Quantum Computing

- Week 8 (June 2-3, 2025)

- Today:
  - Quantum circuits
  - Controlled operations

Qubit Operations

- Single-qubit operations

$$\boldsymbol{I} = \sigma_0 \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\boldsymbol{X} = \sigma_1 \coloneqq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

(Pauli-**X**)

$$\boldsymbol{Y} = \sigma_2 \coloneqq \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

(Pauli-**Y**)

$$\boldsymbol{Z} = \sigma_3 \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

(Pauli-**Z**)

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

Hadamard

$$\boldsymbol{S} \coloneqq \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$$

Phase

$$\boldsymbol{T} \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{i\pi}{4}} \end{bmatrix}$$

$\boldsymbol{\pi/8}$

Qubit Operations

- Understand single-qubit operations via the **Bloch Sphere**

- A single-qubit *pure* state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ can be written as:

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

We **ignore** $e^{i\gamma}$ since it has **no observable effect** (i.e., does not change measurement distribution…)

Represent the state on the **Bloch Sphere** (we ignore the global phase)

- Case 1: Both α and β are real numbers…
- Case 2: α or β is complex number …
- A quick question: **Why 3D space?** (Why not 4D for expressing a qubit?)

Qubit Operations

- Single-qubit operations

$$\boldsymbol{I} = \sigma_0 \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad \boldsymbol{X} = \sigma_1 \coloneqq \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad \boldsymbol{Y} = \sigma_2 \coloneqq \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \boldsymbol{Z} = \sigma_3 \coloneqq \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

(Pauli-**X**) (Pauli-**Y**) (Pauli-**Z**)

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

Hadamard **Phase** **$\pi/8$**

- Illustrate these operations on Bloch Sphere…

Qubit Operations

- Single-qubit operations

$$I = \sigma_0 := \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad X = \sigma_1 := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \qquad Y = \sigma_2 := \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad Z = \sigma_3 := \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

(Pauli-**X**) (Pauli-**Y**) (Pauli-**Z**)

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

Hadamard **Phase** **$\pi/8$**

- Illustrate these operations on Bloch Sphere…
- **Observation: Single-qubit Unitary transformation = Rotations on Bloch Sphere**
  - …(up to a global phase)

Qubit Operations

- Single-qubit Unitary transformation = Rotations on Bloch Sphere **(up to a global phase)**
- Question: Do we have a general way to represent rotations (and thus unitaries)?

Qubit Operations

- Single-qubit Unitary transformation = Rotations on Bloch Sphere (up to a global phase)
- Question: Do we have a general way to represent rotations (and thus unitaries)?

$$\boldsymbol{R_x(\theta)} \coloneqq \cos\frac{\theta}{2}\cdot \boldsymbol{I} - i\sin\frac{\theta}{2}\cdot \boldsymbol{X} = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$\boldsymbol{R_y(\theta)} \coloneqq \cos\frac{\theta}{2}\cdot \boldsymbol{I} - i\sin\frac{\theta}{2}\cdot \boldsymbol{Y} = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$\boldsymbol{R_z(\theta)} \coloneqq \cos\frac{\theta}{2}\cdot \boldsymbol{I} - i\sin\frac{\theta}{2}\cdot \boldsymbol{Z} = \begin{bmatrix} e^{-\frac{i\theta}{2}} & 0 \\ 0 & e^{-\frac{i\theta}{2}} \end{bmatrix}$$ (Euler's formula: $e^{-\frac{i\theta}{2}} = \cos\frac{\theta}{2} - i\sin\frac{\theta}{2}$)

Qubit Operations

- Single-qubit Unitary transformation = Rotations on Bloch Sphere (up to a global phase)
- Question: Do we have a general way to represent rotations (and thus unitaries)?

$$\boldsymbol{R_x(\theta)} \coloneqq \cos\frac{\theta}{2}\cdot \boldsymbol{I} - i\sin\frac{\theta}{2}\cdot \boldsymbol{X}$$ (Rotation about the X axe)

$$\boldsymbol{R_y(\theta)} \coloneqq \cos\frac{\theta}{2}\cdot \boldsymbol{I} - i\sin\frac{\theta}{2}\cdot \boldsymbol{Y}$$ (Rotation about the Y axe)

$$\boldsymbol{R_z(\theta)} \coloneqq \cos\frac{\theta}{2}\cdot \boldsymbol{I} - i\sin\frac{\theta}{2}\cdot \boldsymbol{Z}$$ (Rotation about the Z axe)

- E.g., rotation by 90° about the Z axe: $\boldsymbol{R_z}(90^\circ)$

Qubit Operations

- Single-qubit Unitary transformation = Rotations on Bloch Sphere (up to a global phase)
- Question: Do we have a general way to represent rotations (and thus unitaries)?

$$\boldsymbol{R_x}(\boldsymbol{\theta}) \coloneqq \cos\frac{\theta}{2}\cdot\boldsymbol{I} - i\sin\frac{\theta}{2}\cdot\boldsymbol{X}$$ (Rotation about the X axe)

$$\boldsymbol{R_y}(\boldsymbol{\theta}) \coloneqq \cos\frac{\theta}{2}\cdot\boldsymbol{I} - i\sin\frac{\theta}{2}\cdot\boldsymbol{Y}$$ (Rotation about the Y axe)

$$\boldsymbol{R_z}(\boldsymbol{\theta}) \coloneqq \cos\frac{\theta}{2}\cdot\boldsymbol{I} - i\sin\frac{\theta}{2}\cdot\boldsymbol{Z}$$ (Rotation about the Z axe)

- **Theorem (Z-Y decomposition):** For any unitary $\boldsymbol{U}$, there exist *real numbers* a, b, c, and d such that

$$\boldsymbol{U} = e^{ia}\,\boldsymbol{R_z}(b)\,\boldsymbol{R_y}(c)\,\boldsymbol{R_z}(d)$$

Qubit Operations

- Single-qubit Unitary transformation = Rotations on Bloch Sphere (up to a global phase)
- Question: Do we have a general way to represent rotations (and thus unitaries)?

$$\boldsymbol{R_x(\theta)} \coloneqq \cos\frac{\theta}{2} \cdot \boldsymbol{I} - i\sin\frac{\theta}{2} \cdot \boldsymbol{X}$$ (Rotation about the X axe)

$$\boldsymbol{R_y(\theta)} \coloneqq \cos\frac{\theta}{2} \cdot \boldsymbol{I} - i\sin\frac{\theta}{2} \cdot \boldsymbol{Y}$$ (Rotation about the Y axe)

$$\boldsymbol{R_z(\theta)} \coloneqq \cos\frac{\theta}{2} \cdot \boldsymbol{I} - i\sin\frac{\theta}{2} \cdot \boldsymbol{Z}$$ (Rotation about the Z axe)

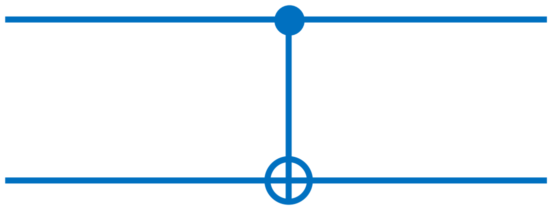
- **Theorem (Z-Y decomposition):** For any unitary $\boldsymbol{U}$, there exist *real numbers* a, b, c, and d such that

$$\boldsymbol{U} = e^{ia}\, \boldsymbol{R_z}(b)\, \boldsymbol{R_y}(c)\, \boldsymbol{R_z}(d)$$

- **Theorem (X-Y decomposition): …**

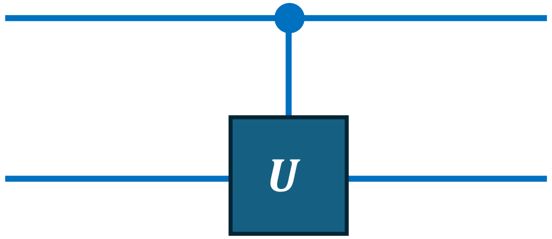
Controlled Operations

- Controlled NOT:



$$\mathbf{cNOT}|c\rangle|t\rangle \rightarrow |c\rangle\mathbf{NOT}^{c}|t\rangle$$

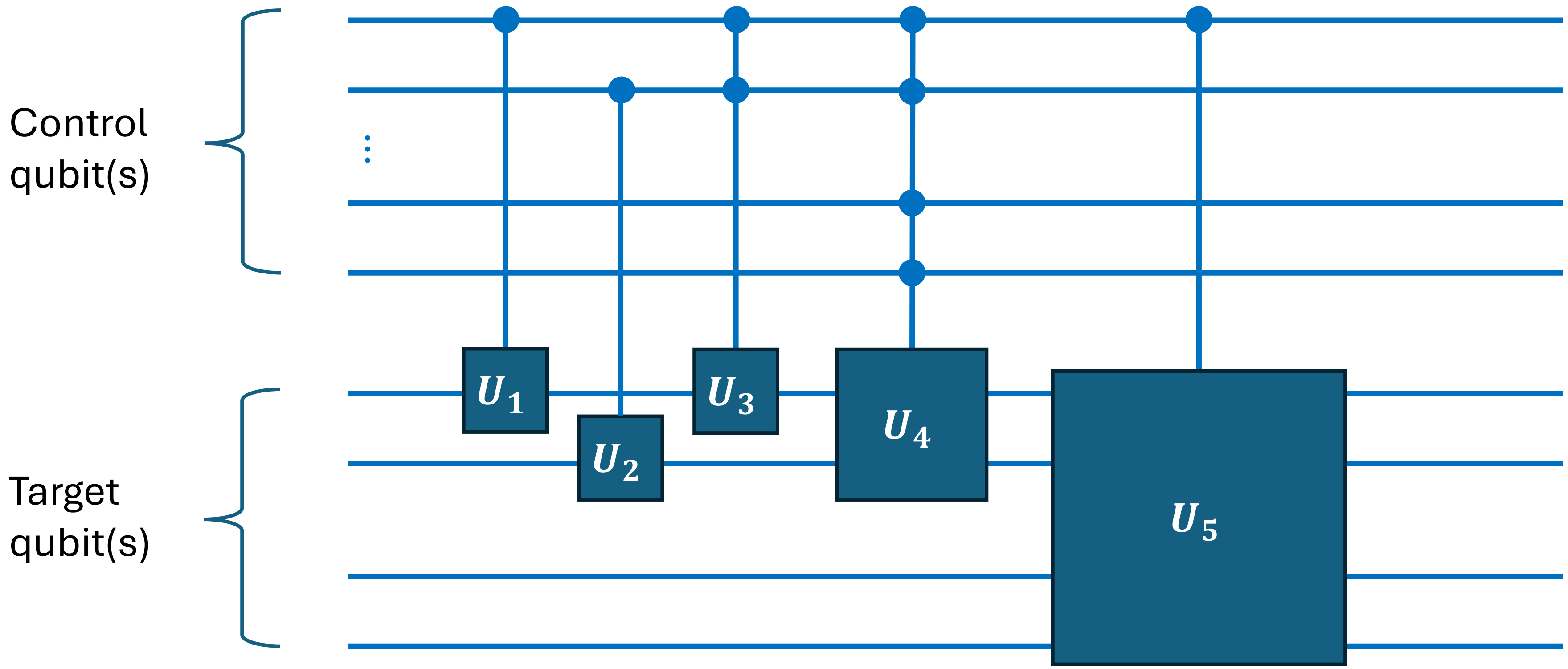
- Generalized controlled gate:



$$\mathbf{c}\boldsymbol{U}|c\rangle|t\rangle \rightarrow |c\rangle\boldsymbol{U}^{c}|t\rangle$$

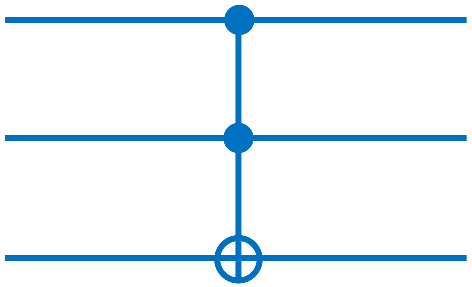
Controlled Operations

- Specify the control qubit(s) and the target qubit(s)



Controlled Operations

- Toffoli Gate:

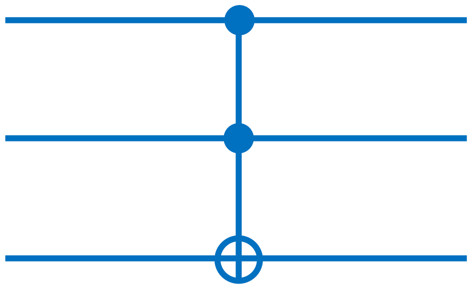


$$\mathbf{cNOT}|c_1c_2\rangle|t\rangle \rightarrow |c_1c_2\rangle\mathbf{NOT}^{c_1c_2}|t\rangle$$

(Flip the target qubit if the two control qubits are 1)

Controlled Operations

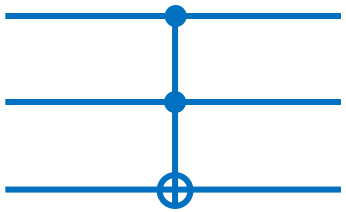
- Toffoli Gate:



$$\mathbf{cNOT}|c_1 c_2\rangle|t\rangle \rightarrow |c_1 c_2\rangle\mathbf{NOT}^{c_1 c_2}|t\rangle$$

(Flip the target qubit if the two control qubits are 1)

- Implement Toffoli Gate via **Hadamard, Phase, CNOT, and $\boldsymbol{T}$**



=

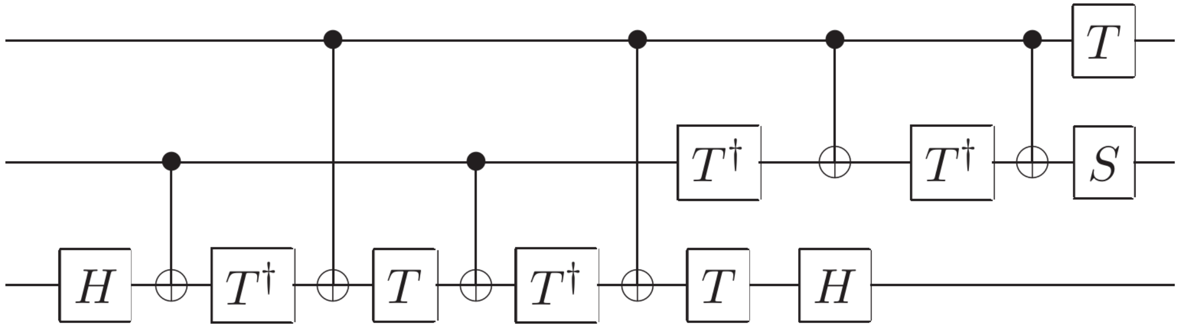
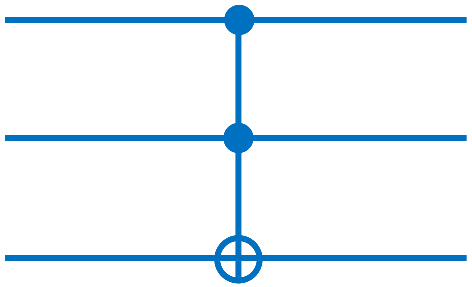


Figure 4.9 of [NC00]

Controlled Operations

- Toffoli Gate:



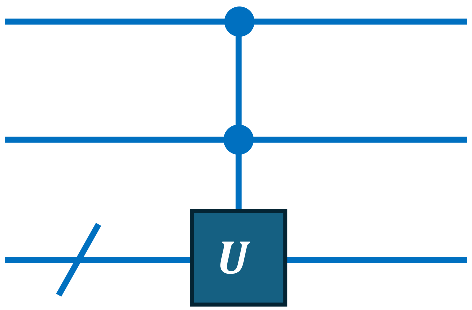
$$\mathbf{cNOT}|c_1c_2\rangle|t\rangle \rightarrow |c_1c_2\rangle\mathbf{NOT}^{c_1c_2}|t\rangle$$

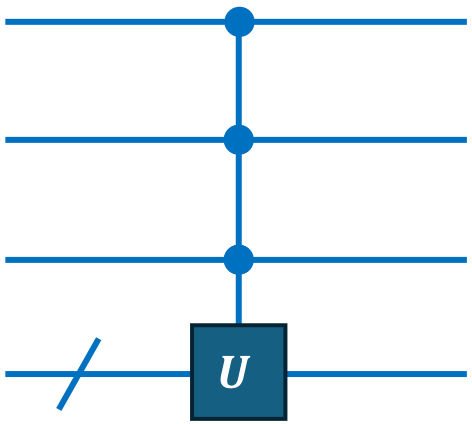
(Flip the target qubit if the two control qubits are 1)

- **Conclusion:** Toffoli Gate can be composed by using **Hadamard, Phase, CNOT, and** $\boldsymbol{T}$

Controlled Operations

- Consider the following controlled-$\boldsymbol{U}$ operations:





- How can we implement them using Toffoli gates and $\boldsymbol{U}$?

Universal Quantum Gates

- Universal set of classical logic gates:
  - Collection of basic logic gates
  - Any Boolean function can be implemented using only gates from this collection

- Universal set of classical gates:
  - {AND, OR, NOT}
  - {NAND}, {NOR}

Universal Quantum Gates

- Universal set of classical logic gates:
  - Collection of basic logic gates
  - Any Boolean function can be implemented using only gates from this collection

- Universal set of classical gates:
  - {AND, OR, NOT}
  - {NAND}, {NOR}

- Universal set of quantum gates:
  - { **{All single-qubit gates}** , **CNOT**} //Infinite

Universal Quantum Gates

- Universal set of classical logic gates:
  - Collection of basic logic gates
  - Any Boolean function can be implemented using only gates from this collection

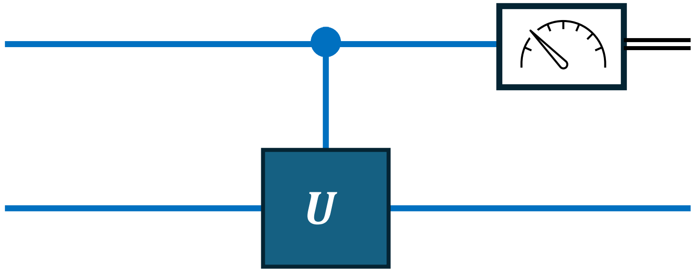
- Universal set of classical gates:
  - {AND, OR, NOT}
  - {NAND}, {NOR}

- Universal set of quantum gates:
  - { **{All single-qubit gates}** , **CNOT**} //Infinite
- Exact Universality: Use an infinite continuous set of single-qubit gates
- Approximate Universality: $\{\boldsymbol{H}, \boldsymbol{T}, \mathrm{CNOT}\}$ //Use H and T to approximate any single-qubit unitary

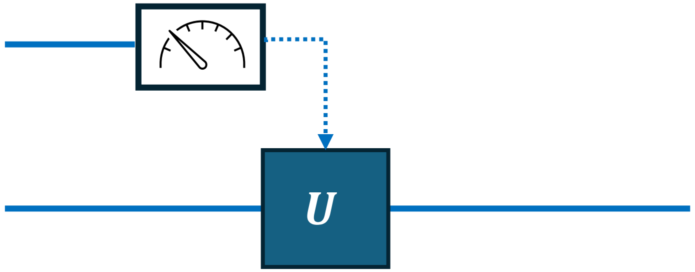
Measurement

- Quantum Measurement and controlled operations

- “Control-then-measure”



- “Measure-then-control”

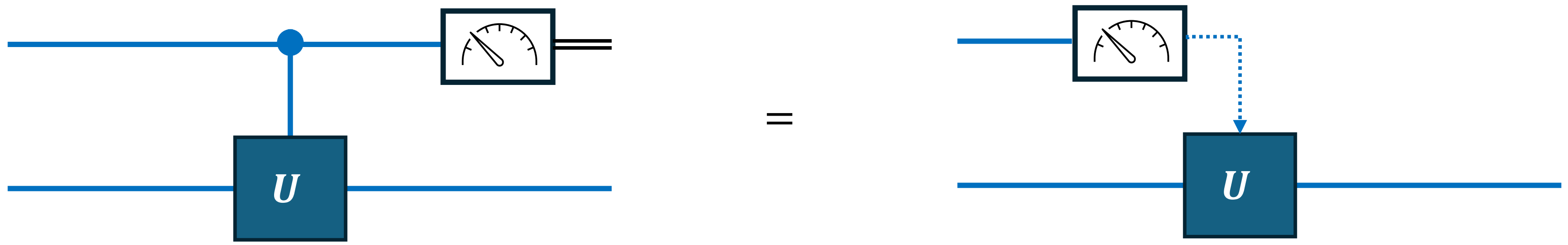


Measurement

- Quantum Measurement and controlled operations

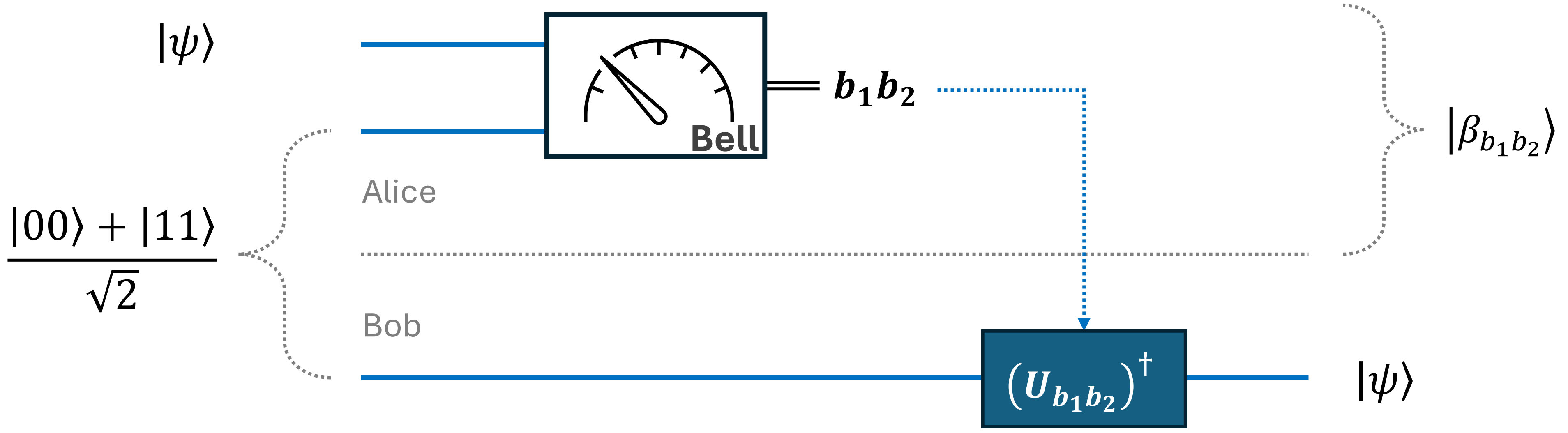
- **“Control-then-measure” = “Measure-then-control”**

  (if the qubit being measured is the control qubit)



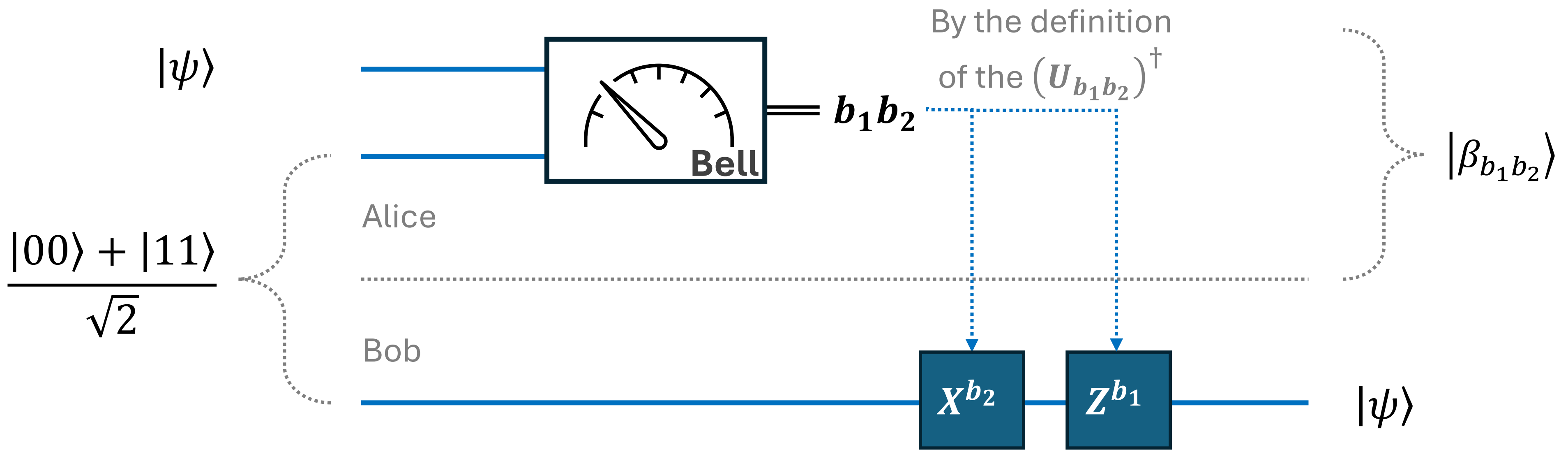
Measurement

- Homework: The quantum teleportation circuit using “delayed measurement”



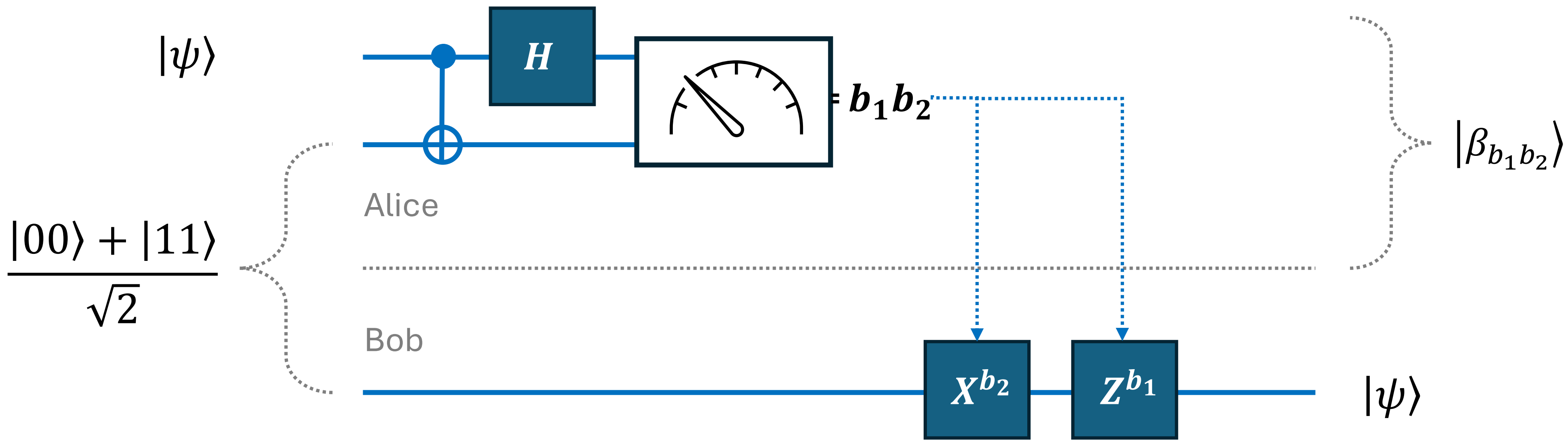
Measurement

- Homework: The quantum teleportation circuit using “delayed measurement”



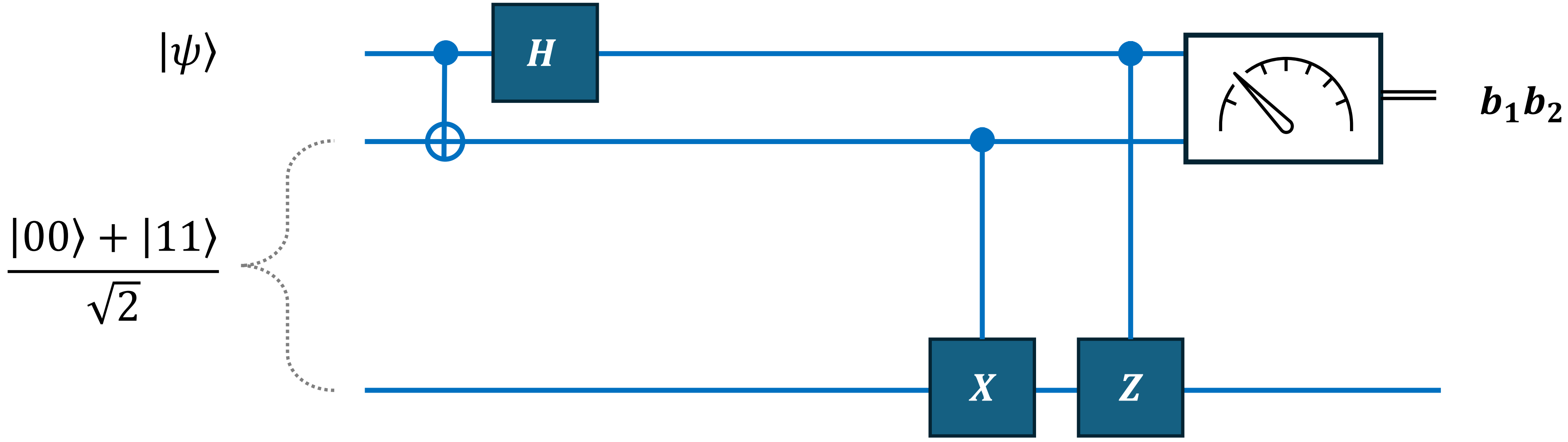
Measurement

- **Homework question 1: Measurement in the bell basis vs in the computational basis**



Measurement

- **Homework question 2: Delayed measurement**



Next Week

- Next few weeks:
  - **Quantum Fourier Transformation**
  - **Order Finding**
  - **Factoring and Discrete Logarithm**

Reference

- **[NC00]:** Section 1.3.1, Chapter 4
- **[KLM07]:** Chapter 4

Homework

- **Second homework set** (will be announced in the Moodle system soon)**:**
  - Submit your handwritten solutions (photos, scanned pdf, etc.), or typeset in LaTeX
  - Please include all intermediate equations and their explanation
  - DDL: **June 10th, 2026 at 23:59** (The last second of the next Wednesday)