Week-3

Date 25/6/21

1. Deutsch problem

1. part 1. Algo for Deutsch's problem. } Mathematical model of BM.

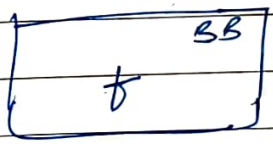
(1) Deutsch problem is about a fxn, that maps one bit to one bit.

$$f: \{0,1\} \longrightarrow \{0,1\}$$

$f(x) = 0$ } constant
$f(x) = 1$ }

$f(x) = x$ } balanced
$f(x) = \bar{x}$ }

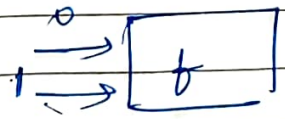
(2) The fxn is implemented as a black box on oracle.



It is very slow.
It takes 24 hrs for 1 query.

Q:- This BB fxn is constant or balanced? How much time do we need to answer it.

in classical



24 + 24 hrs.

in Quantum :- we have one oracle.

$\|U|x\rangle\| \longrightarrow \|x\|$

FREEMIND

Date 25/6

Page

The Quantum oracle.

$f : \{0,1\} \to \{0,1\}$

① $U_f |x\rangle \to |f(x)\rangle$ ✗

$f = \text{const} = 0$ then $U_f |0\rangle \to |0\rangle$ (f(0)) } Not unitary.

$U_f |1\rangle \to$ ~~|1⟩~~ |0⟩

② $U_f |x\rangle |0\rangle \to |x\rangle |f(x)\rangle \Rightarrow |x, f(x)\rangle$

$|00\rangle \to |0\rangle |f(x)\rangle$ or $|0 f(x)\rangle$

$|10\rangle \to |1, f(x)\rangle$

$U_f |x\rangle |1\rangle \to |x\rangle |1 \oplus f(x)\rangle$ } Unitary as it maps orthonormal basis to orthonormal basis.

③ $U_f |x\rangle |y\rangle \to |x\rangle |y \oplus f(x)\rangle$

↳ $\oplus$ = ~~[illegible]~~ X-or operⁿ.

④ * $U_f \frac{1}{\sqrt{2}} |x\rangle \underbrace{(|0\rangle - |1\rangle)}_{1 \to}$

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

$= \frac{1}{\sqrt{2}} \left(U_f |x\rangle |f|x\rangle - U_f |x\rangle |1 \oplus f(x)\rangle \right)$

if $f(x) = 0 \Rightarrow \frac{1}{\sqrt{2}} \left(|x\rangle |0\rangle - |x\rangle |1\rangle \right) = |x\rangle (|0\rangle - |1\rangle)$

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

$U_f \frac{1}{\sqrt{2}} |x\rangle (|0\rangle - |1\rangle)$

Date 28/1

Page

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

$\therefore$ when $f(x) = 0$ — i/p initial state only

$f(x) = 1$ — i/p state (-ve).

2. Deutsch problem part 2.

The Quantum Oracle :

4 functions that maps one bit to one bit.

↳ & the corresp Quantum operator implementation.

(1) $f(x) = 0$

$U_f |x\rangle |y\rangle \rightarrow |x\rangle |y \oplus f(x)\rangle$ ($f(x) = 0$)

$= |x\rangle |y\rangle$.

$\therefore U_f = I$ (Identity matrix)

4×4 as 2 qubits

i/p

$|x\rangle$ ———

$|y\rangle$ ———

$\therefore f(x) = 0$ $|x\rangle$ ———

$U_f = I$ $|y\rangle$ ———

FREEMIND

Date

Page

② $f(x) = 1$

$U_f |x\rangle |y\rangle \longrightarrow |x\rangle |y \oplus f(x)\rangle$ — $= 1$

$|x\rangle |y \oplus 1\rangle$

matrix.

$\begin{cases} y=0 & 0 \oplus 1 = 1 \\ y=1 & 1 \oplus 1 = 0. \end{cases}$ flips

$|x\rangle$ ——————

$|y\rangle$ —— X ——

$\begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix}$

$U_f = I \otimes X$ $\quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes X = \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix}$

$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \Rightarrow$

	00	01	10	11
00	0	1	0	0
01	1	0	0	0
10	0	0	0	1
11	0	0	1	0

$f(x) = 1$

$U_f = I \otimes X$

$|x\rangle$ ——————

$|y\rangle$ —— X ——

balanced fns

③ $f(x) = x$, consider diff. vectors.

$|xy\rangle$	o/p	$y \oplus x$	$y \oplus x$
$\|00\rangle \rightarrow$	$\|00\rangle$	$0 \oplus 0 = 0$	$\|x\rangle$
$\|01\rangle \rightarrow$	$\|01\rangle$	$1 \oplus 0 = 1$	
$\|10\rangle \rightarrow$	$\|11\rangle$	$0 \oplus 1 = 1$	
$\|11\rangle \rightarrow$	$\|10\rangle$	$1 \oplus 1 = 0$	

$\therefore$ CNOT $= U_f$.

$f(x) = x$

U_f = CNOT

$|x\rangle$ ——●——

$|y\rangle$ —— X ——

FREEMIND

Date

Page

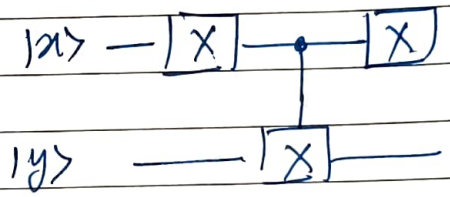
④ $f(x) = \bar{x}$

$$U_f |x\rangle |y\rangle \longrightarrow |x\rangle (|y \oplus f(x)\rangle) \quad (f(x) = \bar{x})$$

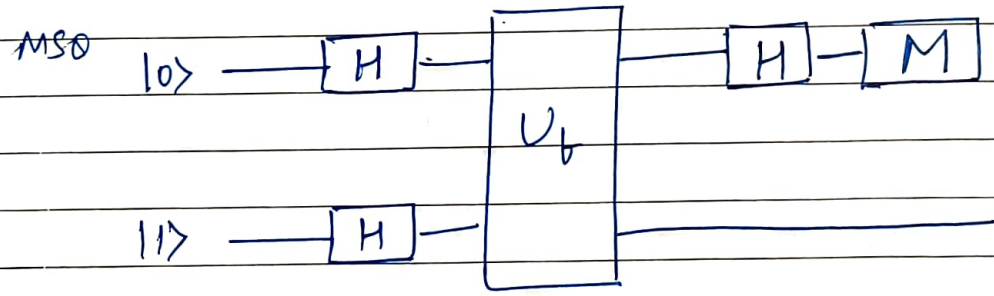
xy		x y	$y \oplus f(x) = y \oplus \bar{x}$
$\|00\rangle$	$\longrightarrow$	$\|0\ 1\rangle$	$0 \oplus 1 = 1$
$\|01\rangle$	$\longrightarrow$	$\|0\ 0\rangle$	$1 \oplus 1 = 0$
$\|10\rangle$	$\longrightarrow$	$\|1\ 0\rangle$	$0 \oplus 0 = 0$
$\|11\rangle$	$\longrightarrow$	$\|1\ 1\rangle$	$1 \oplus 0 = 1$

$$U_f = \begin{pmatrix} X & 0 \\ 0 & I \end{pmatrix}$$

$$U_f = \begin{array}{c} \begin{matrix} 00 & 01 & 10 & 11 \end{matrix} \\ \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{matrix} 00 \\ 01 \\ 10 \\ 11 \end{matrix} \end{array}$$



⑪ Deutsch's Algo : The circuit.



{①, ②, ③, ④} any one

① $|x\rangle$ —— $|y\rangle$ ——

② $|x\rangle$ —— $|y\rangle$ —[X]—

③ $|x\rangle$ —●— $|y\rangle$ —[X]—

④ $|x\rangle$ —[X]—●—[X]— $|y\rangle$ —[X]—

FREEMIND

Date

Page

① $|01\rangle \xrightarrow{H\,H} \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle)$

$= \frac{1}{2}(|0\rangle(|0\rangle - |1\rangle) + \frac{1}{2}(|1\rangle(|0\rangle - |1\rangle)$

$= \frac{1}{2}(|0\rangle(|0\rangle - |1\rangle)) + \frac{1}{2}(|1\rangle(|0\rangle - |1\rangle))$

② Apply U_f.

$\xrightarrow{U_f} \frac{1}{2}(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + \frac{1}{2}(-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)$

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

$(|0\rangle - |1\rangle) \to |-\rangle$

(i) Let $f(x)$ = constant $\quad f(0) = f(1) = 0$

$= \frac{1}{2}(|0\rangle + |1\rangle)\,|-\rangle$

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

$|+\rangle \xrightarrow{H} |0\rangle$

$\frac{1}{2} \xrightarrow{H} |0\rangle$

$|0\rangle$

(ii) f = const. $\quad f(0) = f(1)$

$= \frac{1}{2}(|0\rangle - |1\rangle)\,|-\rangle$

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

Date

Page

(12)

$\frac{1}{2}$ $|+\rangle$ $|-\rangle$ → H M → o/p $|0\rangle$

or

$\frac{1}{2}$ $|-\rangle$ $|-\rangle$ → HM → o/p $|1\rangle$.

But, we still don't know which fun stays in U_f. (B. Black box)

time = 24 hrs, as only one query.

* http://qc-sim.appspot.com] – check

U_f = CNOT

$|0\rangle$ — H — * — H — 1

$|1\rangle$ — H — X — 1

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

2^n terms; y is a no.

H_n maps the i/p vector $|x\rangle$ to a sum of all possible o/p basis vectors $|y\rangle$ in space.

co-eff of $|y\rangle$ are $+1$ or -1 depending on the i/p vector x.

$x \cdot y$ = inner product.

$= x_0 y_0 \oplus x_1 y_1 \oplus \cdots \oplus x_{n-1} y_{n-1}$

$(\mathbb{Z}_2)^n$

2. & computer Prototype

1. & Comp. - DIY.

Grahan → Mohsan

Date 25/6/21

Page

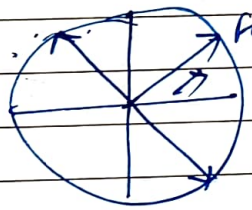
principle of operation :-

① 2 qubits are carried by one photon on particle.
   ↳ Qubit 1 → position
   ↳ Qubit 2 → polarization.

② Measurement - interference pattern.

⇒ CNOT → entangled qubits.
Waveplates → act as gates

2. & Comp. part - 2.



↑ → |1⟩ (2nd qubit)
→ → |0⟩
horizontal polarn

|1⟩ → left path
|0⟩ → Right path.

3. More Quantum Algorithms. 5/7/21

① Part-1.

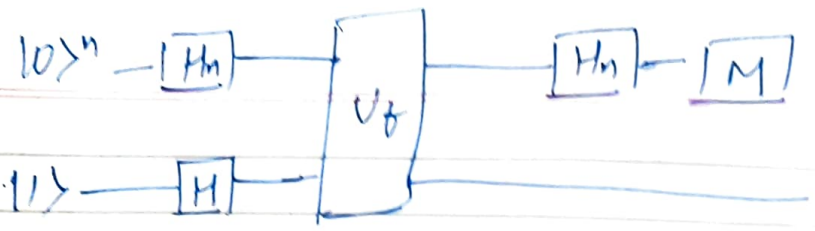
① Deutsch - Jozsa Problem. - 1992

$f: \{0,1\}^n \longrightarrow \{0,1\}$

an oracle fxn that maps 'n' bits to 1 bit.

↳ constant - or
↳ balanced. fxns are fxns that return equal amounts of 1's & 0's.

$$|x: f(x) = 1| = |x; f(x) = 0|$$



Applying n-qubit Hadamard Transform

① $|0\rangle^n |1\rangle \xrightarrow{H_{n+1}} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle)$

② Apply Q. oracle on this state

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

concentrate on this register value

This will be transferred as it is

$\xrightarrow{H_n} \xrightarrow{M}$

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

③

① Let $f(x)$ = constant :

then $(-1)^{f(x)}$ can be put outside

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

$|000\ldots0\rangle$

'n' zeros

FREEMIND

Date

Page

② If $f(x)$ = balanced, then

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

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

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

Now, formula for Hadamard transform is {standard ;) }

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

① vector $|y\rangle$ is all zeroes. $|y\rangle = |00\ldots0\rangle$

$x \cdot y = 0 \quad (-1)^0 = +1$

∴ for any vector $|x\rangle$

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

& we have equal amounts of $\frac{1}{2^{n/2}} \left(\sum_{x:f(x)=0} |x\rangle - \sum_{x:f(x)=1} |x\rangle \right)$ ① & ②

① & ② elements, because the fxn is balanced

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

$2^{n-1}|00\ldots0\rangle \quad -\left(2^{n-1}|00\ldots0\rangle\right)$ (+, −)

∴ these vectors will self-destruct

∴ o/p = No vector of all zeros

Measure.

FREEMIND

Date

Page

④ $\xrightarrow{M}$

when we measure the result, we obtain any other vector, except $|0\rangle^n$.

So, only after 1 application query to the quantum oracle, we can distinguish balanced & constant fns.

M ↓ → No $|0\rangle^n$ o/p

M ↓ → only $|0\rangle^n$ o/p

* This self-destruction is related to interference.

② Bernstein - Vazirani problem 1993

$f: \{0,1\}^n \longrightarrow \{0,1\}$. } fxn maps n-bits to 1 bit

$f(x) = a \cdot x$ → find number 'a'

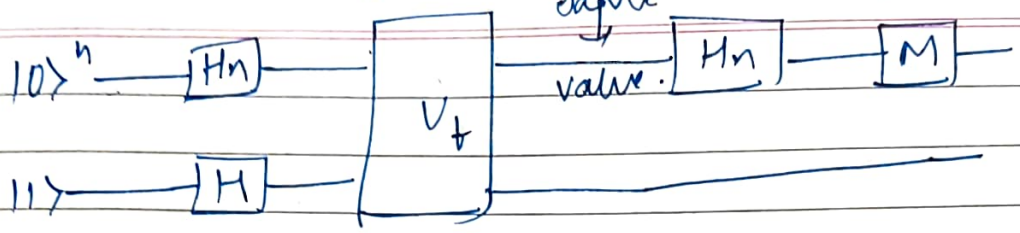
in - classical case.

i/p: $0\ 0\ 0 \ldots \underset{\uparrow i}{1} 0 \ldots 0$

since a = n-bit we need n oracle queries

1 is only one place to obtain diff. bits of a

In Quantum, only 1 oracle query



$$|0\rangle^n|1\rangle \xrightarrow{H_{n+1}} \frac{1}{2^{\frac{n+1}{2}}} \sum_{x=0}^{2^n-1} |x\rangle (|0\rangle - |1\rangle) \xrightarrow{U_f}$$

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

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

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

$$H|a\rangle$$

So, after $-[H_n]-[M]$, we will get as a result of measurement, the value of 'a' in just one oracle query.

Week-3

(2) # Part-2

Date 5/7/21

Page

(1) # Simon's Algo. Problem

$f: \{0,1\}^n \longrightarrow \{0,1\}^n$

~~n-bits to n-bits~~

$\exists\, !\, a \neq 0 : \forall x\ f(x) = f(y) \iff y = x \oplus a$

proved $\mathbb{Z}_2$

$\mathbb{Z}$ mod 2

i/p => x

Find 'a'.

for some i/p x, $(x \oplus a)$ does not change fxn value.

'f' is implemented as an oracle.

Complexity :-

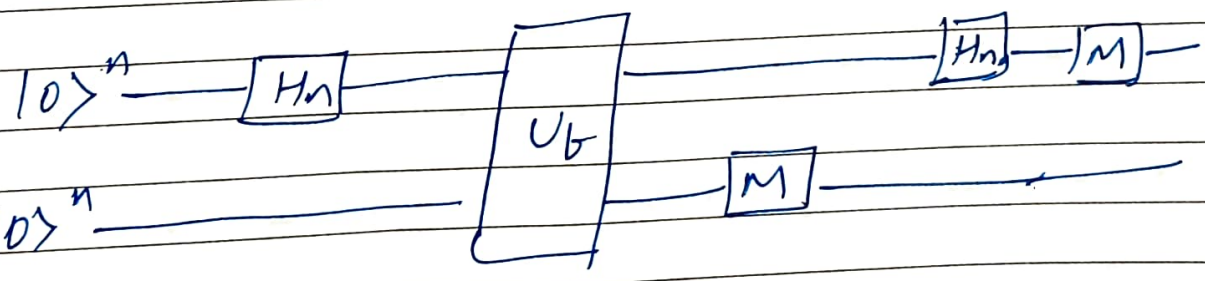
① storage, if $n = 1000$, 2^{1000} values storage capacity req.

② $(2^{n-1}+1)$ fxn queries in worst case

· Time

for classical case.

⇒ For Quantum case :



$y \cdot (x \oplus a)$

FREEMIND

Date

Page

$$|0\rangle^n |0\rangle^n \xrightarrow{H_n} \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x\rangle |0\rangle^n \xrightarrow{U_f}$$

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

$\downarrow M$

$$\frac{1}{\sqrt{2}} \left(|x_0\rangle + |x_0 \oplus a\rangle\right) |f(x_0)\rangle \quad \text{for } x = x_0.$$

$$\Rightarrow \underbrace{\frac{1}{\sqrt{2}} \left(|x\rangle + |x \oplus a\rangle\right) |f(x)\rangle}$$

$\downarrow H_n$.

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

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

if $a \cdot y = 0 \Rightarrow \sum_{y:\, a \cdot y = 0} |y\rangle \xrightarrow{H_n}$ we get one of the $|y\rangle$ vectors.

$\therefore$ $y \cdot a = 0$

eq^n to be solved

① we need n linearly indep. y's to obtain the complete value of a.

$\therefore$ we need the sum this algo $\boxed{O(n)}$ times.

Date 5/7/21.

Quantum computer Simulator =.

qc.sim.appspot.com → not available.

⇒ Week - 4

- Shor's Algo. ← 1, 2
- factoring & RSA ← 1, 2, 3
- Shor's Algo. ← 1, 2, 3, 4, 5, 6.

1.#i. Intro.

8/7/21.

Shor's Algo: 1994.

Polynomial time algos for discrete logarithms & factoring on a quantum computer.

2 prime nos = p & q
↳ 10,000

$N = pq$. , Now, we have to get pq.

find p & q.

2 ... $\sqrt{N}$. } Brute force

No classical algo better than brute force.

RSA → Encryption Algo. https

1973. → 1977

Rivest Shamir Adleman Algo.

→ factoring & RSA
→ n & Period finding
→ QFT
→ Algo Part 1
→ Part 2

#2 factoring & the RSA

Date 12/7/21

Page

RSA Algo.

$N = pq$ $\quad p \neq q$

$\forall a < N : (a, N) = 1$

$a^{\phi(N)} = 1 \ (N)$ → Theorem

$e < N$,

$(e, N) = 1$

$(e, \phi(N)) = 1$

$\phi(N) = \phi(pq)$

$\phi(p) = p - 1$

$\phi(q) = q - 1$

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

If (e') is invertible in the ring $\mathbb{Z}_{\phi(N)}$.

d is the inverse of e.

$\Rightarrow \quad e < N, \ (e, N) = 1, \ (e, \phi(N)) = 1$

$\exists d < N : \quad ed = 1 \ (\phi(N))$

$\exists d, k : \quad ed + \phi(N)k = 1$ gcd.

(e, N) public key.

(d, N) private key.

Message $= m$, $(m, N) = 1$ — m should be coprime with N.

$m^e \ (N)$ ⇒ encode m with public key

$m^e \bmod N$.