양자 논리 게이트

최승주

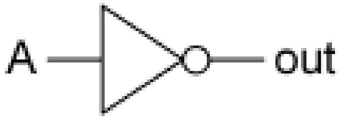
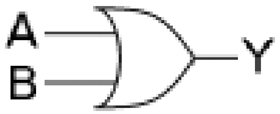
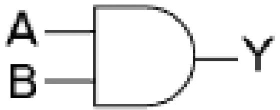
https://youtu.be/AkOnLqn2AvI

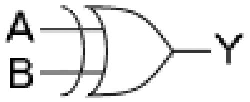
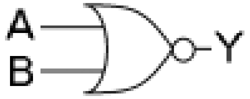
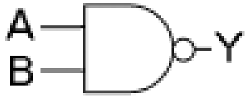
Contents

CryptoCraft LAB

양자 논리 게이트

- 기존 컴퓨터 논리 게이트

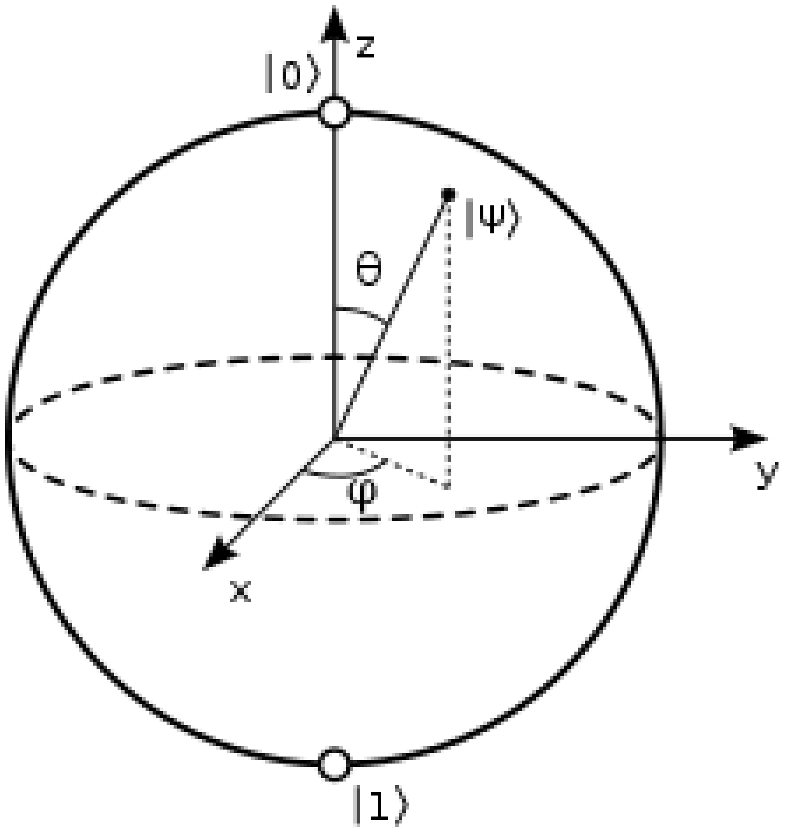
NOT	$\overline{A}$	
OR	$A + B$	
AND	$A \cdot B$	

XOR	$A \oplus B$	
NOR	$\overline{A + B}$	
NAND	$\overline{A \cdot B}$	

양자 논리 게이트

- 양자 컴퓨터 양자 게이트

  복소수 벡터들에 대한 행렬 곱셈



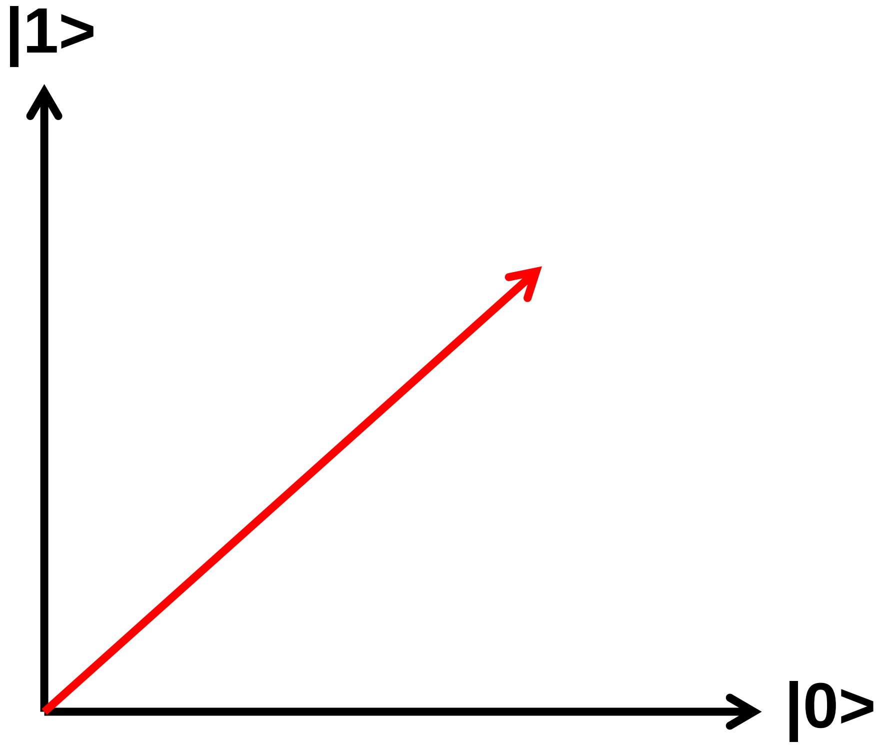
양자 논리 게이트

- 양자 컴퓨터 양자 게이트

큐비트 상태 – 2차원 벡터에서의 상태

a |0> + b |1>

a: 0.6
b: 0.8



양자 논리 게이트

- NOT 게이트

$|0> \rightarrow |1>$

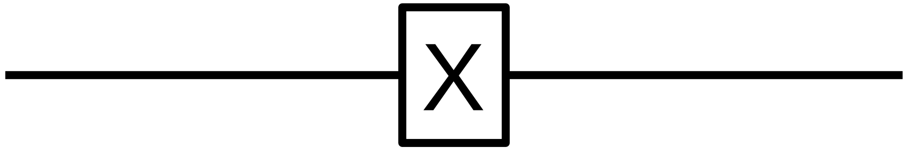
$|1> \rightarrow |0>$

$a\ |0> + b\ |1> \rightarrow a\ |1> + b\ |0>$

양자 논리 게이트

- NOT 게이트

양자 회로



행렬

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

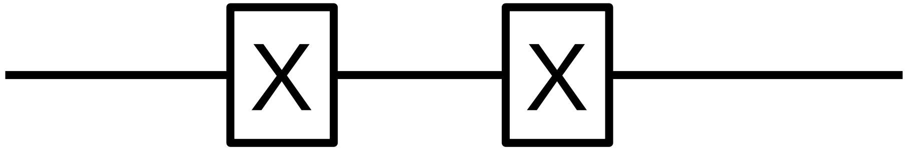
$$X\,|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

$$X\,|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

양자 논리 게이트

- NOT 게이트

양자 회로



$$a\,|0> + b\,|1> \rightarrow a\,|1> + b\,|0> \rightarrow a\,|0> + b\,|1>$$

동일

양자 논리 게이트

- Hadamard 게이트

$$|0> \rightarrow \quad \frac{|0 > + \ |1 >}{\sqrt{2}}$$

$$|1> \rightarrow \quad \frac{|0 > - \ |1 >}{\sqrt{2}}$$

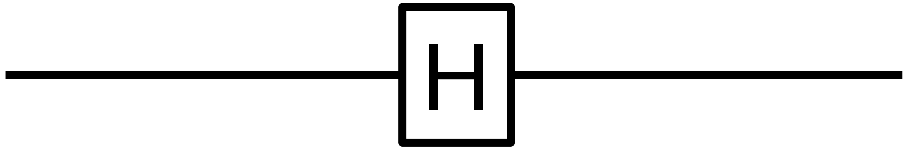
$$a\ |0> + b\ |1> \rightarrow \quad a\left(\frac{|0 > + \ |1 >}{\sqrt{2}}\right) + \ b\left(\frac{|0 > - \ |1 >}{\sqrt{2}}\right)$$

$$= \quad \frac{a + b}{\sqrt{2}}\,|0 > \ + \ \frac{a\ - b}{\sqrt{2}}\ \ |1 >$$

양자 논리 게이트

- Hadamard 게이트

양자 회로



행렬

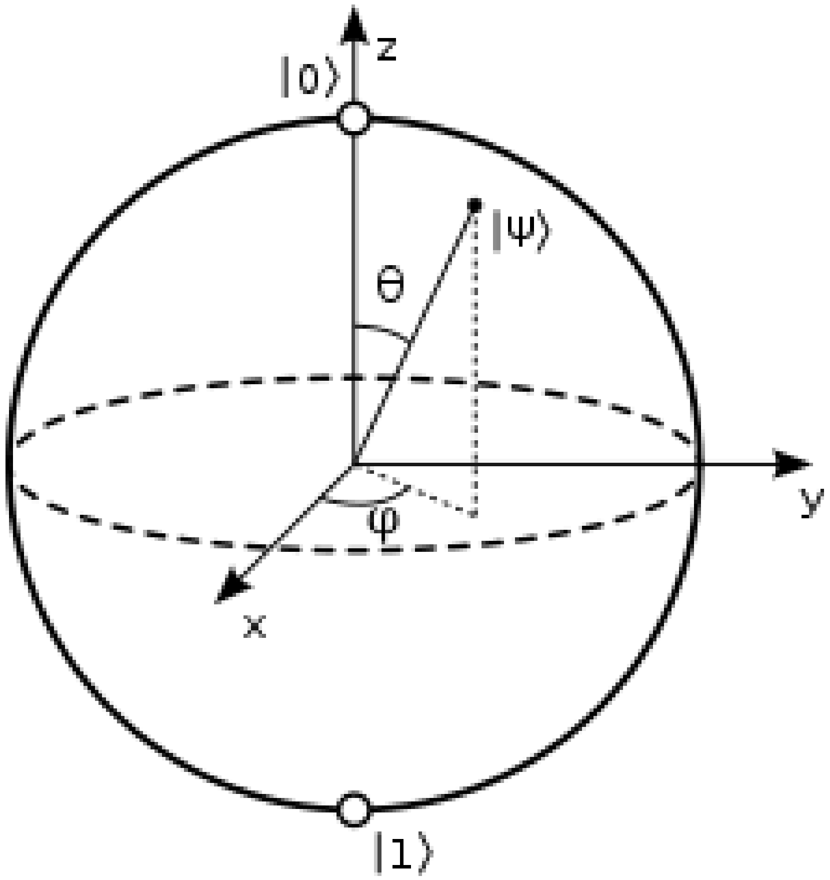
$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H|0\rangle = H \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{|0> + |1>}{\sqrt{2}}$$

$$H|1\rangle = H \begin{bmatrix} 0 \\ 1 \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix} = \frac{|0> - |1>}{\sqrt{2}}$$

양자 논리 게이트

- Pauli X Y Z 게이트



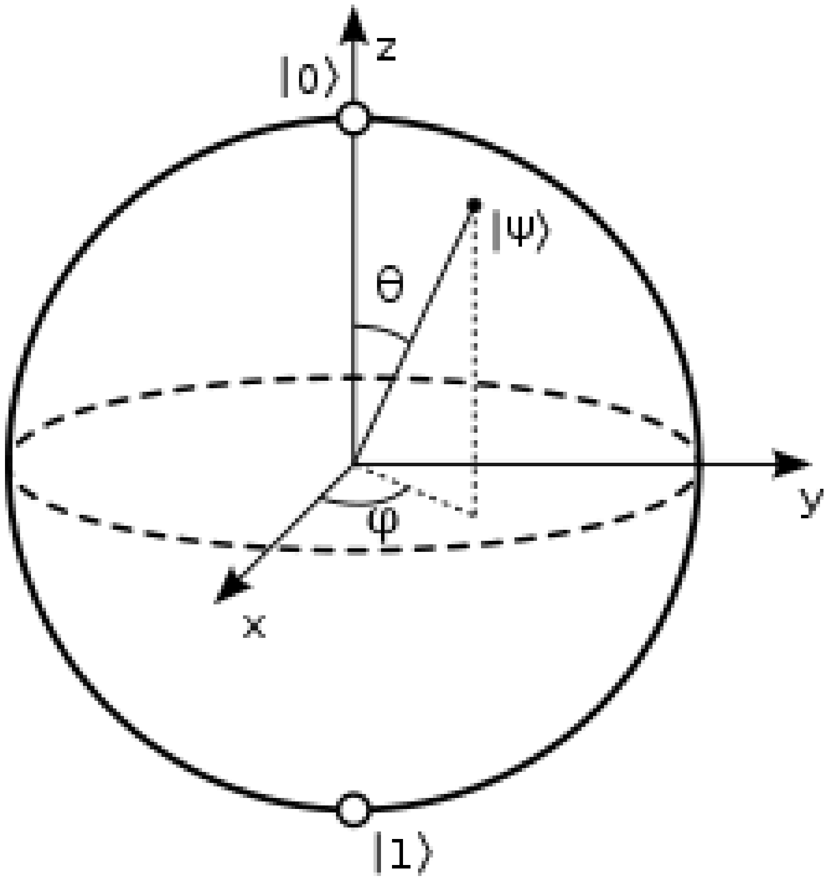
양자 논리 게이트

- Pauli X Y Z 게이트

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}.$$

$$Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}.$$

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



양자 논리 게이트

- Phase shift 게이트

- S 게이트 $\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$

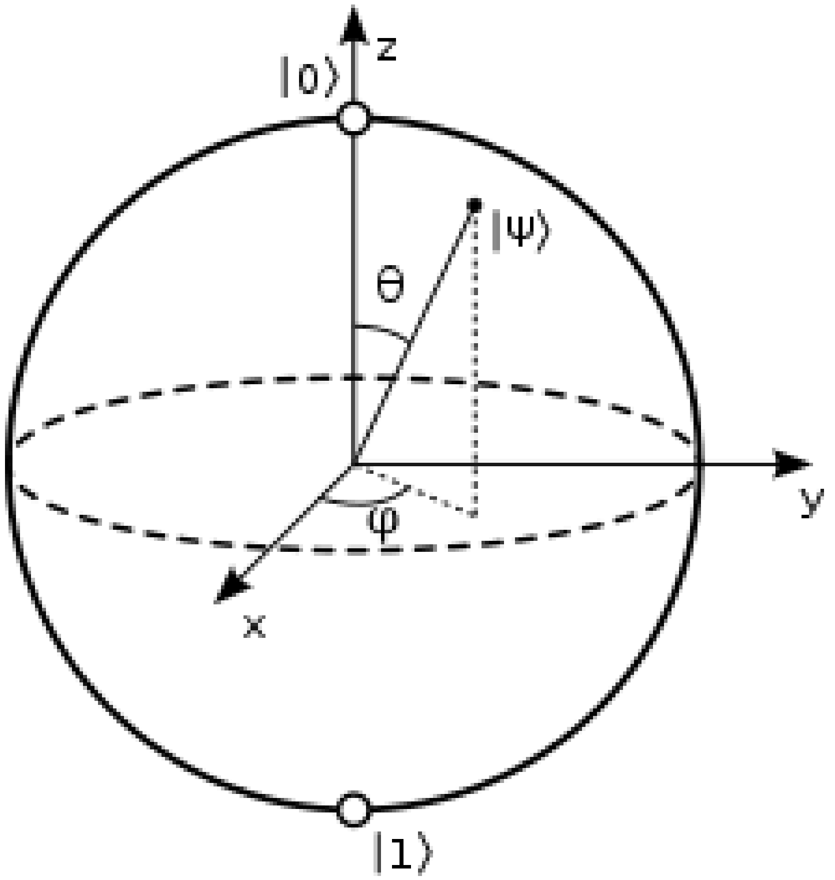
  1의 위상을 i 의 계수로 변경 / Z 축을 중심으로 n / 2 회전

- T 게이트 $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

  Z 축을 중심으로 n / 4 회전

- 위상 이동 게이트 $\begin{bmatrix} 1 & 0 \\ 0 & e^{i\Theta} \end{bmatrix}$

  Z 축을 중심으로 임의의 θ만큼 회전



양자 논리 게이트

- SWAP 게이트

두 큐비트를 교환

$$\mathrm{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

양자 논리 게이트

- CNOT 게이트

첫 번째 큐비트가 1인 경우에 두 번째 큐 비트에 NOT 게이트 연산 수행

중첩 효과

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

양자 논리 게이트

- TOFFOLI 게이트(CCNOT 게이트)

  3 큐비트 게이트

  첫 번째 두 비트가 모두 1인 경우 세 번째 큐비트에 NOT 연산

Truth table

INPUT			OUTPUT		
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

Matrix form

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

양자 논리 게이트

- Fredkin 게이트(CSWAP 게이트)

  첫 번째 비트가 1인 경우 마지막 두 비트를 교체

Truth table

INPUT			OUTPUT		
C	I_1	I_2	*C*	O_1	O_2
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	1	0
1	1	0	1	0	1
1	1	1	1	1	1

Permutation matrix form

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

Q & A