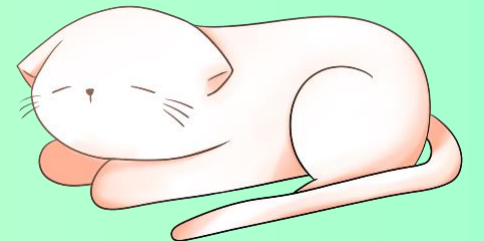


어서 와!
양자 컴퓨팅은
처음이지?



이미지 찰: 어반브러시

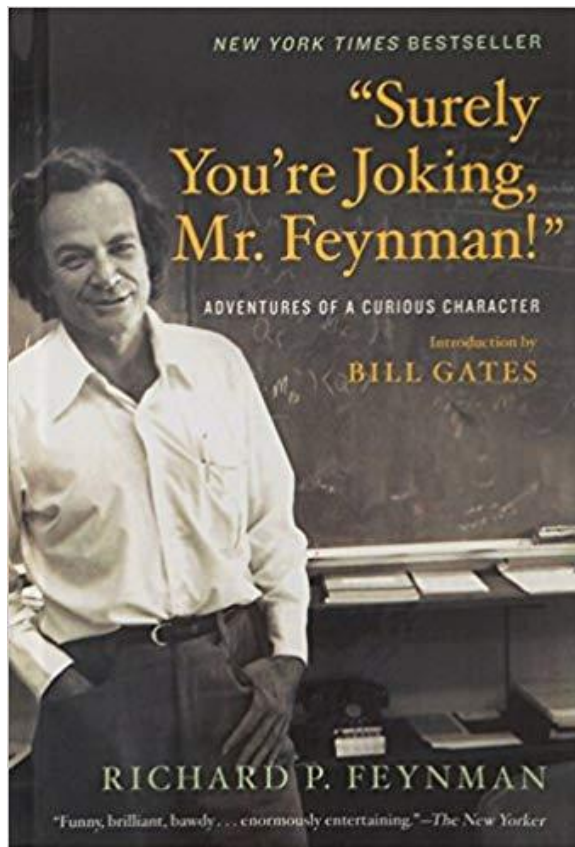
02. 양자 컴퓨터의 **탄생**





01. 양자 컴퓨팅을 위한 양자 역학

- 양자 컴퓨터의 아버지: 리처드 파인만
 - <컴퓨터로 물리계를 시뮬레이션 하는 방법>, 1982.
 - 복잡한 물리계를 연구하려면 양자 현상을 이용할 수 있는 컴퓨터가 필요하다.



파인만씨, 농담도 잘하시네!



01. 양자 컴퓨팅을 위한 양자 역학

■ 양자 컴퓨터로 할 수 있는 일들

- 1994년, 피터 쇼어: 소인수 분해 알고리즘 (쇼어 알고리즘)
 - 소인수 분해를 지수 시간이 아닌 다항 시간에 풀 수 있는 알고리즘 발표
 - 공개키 기반 암호 체계(RSA 암호)에 커다란 위협
- 1996년, 로브 그로버: 건초 더미에서 바늘 찾기 (그로버 알고리즘)
 - $O(\sqrt{n})$ 시간 복잡도를 가진 비구조적 데이터 검색 알고리즘 발표
 - NP-완전, NP-난해 문제를 다항 시간 내에 풀 수 있는 실마리 제공
- 그 외 다수: 양자 암호 통신, 양자 머신 러닝, 양자 원격이동, ...



01. 양자 컴퓨팅을 위한 양자 역학

■ 비트에서 큐비트로

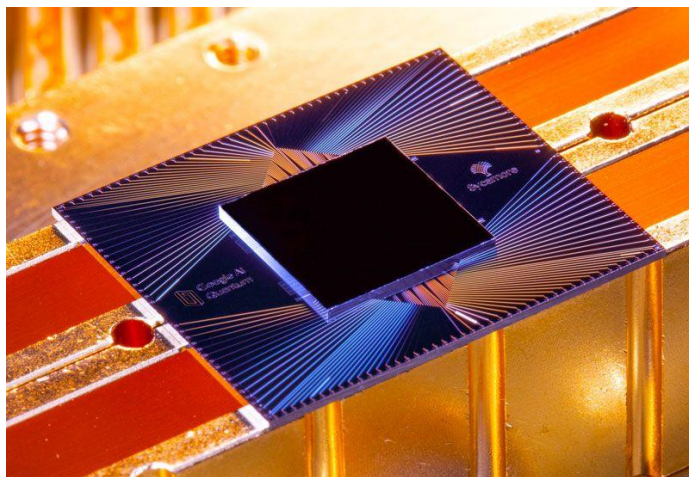
- 비트 (*bit*): 디지털 정보의 최소 단위, 0 또는 1.
 - 정보의 저장: 스위치(트랜지스터)
 - 정보의 처리: 논리 게이트: AND, OR, NOT, XOR, NAND, NOR.
- 큐비트 (*qubit*): 양자 정보의 최소 단위, 0과 1의 중첩.
 - 정보의 저장: 양자(광자, 전자, 이온, ...), 초전도체, 이온트랩, ...
 - 정보의 처리: 양자 게이트: H, X, Y, Z, CX, CCX, ...



01. 양자 컴퓨팅을 위한 양자 역학

■ 양자 컴퓨터의 등장

- 구글 시커모어칩: <프로그램머블 초전도 프로세서로 양자 우위 달성>, 2019.
- IBM Quantum Experience: 초전도 방식의 양자 컴퓨터
 - *Qiskit*: IBM QX 개발환경 (파이썬 기반)





01. 양자 컴퓨팅을 위한 양자 역학

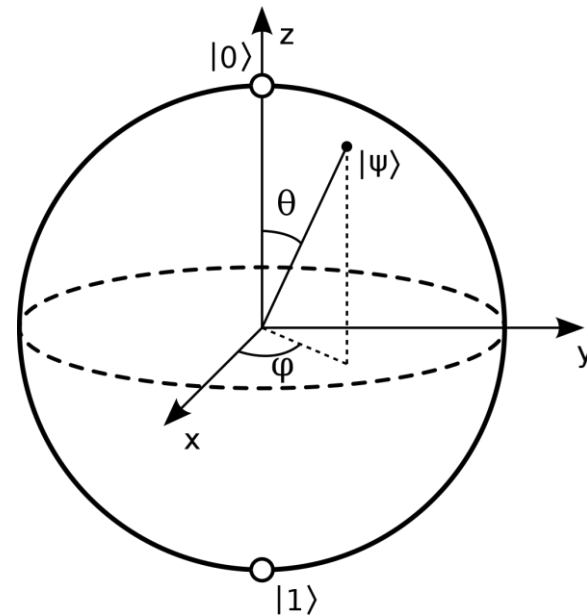
■ 양자 상태의 표현:

- 브라-켓 표기법: *bra-ket notation*
 - 양자 역학에서 양자 상태를 표현하는 표준 기법. 벡터와 선형대수.
- 블로흐 구체: *Bloch Sphere*
 - 양자의 상태 정보를 기하학적으로 이해하기 쉽도록(?) 표현하는 도구

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

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

$$\alpha|0\rangle + \beta|1\rangle \longrightarrow \boxed{H} \longrightarrow \alpha \frac{|0\rangle + |1\rangle}{\sqrt{2}} + \beta \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$



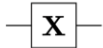

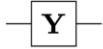
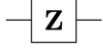
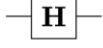
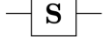
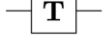
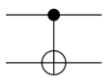
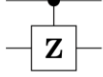



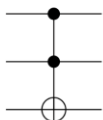


01. 양자 컴퓨팅을 위한 양자 역학

■ 양자 게이트와 양자 회로

• 양자 컴퓨터 프로그래밍:

- 아직은 게이트의 조합으로 양자 회로
- Qiskit에서는 파이썬으로 양자 회로

Operator	Gate(s)	Matrix
Pauli-X (X)	 	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y (Y)		$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z (Z)		$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Hadamard (H)		$\frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Phase (S, P)		$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$ (T)		$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
Controlled Not (CNOT, CX)		$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$
Controlled Z (CZ)	 	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$
SWAP	 	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$
Toffoli (CCNOT, CCX, TOFF)		$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$

Any Questions?



주니온TV@Youtube

자세히 보면 유익한 코딩 채널