Quantum Computer

Things To know befor start

Reversible Computing

- func와 output을 안다면 (input)을 알 수 있음

quantum computing에서 필요한 개념

Von Neumann Vander Limit

⇒ 가능한 최소한의 계산을 위해 필요한 에너지

tensor product of vector

$$\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \otimes \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} = \begin{pmatrix} x_0 \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \\ x_1 \begin{pmatrix} y_0 \\ y_1 \end{pmatrix} \end{pmatrix} = \begin{pmatrix} x_0 y_0 \\ x_0 y_1 \\ x_1 y_0 \\ x_1 y_1 \end{pmatrix}$$

⇒ example $\begin{pmatrix} 1 \\ 2 \end{pmatrix} \otimes \begin{pmatrix} 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 3 \\ 4 \\ 6 \\ 8 \end{pmatrix}$

Operation on one classical bit

Cbit

- Identity $f(x)=x$ $\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$
- Negation $f(x)=\bar{x}$ $\begin{pmatrix}0&1\\1&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$ inverse
- Constant-0 $f(x)=0$ $\begin{pmatrix}1&1\\0&0\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$ fix
- Constant-1 $f(x)=1$ $\begin{pmatrix}0&0\\1&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}$ fix

Classical Gate

* multiple cbits

'0'이 2개

$00 \Rightarrow \begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}1\\0\\0\\0\end{pmatrix}$ product state

'1'(역순) $10 \Rightarrow \begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}=\begin{pmatrix}0\\0\\1\\0\end{pmatrix}$ 그게 맞다.

NAND GATE

INPUT		OUTPUT
A	B	A NAND B
0	0	1
0	1	1
1	0	1
1	1	0

⇒ only returns 'False' when Inputs are 'ALL TRUE'

*CNOT : analogus NAND gate for Reversible Computing

operation on multiple cbits

⇒ CNOT conditional NOT

00 → 00 * control bit이 '0'이라면 target bit를 바꾼다

01 → 01

10 → 11 * control bit이 '1'이라면

11 → 10 target bit을 뒤집는다.

control bit ↑ target bit

'CNOT' Gate

$C|10\rangle = C\left(\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right)=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\end{pmatrix}\Rightarrow\begin{pmatrix}0\\0\\0\\1\end{pmatrix}=\begin{pmatrix}0\\1\end{pmatrix}\otimes\begin{pmatrix}0\\1\end{pmatrix}=|11\rangle$

Quantum Entanglement 에서 제일 중요한 개념

Q bits ≙ 'C bits' one unique case of Q bits

* how to re present
  - ⇒ $\begin{pmatrix} a \\ b \end{pmatrix}$
    - ↳ a, b are Complex Numbers
    - ↳ $\|a\|^2 + \|b\|^2 = 1$
  - example $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{3}} \end{pmatrix}, \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}$ ...etc..

Multiple Q bits

two Qbits

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \otimes \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \\ \frac{1}{2} \end{pmatrix}$$ ← product state

$\left\|\frac{1}{2}\right\|^2 = \frac{1}{4}$ (4 chances $|00\rangle, |10\rangle, |01\rangle, |11\rangle$) $\quad \frac{1}{4} \times 4 = 1$ always

Super Positions

* measure → collapses to '0' or '1' (fix)
  - ⇒ usually do this at the end of a Q computation to get the final result

* $\begin{pmatrix} a \\ b \end{pmatrix}$ ⇒ $\|a\|^2$ probability to collapse to '0'
  $\|b\|^2$ probability to collapse to '1'

example. $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ 100% to '0' / $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ 100% to '1' / $\begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} \Rightarrow \left\|\frac{1}{\sqrt{2}}\right\|^2 = \frac{1}{2}$

$\frac{1}{2}$ chance of (0) or (1)

Hadamard Gate

takes 0 or 1 bit ⇒ puts it into equal superposition

- example $H|0\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix}$ / $H|1\rangle = \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} \end{pmatrix}$

Hadamard Gate (1) super positim

why negative here! Don't get it

⇒ to be reversible, 0, 1 valuse would be the same

* Q bits ⇒ Chits

using Hadamard Gate

$\begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{pmatrix} \begin{pmatrix} \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$

Hadamard Gate — 'Qbit' instead of 'Cbit' — Cbit

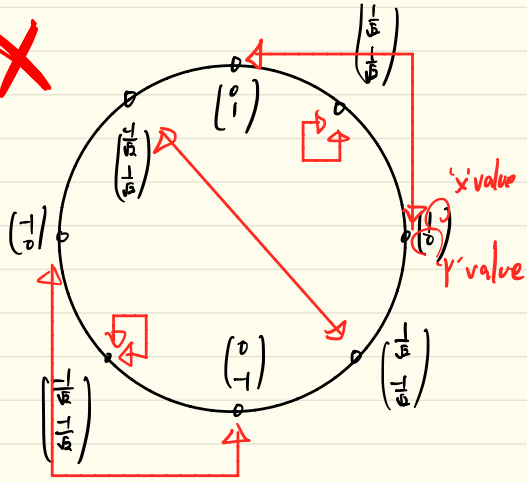
⇒ Suggesting that

Chits ⇒ Convert into Qbits ⇒ do the R stuff ⇒ Qbits ⇒ Chits ⇒ Classical computer output to

What Hadamard Gate could do

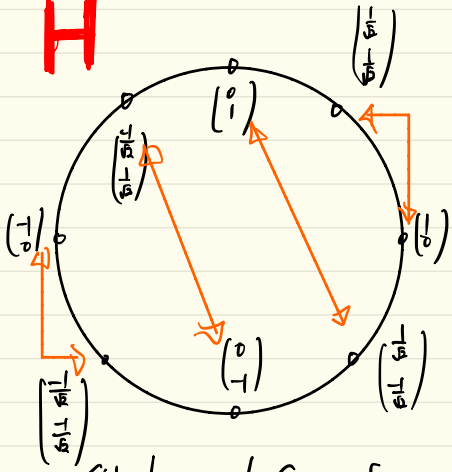
Unit Circle State Machine ⇒ Trigonometry

X



<bit flip operation>

H

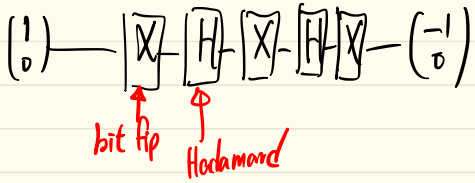


<Hadamard Gate>

#wit Complex Number ⇒ sphere

bloch sphere

Quantum Circuit notation

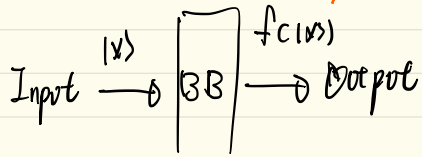


The Deutsch oracle

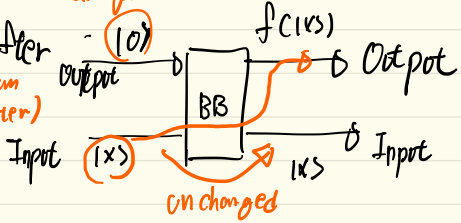
make non-reversible func to reversible way

⇒ constant → Variable
to

: Before (traditional computer)

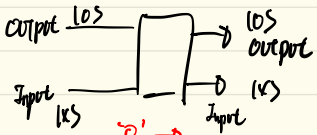


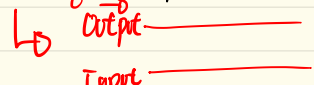
: After (Quantum Computer)



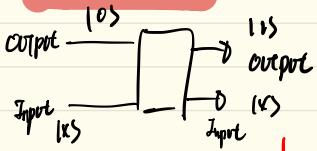
The Deutsch oracle

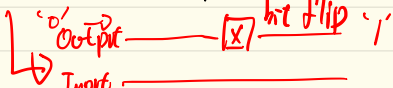
: Constant-0



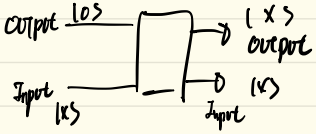


: Constant-1

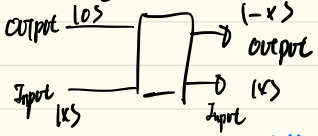


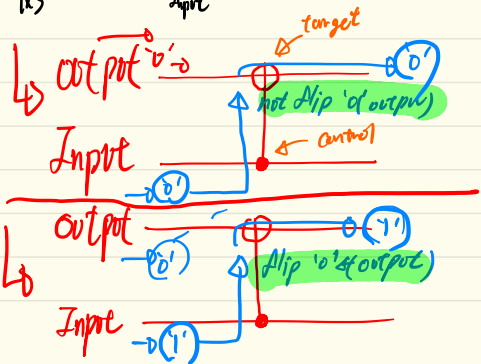


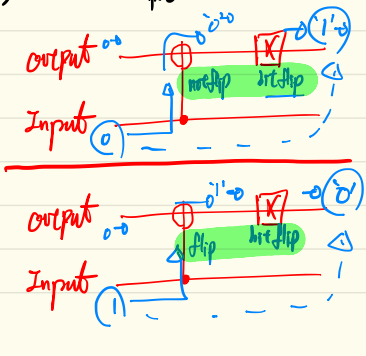
: Identity



: Negation

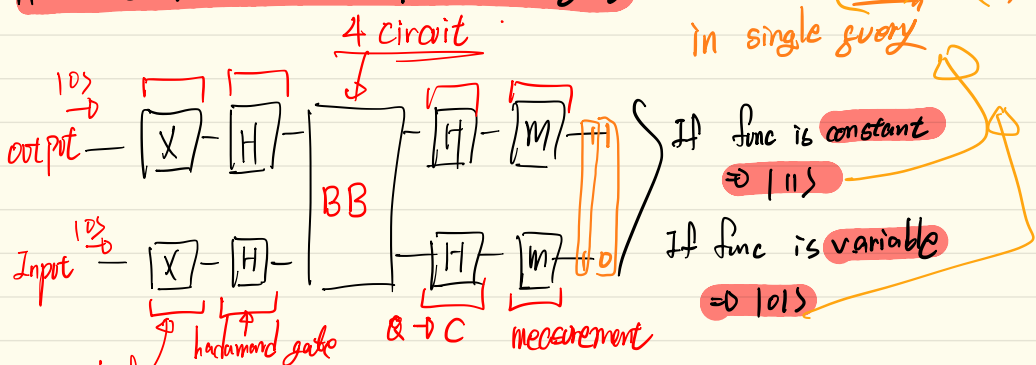


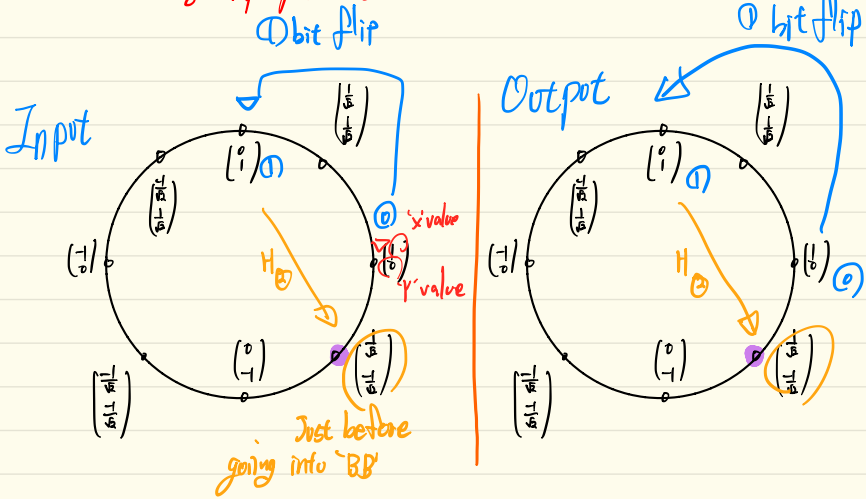




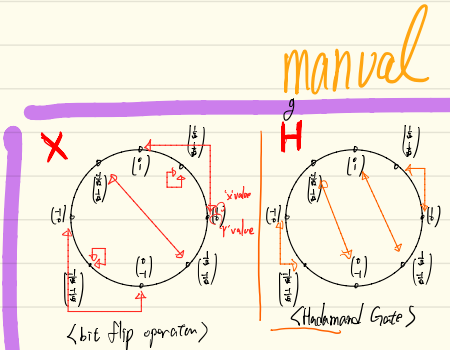
How do we solve it on a Computer in 1 query

able to find out if system is Var or Con in single query

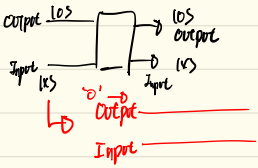




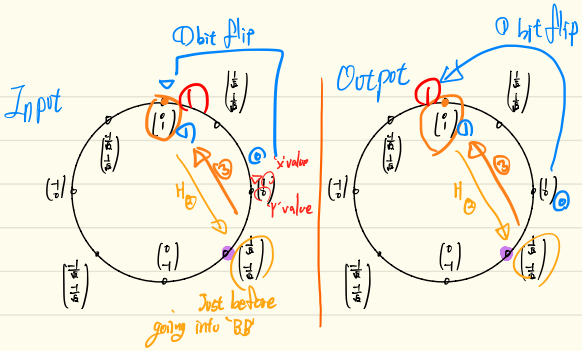
manual



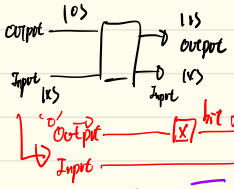
constant-0



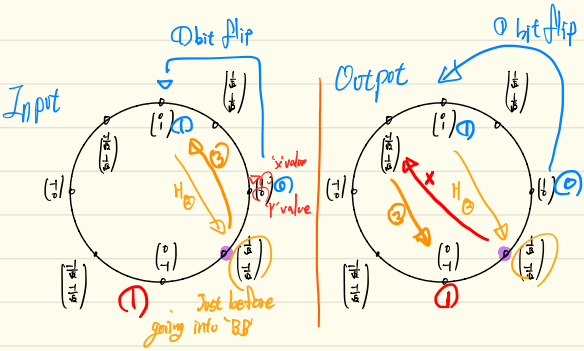
result : |1⟩ ⇐ consent



constant-1



result : |1⟩ ⇐ consent



Identity

*CNOT

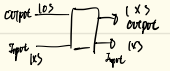
$$C\left(\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}\otimes\begin{bmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{bmatrix}\right)=\begin{bmatrix}\frac{1}{\sqrt{2}}\\ 0\\ 0\\ \frac{1}{\sqrt{2}}\end{bmatrix}=\frac{1}{2}\begin{bmatrix}1\\ -1\\ -1\\ 1\end{bmatrix}=\begin{bmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{bmatrix}\otimes\begin{bmatrix}\frac{1}{\sqrt{2}}\\ -\frac{1}{\sqrt{2}}\end{bmatrix}$$

CNOT Gate

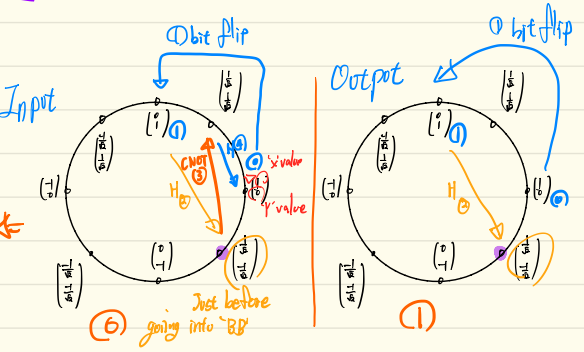
$$\begin{bmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{bmatrix}$$

changed!

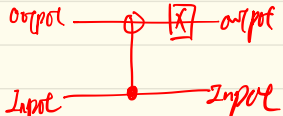
make it readable



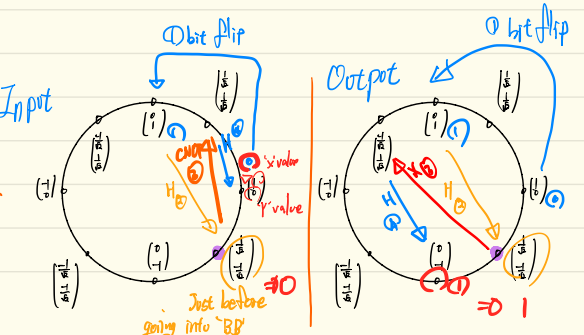
result : |0⟩ ⇐ various



negation



result : |0⟩ ⇐ various



Intuition

Don't get it

- the difference within the categories ⇒ negation
  - ⇒ neutralized (minimize)
- while, the difference between the categories
  - ⇒ magnified ⇒ (NOT)

find more

① Simon's periodicity problem.

② shores Algorithm

Quantum Entanglement

If the product state of two Qbits can't be factored

⇒ we can say its Entangled

⇒ Once Entangled, it's instantaneous (faster than light)

⇒ when you measure one Qbit, then the other (entangled one) is instantaneously collapse
(=fixing the state)

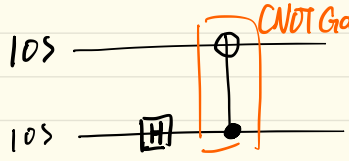
because they are entangled
you just know the state of the other Qbit

Unfactorable state = Entangled

$$\begin{pmatrix} \frac{1}{\sqrt{2}} \\ 0 \\ 0 \\ \frac{1}{\sqrt{2}} \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} \otimes \begin{pmatrix} c \\ d \end{pmatrix} \Rightarrow \begin{cases} ac = \frac{1}{\sqrt{2}} \\ ad = 0 \\ bc = 0 \\ bd = \frac{1}{\sqrt{2}} \end{cases}$$

ad=0 이려면 둘중하나는 '0' 이어야 한다.
하지만 a또는 d는 '0'일경우 $ac=\frac{1}{\sqrt{2}}$, $bc=\frac{1}{\sqrt{2}}$ 라는 식이 성립하지 못하므로, bc=0 또한 마찬가지
a,b,c,d 는 같이 있을 때만 존재할 수 있는 수들이다. ⇒ Entangled(얽힘) 이다.

#How to make Entangled State?



$$C(H_1)\left\{\begin{pmatrix}1\\0\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right\} = C\left(\begin{pmatrix}\frac{1}{\sqrt{2}}\\ \frac{1}{\sqrt{2}}\end{pmatrix}\otimes\begin{pmatrix}1\\0\end{pmatrix}\right) = \begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&0&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\ \frac{1}{\sqrt{2}}\\0\end{pmatrix} = \begin{pmatrix}\frac{1}{\sqrt{2}}\\0\\0\\ \frac{1}{\sqrt{2}}\end{pmatrix}$$

Hadamard Gate
Cbit → Qbit

CNOT Gate

entangled!

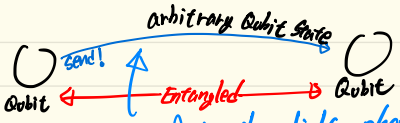
Hidden variable theory

how to prove?

Configuration

*faster than light coordination ok
faster than light communication Not OK!

Teleportation

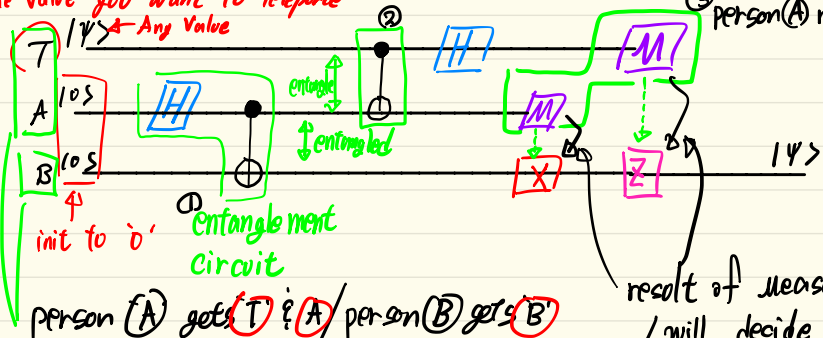


No-Cloning theorem
⇒ transfer qubit states: YES!
↳ copy-paste qbits states: NO.

using faster than light phenomenon of entanglement

⇒ But!, the whole process is NOT faster than light
⇒ Because you need to send Two bits of information

the 'value' you want to Teleporte



person Ⓐ gets 'T' & Ⓐ / person Ⓑ gets 'B'

result of measurement of 'A' will decide whether 'B' has to run Qbit through [X] bit flip

result of [M] of 'T' will decide whether 'B' has to run Qbit through 'phase flip Gate'

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

You can simulate Quantum Computing in Classical Computer, but why is it so slow?

A: If two Qbits become entangled you need to keep full product state around!