Quantum.

1. Quantum bits

(1) 큐비트(qubit)

– 양자 컴퓨터로 계산할 때의 기본 단위를 의미. 0과 1의 고전적인 비트에 대응해 |0>, |1>의 바닥 상태가 존재.

– qubit의 상태는 측정 전에는 superposition(중첩 상태)로 존재, |0>과 |1>의 선형 결합으로 그 상태를 표현

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

– 측정 후, qubit이 상태 |0>으로 측정될 확률이 |a|^2, 상태 |1>으로 측정될 확률이 |b|^2

– e.g.

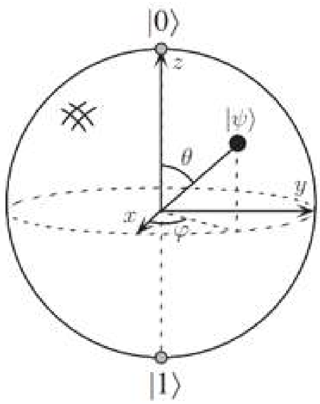
$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

※ 측정 후 qubit이 상태 |0>으로 측정될 확률이 1/2, 상태 |1>으로 측정될 확률이 1/2

※ 정상화 조건(normalization condition)에 의해 |a|^2 + |b|^2 = 1 을 항상 만족

(2) Bloch sphere

– qubit의 상태를 시각적으로 나타나는 데 사용



큐비트 상태 $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$을 극좌표계 θ와 ϕ로 표현

$$\alpha = \cos\left(\frac{\theta}{2}\right)$$

$$\beta = e^{i\phi}\sin\left(\frac{\theta}{2}\right)$$

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle$$

(3) Multiple qubits

– Qubit이 두 개인 System은 4개의 computational basis state, |00>, |01>, |10>, |11>이 존재

– state vector; 각 basis 앞의 complex coefficient(복소수 계수)는 amplitude 라고도 불림

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle$$

- 각 computational basis state를 행렬로 표현하면 다음과 같음

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

(4) Bell state(or EPR pair)
- 2개의 qubit으로 이루어진 상태에서, 양자 회로에서 중요하게 쓰이는 상태

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

- 한 개의 qubit의 상태를 알면, 다른 qubit의 상태를 즉시 알 수 있는 특징이 있음
=> 두 qubit이 서로 얽혀 있는 상태

2. Quantum computation
(1) Single qubit gates
- single qubit에서의 quantum gate는 2x2의 matrix로 대응됨
- quantum gate를 matrix로 대응시키기 위해서는 gate가 unitary[1]한 matrix로 표현될 수 있어야 함
- X gate : classcial한 회로에서의 not gate와 대응

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

- Z gate

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

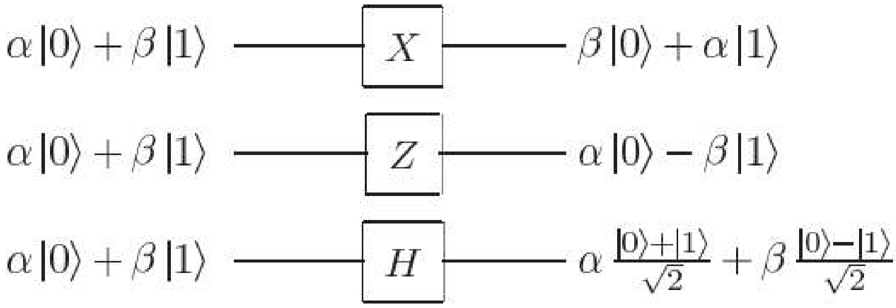
- Hadamard gate

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

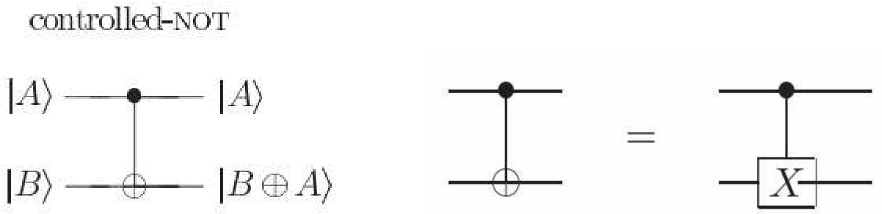
---

1) $U^\dagger U$ = I를 만족하는 행렬 U, †는 Hermitian conjugate(대거) 연산

- 각 gate를 통과한 state vector는 다음과 같이 표현됨



(2) Multiple qubit gates
- controlled-NOT(or CNOT gate)
: 2개의 input qubits와, 2개의 output qubits가 존재
: input qubits는 차례대로 각각 control qubit 과 target qubit으로 불림

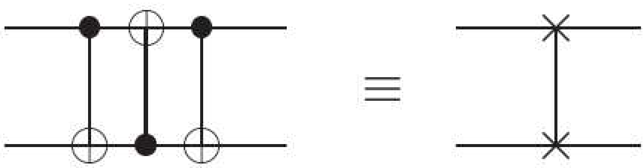


$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

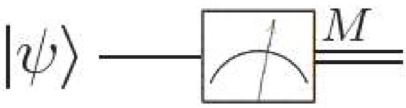
- control qubit이 1일 때만, target bit가 변화하는 것을 알 수 있음

$$|00\rangle \rightarrow |00\rangle;\ |01\rangle \rightarrow |01\rangle;\ |10\rangle \rightarrow |11\rangle;\ |11\rangle \rightarrow |10\rangle$$

3. Quantum circuits
(1) Circuit swapping two qubits
: 두 qubits의 상태를 바꾸는 회로

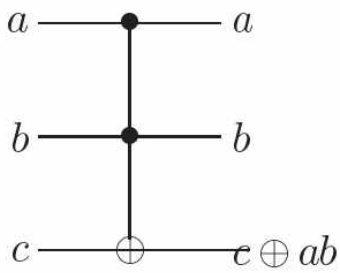


(2) measurement
: qubit의 상태를 측정하는 회로

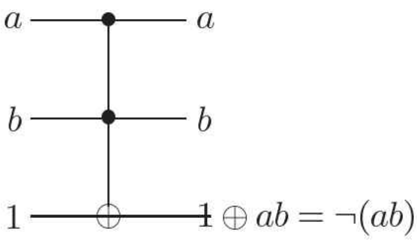


4. Quantum algorithms
(1) Classical computations on a quantum computer
– 일반적으로 classical circuit를 직접적으로 quantum circuit으로 대체하는 것은 불가능
: reversible(가역적인) gate들로만 구성돼 있는 quantum circuit와는 달리, classical circuit에는 irreversible gate들도 존재하기 때문!
– 단, 비가역적인 gate를 가역적 gate로 대체할 수 있는, quantum gate인 Toffoli gate가 존재
(a) Toffoli gate

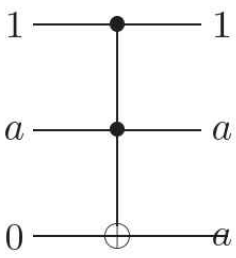
Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



(b) Toffoli gate를 활용한 classical gate 대체 방법



: NAND gate



: FANOUT

(c) NAND gate를 활용하면 고전적인 gate들을 모두 대체할 수 있음
(d) 결론적으로, quantum circuit를 통해 classical circuit를 대체할 수 있음

(2) Quantum parallelism
: quantum algorithms의 근본이 되는 중요한 특징
: 고전적인 parallelism과는 달리, 단 하나의 quantum circuit만으로 서로 다른 x값에 따른 함숫값 f(x)의 값을 동시에 계산할 수 있음

4. Linear algebra
(1) Notation of linear algebra in quantum circuit

Notation	Description
z^*	Complex conjugate of the complex number z. $(1+i)^* = 1-i$
$\|\psi\rangle$	Vector. Also known as a *ket*.
$\langle\psi\|$	Vector dual to $\|\psi\rangle$. Also known as a *bra*.
$\langle\varphi\|\psi\rangle$	Inner product between the vectors $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle \otimes \|\psi\rangle$	Tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
$\|\varphi\rangle\|\psi\rangle$	Abbreviated notation for tensor product of $\|\varphi\rangle$ and $\|\psi\rangle$.
A^*	Complex conjugate of the A matrix.
A^T	Transpose of the A matrix.
$A^\dagger$	Hermitian conjugate or adjoint of the A matrix, $A^\dagger = (A^T)^*$. $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$.
$\langle\varphi\|A\|\psi\rangle$	Inner product between $\|\varphi\rangle$ and $A\|\psi\rangle$. Equivalently, inner product between $A^\dagger\|\varphi\rangle$ and $\|\psi\rangle$.

(2) Bases and linear independence
－A spanning set for a vector space
: 벡터 공간 V의 임의의 벡터 |v>를 set의 원소들의 linear combination으로 생성할 수 있을 때, 그 집합을 spanning set이라고 함

$$|v\rangle = \sum_i a_i |v_i\rangle$$

－Linearly dependent
: 적어도 하나 0이 아닌 complex number이 존재해 다음과 같은 등식을 만족함

$$a_1|v_1\rangle + a_2|v_2\rangle + \cdots + a_n|v_n\rangle = 0.$$

－Linearly independent
: Linearly dependent 하지 않는 집합을 뜻함

(3) Linear operators and matrices

- linear operator $A|v\rangle$

: 어떤 inputs에 대해서도, linear 한 output을 산출하는 operator

- matrix representation of linear operator

: 어떤 operator든 간에 matrix로 표현할 수 있음

$$A|v_j\rangle = \sum_i A_{ij}|w_i\rangle.$$

※ A : V->W라 할 때, v와 w는 각각 벡터공간의 기저

(4) The Pauli matrices

- Quantum machine에서 자주 쓰이는 행렬

$$\sigma_0 \equiv I \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \sigma_1 \equiv \sigma_x \equiv X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$\sigma_2 \equiv \sigma_y \equiv Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_3 \equiv \sigma_z \equiv Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

(5) Inner product

- 두 개의 벡터를 입력으로 받아, 하나의 complex number를 출력으로 내놓는 함수

$\langle v|w\rangle$, where $|v\rangle$ and $|w\rangle$ are vectors

- Inner product space (= Hilbert space)

: 다음 3가지 조건을 만족하는 vector space를 뜻함

(1) $(\cdot,\cdot)$ is linear in the second argument,

$$\left(|v\rangle, \sum_i \lambda_i |w_i\rangle\right) = \sum_i \lambda_i \left(|v\rangle, |w_i\rangle\right)$$

(2) $(|v\rangle, |w\rangle) = (|w\rangle, |v\rangle)^*$.

(3) $(|v\rangle, |v\rangle) \geq 0$ with equality if and only if $|v\rangle = 0$.

- Inner product를 행렬로 표현하면 다음과 같음

$$\langle v|w\rangle = \left(\sum_i v_i|i\rangle, \sum_j w_j|j\rangle\right) = \sum_{ij} v_i^* w_j \delta_{ij} = \sum_i v_i^* w_i$$

$$= \begin{bmatrix} v_1^* \ldots v_n^* \end{bmatrix} \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}.$$

- orthogonal
: 두 벡터의 내적값이 0, 내지는 두 벡터가 서로 직교함을 의미

- norm
: 벡터의 크기를 의미. 자기 자신을 내적한 값의 square root

- orthonormal
: 각 벡터들이 서로 unit vector (norm값이 1) 이고 orthogonal 한 벡터들

- Gram-Schmidt procedure
: 임의의 벡터에 대해, 이를 생성하는 orthonormal 한 basis set을 생성하는 과정

- outer product
: inner product와 dual.

$$|w\rangle\langle v|$$

- Cauchy-Schwarz inequality

$$\begin{aligned}\langle v|v\rangle\langle w|w\rangle &= \sum_i \langle v|i\rangle\langle i|v\rangle\langle w|w\rangle \\ &\geq \frac{\langle v|w\rangle\langle w|v\rangle}{\langle w|w\rangle}\langle w|w\rangle \\ &= \langle v|w\rangle\langle w|v\rangle = |\langle v|w\rangle|^2\end{aligned}$$

(6) Eigenvectors and eigenvalues
- 고유벡터 (Eigenvector)
: operator A에 대해, 그 방향이 변하지 않는 벡터를 의미.

$$A\mathbf{v} = \lambda\mathbf{v}$$

- 고유값 (Eigenvalues)
: 고유벡터에 대응하는 스칼라값
: 고유값을 구하기 위해서는 특성 방정식을 풀어야 함.

$$\det(A - \lambda I) = 0$$

- Diagonal representation
: 임의의 operator (= matrix)를 대각화하여 표현한 것. spectral decomposition이라고도 불림

$$A = \sum_i \lambda_i |i\rangle\langle i|$$

(7) Adjoint and Hermitian operator
- Hermitian conjugate
: 임의의 행렬을 Transpose 취한 후, complex conjugate 연산을 수행하는 연산
: 예시로 다음과 같음. 대거 혹은 허미션 컨쥬게이트 라고 읽음

$$\begin{bmatrix} 1+3i & 2i \\ 1+i & 1-4i \end{bmatrix}^{\dagger} = \begin{bmatrix} 1-3i & 1-i \\ -2i & 1+4i \end{bmatrix}$$

– Hermitian
: 고유값이 모두 실수인 연산자. 다음 등식을 만족함

$$A = A^{\dagger}$$

: hermitian 행렬은 normal하기 때문에 대각화 가능

– normal

$$AA^{\dagger} = A^{\dagger}A$$

: normal <=> it is diagonalizable

– Unitary
: 각 행벡터 내지는 열벡터들이 모두 orthonormal 한 정방행렬. 다음 등식을 만족

$$U^{\dagger}U = I$$

: unitary 행렬은 내적 값을 preserve 하는 성질을 갖고 있음. 아래 등식 참조

$$(U|v\rangle, U|w\rangle) = \langle v|U^{\dagger}U|w\rangle = \langle v|I|w\rangle = \langle v|w\rangle.$$

– Positive operator
: 고유값이 모두 양수인 대칭행렬
: 모든 Positive operator는 자동적으로 Hermitian이 됨.

(8) Tensor product
: 여러 벡터 공간을 결합하여 더 큰 벡터 공간을 만드는 operator
– 다음과 같은 성질을 가짐

1. **선형성**:
   텐서 곱 연산은 선형성을 가집니다. 즉, 벡터 $\mathbf{v}_1, \mathbf{v}_2 \in V$와 $\mathbf{w}_1, \mathbf{w}_2 \in W$, 그리고 스칼라 a, b에 대해 다음이 성립합니다:
   $(a\mathbf{v}_1 + b\mathbf{v}_2) \otimes \mathbf{w} = a(\mathbf{v}_1 \otimes \mathbf{w}) + b(\mathbf{v}_2 \otimes \mathbf{w})$
   $\mathbf{v} \otimes (a\mathbf{w}_1 + b\mathbf{w}_2) = a(\mathbf{v} \otimes \mathbf{w}_1) + b(\mathbf{v} \otimes \mathbf{w}_2)$

2. **차원**:
   벡터 공간 V의 차원이 m이고 W의 차원이 n일 때, 텐서 곱 $V \otimes W$의 차원은 $m \times n$입니다.

3. **기저**:
   만약 $\{\mathbf{v}_i\}$가 V의 기저이고 $\{\mathbf{w}_j\}$가 W의 기저라면, $\{\mathbf{v}_i \otimes \mathbf{w}_j\}$는 $V \otimes W$의 기저를 이룹니다.

- 행렬에서의 tensor product는 다음과 같음

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B \\ a_{21}B & a_{22}B \end{pmatrix} = \begin{pmatrix} a_{11}b_{11} & a_{11}b_{12} & a_{12}b_{11} & a_{12}b_{12} \\ a_{11}b_{21} & a_{11}b_{22} & a_{12}b_{21} & a_{12}b_{22} \\ a_{21}b_{11} & a_{21}b_{12} & a_{22}b_{11} & a_{22}b_{12} \\ a_{21}b_{21} & a_{21}b_{22} & a_{22}b_{21} & a_{22}b_{22} \end{pmatrix}$$

(9) Operator functions

- 임의의 행렬 A가 normal일 때, 이를 대각화 한 후, 임의의 함수 f에 대응하는 matrix function f(A)를 정의할 수 있음.
- 예로 normal matrix인 Z에 exp 함수를 취한 matrix function은 다음과 같음

$$\exp(\theta Z) = \begin{bmatrix} e^{\theta} & 0 \\ 0 & e^{-\theta} \end{bmatrix}$$

- Trace of a matirx

: 임의의 행렬 A의 대각성분들의 합

: cyclic하고 linear하다는 특징이 있음

(10) The commutator and anti-commutator

- The commutator of A, B

: [A, B] = AB - BA

: commutator 값이 0이면, A, B는 서로 commute 하다고 함

- The anti-commutator of A, B

: {A, B} = AB + BA

: anti-commutator 값이 0이면, A, B는 서로 anti-commute 하다고 함

- simultaneously diagonalize

: 만일 Hermitian 인 A, B가 서로 commute 하다면, A, B를 동시에 생성하는 orthonormal set이 존재함.

(11) The polar and singular value decomposition

- Polar decomposition

: 임의의 linear operator A를 positive operator와 unitary operator로 분해하는 과정

- Singular value decomposition

: 임의의 행렬 A를 unitary한 두 행렬과 diagonal한 matrix D로 분해하는 과정

: D의 각 대각성분은 A의 특이값

$$A = UDV$$