Introduction to quantum computation -Heisenberg picture in quantum computation and the Gottesman-Knill theorem

Shunji Tsuchiya
Chuo University and ITP ETHZ

Qubit

- any quantum mechanical system that has two distinct quantum states can be a qubit

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

- spin-1/2 $|0\rangle = |\uparrow\rangle, \quad |1\rangle = |\downarrow\rangle$
- atom $|0\rangle = |\text{ground state}\rangle, \ |1\rangle = |\text{excited state}\rangle \quad \cdots$

- qubit can be in superposition of $|0\rangle$ and $|1\rangle$

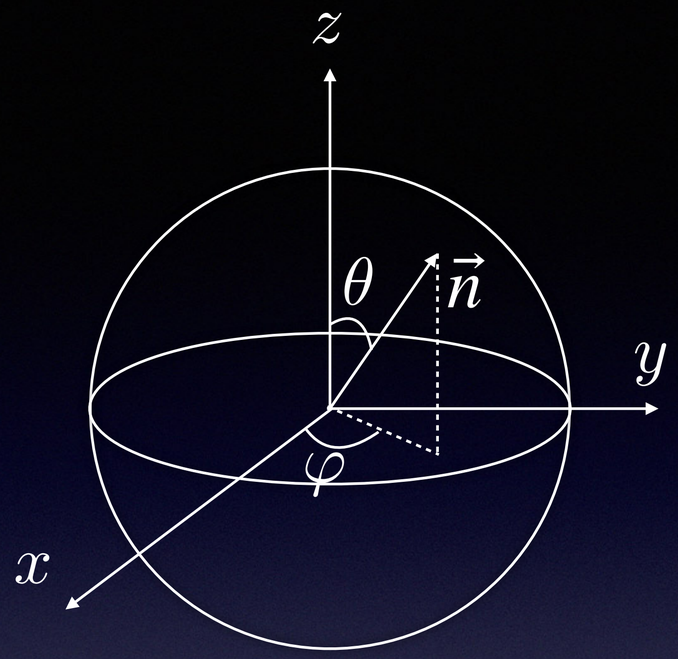
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \alpha, \ \beta \in \mathbb{C} \quad |\alpha|^2 + |\beta|^2 = 1$$

Bloch sphere

- general form of a single qubit state

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

$$(0 \leq \theta \leq \pi,\ 0 \leq \varphi \leq \pi)$$



・single qubit state can be visualized as a single vector on a unit sphere

$$\vec{n} = (\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$$

Exercise1

Show $|\psi\rangle = R_z(\varphi)R_y(\theta)|0\rangle$

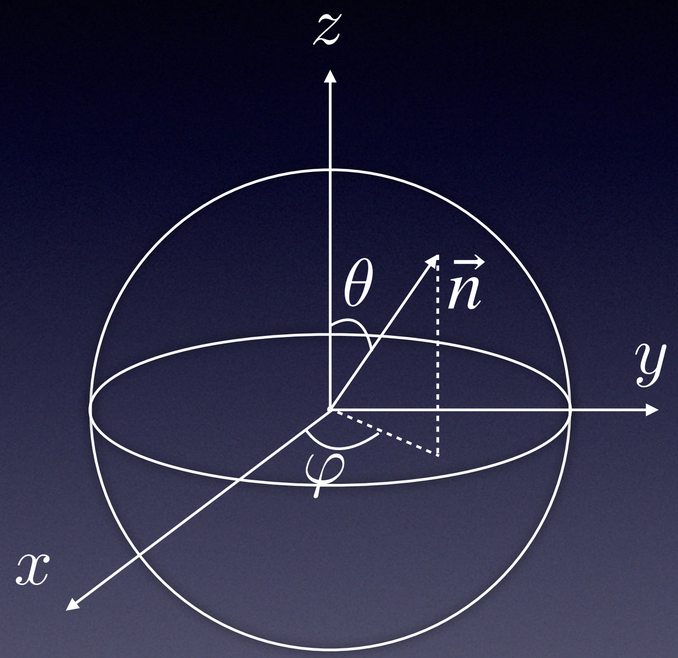
this means that $|\psi\rangle$ corresponds to the ”up” state in the direction of $\vec{n}$

Bloch sphere

- general form of a single qubit state

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

$$(0 \le \theta \le \pi,\ 0 \le \varphi \le \pi)$$



Exercise 2

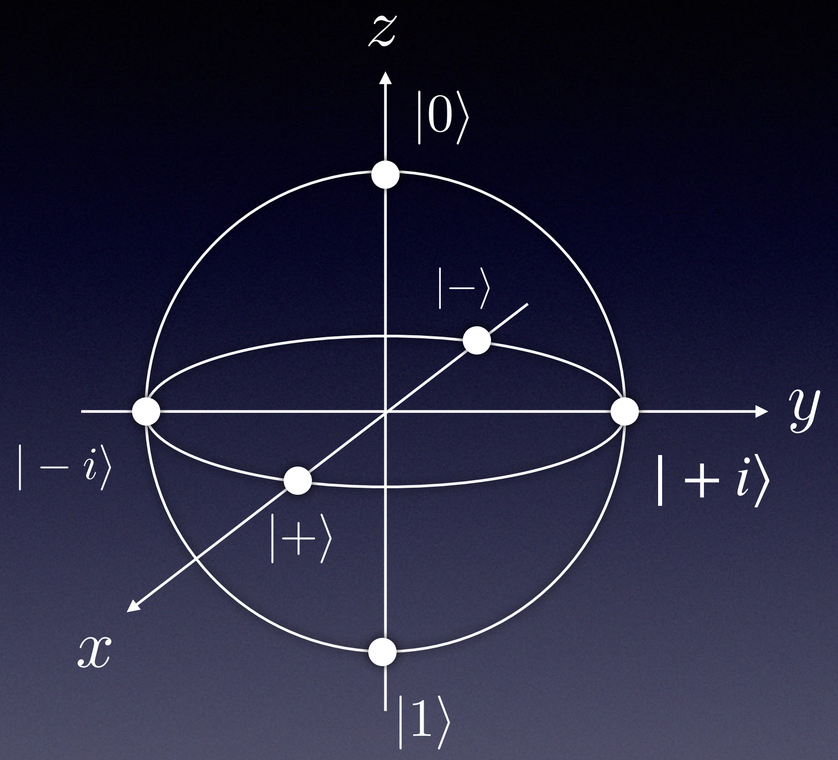
Show

$$\langle\psi|X|\psi\rangle = \sin\theta\cos\phi$$
$$\langle\psi|Y|\psi\rangle = \sin\theta\sin\phi$$
$$\langle\psi|Z|\psi\rangle = \cos\theta$$

$$\langle\psi|\vec{\sigma}|\psi\rangle = \vec{n}$$

$$(X = \sigma_x,\ Y = \sigma_y,\ Z = \sigma_z)$$

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$



$$X|\pm\rangle = \pm|\pm\rangle$$

$$Y|\pm i\rangle = \pm|\pm i\rangle$$

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \qquad |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$$

$$|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \qquad |-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$$

Single-qubit unitary

- U : single qubit operation

$$|\psi'\rangle = U|\psi\rangle \qquad \langle\psi'|\psi'\rangle = \langle\psi|U^\dagger U|\psi\rangle$$

$$\langle\psi'|\psi'\rangle = \langle\psi|\psi\rangle = 1$$

$$\Rightarrow \quad U^\dagger U = I$$

- a general U transforms $|0\rangle$ to $\cos(\theta/2)|0\rangle + e^{i\varphi}\sin(\theta/2)|1\rangle$

$$U|0\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle$$

$$U^\dagger U = I$$

$$\Rightarrow \quad U = \begin{pmatrix} \cos(\theta/2) & -e^{i\lambda}\sin(\theta/2) \\ e^{i\varphi}\sin(\theta/2) & e^{i(\lambda+\varphi)}\cos(\theta/2) \end{pmatrix}$$

Euler decomposition

- any single-qubit unitary U can be witten as

$$U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$$

$$R_z(\beta) = \cos(\beta/2) I - i \sin(\beta/2) Z = \begin{pmatrix} e^{-i\beta/2} & 0 \\ 0 & e^{i\beta/2} \end{pmatrix}$$

$$R_y(\beta) = \cos(\gamma/2) I - i \sin(\gamma/2) Y = \begin{pmatrix} \cos(\gamma/2) & -\sin(\gamma/2) \\ \sin(\gamma/2) & \cos(\gamma/2) \end{pmatrix}$$

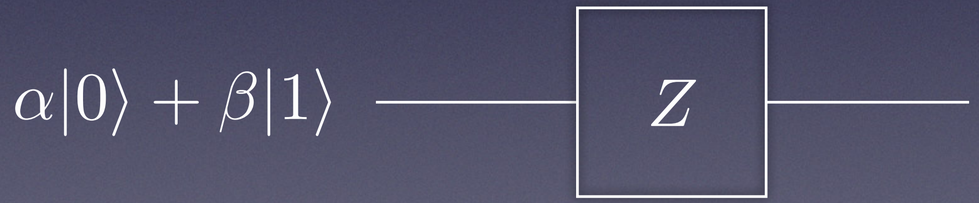
- any single-qubit operation can be decomposed into rotations about two orthogonal axes
- any single-qubit operation can be realized if rotations about two orthogonal axes can be implemented

Pauli gates

- X-gate

$$X = |1\rangle\langle 0| + |0\rangle\langle 1|$$: bit flip gate

- Z-gate



$$Z = |0\rangle\langle 0| - |1\rangle\langle 1|$$: phase flip gate

Pauli gates

- X-gate

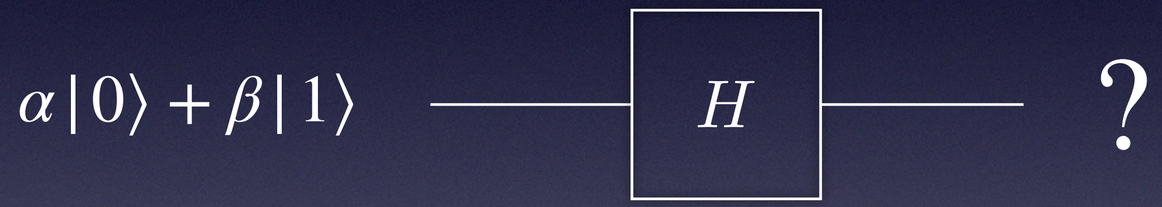
$$X = |1\rangle\langle 0| + |0\rangle\langle 1|$$: bit flip gate

- Y-gate

$$Y = i|1\rangle\langle 0| - i|0\rangle\langle 1|$$: bit-phase flip gate

Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$



Exercise 3

$$H(\alpha|0\rangle + \beta|1\rangle) = ?$$

Hadamard gate

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

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H : |0\rangle \to |+\rangle,\ |1\rangle \to |-\rangle \qquad H = |+\rangle\langle 0| + |-\rangle\langle 1|$$

- H exchanges x and z axes of the Bloch sphere

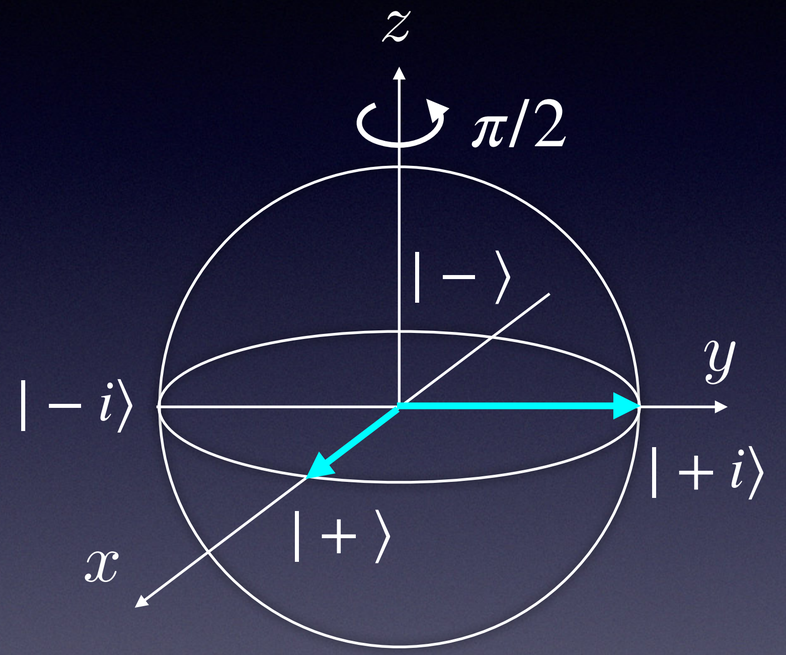
an important gate for making superposition of $|0\rangle$ and $|1\rangle$

Phase gate

$$S = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$$

$$S = e^{i\pi/4} \begin{pmatrix} e^{-i\pi/4} & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = e^{i\pi/4} R_z(\pi/2)$$

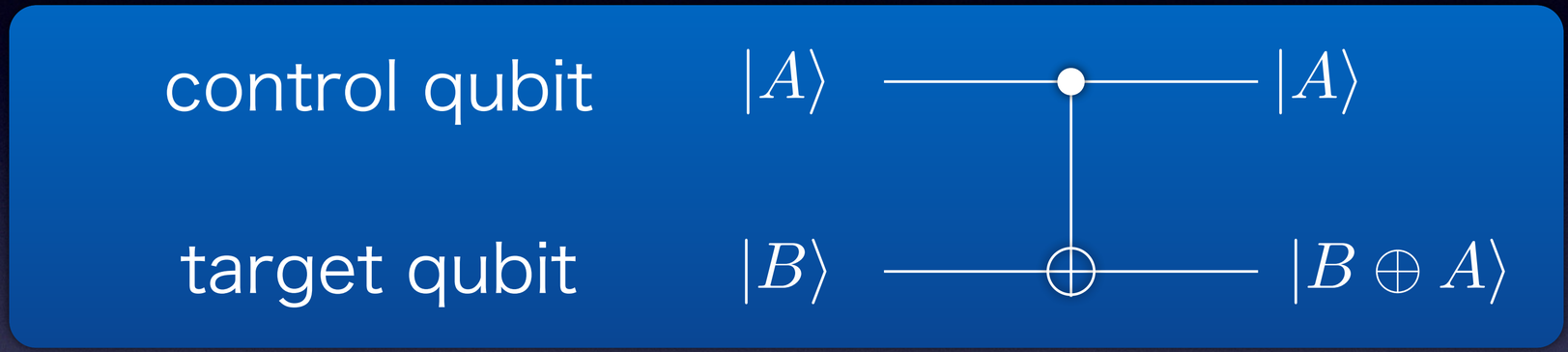
$\pi/2$ rotation about z-axis



$$S : |+\rangle \to |+i\rangle, \quad |-\rangle \to |-i\rangle$$

Two-qubit gates

- CNOT(controlled-NOT) gate



$\oplus$: sum in mod 2

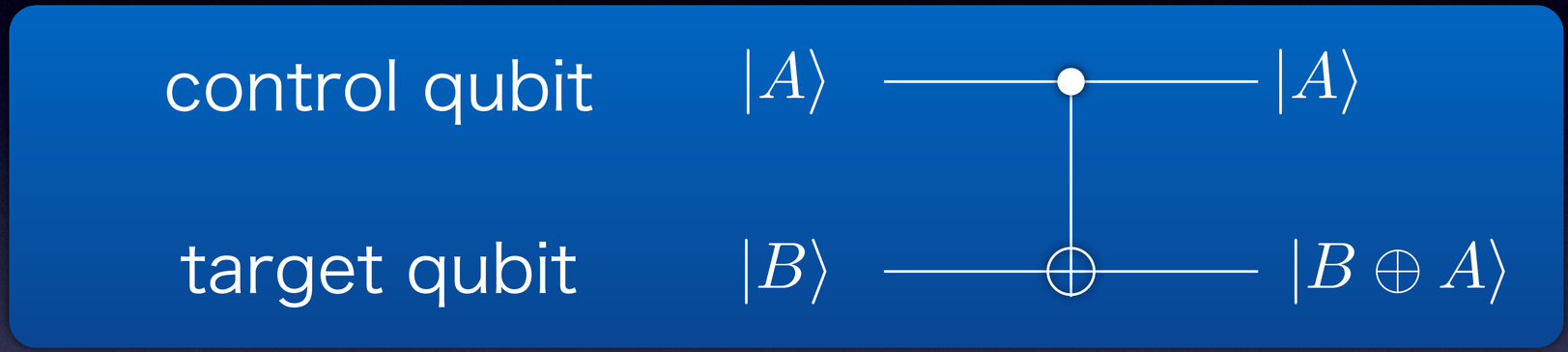
$|00\rangle \to |00\rangle \quad |01\rangle \to |01\rangle \quad |10\rangle \to |11\rangle \quad |11\rangle \to |10\rangle$

Exercise 4

Express the CNOT gate in a matrix form

Two-qubit gate

- CNOT(controlled-NOT) gate



$\oplus$: sum in mod 2

$$|00\rangle \to |00\rangle \quad |01\rangle \to |01\rangle \quad |10\rangle \to |11\rangle \quad |11\rangle \to |10\rangle$$

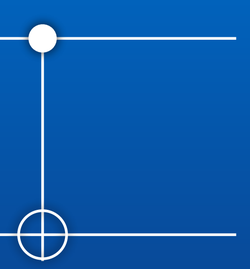
$$U_{CN} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \qquad U_{CN}^{\dagger} U_{CN} = I$$

Two-qubit gate

- CNOT(controlled-NOT) gate

control qubit $|A\rangle$ — $|A\rangle$

target qubit $|B\rangle$ — $|B \oplus A\rangle$



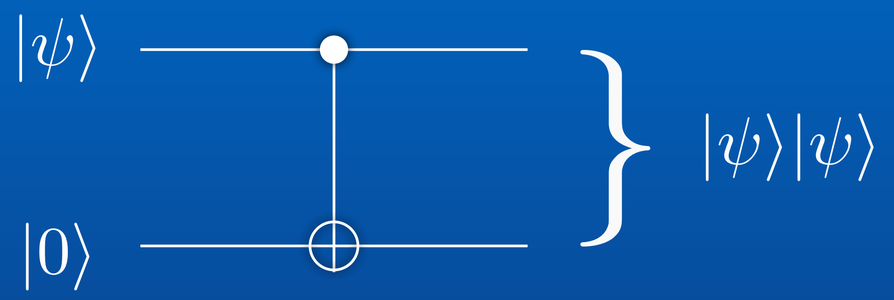
$$\mathrm{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X$$

CNOT gate

$|\psi\rangle = |0\rangle$

or

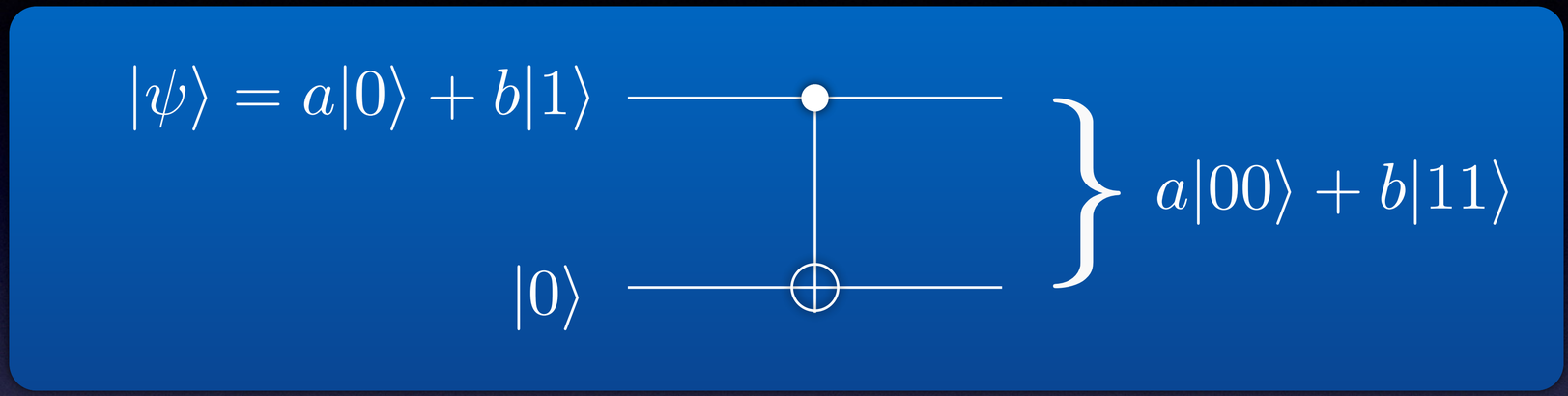
$|\psi\rangle = |1\rangle$



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

- CNOT gate can copy the state of a classical bit

CNOT gate



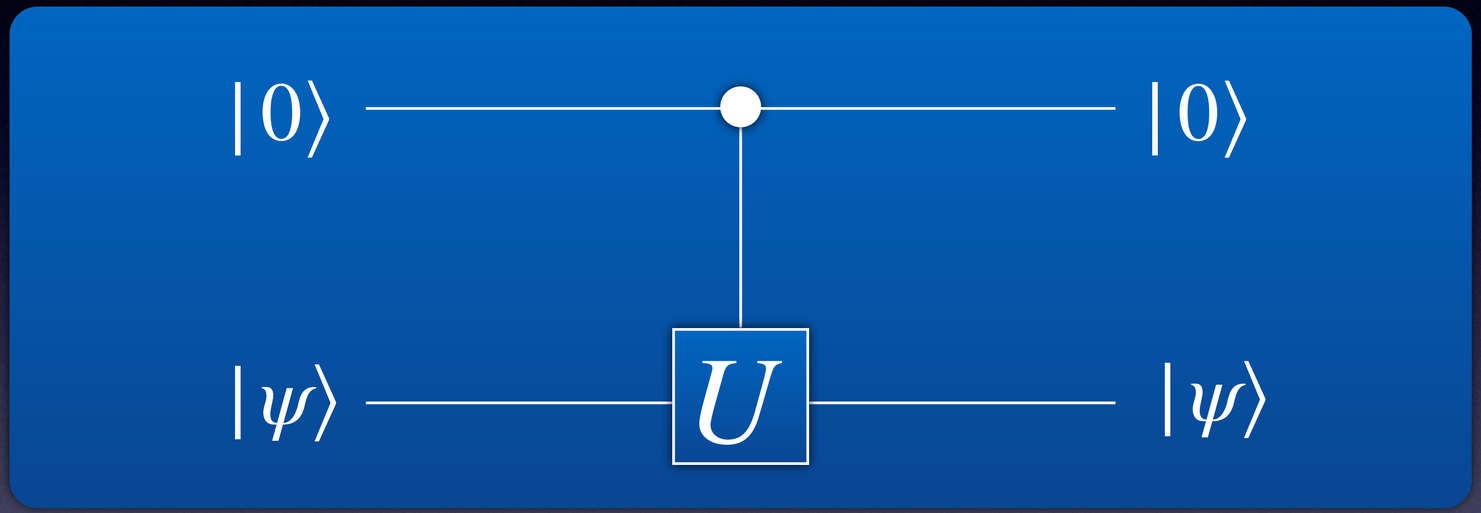
$$a|00\rangle + b|11\rangle \neq |\psi\rangle|\psi\rangle \quad \text{unless} \quad ab = 0$$

- CNOT gate cannot copy the state of a qubit in superposition

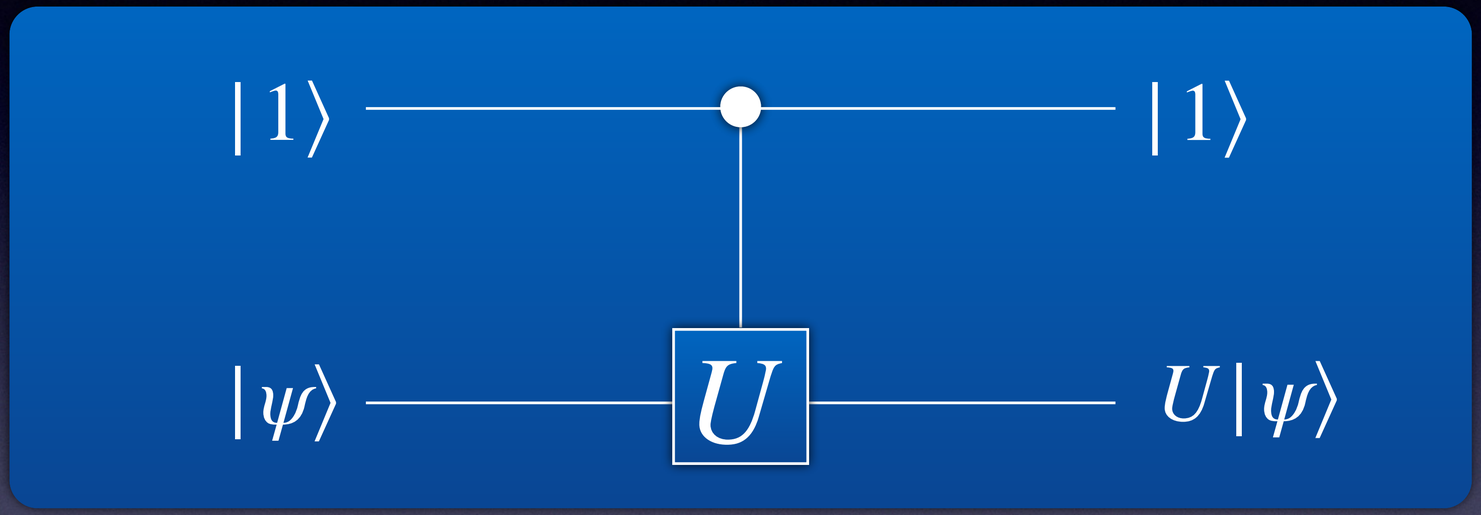
⇐ no-cloning theorem

It is impossible to create an independent and identical copy of an arbitrary unknown quantum state

Controlled-U gate



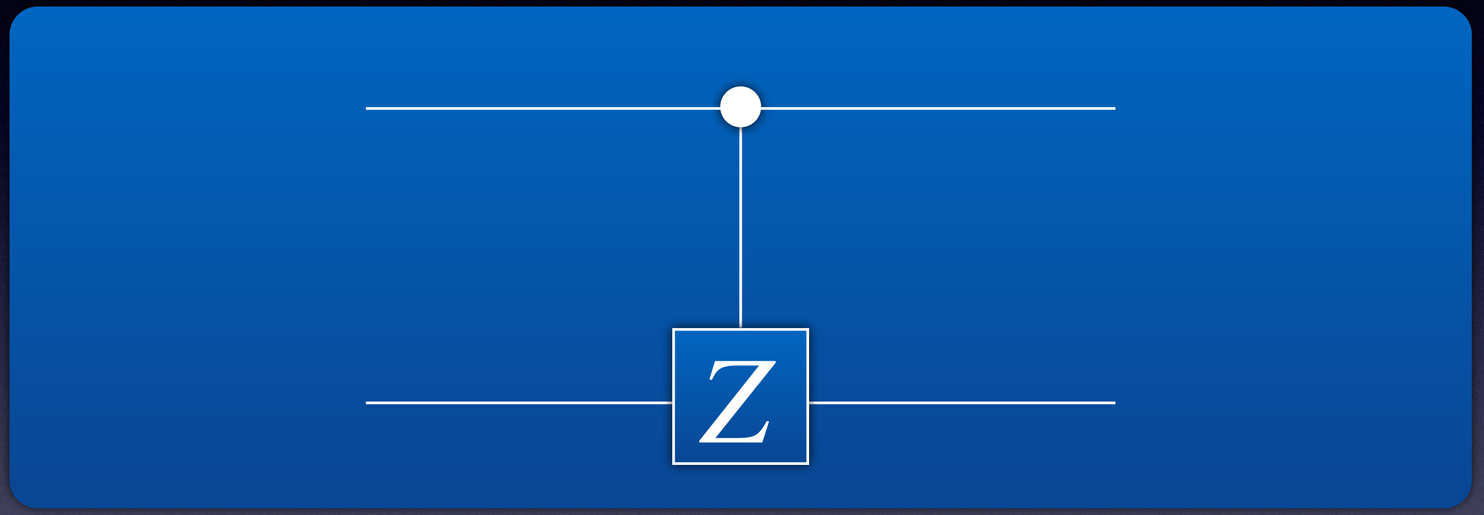
Controlled-U gate



$$\Lambda(U) = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

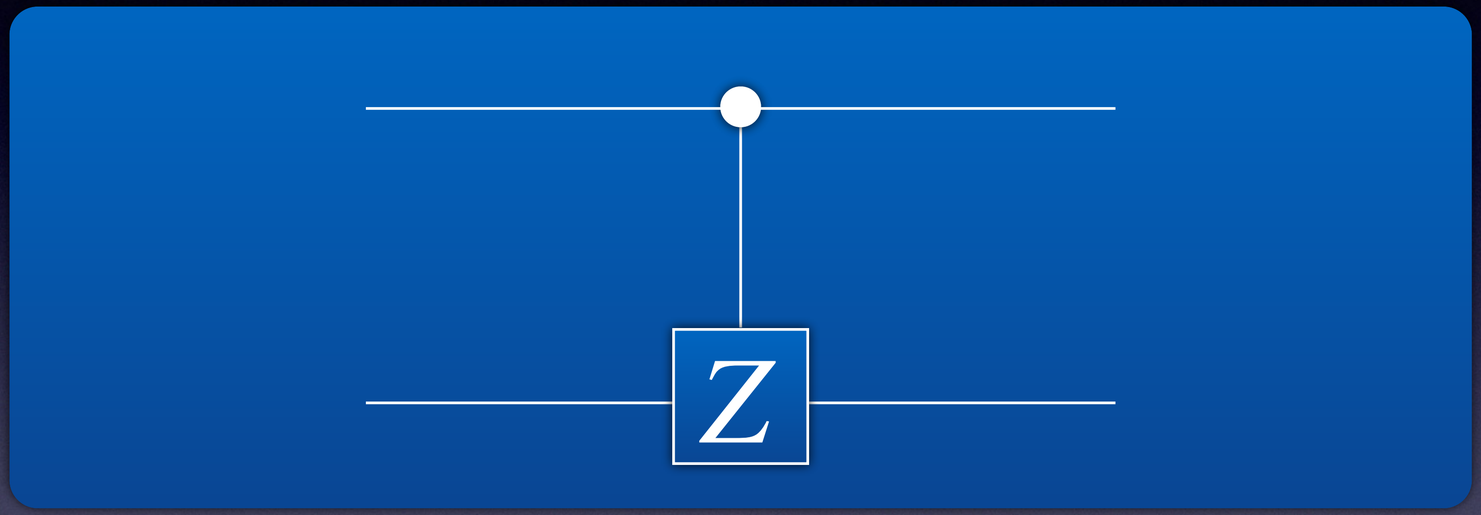
CNOT gate : $U = X$ CZ gate : $U = Z$

Controlled-Z gate



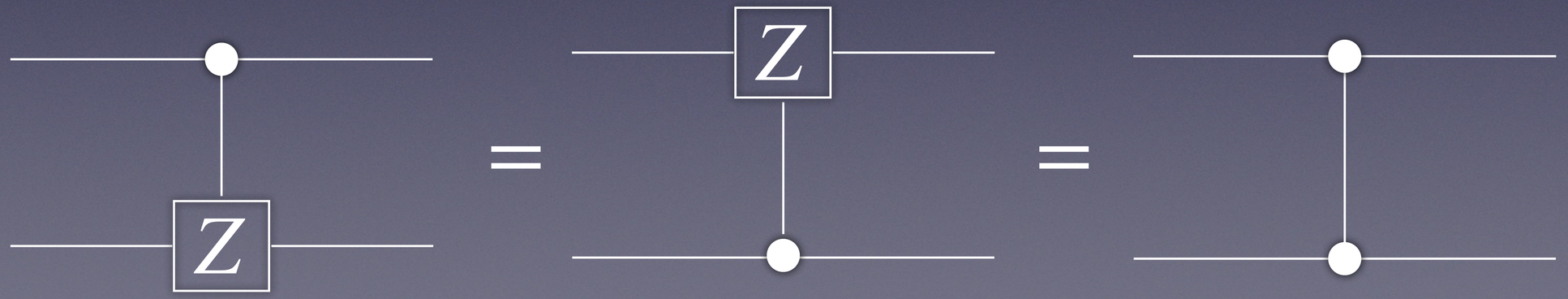
$$CZ = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$$

Controlled-Z gate

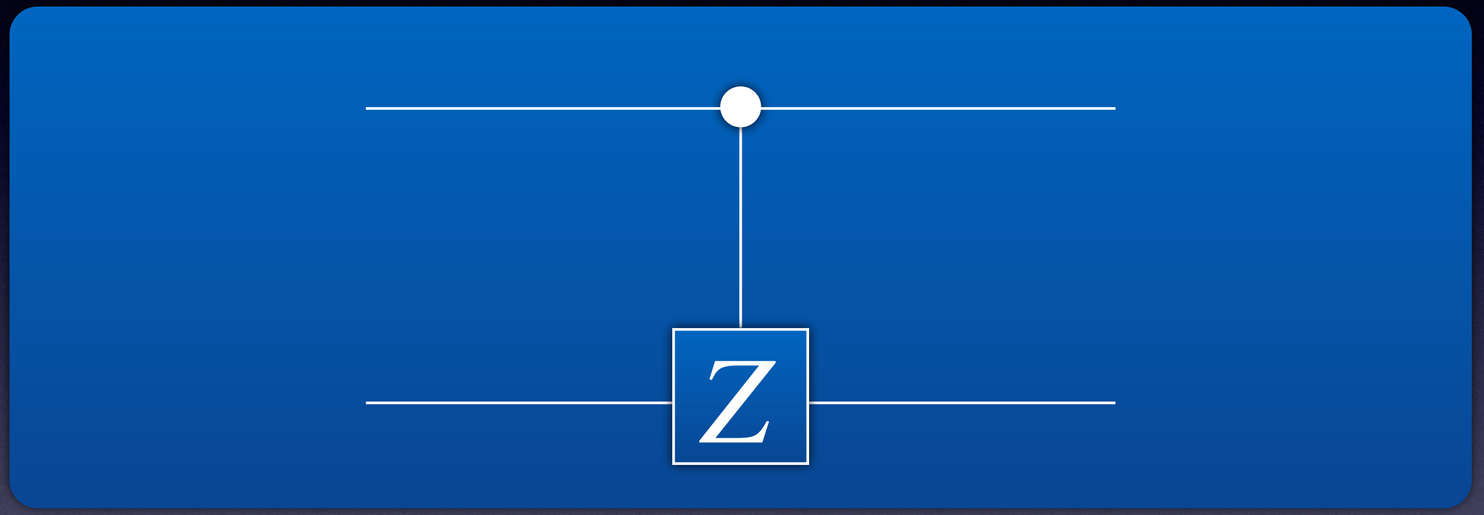


Exercise 5.1

Show



Controlled-Z gate

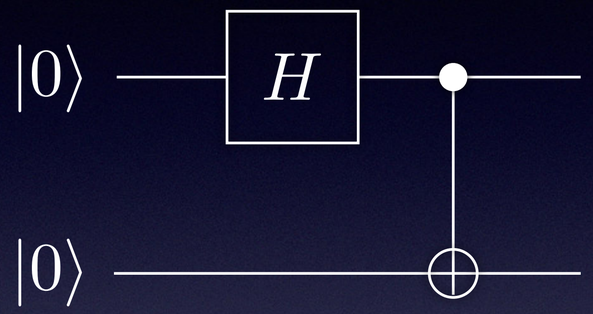


Exercise 5.2

Show

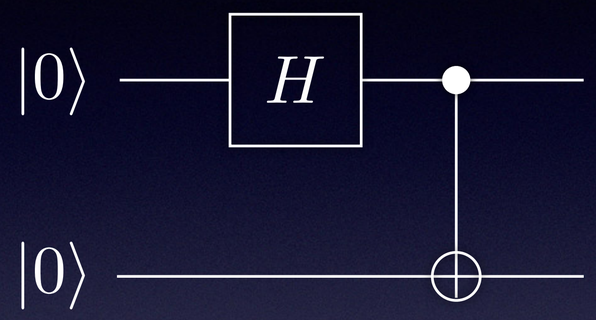
Quantum circuits

example



Quantum circuits

example

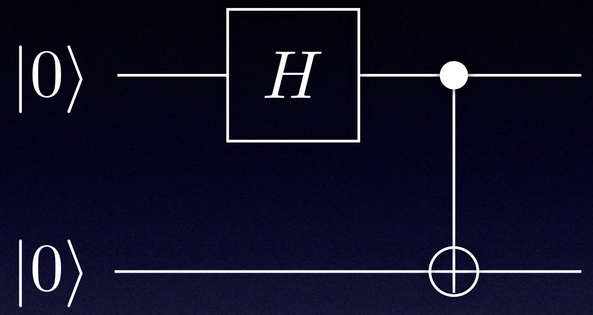


$$|00\rangle \longrightarrow H|00\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle) \longrightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \neq |\psi\rangle\,|\phi\rangle$$

Bell state

- the circuit outputs an entangled state from the input of a product state

Quantum circuits



Exercise 6

Show

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

$$|10\rangle \longrightarrow \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \qquad |11\rangle \longrightarrow \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$

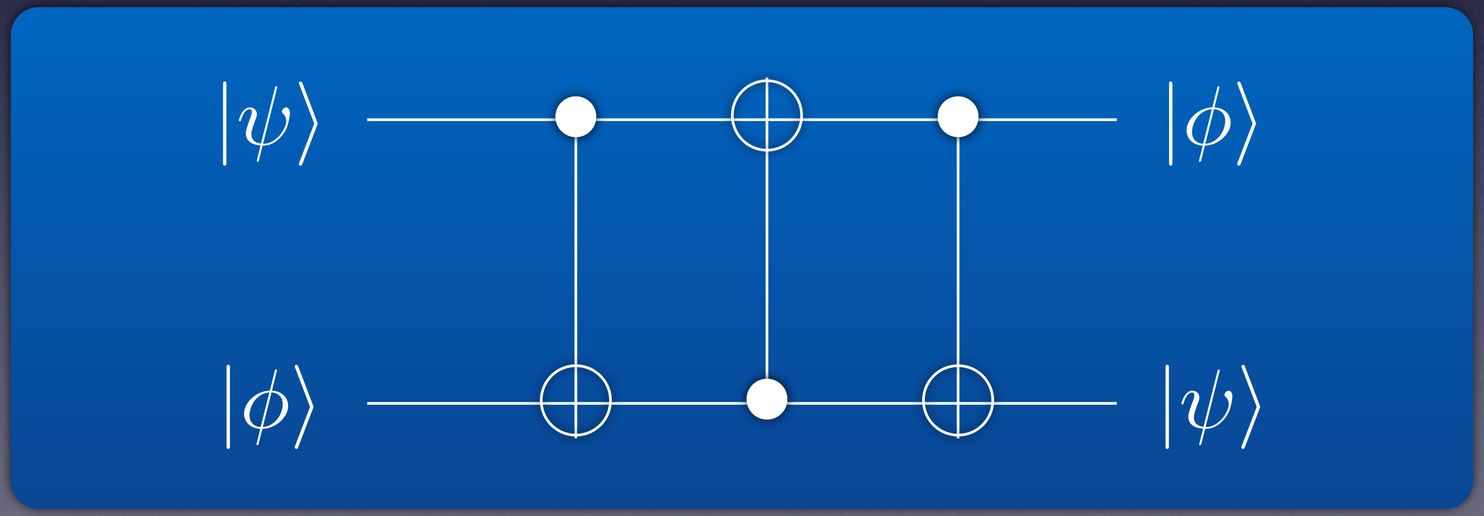
Confirm that this set of states form a orthonormal basis.

Bell basis

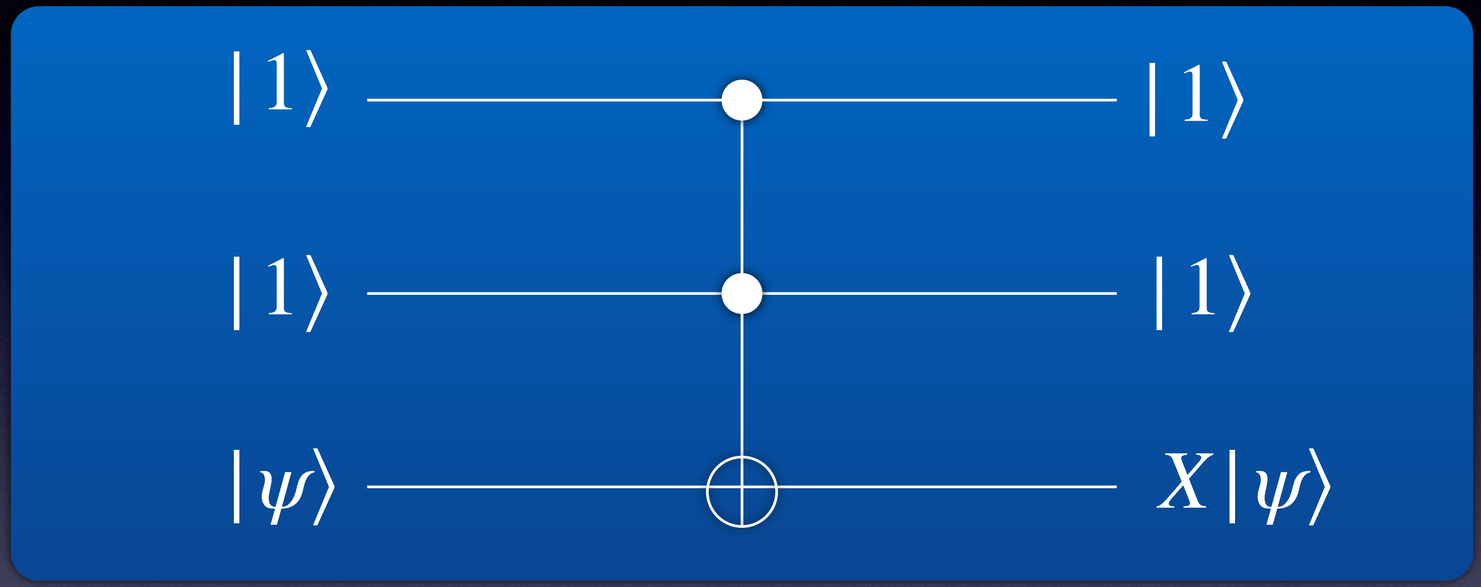
SWAP gate

Exercise 7

Show that operation of three CNOT gates is equivalent to a SWAP gate



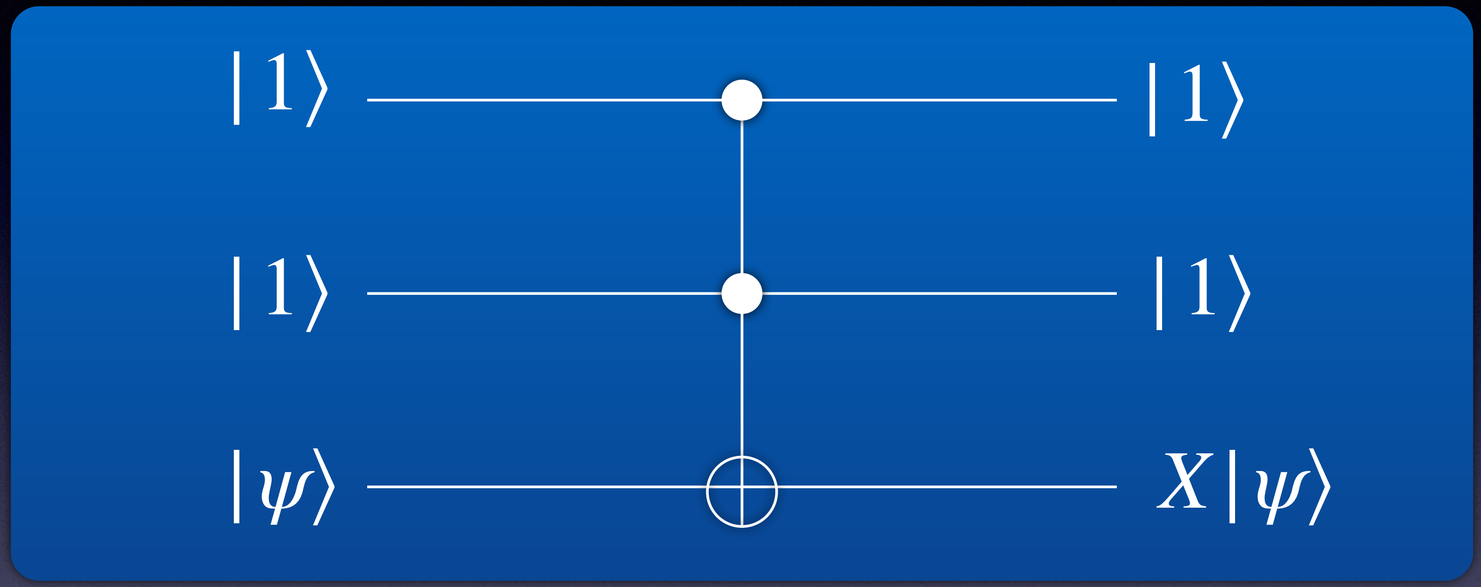
Toffoli gate



$$T = (I^{\otimes 2} - |11\rangle\langle 11|) \otimes I + |11\rangle\langle 11| \otimes X$$

- a universal logic gate for reversible logic circuits: any classical reversible logic circuit can be constructed from Toffoli gates

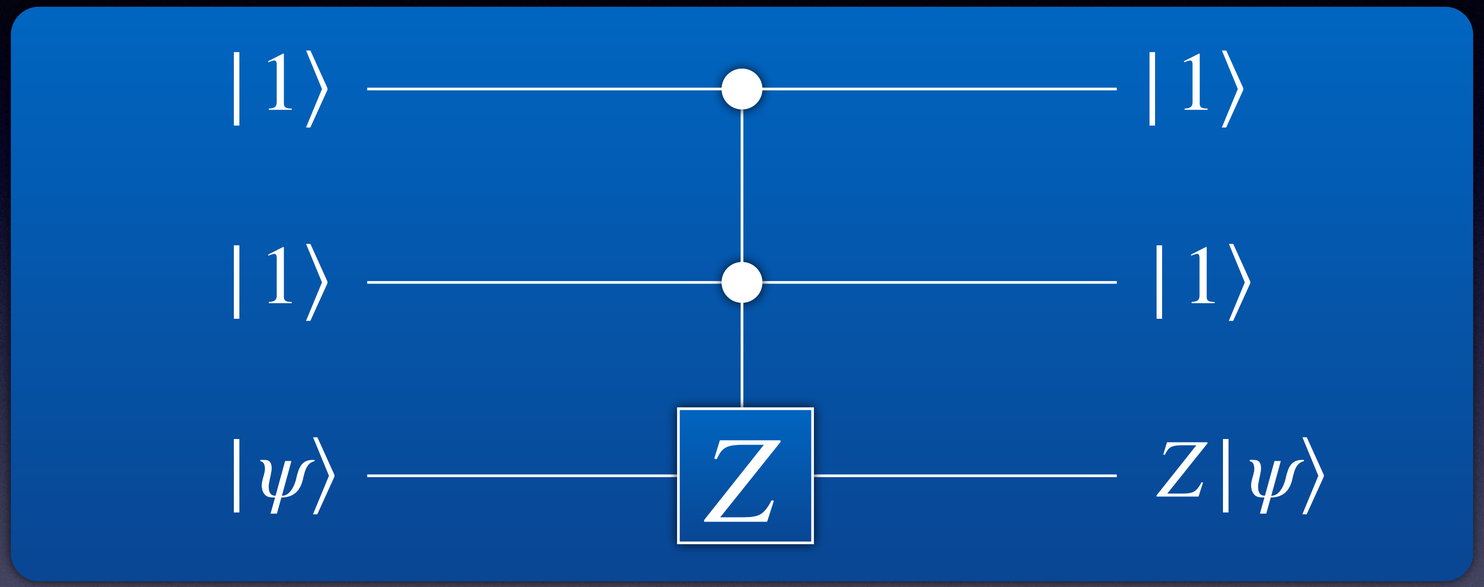
Toffoli gate



$$T = (I^{\otimes 2} - |11\rangle\langle 11|) \otimes I + |11\rangle\langle 11| \otimes X$$

- any classical reversible logic circuit can be implemented on a quantum computer

CCZ gate

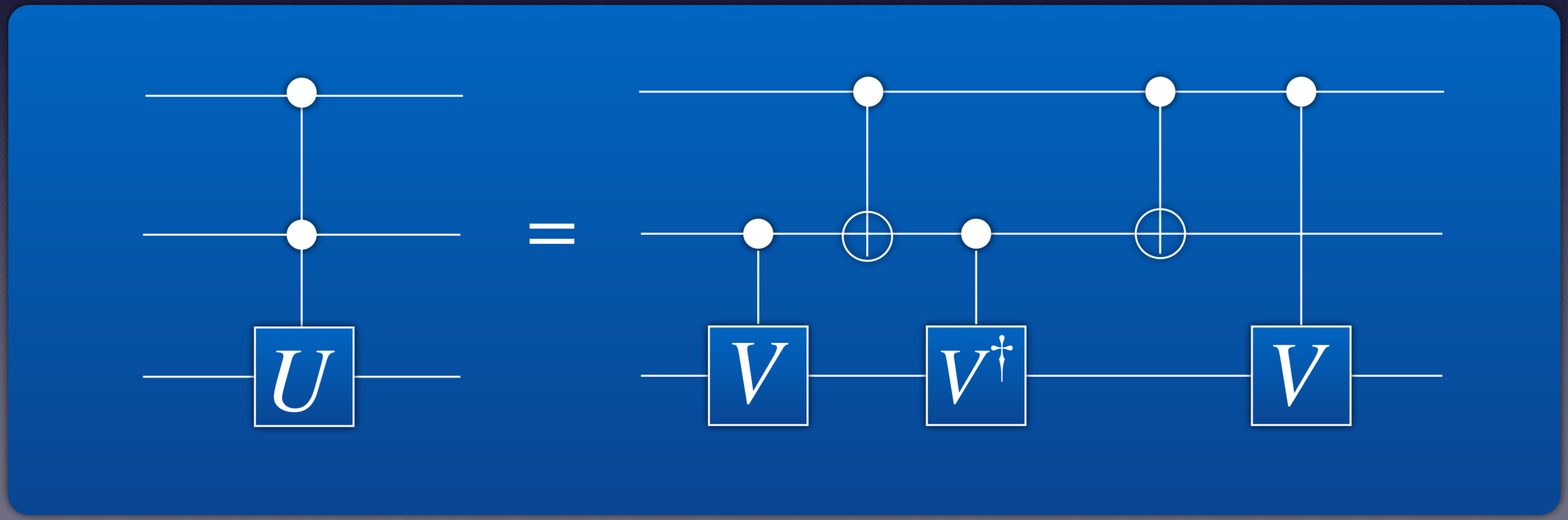


$$CCZ = (I^{\otimes 2} - |11\rangle\langle 11|) \otimes I + |11\rangle\langle 11| \otimes Z$$

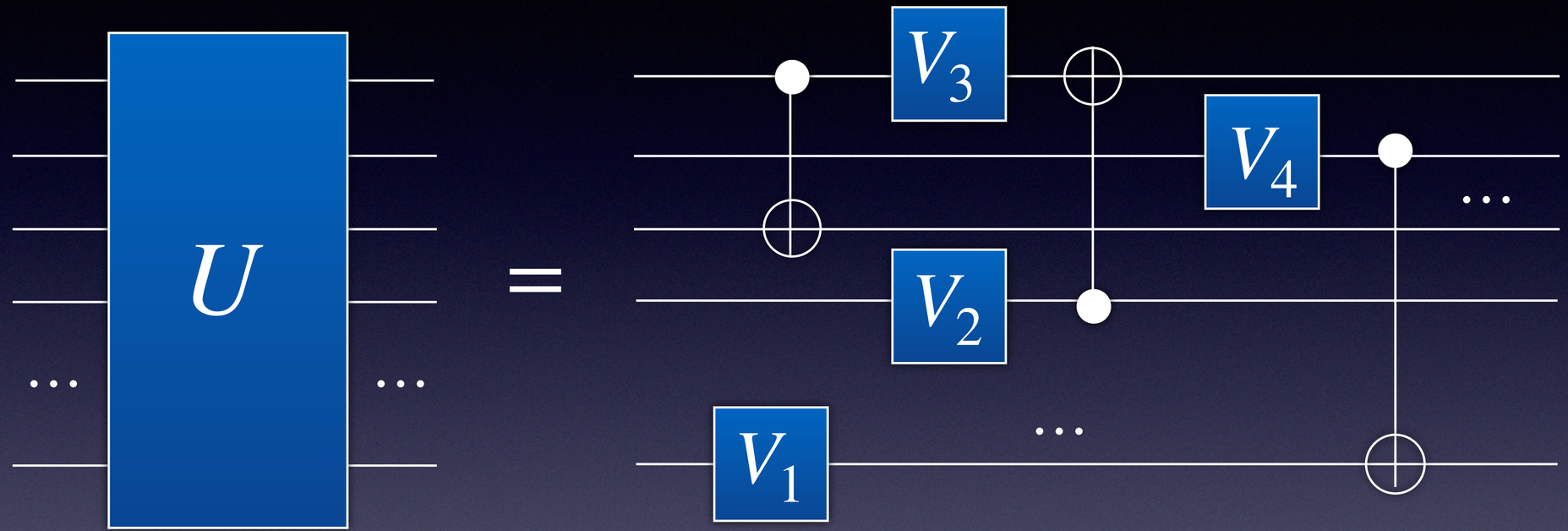
CCU gate

Exercise 8

Show that any CCU gate can be decomposed into the two-qubit gates as below, where $V^2 = U$ and $V^\dagger V = I$



Universal quantum gates



- single qubit and CNOT (CZ) gates can be used to implement an arbitrary unitary operation on n qubits, therefore they are universal for quantum computation

Universal quantum gates

T-gate $T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix} = e^{-i(\pi/8)} R_z(\pi/4) \qquad S = T^2$

$\pi/4$ rotation about the z-axis

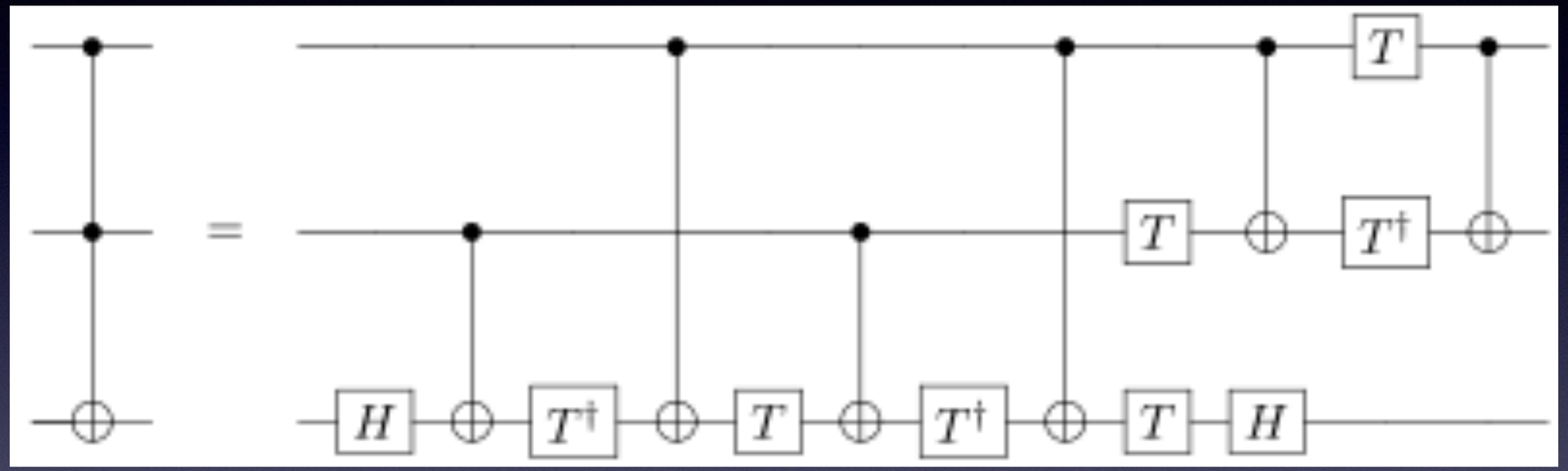
- any single qubit operation can be approximated to arbitrary accuracy by $\{H, T\}$

  $\because THTH$ = rotation of an angle irrational multiple of π

- any n-qubit unitary operation can be approximated to arbitrary accuracy using $\{H, T, \mathrm{CNOT}\}$

→ $\{H, T, \mathrm{CNOT}\}$ is a universal set of gates

Universal quantum gates



Implementation of the Toffoli gate using $\{H, T, \mathrm{CNOT}\}$