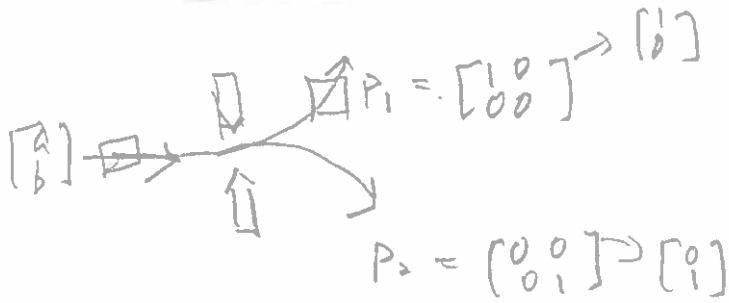


Measurement

Operator for mixed states: $|\psi_1\rangle \cdot |\psi_2\rangle \dots |\psi_m\rangle$
 $P_1 \quad P_2 \quad P_m$

$$\rho = \sum p_i |\psi_i\rangle \langle \psi_i|$$

$$\langle A \rangle = \sum p_i \langle \psi_i | A | \psi_i \rangle = \text{tr} A \rho$$



$$\frac{P_i |\psi\rangle}{\|P_i |\psi\rangle\|}$$

In vector state form (1) For pure state, $\rho = |\psi\rangle \langle \psi|$

$$\frac{M |\psi\rangle}{\|M |\psi\rangle\|}$$

In density matrix form (2)

$$\rho = |\psi\rangle \langle \psi| \mapsto \frac{M |\psi\rangle \langle \psi| M^\dagger}{\|M |\psi\rangle\|^2}$$

$$= \frac{M |\psi\rangle \langle \psi| M^\dagger}{\langle \psi | M^\dagger M | \psi \rangle}$$



ρ is a mixed state,

$$\rho \mapsto \frac{M \rho M^\dagger}{\text{tr}(M \rho)}$$

$$M_1^\dagger M_1 + M_2^\dagger M_2 + M_3^\dagger M_3 = I$$

$$P_1^2 + P_2^2 + P_3^2 = P_1 + P_2 + P_3 = I$$

4.1 Basic set up of Quantum computing

- (1) Prepare a set of registers (qubits). →
- (2) Apply some unitary transforms to carry out quantum algorithms. →
- (3) Measure the outcome to derive conclusion. →

Mathematically, qubit is a vector in $|x\rangle = a|0\rangle + b|1\rangle = \begin{pmatrix} a \\ b \end{pmatrix} \in \mathbb{C}^2$ with $|a|^2 + |b|^2 = 1$ realized by physical quantum states such as the vertically and horizontally polarized photons, or spin 1/2 in NMR system.

One often starts with a pure state $|psi\rangle = |0\dots 0\rangle$ and apply a series of quantum gate U_1, U_2, \dots , to the initial states so that a careful measurement of the resulting state will provide us the needed information.

$$\begin{array}{c}
 \downarrow \\
 2^n \\
 |0\rangle \otimes |0\rangle \otimes |0\rangle \otimes \dots \otimes |0\rangle \\
 \\
 U \quad 2^n \\
 2^n
 \end{array}$$



$$\begin{array}{ccc}
 X & Y & Z \\
 \parallel & \parallel & \parallel \\
 \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} & \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}
 \end{array}$$

4.2 Quantum gates

Mathematically, quantum gates are realized as unitary transformations/maps. For example, we can use the Pauli matrices:

$$X = \sigma_x, \quad Y = -i\sigma_y, \quad Z = \sigma_z$$

There are other quantum gates involving states represented by multiple qubits:

Walsh-Hadamard gate: $U_H = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\langle 0| + \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\langle 1|$. $= \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$

The matrix form is:

CNOT (controlled-NOT) gate:

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

$$U_{\text{CNOT}} : |00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11| = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

The matrix form is:

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \otimes I_2 + \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} \otimes \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

The circuit diagram is:



CCNOT (controlled-controlled-NOT) gate (a.k.a. Toffoli gate):

$$U_{\text{CCNOT}} = (|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10|) \otimes I + |11\rangle\langle 11| \otimes X$$

The matrix form is:

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

The circuit diagram is:

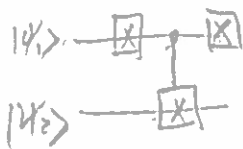


Extension: Walsh-Hadamard transformation $H \otimes H \otimes H \dots$ to a quantum gate on n qubits.

There are other basic quantum gates: SWAP gate and Fredkin gate.

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

$$X \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a \end{bmatrix}$$



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

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

$$(H \otimes H)(|0\rangle \otimes |0\rangle)$$

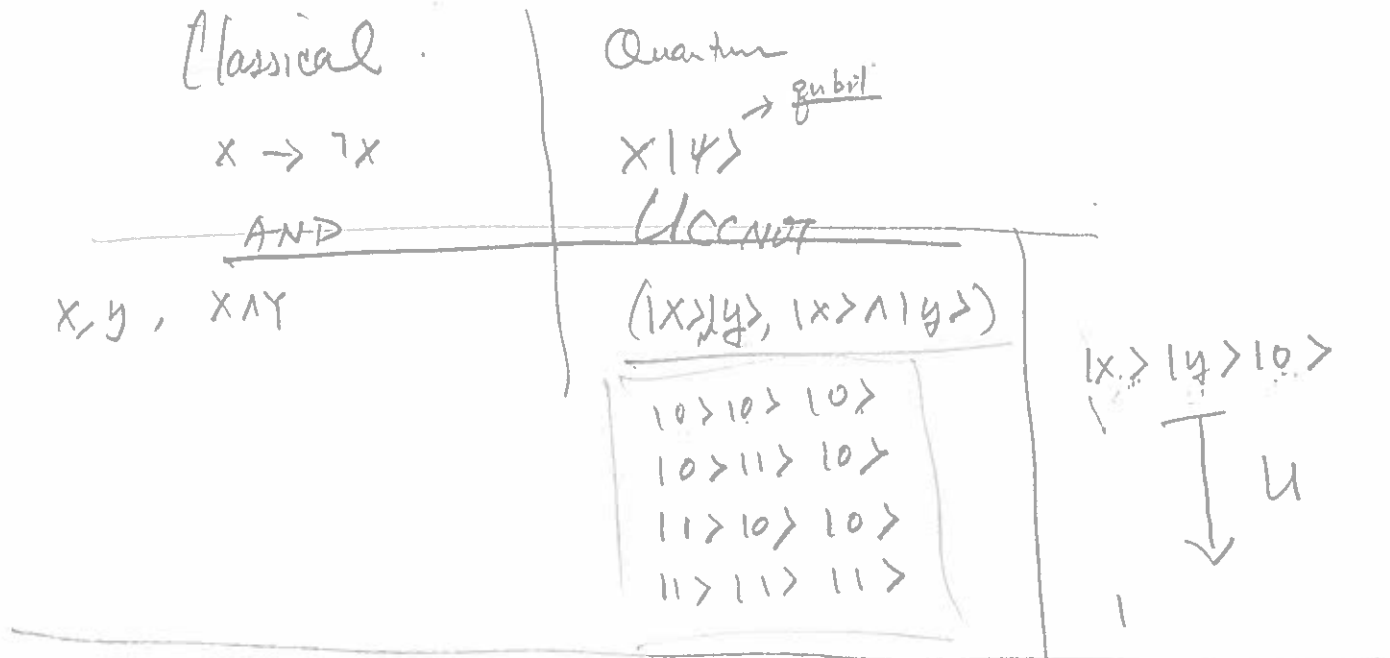
$$= (H|0\rangle) \otimes (H|0\rangle) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \otimes \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} = \frac{1}{2} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}$$

$$\begin{aligned}
 |x\rangle|y\rangle &\rightarrow \\
 \langle y|x\rangle \langle x|y\rangle &= \langle x|x\rangle \langle y,y\rangle
 \end{aligned}$$

4.3 Comparison with Classical logical gates

It is interesting to compare their actions on qubits to the classical Boolean gates.

NOT, AND, XOR, OR, NAND gates.



In general, we prepare

$|y_1\rangle \dots |y_k\rangle, |0\rangle \dots |0\rangle$
 $\underbrace{\hspace{10em}}_{k \text{ input}} \quad \underbrace{\hspace{10em}}_{m \text{ outputs}}$

\downarrow
 $(|y_1 \dots y_k\rangle \mathcal{F}(|y_1, \dots, y_k\rangle))$

4.4 No-Cloning Theorem

Theorem An unknown quantum system cannot be cloned by unitary transformations.

That is, there is no unitary $U \in M_n$ and $|y\rangle \in \mathbb{C}^n$ such that $U|x\rangle|y\rangle = |x\rangle|x\rangle$ for any given $|x\rangle \in \mathbb{C}^n$.

Proof: No unitary exists such that

$$U \underbrace{|\psi\rangle}_{\in \mathbb{C}^n} \underbrace{|0\rangle}_{\in \mathbb{C}^n} = |\psi\rangle|\psi\rangle$$
 for any $\underbrace{|\psi\rangle}_{\text{unit vectors}} \in \mathbb{C}^n$

Suppose there is such an U .

Consider $\{|\phi\rangle, |\psi\rangle\}$ an orthonormal set.

Then $U(|\phi\rangle|0\rangle) = |\phi\rangle|\phi\rangle$

$U(|\psi\rangle|0\rangle) = |\psi\rangle|\psi\rangle$

$$U\left(\frac{1}{\sqrt{2}}(|\phi\rangle + |\psi\rangle)|0\rangle\right) = \frac{1}{\sqrt{2}}\left(|\frac{\phi+\psi}{\sqrt{2}}\rangle \otimes \left|\frac{\phi+\psi}{\sqrt{2}}\right\rangle\right)$$

$$\parallel \frac{1}{\sqrt{2}}\left(|\phi\rangle|\phi\rangle + |\psi\rangle|\psi\rangle + |\phi\rangle|\psi\rangle + |\psi\rangle|\phi\rangle\right)$$

$$\frac{1}{\sqrt{2}}U(|\phi\rangle|0\rangle)$$

$$+ \frac{1}{\sqrt{2}}U(|\psi\rangle|0\rangle) = \frac{1}{\sqrt{2}}(|\phi\rangle|\phi\rangle + |\psi\rangle|\psi\rangle)$$

which is impossible