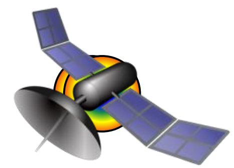
Summary of previous lecture

- Quantum circuits
  - Quantum SWAP gate
  - No loop, No FANOUT
  - Controlled-U gate
  - Measurement symbol
- No cloning theorem
  - We cannot copy the same quantum state when an arbitrary quantum state is given
- Measurement in other bases
  - Basis transformation (unitary transform) before the measurement
  - Bell basis
  - Generation of Bell basis
  - Measurement in Bell basis

Quantum entanglement

- Recently Chinese quantum satellite succeeded in distributing quantum entangled state:

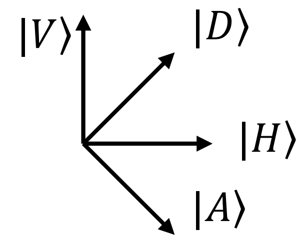


Station A $\qquad (|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B)/\sqrt{2} \qquad$ Station B

- Case 1) What happens if station A and station B measure respective photons in H-V basis?
  - Their measurement will be always opposite to each other ➔ anti-correlation
- Case 2) What happens if station A and station B measure respective photons in D-A basis?
  - Their measurement will be always opposite to each other ➔ anti-correlation !!!

Quantum entanglement

- Case 2) What happens if station A and station B measure respective photons in D-A basis?
  - We know that $\begin{cases} |D\rangle = (|H\rangle + |V\rangle)/\sqrt{2} \\ |A\rangle = (|H\rangle - |V\rangle)/\sqrt{2} \end{cases}$.



  - Also we know that $\begin{cases} |H\rangle = (|D\rangle + |A\rangle)/\sqrt{2} \\ |V\rangle = (|D\rangle - |A\rangle)/\sqrt{2} \end{cases}$.
  - $|\psi^-\rangle = [|H\rangle_A|V\rangle_B - |V\rangle_A|H\rangle_B]/\sqrt{2}$

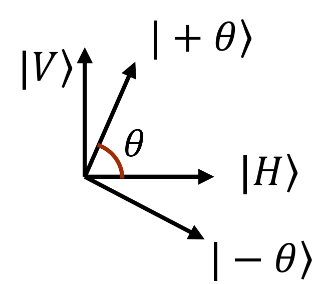
$$= [(|D\rangle + |A\rangle)_A(|D\rangle - |A\rangle)_B - (|D\rangle - |A\rangle)_A(|D\rangle + |A\rangle)_B]/2\sqrt{2}$$

$$= [|D\rangle_A|D\rangle_B - |D\rangle_A|A\rangle_B + |A\rangle_A|D\rangle_B - |A\rangle_A|A\rangle_B]/2\sqrt{2}$$

$$-[|D\rangle_A|D\rangle_B + |D\rangle_A|A\rangle_B - |A\rangle_A|D\rangle_B - |A\rangle_A|A\rangle_B]/2\sqrt{2}$$

$$= [\quad -|D\rangle_A|A\rangle_B + |A\rangle_A|D\rangle_B \quad]/\sqrt{2}$$

  - Homework: prove that the same argument is valid even for any arbitrary angle.



Quantum entanglement

- Can we reproduce the same results using a classical device?
  - We can reproduce the same result as case 1) by making a device which generates random number 0 or 1, and when that random number is 0, send out H-polarized photon to A and V-polarized photon to B. When the random number is 1, send out V-polarized photon to A and H-polarized photon to B.
  - Can such device reproduce the same result as case 2)? No
- How can we distinguish such kind of fake device and the real quantum entanglement device?
  - Randomize the choice of measurement basis and check the measured correlation

Quantum entanglement

- Schrödinger's cat state
  - $|\psi\rangle = (|\text{excited}\rangle_{atom}|\text{Alive}\rangle_{cat} + |\text{ground}\rangle_{atom}|\text{Dead}\rangle_{cat})/\sqrt{2}$

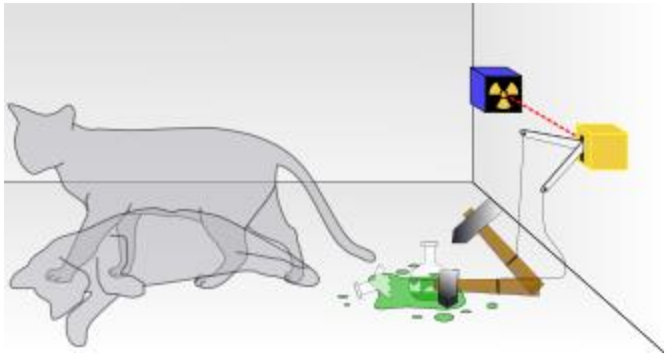
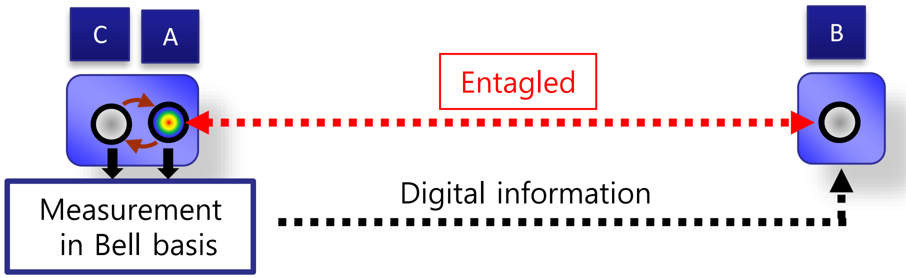


Image from
https://en.wikipedia.org/wiki/Schr%C3%B6dinger%27s_cat#/media/File:Schrodingers_cat.svg

- "Is the moon there when nobody looks?"

Quantum teleportation



- $|\Psi\rangle_C = (\alpha|0\rangle_C + \beta|1\rangle_C)$: arbitrary quantum state to teleport
- $|\Psi\rangle_C|\psi^-\rangle_{AB} = (\alpha|0\rangle_C + \beta|1\rangle_C)(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)/\sqrt{2}$

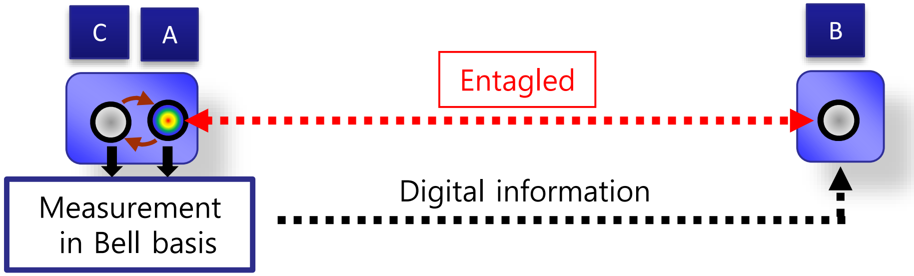
$$= [\alpha|0\rangle_C|0\rangle_A|1\rangle_B - \alpha|0\rangle_C|1\rangle_A|0\rangle_B + \beta|1\rangle_C|0\rangle_A|1\rangle_B - \beta|1\rangle_C|0\rangle_A|0\rangle_B]/\sqrt{2}$$

$$\begin{aligned} &= [\alpha(|\phi^+\rangle_{CA} + |\phi^-\rangle_{CA})|1\rangle_B - \alpha(|\psi^+\rangle_{CA} + |\psi^-\rangle_{CA})|0\rangle_B \\ &\quad +\beta(|\psi^+\rangle_{CA} - |\psi^-\rangle_{CA})|1\rangle_B + \beta(|\phi^+\rangle_{CA} - |\phi^-\rangle_{CA})|0\rangle_B]/2 \end{aligned}$$

$$\begin{aligned} &= [|\psi^+\rangle_{CA}(-\alpha|0\rangle_B + \beta|1\rangle_B) - |\psi^-\rangle_{CA}(\alpha|0\rangle_B + \beta|1\rangle_B) \\ &\quad +|\phi^+\rangle_{CA}(\quad \alpha|1\rangle_B + \beta|0\rangle_B) + |\phi^-\rangle_{CA}(\alpha|1\rangle_B - \beta|0\rangle_B)]/2 \end{aligned}$$

$$\begin{cases} |\psi^+\rangle_{CA} = [|0\rangle_C|1\rangle_A + |1\rangle_C|0\rangle_A]/\sqrt{2} \\ |\psi^-\rangle_{CA} = [|0\rangle_C|1\rangle_A - |1\rangle_C|0\rangle_A]/\sqrt{2} \\ |\phi^+\rangle_{CA} = [|0\rangle_C|0\rangle_A + |1\rangle_C|1\rangle_A]/\sqrt{2} \\ |\phi^-\rangle_{CA} = [|0\rangle_C|0\rangle_A - |1\rangle_C|1\rangle_A]/\sqrt{2} \end{cases} \Leftrightarrow \begin{cases} |0\rangle_C|1\rangle_A = [|\psi^+\rangle_{CA} + |\psi^-\rangle_{CA}]/\sqrt{2} \\ |1\rangle_C|0\rangle_A = [|\psi^+\rangle_{CA} - |\psi^-\rangle_{CA}]/\sqrt{2} \\ |0\rangle_C|0\rangle_A = [|\phi^+\rangle_{CA} + |\phi^-\rangle_{CA}]/\sqrt{2} \\ |1\rangle_C|1\rangle_A = [|\phi^+\rangle_{CA} - |\phi^-\rangle_{CA}]/\sqrt{2} \end{cases}$$

Quantum teleportation



- $|\Psi\rangle_C = (\alpha|0\rangle_C + \beta|1\rangle_C)$: arbitrary quantum state to teleport
- $|\Psi\rangle_C|\psi^-\rangle_{AB} = [|\psi^+\rangle_{CA}(-\alpha|0\rangle_B + \beta|1\rangle_B) - |\psi^-\rangle_{CA}(\alpha|0\rangle_B + \beta|1\rangle_B)$
  $+|\phi^+\rangle_{CA}(\quad\alpha|1\rangle_B + \beta|0\rangle_B) + |\phi^-\rangle_{CA}(\alpha|1\rangle_B - \beta|0\rangle_B)]/2$

- If we can measure $|\psi^-\rangle_{CA}$, original state $|\Psi\rangle_C$ seems to be reproduced at qubit B.
- What happens if we measure other Bell basis such as $|\psi^+\rangle_{CA}$ or $|\phi^-\rangle_{CA}$?
  - We need to apply different unitary operations on qubit B depending on the measurement result of qubit C and qubit A.
  - For example, if we measure $|\phi^+\rangle_{CA}$, X gate should be applied to qubit B.

- How can we measure qubit C and qubit A in Bell basis?
- Can we claim that we can implement communication faster than the speed of light using quantum teleportation?

Reversible gate

- Section 1.4.1
- Classical AND gate: irreversible ⇔We cannot tell what the input was, when only the output is given
- However, unitary operation is reversible

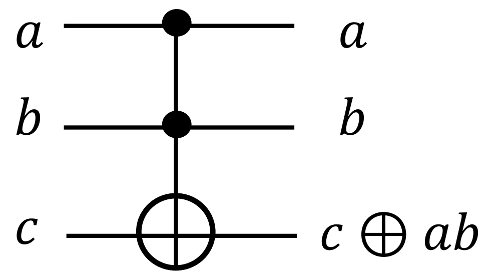
  ⇔Preservation of orthogonality
  - Unitary operator maps different inputs to distinguishable outputs
    - Proof) If not, there exist $|x\rangle$ and $|y\rangle$ such that $|x\rangle \neq |y\rangle$ and $U|x\rangle = U|y\rangle$. Apply $U^\dagger$ to both sides, $U^\dagger U|x\rangle = U^\dagger U|y\rangle$. Therefore the assumption is contradictory!
- Can we simulate a classical logic circuit using a quantum circuit?

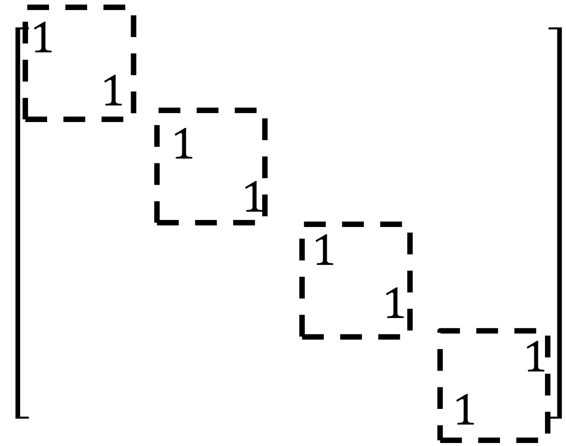
➔ Replace the digital gate with reversible gate.

- Toffoli gate, Fredekin gate are reversible gate.

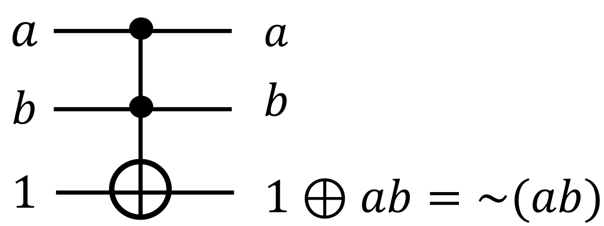
Toffoli gate

Input			Output		
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

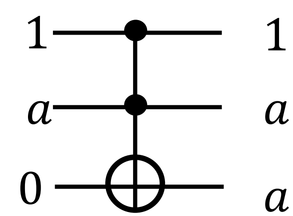




NAND



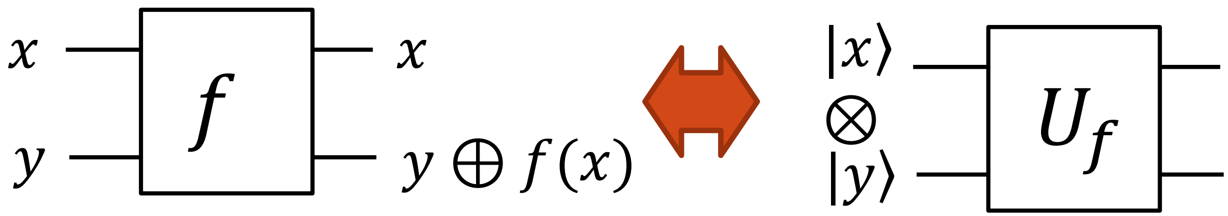
FANOUT



An arbitrary classical circuit can be simulated by an equivalent reversible circuit.
Toffoli gate can be implemented by unitary gate.

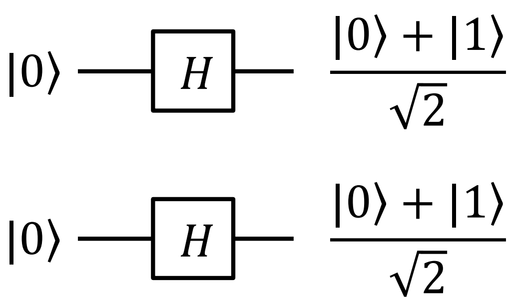
Quantum parallelism

- Section 1.4.2
- Suppose $f(x)\colon \{0,1\} \to \{0,1\}$
- Assume we built the following circuit:



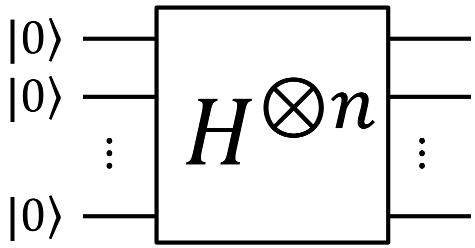
$$|\psi\rangle = |x\rangle \otimes |y \oplus f(x)\rangle$$

- Instead of $|x\rangle = |0\rangle$ or $|1\rangle$, try $|x\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|y\rangle = |0\rangle$
- $U_f\left(\frac{|0\rangle+|1\rangle}{\sqrt{2}} \otimes |0\rangle\right) = U_f\left(\frac{|0\rangle\otimes|0\rangle}{\sqrt{2}}\right) + U_f\left(\frac{|1\rangle\otimes|0\rangle}{\sqrt{2}}\right) = \frac{|0\rangle\otimes|f(0)\rangle+|1\rangle\otimes|f(1)\rangle}{\sqrt{2}}$
- It looks like we obtained the multiple results with a single processing.



$$= \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle)$$

Quantum parallelism



$$\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle$$

- With such kind of parallel input, even if we obtain $\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x, f(x)\rangle$, it is not efficient by itself due to the quantum state collapse during the measurement process.
  ➔ We need an algorithm to utilize such kind of superposition.