Lecture 2 – Quantum Logics and Circuits

Elementary Unitary Operators on a Single Qubit

- $\mathcal{B} = \{|0\rangle, |1\rangle\}$: an orthonormal basis of state space of the qubit
- $\sigma_x, \sigma_y, \sigma_z$: Pauli operators with matrix representations $X = [\sigma_x]_{\mathcal{B}}, Y = [\sigma_y]_{\mathcal{B}}, Z = [\sigma_z]_{\mathcal{B}}$ respectively

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

- Spectral decompositions of Pauli operators

  $\sigma_x = |+\rangle\langle +| - |-\rangle\langle -|, \sigma_y = |+'\rangle\langle +'| - |-'\rangle\langle -'|, \sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1$

  - $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}, |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$
  - $|+'\rangle = (|0\rangle + i|1\rangle)/\sqrt{2}, |-'\rangle = (|0\rangle - i|1\rangle)/\sqrt{2}$

Elementary Unitary Operators on a Single Qubit (Cont')

- $\sigma_h, \sigma_s, \sigma_t$: Hadamard, phase, $\pi/8$ operators with matrix representations $H = [\sigma_h]_{\mathcal{B}}, S = [\sigma_s]_{\mathcal{B}}, T = [\sigma_t]_{\mathcal{B}}$ respectively

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, S = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}, T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$$

- $\sigma_h, \sigma_x, \sigma_y, \sigma_z$: Hermitian operators

Single Qubit Operations

Algebraic Relations on Elementary Unitary Operators

- $\sigma_h = (\sigma_x + \sigma_z)/\sqrt{2}$
- $\sigma_z = \sigma_s^2$ and $\sigma_s = \sigma_t^2$
- $\sigma_h^2 = \sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I$
- $\sigma_x\sigma_y = -\sigma_y\sigma_x$, $\sigma_x\sigma_z = -\sigma_z\sigma_x$, $\sigma_y\sigma_z = -\sigma_z\sigma_y$
- $\sigma_x\sigma_y\sigma_x = -\sigma_y$, $\sigma_x\sigma_z\sigma_x = -\sigma_z$, $\sigma_y\sigma_x\sigma_y = -\sigma_x$, $\sigma_y\sigma_z\sigma_y = -\sigma_z$, $\sigma_z\sigma_x\sigma_z = -\sigma_x$, $\sigma_z\sigma_y\sigma_z = -\sigma_y$
- $\sigma_h\sigma_x = \sigma_z\sigma_h$, $\sigma_h\sigma_y = -\sigma_y\sigma_h$, $\sigma_h\sigma_z = \sigma_x\sigma_h$
- $\sigma_h\sigma_x\sigma_h = \sigma_z$, $\sigma_h\sigma_y\sigma_h = -\sigma_y$, $\sigma_h\sigma_z\sigma_h = \sigma_x$

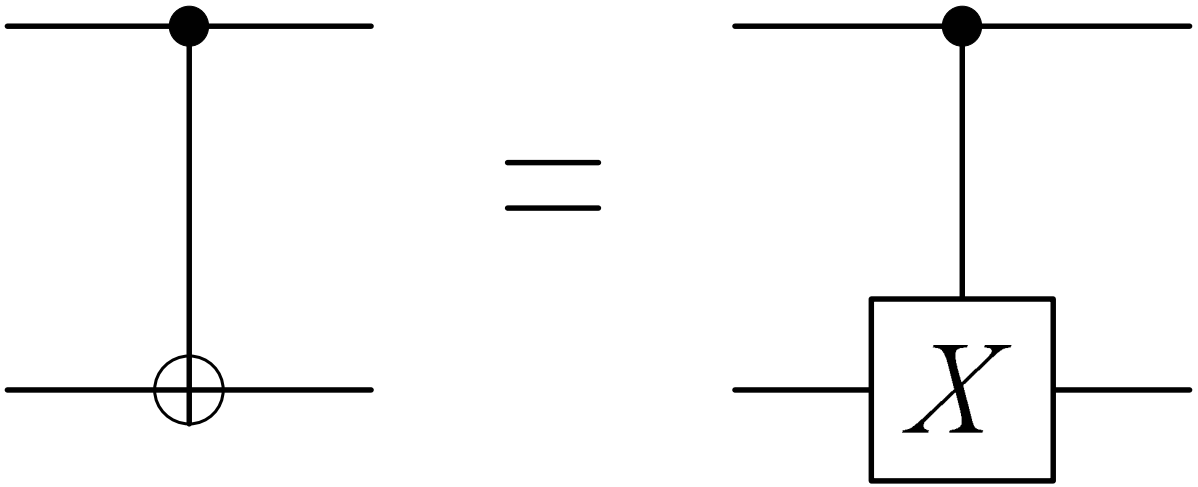
Controlled Operations

The CNOT Gate

- Prototypical control operation
- $|c\rangle|t\rangle \rightarrow |c\rangle|t \oplus c\rangle$: a unitary operation on two-qubit system, where c for the control qubit and t for the target qubit
- Matrix representation : realtive to a computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$

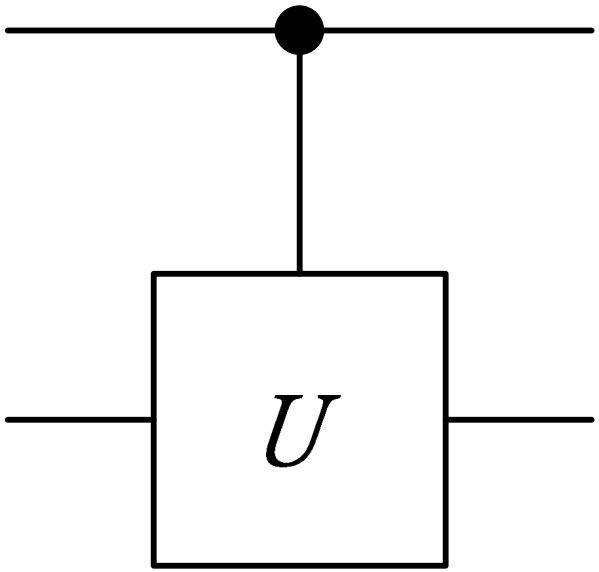
$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Circuit Representation of CNOT Gate

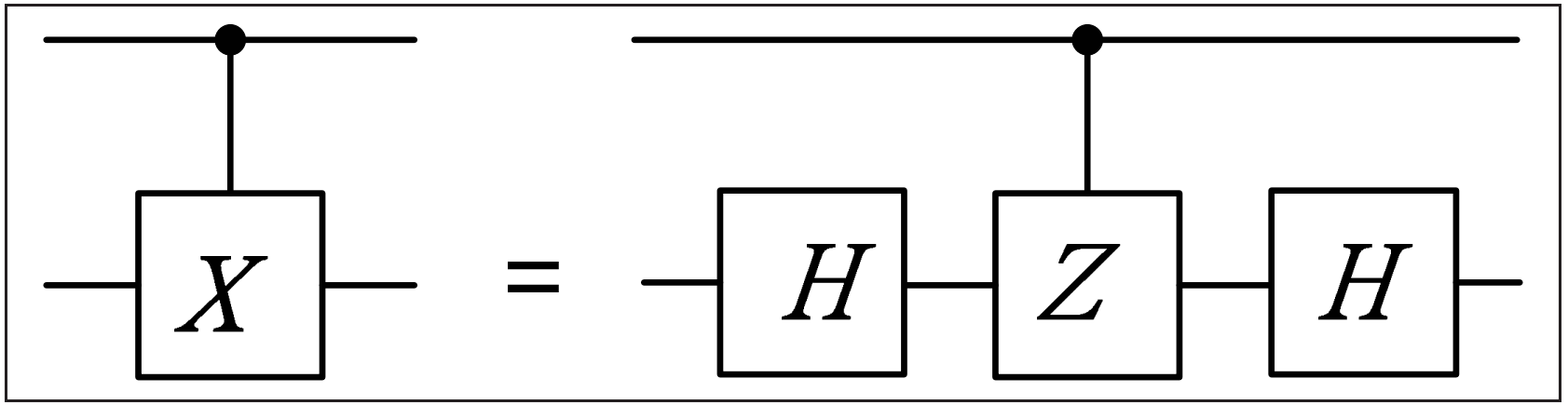


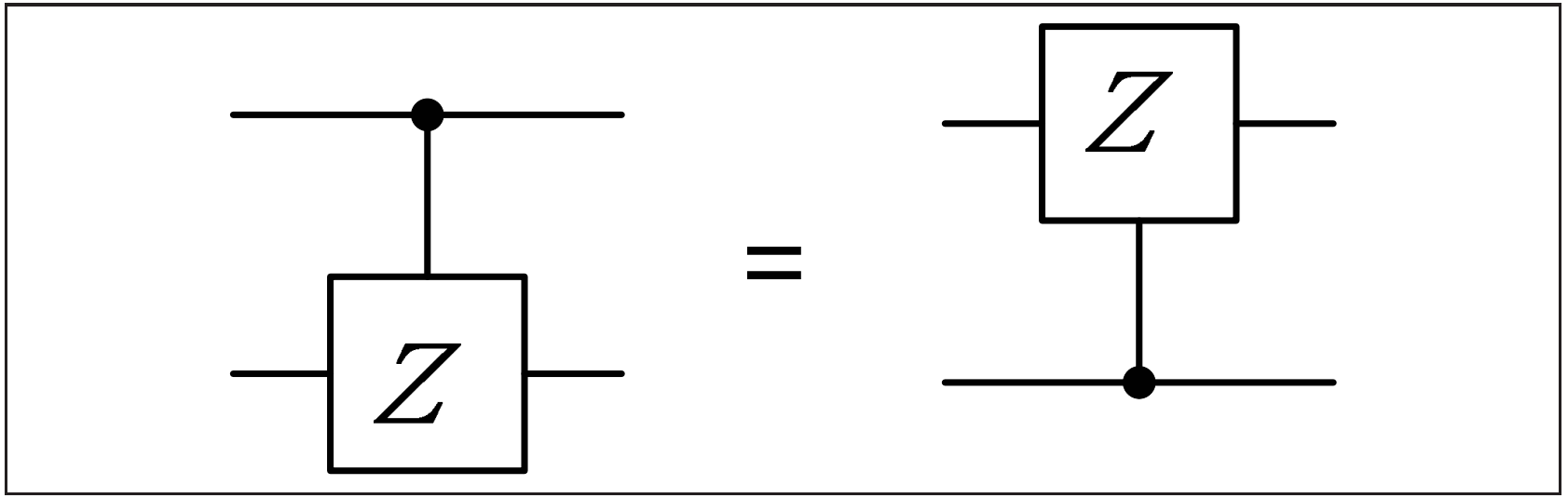
The Controlled-U Gate

- U : a unitary operator on a qubit
- $|c\rangle|t\rangle \rightarrow |c\rangle U^c|t\rangle$: if the controlled qubit is in state $|1\rangle$, then the single qubit operation U will operate on the target qubit; otherwise, no action
- Circuit representation

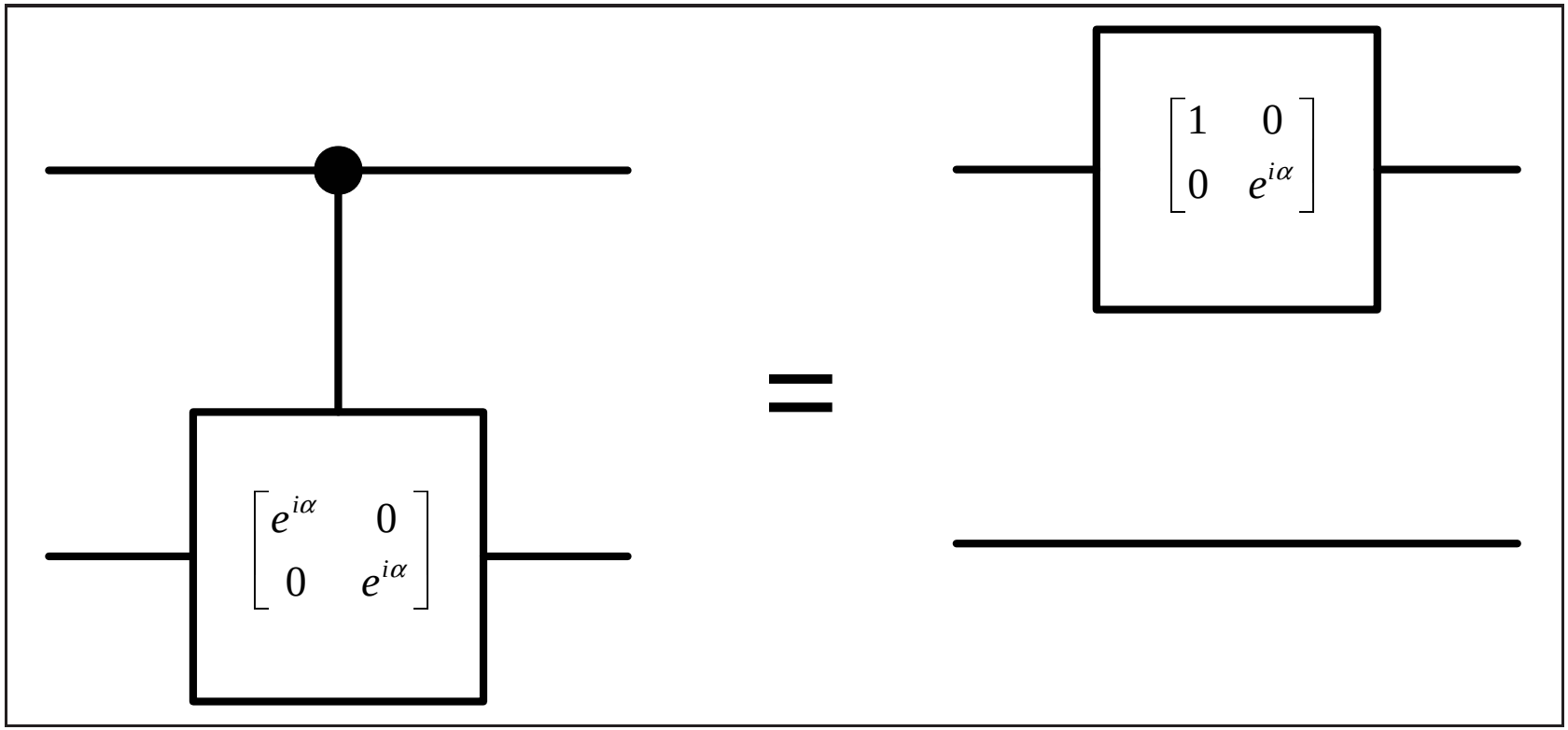


Some Circuit Identities of Gates



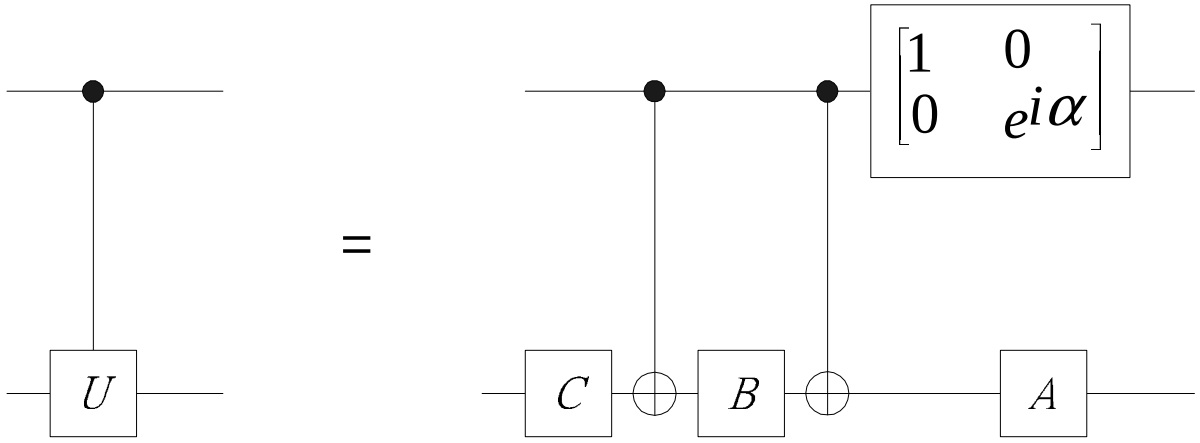


- Controlled phase shift $e^{i\alpha}$



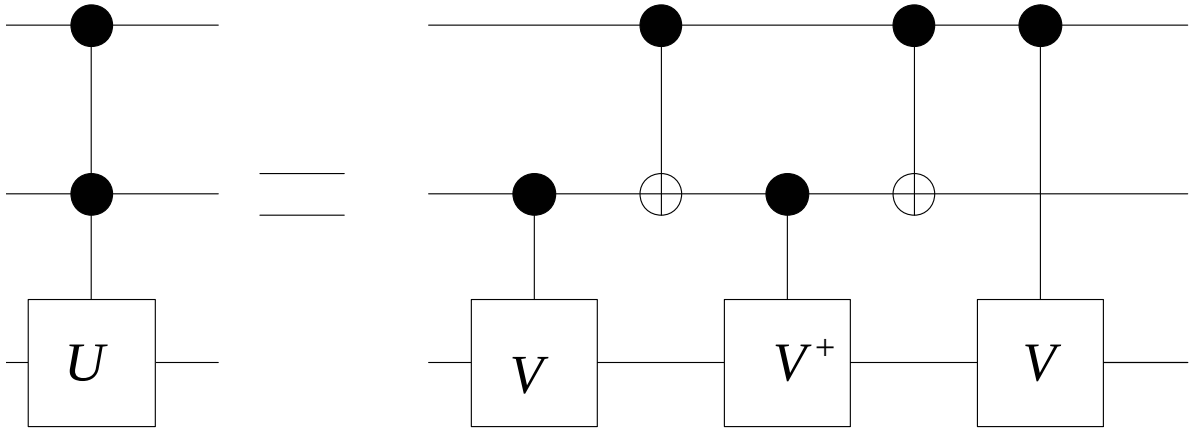
Circuit Implementation of Controlled-U Operations

- $U = e^{i\alpha} A\sigma_x B\sigma_x C$: decomposition of a single qubit operation
  - A, B, C : single qubit operations
  - $ABC = I$



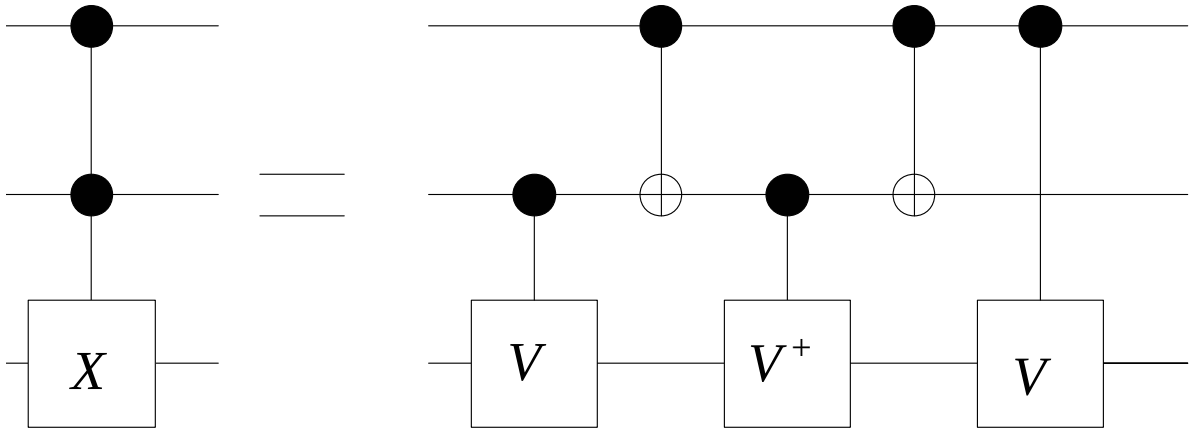
Implementation of two-qubit controlled-U operations

- U : a single qubit operation
- $C^2(U)|c_1c_2\rangle|t\rangle = |c_1c_2\rangle U^{c_1c_2}|t\rangle$: if the states of both control qubits are in $|1\rangle$, i.e., $c_1 = c_2 = 1$, then U will operate on the target qubit; otherwise, no action
- V : a unitary operator on a single qubit such that $V^2 = U$



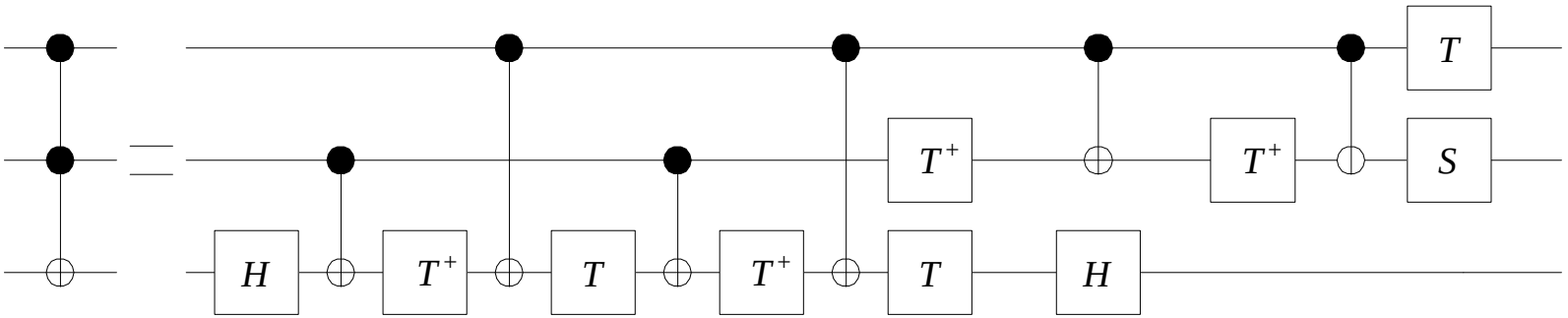
An Example – the Toffoli Gate

- $V = (1-i)(I+iX)/2 : V^2 = X$



The Toffoli Gate

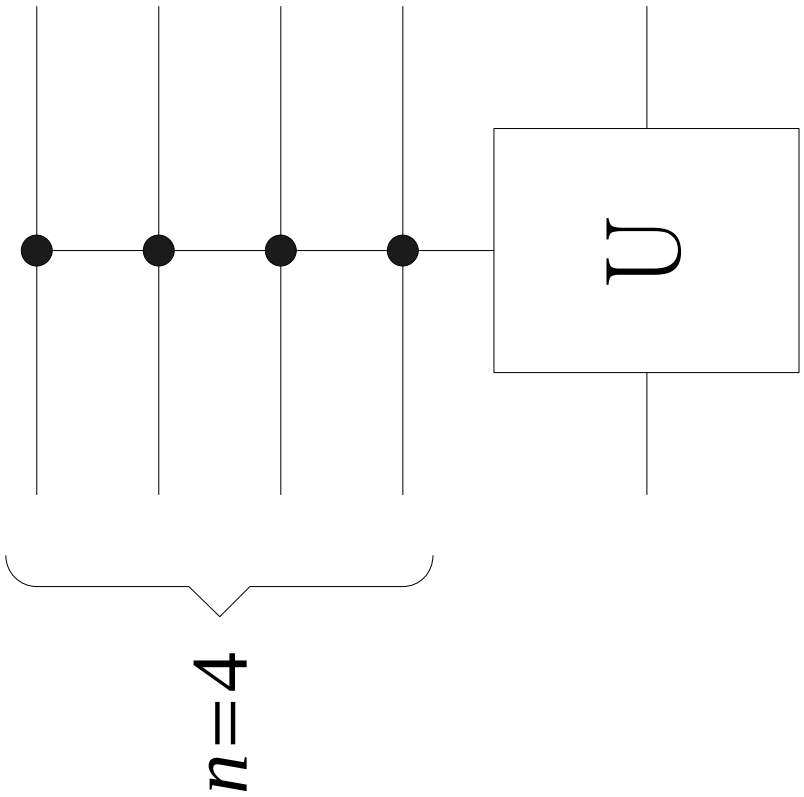
- Built by a universal set of gates : CNOT, Hadamard, phase and $\pi/8$ gates



- $XTX = X(e^{i\pi/8}R_z(\pi/4))X = e^{i\pi/8}R_z(-\pi/4)$
- $XT^\dagger X = X(e^{-i\pi/8}R_z(-\pi/4))X = e^{-i\pi/8}R_z(\pi/4)$
- $\sigma_h\sigma_t\sigma_h = e^{i\pi/8}\sigma_h R_z(\pi/4)\sigma_h = e^{i\pi/8}R_x(\pi/4)$
- $\sigma_x = e^{i\pi/2}R_x(\pi)$

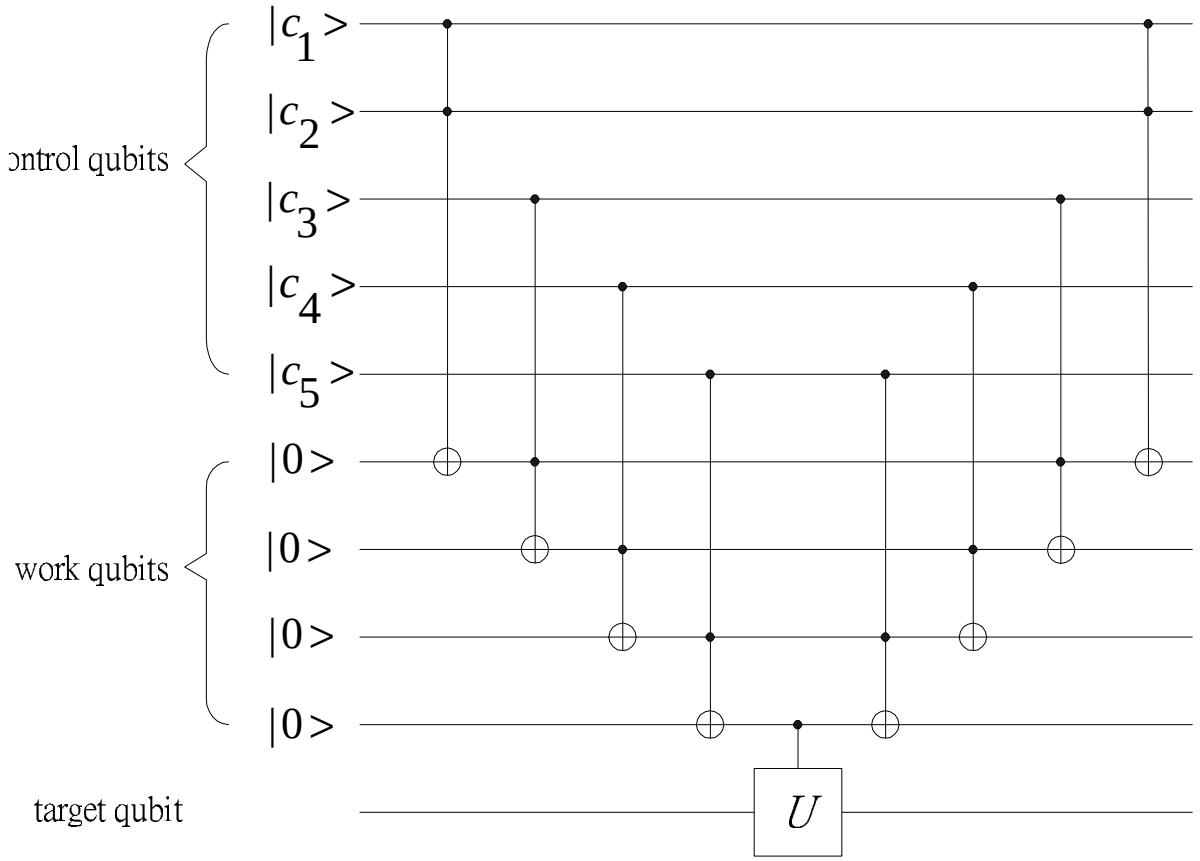
n-qubit controlled-U operations

- U : a single qubit operation
- $C^n(U)|c_1c_2\cdots c_n\rangle|t\rangle = |c_1c_2\cdots c_n\rangle U^{c_1c_2\cdots c_n}|t\rangle$: if the states of all n control qubits are in $|1\rangle$, i.e., $c_1 = c_2 = \cdots = c_n = 1$, then U will operate on the target qubit; otherwise no action

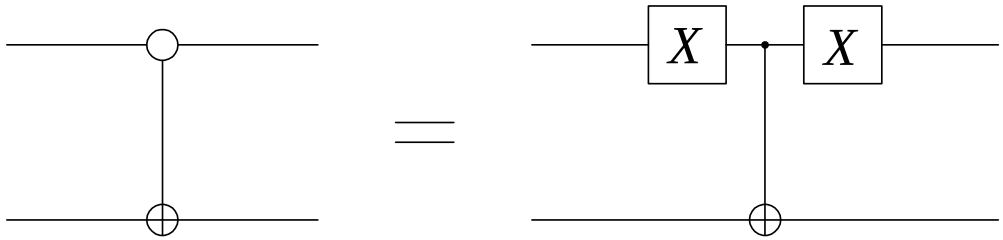

U
n=4

An Implementation of n-qubit controlled-U operations

- Need $(n-1)$ work qubits, $2(n-1)$ Toffoli gates and one single-qubit controlled-U gate

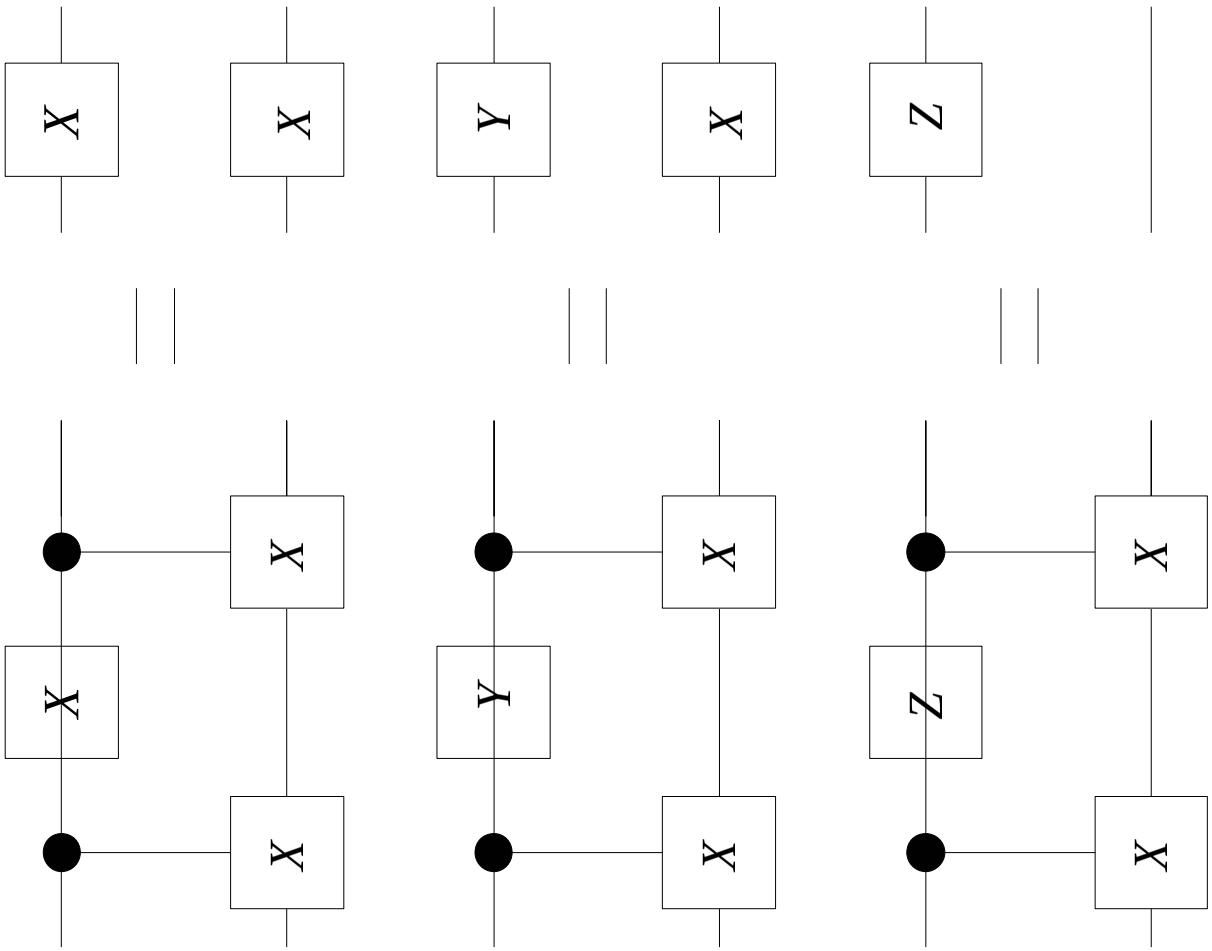


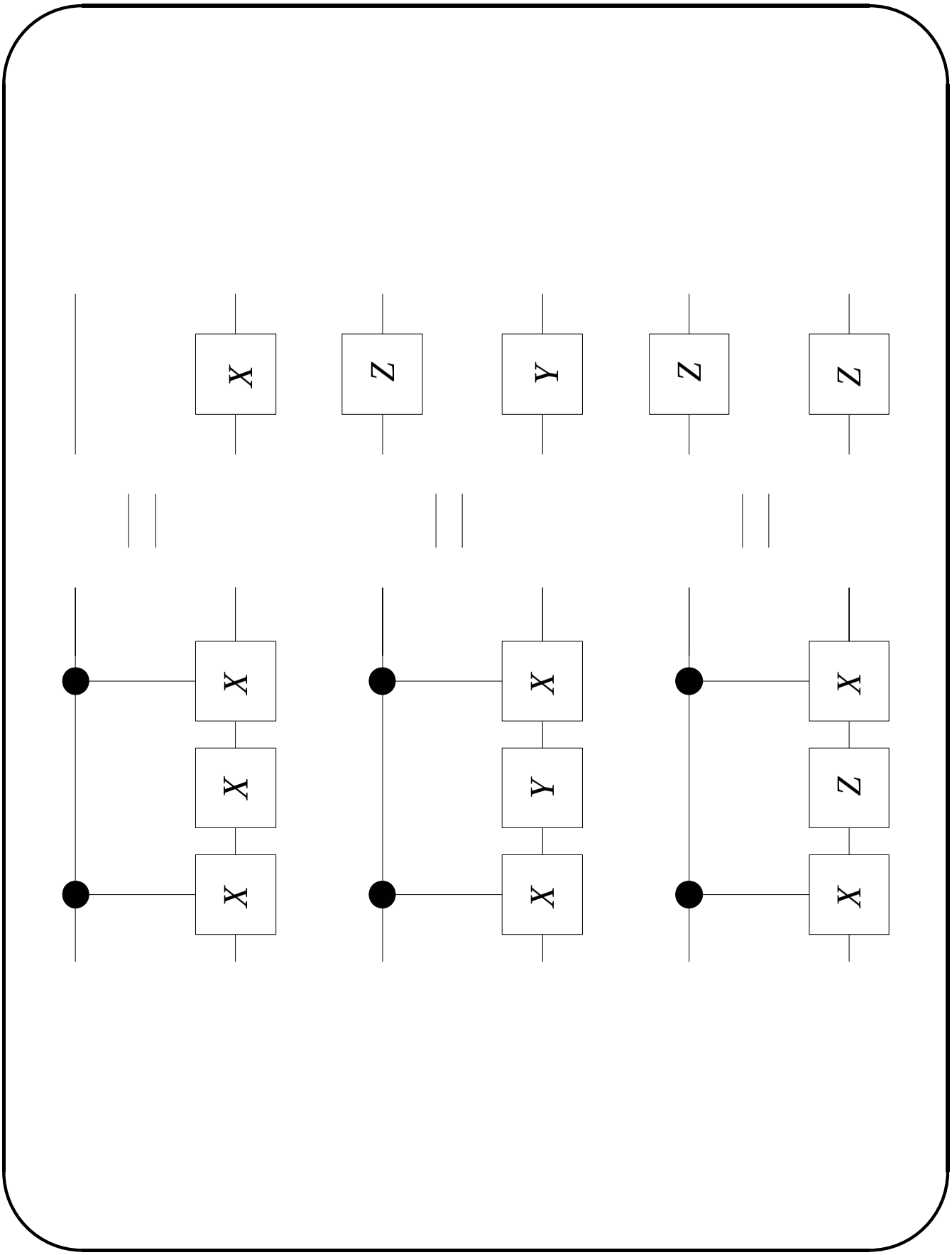
CNOT Gate Controlled by Setting Control Qubit to Zero



Some Circuit Identities

- C : a CNOT with qubit 1 the control qubit and qubit 2 the target qubit
- $C\sigma_{x,1}C = \sigma_{x,1}\sigma_{x,2}$, $C\sigma_{y,1}C = \sigma_{y,1}\sigma_{x,2}$, $C\sigma_{z,1}C = \sigma_{z,1}$
- $C\sigma_{x,2}C = \sigma_{x,2}$, $C\sigma_{y,2}C = \sigma_{z,1}\sigma_{y,2}$, $C\sigma_{z,2}C = \sigma_{z,1}\sigma_{z,2}$


X
X
Y
X
Z
X
X
X
Y
X
X
Z
X
X


X
Z
Y
Z
Z
X
X
X
X
Y
X
X
Z
X

Measurement in Quantum Circuits

General Measurements Through Projective Measurements

- $\{M_m\}$: a collection of general measurement operators on the state space H of a quantum system
  - $\mathcal{P}(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$: the probability that result m occurs, given the pre-measurement state $|\psi\rangle$
  - $\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}$: the post-measurement state of the quantum system
- $\{|m\rangle\}$: an orthonormal basis of the state space G of an ancilla quantum system
- $|0\rangle$: any fixed state vector of G
- $E \equiv \mathrm{Span}(|0\rangle)$: the subspace of G generated by $|0\rangle$

- U : a linear transformation from $H \otimes E$ into $H \otimes G$ defined as

$$U|\psi\rangle|0\rangle \equiv \sum_m M_m|\psi\rangle|m\rangle$$

  - U preserves inner product

$$\langle\varphi|\langle 0|U^\dagger U|\psi\rangle|0\rangle = \sum_{m,m'} \langle\varphi|M_m^\dagger M_{m'}|\psi\rangle\langle m|m'\rangle$$

$$= \sum_m \langle\varphi|M_m^\dagger M_m|\psi\rangle = \langle\varphi|\psi\rangle = \langle\varphi 0|\psi 0\rangle$$

  - U can be extended to be a unitary operator on $H \otimes G$

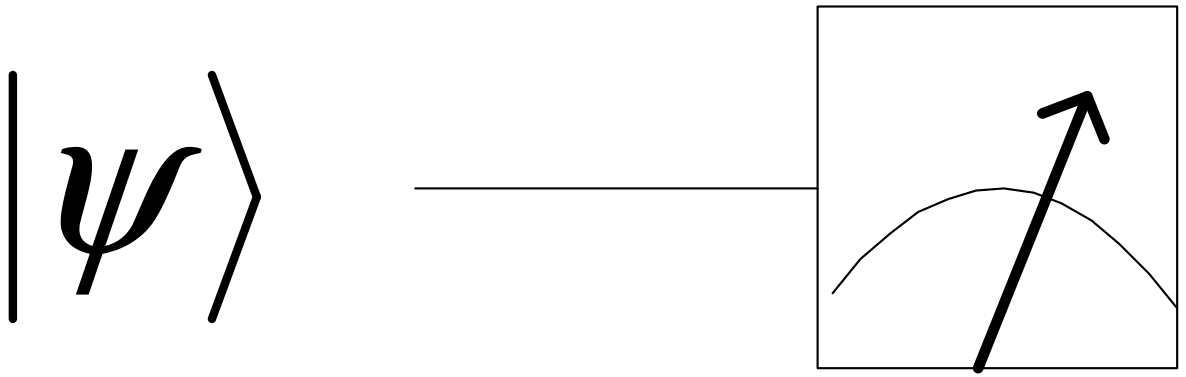
- $\{P_m = I_H \otimes |m\rangle\langle m|\}$: projective measurements on the state space $H \otimes G$ of the composite system
  - $\mathcal{P}'(m) = \langle\psi|\langle 0|U^\dagger P_m U|\psi\rangle|0\rangle$: the probability that result m occurs, given the pre-measurement state $U|\psi\rangle|0\rangle$ of the composite quantum system

$$\begin{aligned}\mathcal{P}'(m) &= \sum_{m',''} \langle\psi|M_{m'}^\dagger\langle m'|(I_H \otimes |m\rangle\langle m|)M_{m''}|\psi\rangle|m''\rangle \\ &= \langle\psi|M_m^\dagger M_m|\psi\rangle = \mathcal{P}(m)\end{aligned}$$

  - $\frac{P_m U|\psi\rangle|0\rangle}{\langle\psi|\langle 0|U^\dagger P_m U|\psi\rangle|0\rangle} = \frac{M_m|\psi\rangle|m\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \otimes |m\rangle$: the post-measurement state of the composite system

- A general measurement on a quantum system can be implemented by a projective measurement on a composite quantum system of the original quantum system and an ancilla quantum system after applying a unitary operator on the composite system

The Meter Symbol in Quantum Circuits



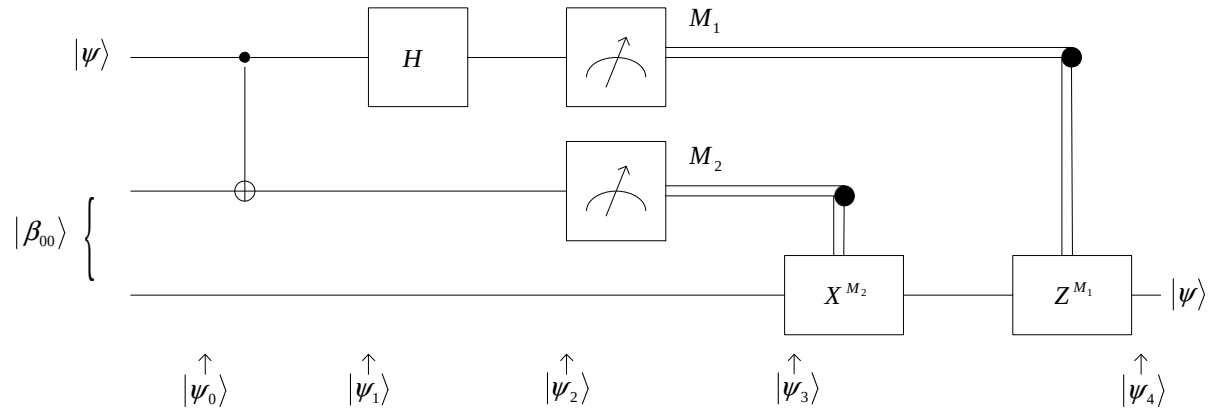
- $\{|m\rangle\langle m|\}$: projective measurement in the computational basis

Two Principles

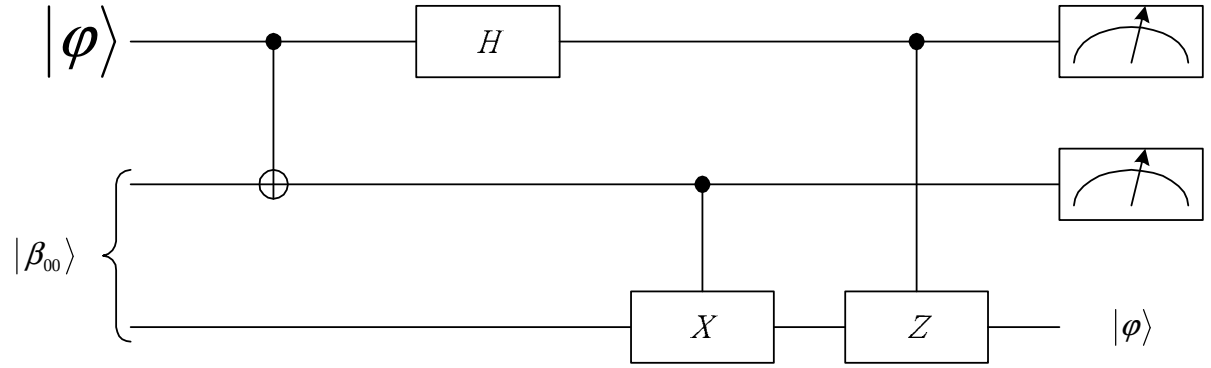
- Principle of deferred measurement : measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit and if the measurement results are used at any stage of the circuit then the classically controlled operations can be replaced by conditional quantum operations
- Principle of implicit measurement : without loss of generality, any unterminated quantum wires (qubits which are not measured) at the end of a quantum circuit may be assumed to be measured

An Illustration of the Principle of Deferred Measurement

- Quantum teleportation circuit



- Deferred measurement in quantum teleportation circuit



An Illustration of the Principle of Implicit Measurement

- $\rho = \sum_i \alpha_i T_i \otimes S_i$: density operator describing a two-qubit system
- $\{P_0 = I \otimes |0\rangle\langle 0|, P_1 = I \otimes |1\rangle\langle 1|\}$: projective measurement in the computational basis of the 2nd qubit
- ρ' : density operator after the measurement

  $$\rho' = P_0 \rho P_0 + P_1 \rho P_1 = \sum_i \alpha_i T_i \otimes (|0\rangle\langle 0|S_i|0\rangle\langle 0| + |1\rangle\langle 1|S_i|1\rangle\langle 1|)$$

- $\mathrm{tr}_2(\rho) = \mathrm{tr}_2(\rho')$: the reduced density operators for the first qubit are the same no matter whether the second qubit is measured or not

$$
\begin{aligned}
\mathrm{tr}_2(\rho) &= \sum_i \alpha_i T_i \mathrm{tr}(S_i) \\
\mathrm{tr}_2(\rho') &= \sum_i \alpha_i T_i \mathrm{tr}(|0\rangle\langle 0|S_i|0\rangle\langle 0| + |1\rangle\langle 1|S_i|1\rangle\langle 1|) \\
&= \sum_i \alpha_i T_i (\langle 0|S_i|0\rangle + \langle 1|S_i|1\rangle) \\
&= \sum_i \alpha_i T_i \mathrm{tr}(S_i)
\end{aligned}
$$

Applications

Non-orthogonal States Cannot Be Distinguished

- $\{M_j\}$: measurement operators
- $|\psi_1\rangle$ and $|\psi_2\rangle$: two non-orthogonal states to be distinguished and

$$|\psi_2\rangle = \alpha|\psi_1\rangle + \beta|\psi\rangle,$$

  where $|\psi_1\rangle$ and $|\psi\rangle$ are orthonormal. Note that $|\alpha|^2 + |\beta|^2 = 1$ and then $|\beta| < 1$.

- $f(\cdot)$: a rule to guess which state vector is observed based on the outcome of the measurement, i.e., either $f(j) = 1$ or $f(j) = 2$.

Suppose that $|\psi_1\rangle$ and $|\psi_2\rangle$ can be distinguished reliably, i.e.,

$$\sum_{j:f(j)=1} \langle\psi_1|M_j^\dagger M_j|\psi_1\rangle = \langle\psi_1|\left(\sum_{j:f(j)=1} M_j^\dagger M_j\right)|\psi_1\rangle = \langle\psi_1|G_1|\psi_1\rangle = 1$$

$$\sum_{j:f(j)=2} \langle\psi_2|M_j^\dagger M_j|\psi_2\rangle = \langle\psi_2|\left(\sum_{j:f(j)=2} M_j^\dagger M_j\right)|\psi_2\rangle = \langle\psi_2|G_2|\psi_2\rangle = 1$$

where $G_i = \sum_{j:f(j)=i} M_j^\dagger M_j$, for $i = 1, 2$.

Since $G_1 + G_2 = I$, we have $\langle\psi_1|(G_1 + G_2)|\psi_1\rangle = 1$ and then

$$\langle\psi_1|G_2|\psi_1\rangle = 0 \Rightarrow \sqrt{G_2}|\psi_1\rangle = 0 \Rightarrow \sqrt{G_2}|\psi_2\rangle = \beta\sqrt{G_2}|\psi\rangle$$

Thus a contradiction is obtained as follows

$$\langle\psi_2|G_2|\psi_2\rangle = |\beta|^2\langle\psi|G_2|\psi\rangle \leq |\beta|^2 < 1$$

since $\langle\psi|G_2|\psi\rangle \leq \langle\psi|(G_1 + G_2)|\psi\rangle = \langle\psi|\psi\rangle = 1$.

Distinquishing Two State Vectors

- $|\psi_1\rangle = |0\rangle$ and $|\psi_2\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$: two test state vectors
- A POVM

$$E_1 = \frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1|,\ E_2 = \frac{\sqrt{2}}{1+\sqrt{2}}\frac{(|0\rangle - |1\rangle)(\langle 0| - \langle 1|)}{2},\ E_3 = I - E_1 - E_2$$

- When $|\psi_1\rangle$ is given,

$$\mathcal{P}(1) = 0,\ \mathcal{P}(2) = \frac{\sqrt{2}}{2(1+\sqrt{2})},\ \mathcal{P}(3) = 1 - \frac{\sqrt{2}}{2(1+\sqrt{2})}$$

- When $|\psi_2\rangle$ is given,

$$\mathcal{P}(1) = \frac{\sqrt{2}}{2(1+\sqrt{2})},\ \mathcal{P}(2) = 0,\ \mathcal{P}(3) = 1 - \frac{\sqrt{2}}{2(1+\sqrt{2})}$$

Superdense Coding

- Goal : Alice wants to send two classical bits of information to Bob by transmitting only one qubit to Bob
- Initialization : preparing a pair of qubits in a Bell State

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

  Alice held the first qubit and Bob held the second qubit before apart (may send by a third party)

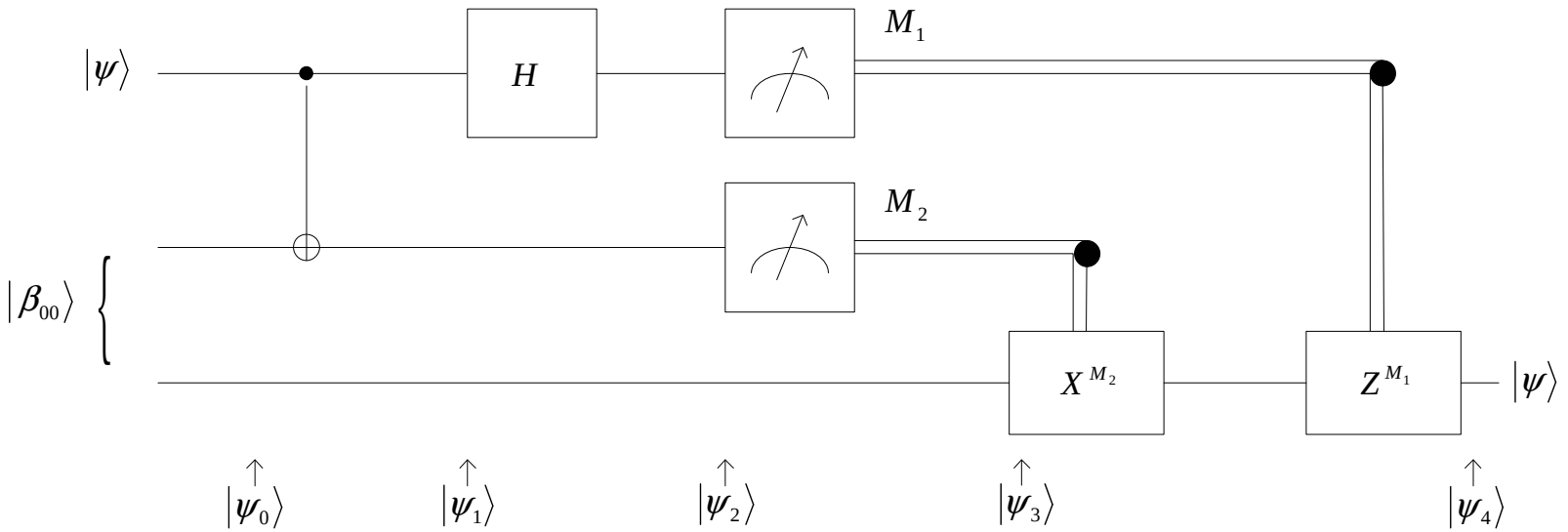
- Alice takes action on her qubit according the two bits of

information she wants to send

$$
\begin{aligned}
00 : |\psi\rangle &\rightarrow (I \otimes I)|\psi\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \\
01 : |\psi\rangle &\rightarrow (Z \otimes I)|\psi\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \\
10 : |\psi\rangle &\rightarrow (X \otimes I)|\psi\rangle = \frac{|10\rangle + |01\rangle}{\sqrt{2}} \\
11 : |\psi\rangle &\rightarrow (iY \otimes I)|\psi\rangle = \frac{|10\rangle - |01\rangle}{\sqrt{2}}
\end{aligned}
$$

- Alice sends her qubit to Bob
- The four Bell states form an orthonormal basis of the two-qubit system and can form a projective measrement
- With two qubits together, Bob makes the projective measurement

Quantum Teleportation



Quantum Teleportation

- $|\psi_2\rangle$: state of the three-qubit system before Alice makes her measurement

$$\begin{aligned} |\psi_2\rangle &= \frac{1}{2}\left(|00\rangle(\alpha|0\rangle + \beta|1\rangle) + |01\rangle(\alpha|1\rangle + \beta|0\rangle)\right. \\ &\quad \left. +|10\rangle(\alpha|0\rangle - \beta|1\rangle) + |11\rangle(\alpha|1\rangle - \beta|0\rangle)\right) \end{aligned}$$

- $\{|00\rangle\langle 00|, |01\rangle\langle 01|, |10\rangle\langle 10|, |11\rangle\langle 11|\}$: a POVM measurement made by Alice on her two qubits
- $\rho = |\psi_2\rangle\langle\psi_2|$: density operator for the three-qubit system before the measurement
- ρ' : density operator for the three-qubit system after the unspecified (from Bob's point of view) measurement

$$\rho' = \sum_m M_m \rho M_m^\dagger = \sum_m M_m |\psi_2\rangle\langle\psi_2| M_m^\dagger$$

- $|00\rangle\langle 00|\psi_2\rangle = (1/2)|00\rangle(\alpha|0\rangle + \beta|1\rangle)$
- $|01\rangle\langle 01|\psi_2\rangle = (1/2)|01\rangle(\alpha|1\rangle + \beta|0\rangle)$
- $|10\rangle\langle 10|\psi_2\rangle = (1/2)|10\rangle(\alpha|0\rangle - \beta|1\rangle)$
- $|11\rangle\langle 11|\psi_2\rangle = (1/2)|11\rangle(\alpha|1\rangle - \beta|0\rangle)$
- ρ^B : the reduced density operator of Bob's qubit

$$\rho^B = \mathrm{tr}_A(\rho') = \sum_m \mathrm{tr}_A(M_m|\psi_2\rangle\langle\psi_2|M_m^\dagger)$$

$$\begin{aligned} = & \frac{1}{4}((\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)^\dagger + (\alpha|1\rangle + \beta|0\rangle)(\alpha|1\rangle + \beta|0\rangle)^\dagger \\ & +(\alpha|0\rangle - \beta|1\rangle)(\alpha|0\rangle - \beta|1\rangle)^\dagger + (\alpha|1\rangle - \beta|0\rangle)(\alpha|1\rangle - \beta|0\rangle)^\dagger) \\ = & \frac{2(|\alpha|^2 + |\beta|^2)|0\rangle\langle 0| + 2(|\alpha|^2 + |\beta|^2)|1\rangle\langle 1|}{4} \\ = & \frac{|0\rangle\langle 0| + |1\rangle\langle 1|}{2} = \frac{I}{2} \end{aligned}$$

- Bob does not have any information about the state $|\psi\rangle$ if Alice does not send him her measurement result, preventing Alice from using teleportation to transmit information to Bob faster than light