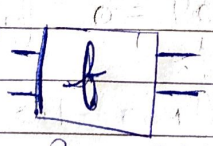
$f_0 : \mathbb{B} \to 0$ { const. Function }

f_1 : takes 0 to 0 & 1 to 1 { Identity }

f_2 : takes 0 to 1 & 1 to 0 { NOT }

$f_3 : \mathbb{B} \to 1$ { Const. Function }

In classical case, ~~must~~ need ~~two~~ two queries to figure out const. func^n or not.

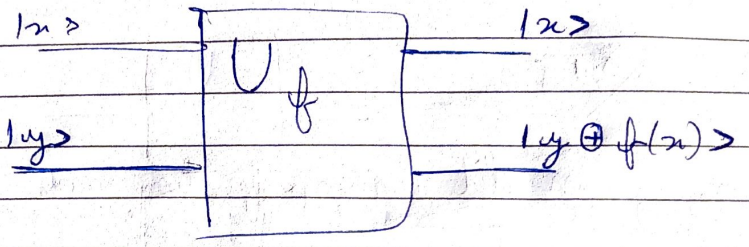


Reversible

1. $\bar{a} + 0.a$ $\quad$ $1 \text{ if } \overline{f(x)}$

PAGE NO. :
DATE : / /

Ex: Confirm that calling the oracle only once reduces the options from 4 to 2 but does not tell whether f is const. or not.



$$\Rightarrow \frac{1}{2}\Big[\,|0\rangle\,|0\oplus f(0)\rangle \;-|0\rangle\,|1\oplus f(0)\rangle + |1\rangle\,|0\oplus f(1)\rangle \;-|1\rangle\,|1\oplus f(1)\rangle\,\Big]$$

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

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

$$\Rightarrow \frac{1}{2}\Big[\,|0\rangle\,|f(0)\rangle \;-|0\rangle\,|\overline{f(0)}\rangle + |1\rangle\,|f(1)\rangle \;-|1\rangle\,|\overline{f(1)}\rangle\,\Big]$$

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

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

$$U_{f_0}(|+\rangle\,|-\rangle) = |+\rangle\,|-\rangle \xrightarrow{H\otimes H} |0\rangle\,|1\rangle$$

PAGE NO.:
DATE: / /

Case 2: $f = f_1 \Rightarrow f_1(0) = 0 \;, f_1(1) = 1$

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

$$U_{f_1}(|+\rangle|-\rangle) = |-\rangle|-\rangle \xrightarrow{H\otimes H} |1\rangle|1\rangle$$

Case 3: $f = f_2$

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

↓ Phase Factor not of concern.

Case 4: $f = f_4$

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

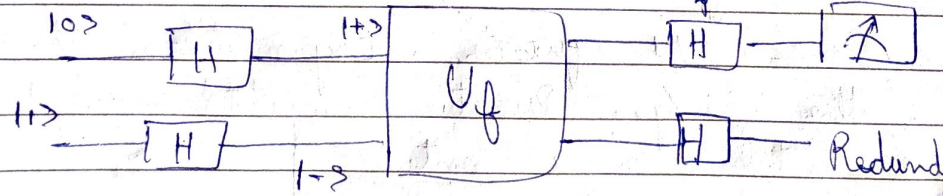
So generalising:

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

For Const. Function: $|f(0)\rangle = |f(1)\rangle$

Applying Hadamard:

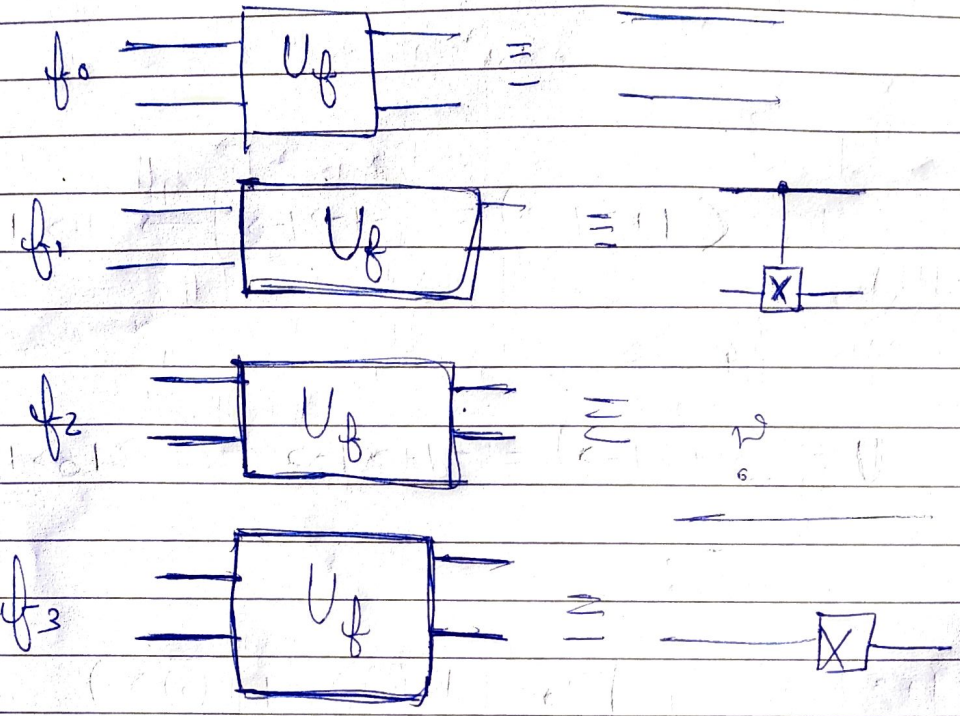
Important



Note: Result Deterministic in nature

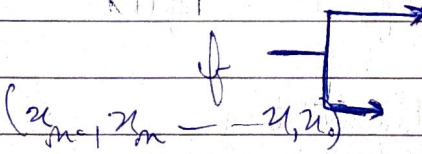
PAGE NO. :
DATE : / /

Ex: Show that the quantum circuit for the Black box U_f that implements the four possible functions f_0, f_1, f_2 & f_3 are



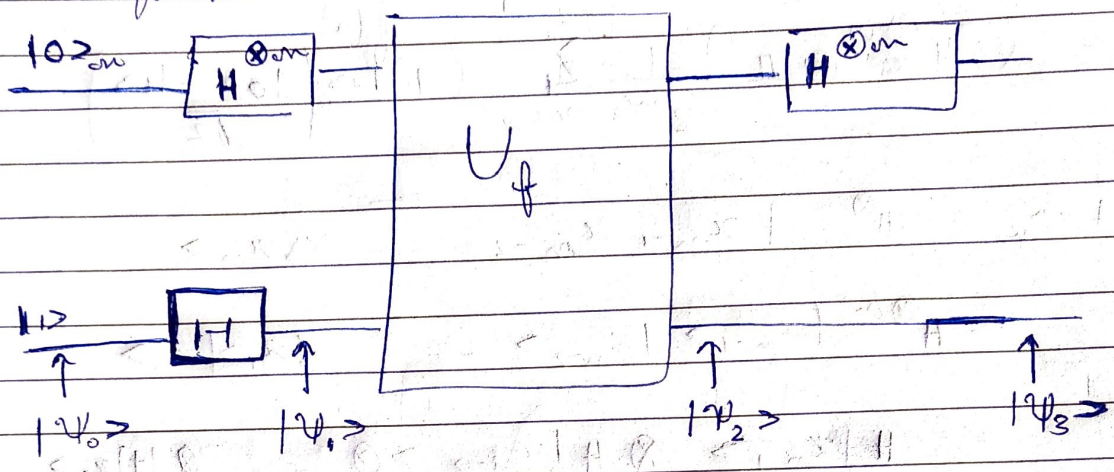
✱ Deutsch-Jozsa Algorithm:

Multi-Qubit generalized of the Deutsch algo



Classically => $2^{n-1}+1$ queries. Exponentials in the size of the i/p: Quantum Computation → only 1 query
=> exponential improvement.

In quantum :



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

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

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

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

$$= \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle_m \left(\frac{|f(x)\rangle - |f(\bar{x})\rangle}{\sqrt{2}}\right)$$

$$= \frac{|f(x)\rangle - |f(\bar{x})\rangle}{\sqrt{2}}$$

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

$$|\psi_2\rangle = \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} (-1)^{f(x)} |x\rangle_m \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

Generalization:

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

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

PAGE NO.:
DATE: / /

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

$$= (H^{\otimes m} \otimes \mathbb{I}) \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} (-1)^{f(x)} |x\rangle_m \left(\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right)$$

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

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

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

$$= \sum_{z_{m-1}, z_{m-2}, \ldots, z_1, z_0 = 0}^{1} (-1)^{x_{m-1}z_{m-1} + x_{m-2}z_{m-2} + \cdots + x_1 z_1 + x_0 z_0} \frac{|z_{m-1} \cdots z_0\rangle}{2^{m/2}}$$

or even more compactly:

$$H^{\otimes m}|x\rangle_m = \sum_{z=0}^{2^m-1} (-1)^{x.z} |z\rangle_m$$

where, $x.z = x_{m-1}z_{m-1} \oplus x_{m-2}z_{m-2} \oplus \cdots \oplus x_0 z_0$.

the modulo 2 dot product of x & z.

$$|\psi_3\rangle = \sum_{x=0}^{2^m-1} \sum_{z=0}^{2^m-1} (-1)^{x.z + f(x)} |z\rangle_m \frac{(|0\rangle - |1\rangle)}{2^{m/2}}$$

Now, if $f(x) = \text{const.}$, & $|z\rangle_m = |0\rangle_m$ $\Rightarrow z = 0$

$$\sum_{x=0}^{2^m-1} (1) \left(\frac{|0\rangle - |1\rangle}{2^{m/2}}\right)$$

Imposing $|z\rangle_m = |0\rangle_m$

$$\left[\left(\frac{\langle 0| - \langle 1|}{\sqrt{2}}\right)^{\otimes m}\right] |\psi_3\rangle = 1$$

PAGE NO.:
DATE: / /

→ if f is a const. function, with certainty the i/p register is in state $|0\rangle_n$.

If on the other hand, $f(x)$ is balanced then for half the terms in $|\psi_3\rangle$ there will be a factor $(-1)^{x.z + f(x)}$ & for remaining $(-1)^{x.z + f(x)} = 1$

$= -1$

if $|z\rangle_n = |0\rangle_n$

$\Rightarrow \left(\frac{\langle 0| - \langle 1|}{\sqrt{2}} \right)_n |\psi_3\rangle = 0$ i.e.

this case i.e. with certainty the i/p register is NOT in state $|0\rangle_n$.

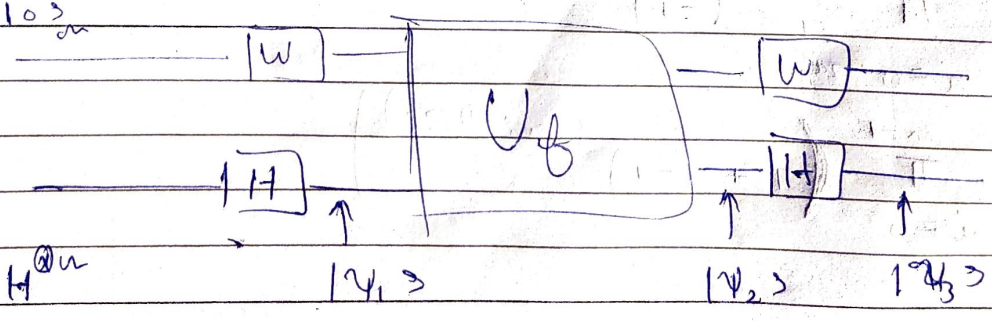
Bernstein - Vazirani Problem: (Linear Speed-Up)

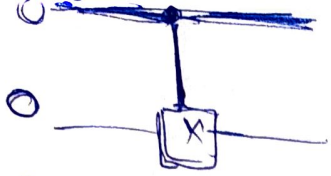
Given an unknown n-bit binary "a" & a subroutine (Black box) which evaluates $f(x) = x.a$, find a?

$a = 11\ 01\ 00\ 111$

$x = 00\ 00\ 00\ 010$

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





$0 \cdot 0 + 1 \cdot 1 = 1$

$a \cdot \bar{b} + \bar{a} \cdot b$

$0 \oplus 1$

$0 \oplus x = 0 \cdot \bar{x} + 1 \cdot x = x$

$1 \oplus f(a) \quad 1 \oplus a = 0 + \bar{a}$

PAGE NO.:
DATE: / /

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

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

$$|\psi_2\rangle = \left(H^{\otimes m} \otimes H \right) |\psi_2\rangle$$

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

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

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

Writing the sum over x explicitly.

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

$$\Rightarrow (-1)^{(z_{m-1} + a_{m-1}) x_{m-1}} (-1)^{(z_{m-2} + a_{m-2}) x_{m-2}} \cdots (-1)^{(z_1 + a_1) x_1} (-1)^{(z_0 + a_0) x_0}$$

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

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

PAGE NO.:
DATE: / /

If $a_i \neq z_i$, $\Rightarrow a_i \oplus z_i = 1$

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

& this factor becomes 0.

For $a_i = z_i$, $a_i \oplus z_i = 0$

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

$$\frac{1}{2^n} \sum_{z_i=0}^{} \prod_{a_i=0}^{n-1} \left(1 + (-1)^{(a_i + z_i)}\right) |z\rangle_n |1\rangle = |a\rangle_n |1\rangle$$

implies

* Simon's Problem:

Given a function $B^n \rightarrow B^{n-1}$

satisfying $f(x \oplus a) = f(x)$

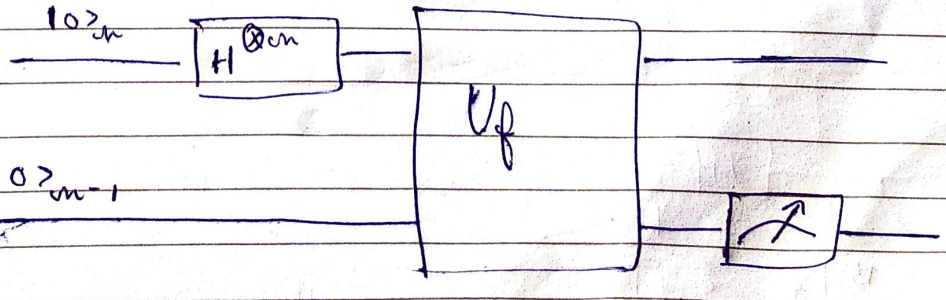
find the n-bit no. "a"

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

$$y = x \oplus a$$

i.e. $f(x)$ is periodic under modulo 2 addition & we want to find the periodic "a"

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



PAGE NO.:
DATE: / /

$$U_f \left(H^{\otimes m} \otimes I_{2^{m-1}} \right) |0\rangle_m |0\rangle_{m-1}$$

$$\Rightarrow U_f \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle_m |0\rangle_{m-1}$$

$$\Rightarrow \frac{1}{2^{m/2}} \sum_{x=0}^{2^m-1} |x\rangle_m |f(x)\rangle_{m-1}$$

$$\rightarrow \frac{1}{2^{m/2}} \left[|0\rangle_m |f(0)\rangle_{m-1} + |1\rangle_m |f(1)\rangle_{m-1} + \cdots + |2^m-1\rangle_m |f(2^m-1)\rangle_{m-1} \right]$$

If we make a measurement on o/p register we get, say $|f(x_0)\rangle \Rightarrow$ the complete state after measurement is generalised by a Born Rule.

$$\left(\frac{|\tilde{x}\rangle + |\tilde{x} \oplus a\rangle}{\sqrt{2}} \right) |f(\tilde{x})\rangle_{m-1}$$

$\because$ we know that $f(\tilde{x}) = f(\tilde{x} + a)$

Ex: Show that if quantum cloning was possible then preparing a mere 10 copies of the given state of the i/p or query register $\left(\frac{|x_0\rangle + |x_0 \oplus a\rangle}{\sqrt{2}} \right)$ would allow determinant of "a" with prob. 0.998

ANS

$x \oplus a$

$x \cdot \bar{a} + \bar{x} \cdot a$

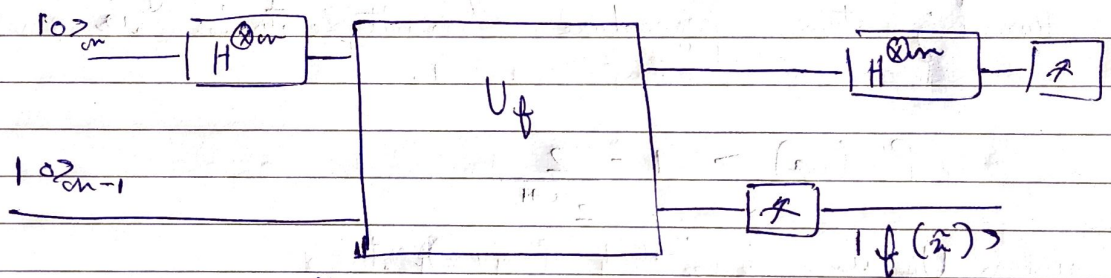
We need to work only with the i/p register from here on. We first apply the Hadamard-Walsh form to the i/p.

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

$$x.y = x_{m-1} y_{m-1} \oplus x_{m-2} y_{m-2} \oplus \cdots \oplus x_1 y_1 \oplus x_0 y_0$$

$$\Rightarrow H^{\otimes} \left[\frac{|\tilde{x}\rangle + |\tilde{x} \oplus a\rangle}{\sqrt{2}} \right]$$

$$\Rightarrow \frac{1}{\sqrt{2^{m+1}}} \sum_{y=0}^{2^m - 1} \left[(-1)^{\tilde{x}.y} + (-1)^{(\tilde{x} \oplus a).y} \right] |y\rangle$$



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

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

& $1 + (+1)^{a.y} = 2$ if $a.y = 0$

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

$n \rightarrow$ Inputs

PAGE NO.:
DATE: / /

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

Now, $a \cdot y = 0$ is

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

If we make a measurement on the query register now, we will get one of states $|y\rangle$ satisfying $a \cdot y = 0$. Run the procedure $O(n)$ times to obtain n equation for a.

(Not Imp.) Prob. 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 $(n+n)$ times

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

$f(x_1), f(x_2) \cdots f(x_m) \sim 2^n \Rightarrow m \sim 2^{n/2}$

m Inputs

m outputs are distinct

$${}^m C_2 \Rightarrow \frac{m(m-1)}{2}$$

RSA :

Class

Shor's Al

O [

Number Th

In Mo

by m

$\Rightarrow$ there

given

express

Ex : (2

[

$\neq 1$

≤ 1

Theorem :

+ve

Multiplicat

by

We

n → Inputs

PAGE NO.:
DATE: / /

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

Now, $a \cdot y = 0$ is

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

If we make a measurement on the query register now, we will get one of states $|y\rangle$ satisfying $a \cdot y = 0$. Run the procedure $O(n)$ times to obtain n equation for a.

(Not Imp.) Prob. 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 $(n+n)$ times

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

$f(x_1), f(x_2) \cdots f(x_m) \sim 2^n \Rightarrow m \sim 2^{n/2}$

m → Inputs

m outputs are distinct ⇒

$${}^m C_2 \Rightarrow \frac{m(m-1)}{2}$$

PAGE NO. :
DATE : / /

RSA :

Classical Complexity : $\sim \exp\left[n^{1/3} \log^{2/3} n\right]$

Shor Algo Uses : $f(x+r) = f(x)$

Plus

$O\left[n^2 (\log n)(\log \log n)\right]$

$P \subseteq NP$

Number Theory → Modulo Arithmetic

In Modulo - N - Arithmetic all integers which differs by multiples of N are identified.

⇒ there are only N distinct integers $0, 1, 2 \ldots, N-1$.
Given any +ve integer x, it can always be expressed as

$$x = kN + r \quad (r < N)$$

Ex : $(24 + 31) \bmod 6 = 0 + 1 = 1$

$[(24 \bmod 6) + (31 \bmod 6)] \bmod 6$

$= (0 + 1) \bmod 6$

$= 1$

Theorem : GCD of 2 integers x & y is the least +ve integer that can be written as $ax + by$ where $a, b \in Z$.

Multiplicative Inverse of x modulo N is an integer y such that $xy = 1 \bmod N$.
We denote the modulo N inverse of x by x^{-1}.

PAGE NO. :
DATE : / /

→ When does an integer x have a multiplicative inverse modulo N?

Theorem: Let N be an integer greater than 1. An integer x has a multiplicative inverse modulo N if & only if $\gcd(x, N) = 1$ i.e. when x & N are relatively prime (or coprime)

Proof: Let x have a multiplicative inverse mod N (denoted by x^{-1}) then:

$$x x^{-1} = kN + 1 \text{ for } k \in Z_+.$$

$\Rightarrow x x^{-1} + kN = 1$ which by Bez. thm $\Rightarrow x$ & N are co-prime

Conversely, if $\gcd(x, N) = 1$.

$\Rightarrow \exists$ integers x^{-1} & b such that

$$x x^{-1} + bN = 1$$

Eg Multiplicative inverse of 4 Mod 7?

Step 1: Check for Co-Prime.

$\therefore GCD(4, 7) = 1$ ✓

Step 2: $4x_{-} = 1 \pmod 7$.

$4 \times 2 = 8 = 1 \pmod 7$

↓

Inverse

PAGE NO. :
DATE : / /

Euclids Algorithm : (Polynomial Time) Help find gcd( ).

Theorem : Suppose p is a prime & k is an integer such that $1 \le k \le p-1$, then p divides

$$\binom{p}{k} = {}^{p}C_{k} = \frac{p\,(p-1)\,\cdots\,(p-(k-1))}{k\,(k-1)\,\cdots\,2.1}$$

$$\Rightarrow \binom{p}{k} k! = p\,(p-1)\,\cdots\,(p-(k-1))$$

$k \ge 1$ $\therefore$ L.H.S & R.H.S are both divisible by p.

On the R.H.S the factor $k!$ is not divisible by p $\because$ $k \le p-1$.

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

Fermat's Little Theorem :

Suppose p is a prime & "a" is any 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 as if "a" is not divisible by p then $a^{-1} \bmod p$ exists.

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

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

PAGE NO. :
DATE : / /

To prove the first part we use mathematical induction.

If $a = 1$ then $a^p = 1^p = 1 \bmod p = a \bmod p$ — (1)

Let $a^p = a \bmod p$ hold for "a" (Induction Hypothesis)

Now consider the case for $(a+1)$

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

For $1 \le k \le p-1$, $\binom{p}{k}$ is divisible by p i.e.

$\binom{p}{k} = 0 \bmod p$. (All Terms zero except for k=0 & p)

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

But $a^p = a \bmod p$ by induct. hypothesis

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

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 to q.

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

By Fermat's Little Theorem $\Rightarrow (a^{q-1})^{p-1} = 1 \bmod p$.

PAGE NO. :
DATE : / /

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

By same reasoning,

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

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

Since p & q are distinct primes,

(1) & (2) $\Rightarrow$

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

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

Eg: Let $p = 2, q = 3 \Rightarrow p-1 = 1, q-1 = 2$

$pq = 6$

Let $a = 5$

$a^{(p-1)(q-1)} = 5^2 = 25$

$= 6 \times 4 + 1$

$5^2 \equiv 1 \bmod 6$

$a^{s(p-1)(q-1)} \equiv 1 \bmod pq$

$s \in Z_+$

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

PAGE NO.:
DATE: / /

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

Interestingly this result hold even when "a" is divisible by p & / or q.

Let e be an integer coprime to $(p-1)(q-1)$
⇒ inverse of e modulo $(p-1)(q-1)$ exists.

Call this inverse as d.

⇒ $ed = 1 \bmod (p-1)(q-1)$

ie $ed = 1 + s(p-1)(q-1)$ - (4)

for some integer s.

From (3) using (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 primes p & q (~ 200 digits)

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

She also finds e which is coprime

PAGE NO. :
DATE : / /

to $(p-1)(q-1)$ & d which is inverse to e modulo $(p-1)(q-1)$

(N, e) is the public key.

& (N, d) is the private key.

Bob wants to send msg. to Alice.

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

M is the message.

& Bob encodes it to

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

& sends it to Alice.

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

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

$\Downarrow$

N

PAGE NO. :
DATE : / /

Primality V/s Factorisation :

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

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

One way to test if N is prime or not is 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.

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

If $x \sim 10^{154}$

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

Suppose 10^{40} primes per sec.

If all humans have a super-computer

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

$\Rightarrow$ to check all 10^{151} primary requires $\sim \frac{10^{151}}{10^{50}}$ sec.

$\sim 10^{101}$ sec

Age of the universe $\sim 10^{17}$ sec. $\Rightarrow$ (10^{-84} fraction of time)

Eg :

②

* Shor's like Howe solves funct

Def If of such

=>

21 X 5
105

PAGE NO. :
DATE : / /

∴ For primality use Fermat's Little Theorem:

Eg: ① $n = 151\,44781$, $a = 2$

$2^{n-1} = 2^{15144781} \equiv 1789293$ modulo 15144781

$\neq 1$

∴ n is not prime.

② $n = 15\,231691$

$a = 2, 3, 4, 5, 67$

& every time one finds

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

⇒ with very high prob. n is prime.

* Shor's Algorithm: allows one to factor a large number like N quickly.

However the prob. that it actually solves is finding the period of a periodic function very quickly.

Def: If a & N are relatively prime then the order of "a" modulo N is the smallest integer r such that $a^r = 1 \bmod N$

⇒ if $f(x) = a^x \bmod N$

then $f(x+r) = a^{x+r} \bmod N$

$= a^x \cdot a^r \bmod N$

$= a^x \bmod N$

$f(x+r) = f(x)$

PAGE NO. :
DATE : / /

=> $f(x)$ is periodic with period r.

Eg: $a = 5 \quad N = 21$

$5^0 = 1 \bmod 21$

$5^1 = 5 \bmod 21$

$5^2 = 4 \bmod 21$

⋮

$5^6 = 1 \bmod 21 \quad \boxed{r = 6}$

Efficient Period finding allows one to Break RSA without the need to find the factors p, q of N.

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

Using Efficient period finding one can find the period of $E(M)$ modulo N.

Let r be the order of $E(M)$ modulo N (assuming $E(M)$ & N are coprime, if they are not coprime then using Euclid's algo. We can find the factor of N)

$$\Rightarrow E(M)^r = M^{er} = 1 \bmod N$$

Find the inverse d' of e modulo r.
(it can be shown that e & r are coprime)

ie. $ed' = 1 \bmod r$

$\Rightarrow ed' = 1 + nr$

$\Rightarrow E(M)^{d'} = M^{ed'} = M^{1+nr}$

$= M (M^r)^n$

PAGE NO.:
DATE: / /

It turns out that if order of M^d modulated N is r then order of M modulo N is also r $\Rightarrow M^r = 1 \bmod N$

$\Rightarrow (M^{dr})^m = 1 \bmod N$

$\Rightarrow E(M)^{d'} = M \bmod N$

ie. RSA is broken without the need to find p & q.

Period finding & Factorization : (Method 2)

*E(M) not required to find p & q.

Suppose the period r of $E(M)$ modulo N is even

$$E(M)^r - 1 = 0 \bmod N$$

$$\Rightarrow [E(M)^{r/2} - 1][E(M)^{r/2} + 1] = 0 \bmod N.$$

Obviously $E(M)^{r/2} - 1 \neq 0 \bmod N$ (Def. of order r).

& suppose we are lucky so that

$$E(M)^{r/2} + 1 \neq 0 \bmod N$$

This $\Rightarrow$ that neither of the two terms $(E(M)^{r/2} - 1)$ or $(E(M)^{r/2} + 1)$ is a multiple of N but their product is the only factors of N are p & q.

$\Rightarrow$ $(E(M)^{r/2} - 1)$ is a multiple of p (or q)

& $(E(M)^{r/2} + 1)$ is a multiple of q (or p)

we will know if we find gcd of $(E(M)^{r/2} - 1)$ & N and also of $(E(M)^{r/2} + 1)$ & N using Euclid's Algo.

10^{200}

PAGE NO. :
DATE : / /

Shor's Algo:

(0) Generate a +ve integer b.

(1) Use Euclid's Algo to find if b & N are coprime. If not, then we have a factor of N. Problem Solved.

(2) Use quantum parallelism to compute $f(x) = b^x \bmod N$. on the superposition of i/p as

$$x \in (0, 1, 2, \ldots, 2^m - 1)$$
$$\text{with } N^2 \leq 2^m \leq 2N^2$$

& get the result in o/p register which is of size $n_o = \log_2 N$.

Optional step but we will follow this.

(2.a) Make a measurement on o/p register.

(2.b) Apply Quantum Fourier Transform on the i/p register.

(3) Measurement the i/p register with high prob. a value v close to a multiple of $2^m/r$ will be obtained (where r is period of $f(x)$)

(4) Use classical procedures to obtain a conjectured period $\tilde{r}$ from N.

(5) If $\tilde{r}$ is even follow the steps discussed to find the factors of N (using Euclid's Algo).

PAGE NO.:
DATE: / /

(6) Repeat the steps if necessary.

Quantum treatment of (2) & (3):

(2) Apply Hadamard-Walsh born:

$$\left[H^{\otimes m} \otimes \underbrace{I^{\otimes m_0}}_{2^m - 1} \right] |0\rangle_m |0\rangle_{m_0}$$

$$= \frac{1}{2^{m/2}} \sum_{x=0}^{2^m - 1} |x\rangle_m |0\rangle_{m_0}$$

Next we need to do modular exponential $f(x) = b^x \bmod N$.

A quantum subroutine for this exists & we will assume we are given the Unitary $U_{f(x)}$.

$$U_{f(x)} \left[\frac{1}{2^{m/2}} \sum_{x=0}^{2^m - 1} |x\rangle_m |0\rangle_{m_0} \right] = \frac{1}{2^{m/2}} \sum_{x=0}^{2^m - 1} |x\rangle_m |f(x)\rangle_{m_0}$$

As in Simon's Algo, make a measurement on o/p register. This will give a state $|f_0\rangle$ corresponding to $x = x_0$.

$$|\psi\rangle_m = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle_m$$

is the state of the i/p register corresponding to the measurement $|f_0\rangle$ in the o/p register.

m is the smallest integer satisfying $x_0 + mr \geq 2^m$

PAGE NO. :
DATE : / /

At this stage one applies Quantum Fourier Transform to $|x\rangle_n$ & this allows the x_0 dependence to come out of the state & appears as a phase factor.

* Fourier Transform:

$$\tilde{f}(\omega) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} e^{-i\omega t} f(t)\, dt$$

$$\tilde{f}(\omega_p) = \frac{1}{\sqrt{N}} \sum_{i=0}^{N-1} e^{-i\, \omega_p t_i} f(t_i)$$

↓ Frequency.

$N = 2^n$ → n-qubits.

Complexity:

DFT $\Rightarrow$ $O(N^2) \sim O(2^n \times 2^n)$

FFT $\Rightarrow$ $O(N \ln N) \sim O(n\, 2^n)$

QFT $\Rightarrow$ $O(n^2)$

$$\tilde{f}(y_j) = \sum_{i=0}^{N-1} K(y_j, x_i) f(x_i)$$

Suppose $\hat{K}$ is a n-qubit ope.

$$\hat{K}|x\rangle_n = \sum_y |y\rangle\langle y|\hat{K}|x\rangle$$

$$\Rightarrow \hat{K}|x\rangle = \sum_y K(y, x)|y\rangle$$

$$\hat{K} \sum_x f(x)|x\rangle \qquad \left(\sum |f(x)|^2 = 1\right)$$

↳ Normalized

$$\Rightarrow \sum_x f(x)\hat{K}|x\rangle$$

PAGE NO.:
DATE: / /

$$\Rightarrow \sum_x f(x) \sum_y K(y,x)|y\rangle$$

$$\Rightarrow \sum_x f(x) \sum_y K(y,x)|y\rangle$$

$$\Rightarrow \sum_y \left(\sum_x K(y,x) f(x) \right) |y\rangle$$

Discrete Integral Transform of $f(x)$

$$\Rightarrow \hat{K} \sum_x f(x)|x\rangle = \sum_y \tilde{f}(y)|y\rangle$$

where $\tilde{f}(y) = \sum_x K(y,x) f(x)$

For QFT the function $K(y,x)$ is given by

$$K_m(y,x) = \frac{e^{-2\pi i xy/2^m}}{2^{m/2}}$$

Ex: Prove that $K_m(y,x) = \frac{e^{-2\pi i xy/2^m}}{2^{m/2}}$

is Unitary $\Rightarrow K_m^{-1}$ (U_{FT} exists)

PAGE NO.:
DATE: / /

$n = 1$

$$K_n = K_1(x,y) = \frac{e^{-2\pi i xy/2^1}}{\sqrt{2}}$$

& x, y takes 0 & 1

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

Ex: Check for $n = 2$ (so that K is 4×4 Matrix)

$$K_2(y,x) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & -1 & 1 & -1 \\ 1 & -i & 1 & -i \end{pmatrix}$$

Walsh-Hadamard Transform Versus QFT:

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

$$x.y = x_{n-1} y_{n-1} \oplus x_{n-2} y_{n-2} \oplus \cdots \oplus x_0 y_0$$

$$U_{fft} |x\rangle_n = \frac{1}{2^{n/2}} \sum_{y=0}^{2^n-1} e^{-2\pi i xy/2^n} |y\rangle_n$$

xy is the usual or ordinary multiplication for two integers.

$e^{2\pi i} = 1$

PAGE NO.:
DATE: / /

Implementation of QFT:

$n = 1$ $\quad U_{FT}^{(1)} = H$ as seen.

$$U_{FT}^{(1)} |x\rangle_1 = \frac{1}{\sqrt{2}} \sum_{y=0}^{1} e^{-\pi i x y} |y\rangle$$

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

$U_{FT}^{(1)} |x\rangle_1 = H|x\rangle$ (as seen)

$x \longrightarrow \boxed{H} \longrightarrow U_{FT}^{(1)} |x\rangle$

$n = 2$

$$U_{FT}^{(2)} |x\rangle_2 = \frac{1}{2} \sum_{y=0}^{3} e^{-2\pi i x y / 2^2} |y\rangle$$

Now $|x\rangle_2 = |x_1\rangle |x_0\rangle$ $\quad |y\rangle_2 = |y_1\rangle |y_0\rangle$

$$\Rightarrow \frac{1}{2} \sum_{y_0, y_1 = 0}^{1} e^{\frac{-2\pi i x (2^1 y_1 + 2^0 y_0)}{2^2}} |y_1, y_0\rangle$$

$$\Rightarrow \frac{1}{2} \left[\sum_{y_1=0}^{1} e^{-\pi i (2x_1 + 2^0 x_0) y_1} |y_1\rangle \right] \otimes \left[\sum_{y_0=0}^{1} e^{\frac{-\pi i (2^1 x_1 + 2^0 x_0) y_0}{2^2}} |y_0\rangle \right]$$

$$\Rightarrow \frac{1}{2} \left[|0\rangle + e^{-\pi i (2x_1 + x_0)} |1\rangle \right] \otimes \left[|0\rangle + e^{\frac{-\pi i (2x_1 + x_0)}{2}} |1\rangle \right]$$

$$\Rightarrow \frac{1}{2} \left[|0\rangle + (-1)^{x_0} |1\rangle \right] \otimes \left[|0\rangle + e^{-\pi i x_0/2} (-1)^{x_1} |1\rangle \right]$$

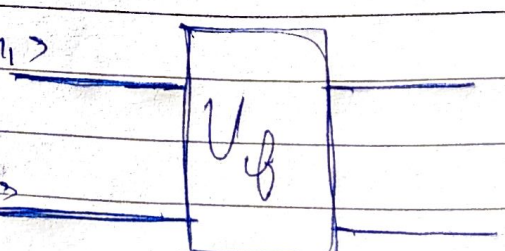
This acts only when $x_0 = 1$

$\mathcal{B}$ is like a controlled gate which we call.

$B_{01}^{(x_0)}$

↓ ↳ Target

Control



PAGE NO.:
DATE: / /

Notice that B is controlled phase shift.

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

or

$$B = \left(|0\rangle\langle 0| + e^{i\theta} |1\rangle\langle 1| \right) |0\rangle$$

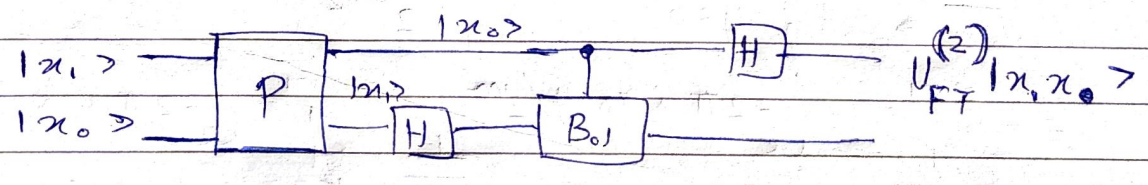
$$U_{FT}^{(2)} |x_1 x_0\rangle = \frac{1}{2} \left[|0\rangle + (-1)^{x_0} |1\rangle \right] B_{01}^{(x_0)} \left[|0\rangle + (-1)^{x_1} |1\rangle \right]$$

Looks very much like the action of H except that instead of x_1, x_0 appears in the first bracket & instead of x_0, x_1 appears in the 2nd bracketed term.

This suggests that we SWAP the qubits $|x_1\rangle$ & $|x_0\rangle$ before applying any other gate.

$$P|x_1 x_0\rangle = P(|x_0 x_1\rangle)$$

$$(H \otimes I)\, B_{01}^{x_0}\, (I \times H)\, P |x_1 x_0\rangle \Rightarrow \text{Final}$$



$$U_{FT} \{ f(x) |x\rangle_2 = \sum_{x,y} f(x) K_{(y,x)} |y\rangle$$

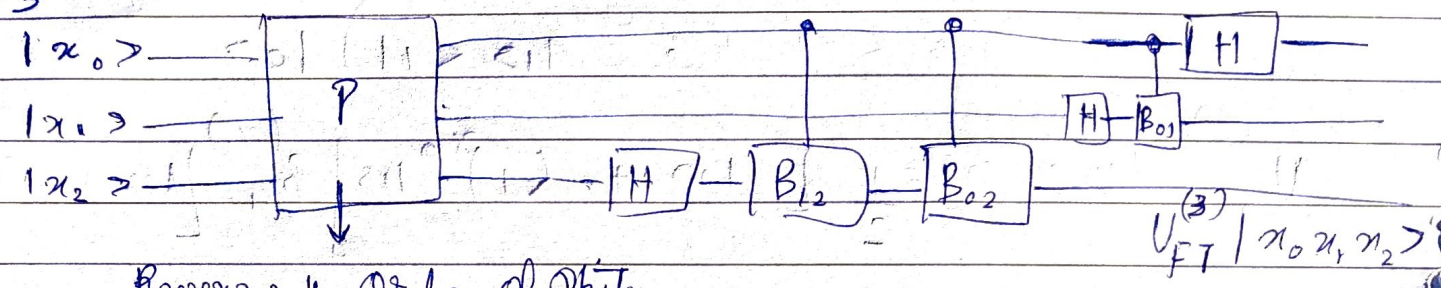
$$= \sum_{y} \tilde{f}(y) |y\rangle$$

PAGE NO. :
DATE : / /

where $B_{01}^{x_0} = |0\rangle\langle 0| \otimes \mathbb{I} + |1\rangle\langle 1| \otimes B$

$B = |0\rangle\langle 0| + e^{-\pi i/2} |1\rangle\langle 1|$

$n = 3$



Reverses the Order of bits

$n \rightarrow$ H gates

$\frac{n(n-1)}{2} \rightarrow$ B gates (2 Qubit Controlled

$O(n^2) \rightarrow$ Complexity

We know

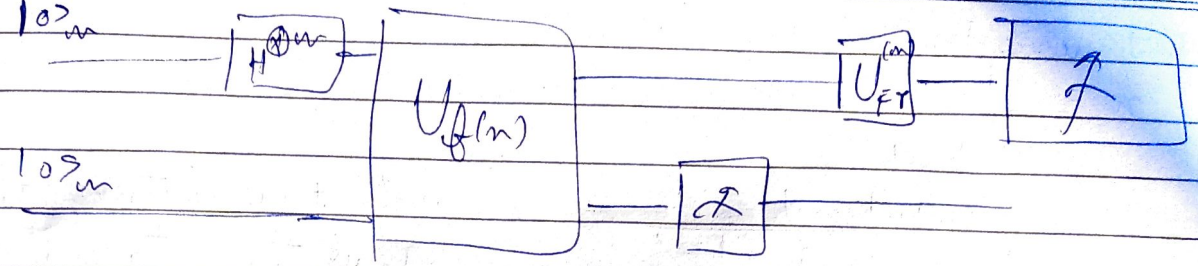
$$|\psi\rangle_n = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} |x_0 + kr\rangle$$

$$U_{FT}^{(n)} |\psi\rangle_n = \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} U_{FT} |x_0 + kr\rangle$$

$$= \frac{1}{\sqrt{n}} \sum_{k=0}^{n-1} \sum_{y=0}^{2^n-1} \frac{e^{-2\pi i (x_0 + kr) y / 2^n}}{2^{n/2}} |y\rangle$$

$$= \sum_{y=0}^{2^n-1} e^{-2\pi i x_0 y / 2^n} \frac{1}{\sqrt{2^n n}} \sum_{k=0}^{n-1} e^{-2\pi i k r y / 2^n} |y\rangle$$

Continued



Make a measurement on the i/p register & it will give one of the states $|y_j\rangle$ in the above superposition

$$p(y_j) = \frac{1}{2^m m} \left| \sum_{k=0}^{m-1} e^{-2\pi i k r y_j / 2^m} \right|^2$$

$$p(y_j) = \frac{1}{2^m m} \frac{\sin^2 \pi m r y_j / 2^m}{\sin^2 \pi r y_j / 2^m}$$

It turns out that when we make a measurement then those states $|y\rangle$ for which y is close to an integral multiple of $\frac{2^m}{r}$ occur with high prob.

$$y = j\frac{2^m}{r} + \delta_j \,, \quad j \in \mathbb{Z}$$

$$|\delta_j| < 1/2$$

$$p(y) \approx 0.9$$

ie $$\left| \frac{y}{2^m} - \frac{j}{r} \right| < \frac{1}{2^{m+1}} \qquad m > 2n_0$$
(will be required later)

Theorem:

-> If x is an estimate of j/r that differs from it by less than $1/2^{2n_0}$ then j/r appears as one of the partial sums in the continued fraction expansion of x.

PAGE NO. :
DATE : / /

Continuous Fraction Expansion

$$x = \cfrac{1}{a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + 1/a_3 + \cdots}}}$$

with +ve integers a_i.
a_0 is the integral part of $1/x$

$\Rightarrow x = 1/a_0 + R \rightarrow$ Remainder

Ex: Suppose $n_0 \Rightarrow 2m = 14$

$\Rightarrow 2^{2m} = 2^{14} = 16384$

$r < N \Rightarrow r < 2^7$ or $r < 128$

Let $y_1 = 11343$

$$\frac{11343}{2^{14}} = \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{1 + \cfrac{1}{4\,19}}}}}$$

$4\,19 > 128$ Therefore don't go beyond it.

$$\Rightarrow \frac{11343}{2^{14}} = \frac{1}{1 + 1/2 + 1/3 + 1} \Rightarrow \frac{1}{1 + 1/2 + 1/4} = \frac{1}{1 + 4/9} = \frac{9}{13}$$

$$\therefore \frac{y}{r} = \frac{y'}{r'} = \frac{9}{13}$$