Quantum Computing

- Lectures 11 and 12 (June 11-12, 2025)

- Today:
  - Quantum circuits
  - Controlled operations

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**)

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

Hadamard **Phase** **π/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**

- 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**)

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

Hadamard **Phase** **π/8**

- Illustrate these operations on Bloch Sphere…

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**)

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

Hadamard **Phase** **π/8**

- Illustrate these operations on Bloch Sphere…
- **Observation: Single-qubit Unitary transformation = Rotations (on Bloch Sphere)**
- Linear Algebra Fact: (Generalized) Rotation = “Length-preserving” = Unitary

Qubit Operations

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

Qubit Operations

- **Single-qubit Unitary transformation = Rotations on Bloch Sphere**
- 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**
- 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
- 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

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

Qubit Operations

- Single-qubit Unitary transformation = Rotations on Bloch Sphere
- 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)

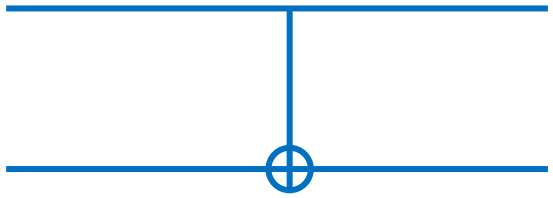
- **Theorem (Z-Y decomposition):** For any unitary $\boldsymbol{U}$, there exist *real numbers* a, b, c, and d such that

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

- **Theorem (X-Y decomposition): …**

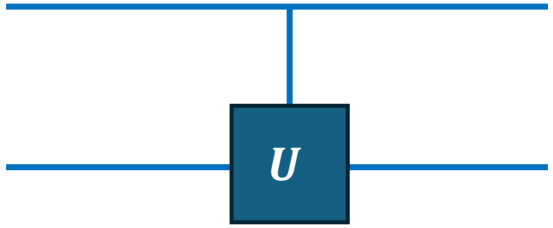
Controlled Operations

- Controlled NOT:



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

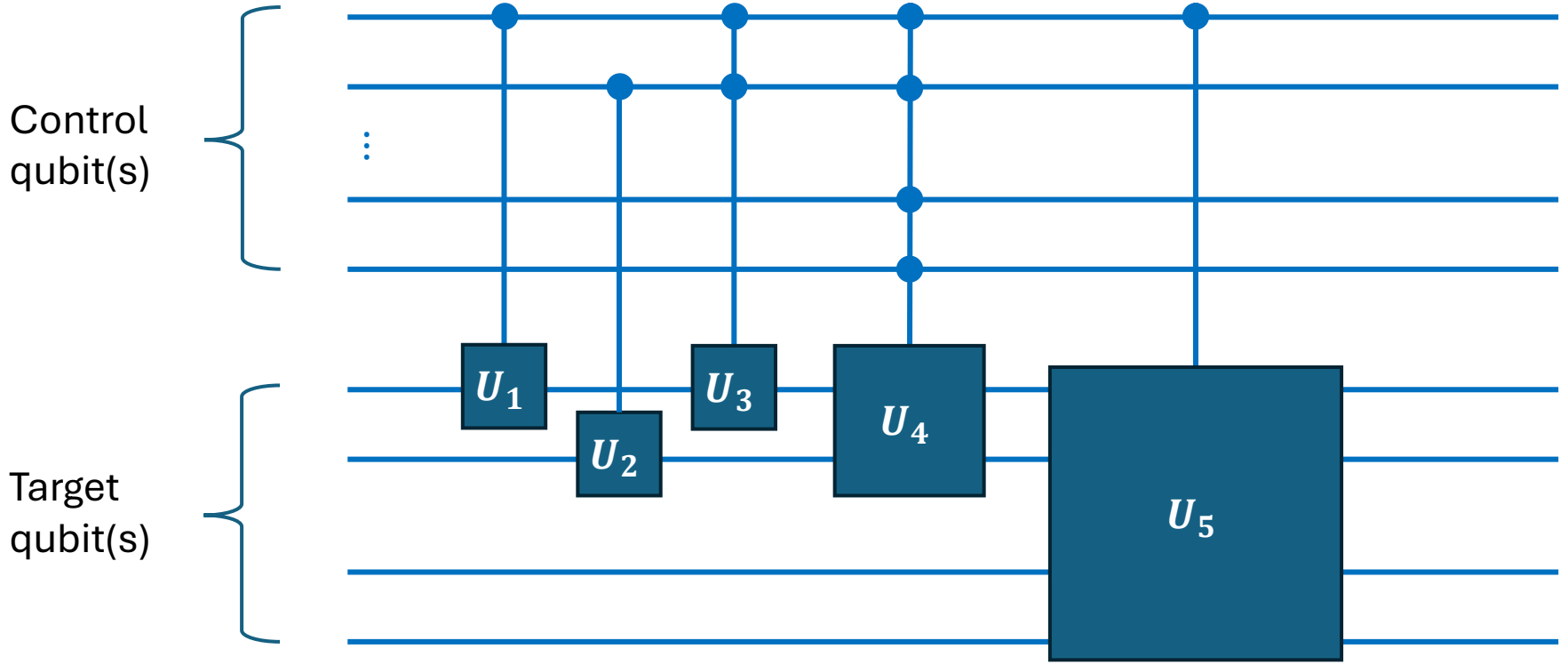
- Generalized controlled gate:



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

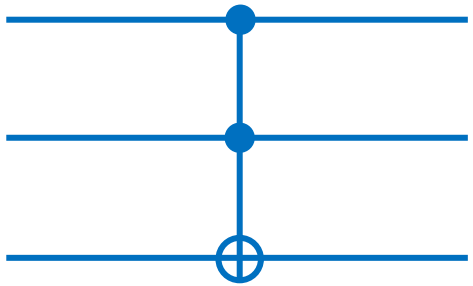
Controlled Operations

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



Controlled Operations

- Toffoli Gate:

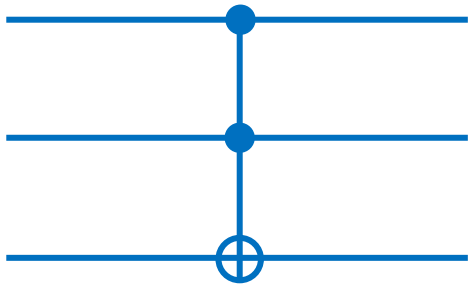


$$\mathbf{cNOT}|c_1 c_2\rangle|t\rangle \rightarrow |c_1 c_2\rangle \mathbf{NOT}^{c_1 c_2}|t\rangle$$

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

Controlled Operations

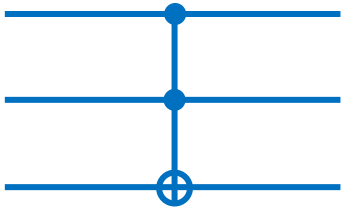
- Toffoli Gate:



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

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

- Implement Toffoli Gate via **Hadamard, Phase, CNOT, and π/8**



=

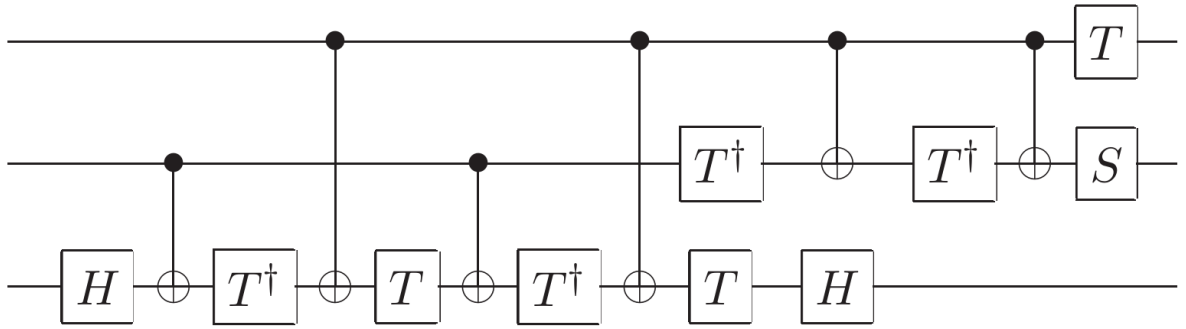
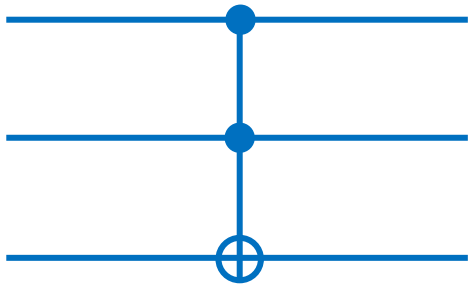


Figure 4.9 of [NC00]

Controlled Operations

- Toffoli Gate:



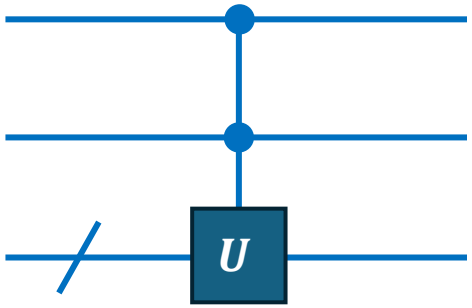
$$\mathbf{cNOT}|c_1 c_2\rangle|t\rangle \rightarrow |c_1 c_2\rangle \mathbf{NOT}^{c_1 c_2}|t\rangle$$

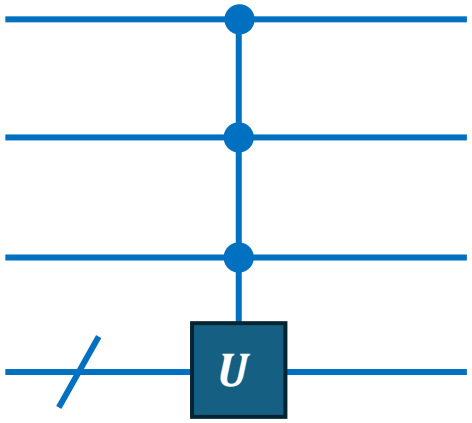
(Flip the target qubit if the two control qubits are 1)

- **Conclusion:** Toffoli Gate can be composed by using **Hadamard, Phase, CNOT, and π/8**

Controlled Operations

- Consider the following controlled operations:

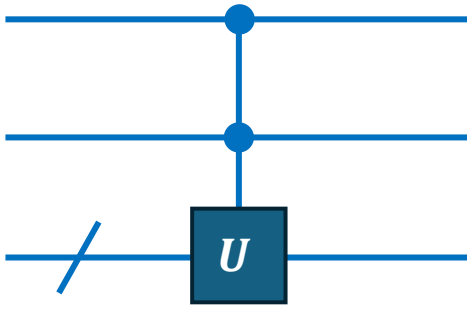


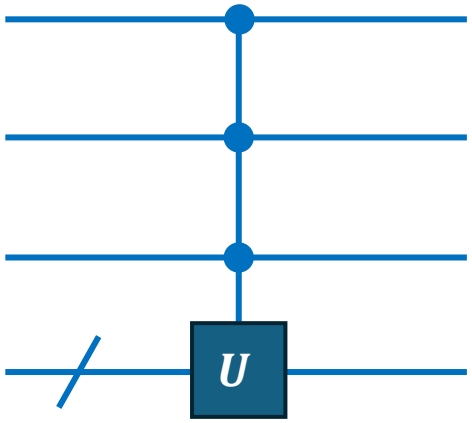


- How can we implement them using Toffoli gates and U?

Controlled Operations

- Consider the following controlled operations:





- How can we implement them using Toffoli gates and U?
- **Theorem (informal):** Any quantum gate of controlled operations can be implemented via U (the controlled unitary), CNOT, and some single-qubit gates.

Universal Quantum Gates

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

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

- Universal set of quantum gates:
  - {Single-qubit gates, CNOT}

Universal Quantum Gates

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

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

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

Universal Quantum Gates

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

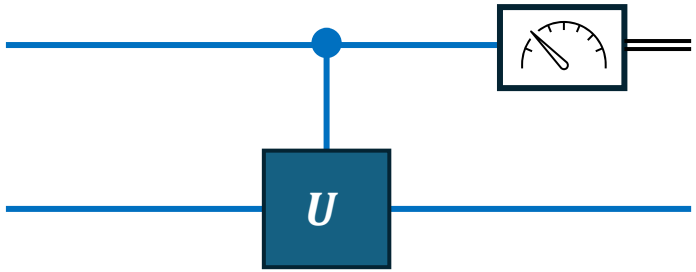
- Universal set of classical gates:
  - {AND, OR, NOT}
  - {NAND, NOR}

- Universal set of quantum gates:
  - {**Single-qubit gates**, CNOT} //Infinite
- Exact Universality: Not physically realizable
- Approximate Universality: $\{\boldsymbol{H}, \boldsymbol{T}, \mathrm{CNOT}\}$ //Use H and T to approximate any single-qubit unitary

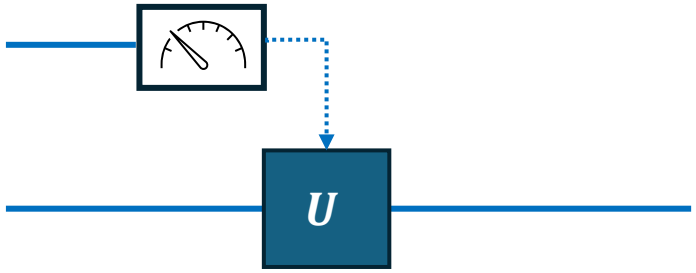
Measurement

- Quantum Measurement and controlled operations

- “Control-then-measure”



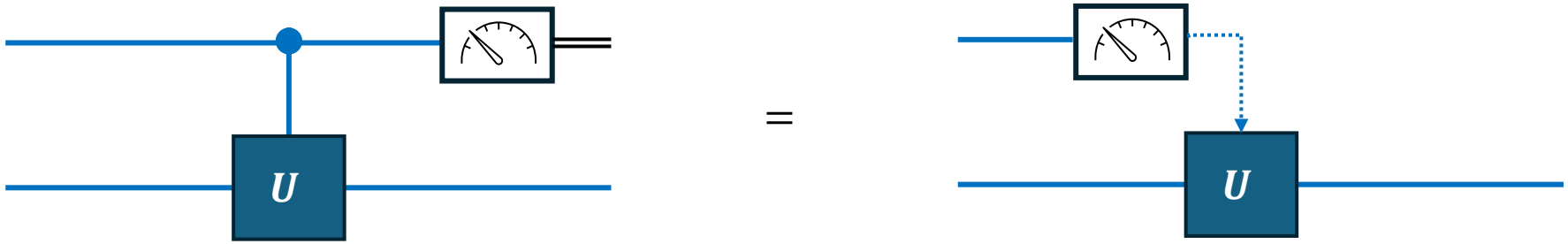
- “Measure-then-control”



Measurement

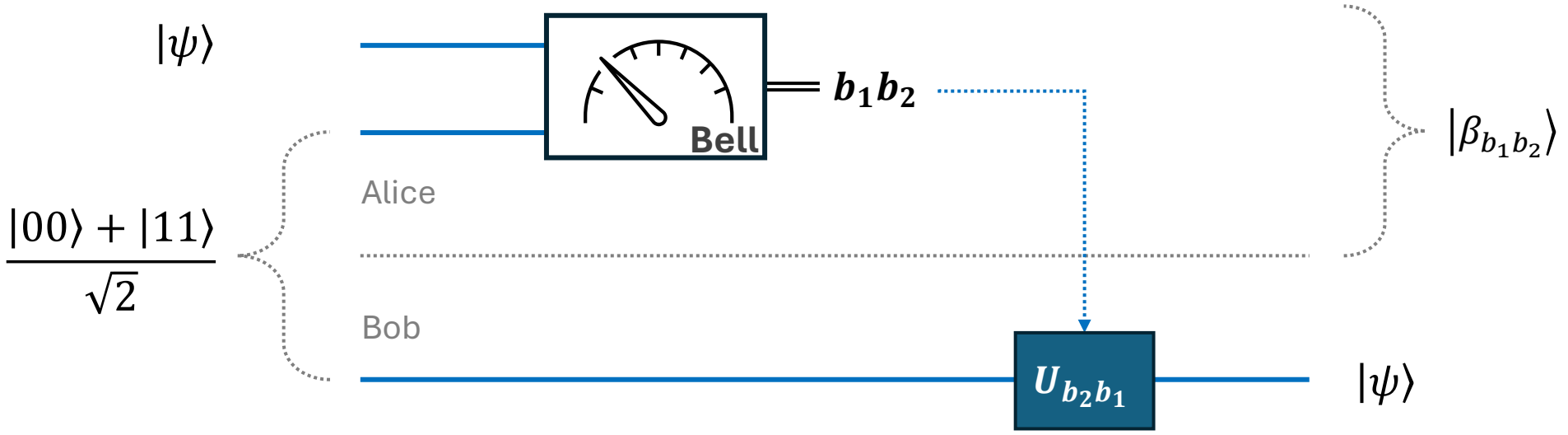
- Quantum Measurement and controlled operations

- **“Control-then-measure” = “Measure-then-control”**
  (if the qubit being measured is the control qubit)



Measurement

- Example: Quantum Teleportation



Total states:

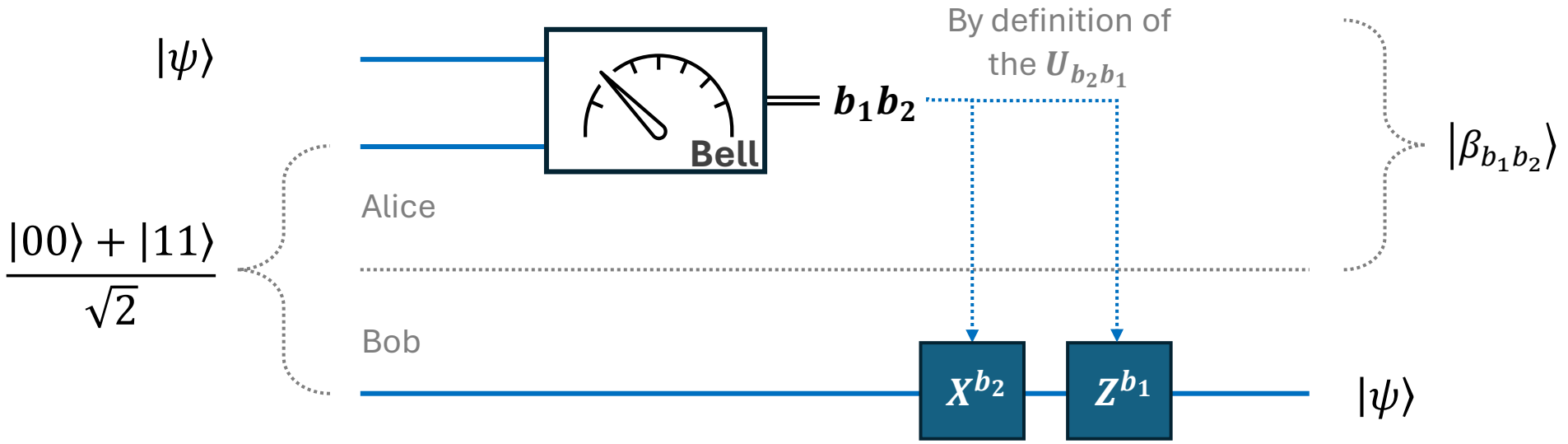
$$|\phi_0\rangle = \sum_{b_1,b_2 \in \{0,1\}} |\beta_{b_1 b_2}\rangle \boldsymbol{U^{\dagger}_{b_2 b_1}} |\psi\rangle$$

$$|\phi_1\rangle = |\beta_{b_1 b_2}\rangle \boldsymbol{U^{\dagger}_{b_2 b_1}} |\psi\rangle$$

$$|\phi_2\rangle = |\beta_{b_1 b_2}\rangle \otimes |\psi\rangle$$

Measurement

- Example: Quantum Teleportation



Total states:

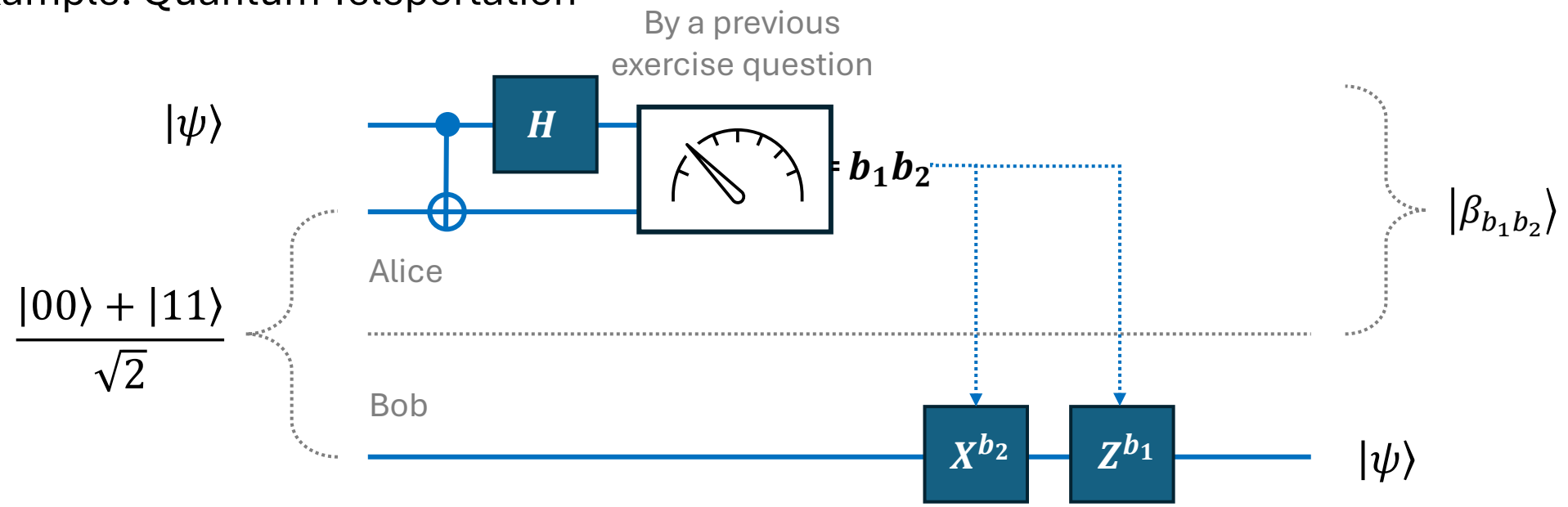
$$|\phi_0\rangle = \sum_{b_1,b_2 \in \{0,1\}} |\beta_{b_1 b_2}\rangle \boldsymbol{U^{\dagger}_{b_2 b_1}} |\psi\rangle$$

$$|\phi_1\rangle = |\beta_{b_1 b_2}\rangle \boldsymbol{U^{\dagger}_{b_2 b_1}} |\psi\rangle$$

$$|\phi_2\rangle = |\beta_{b_1 b_2}\rangle \otimes |\psi\rangle$$

Measurement

- Example: Quantum Teleportation



Total states:

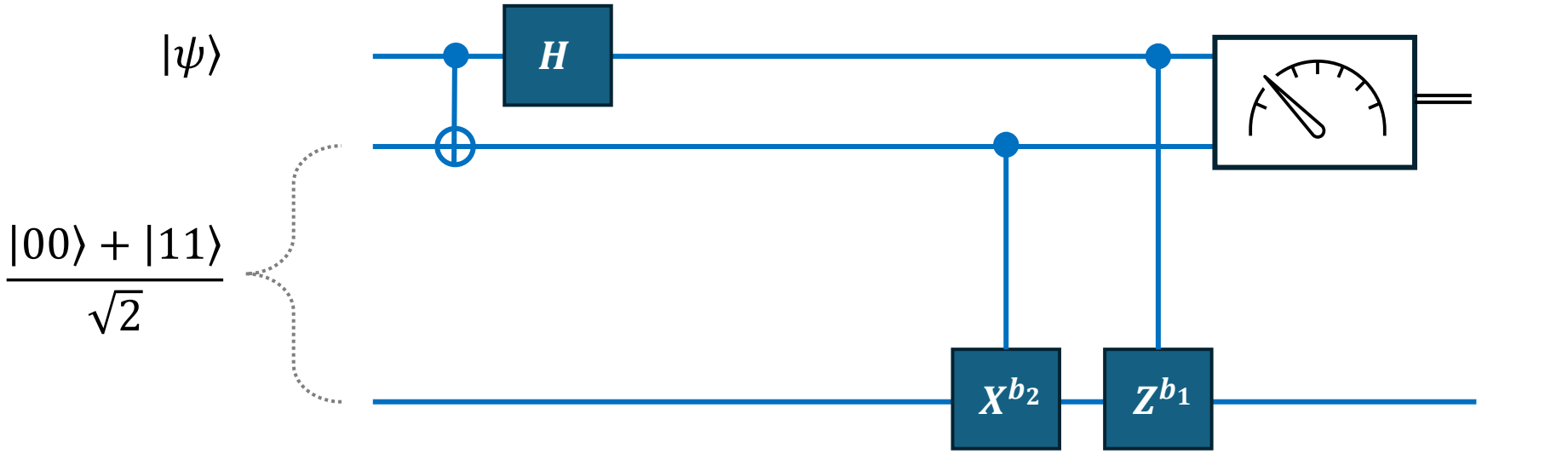
$$|\phi_0\rangle = \sum_{b_1,b_2\in\{0,1\}} |\beta_{b_1 b_2}\rangle \boldsymbol{U^{\dagger}_{b_2 b_1}} |\psi\rangle$$

$$|\phi_1\rangle = |\beta_{b_1 b_2}\rangle \boldsymbol{U^{\dagger}_{b_2 b_1}} |\psi\rangle$$

$$|\phi_2\rangle = |\beta_{b_1 b_2}\rangle \otimes |\psi\rangle$$

Measurement

- **Exercise: Quantum Teleportation**



Total states: $|\phi_0\rangle$ $|\phi_1\rangle$ $|\phi_2\rangle$

Measurement

- Two principles about measurement
- **Principle of Deferred Measurement**
- **Principle of Implicit Measurement**

Measurement

- **Principle of Deferred Measurement:**
  - “Intermediate measurements” can be moved to the end

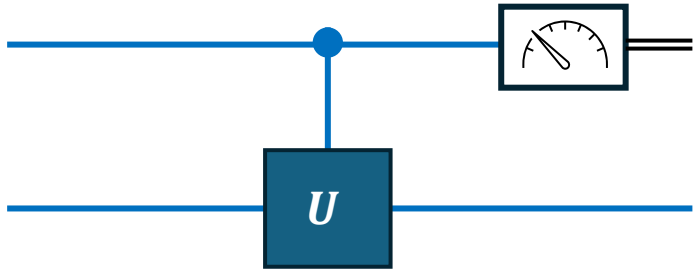
Measurement

- **Principle of Deferred Measurement:**
  - “Intermediate measurements” can be moved to the end

  - Specifically, “Measure-then-control” = “Control-then-measure”…

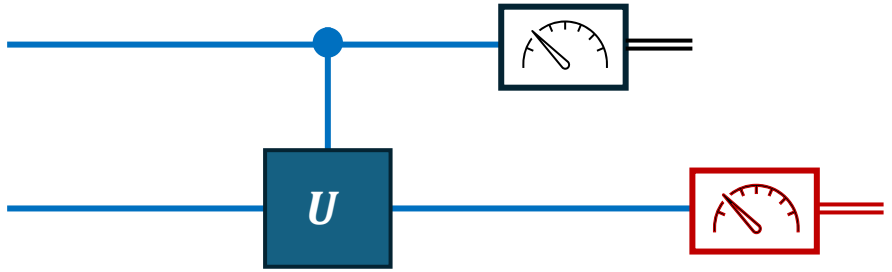
Measurement

- **Principle of Implicit Measurement**
  - WLOG, all unmeasured qubits may be assumed to be measured at the end of the circuit…



Measurement

- **Principle of Implicit Measurement**
  - WLOG, all unmeasured qubits may be assumed to be measured at the end of the circuit…



Measurement

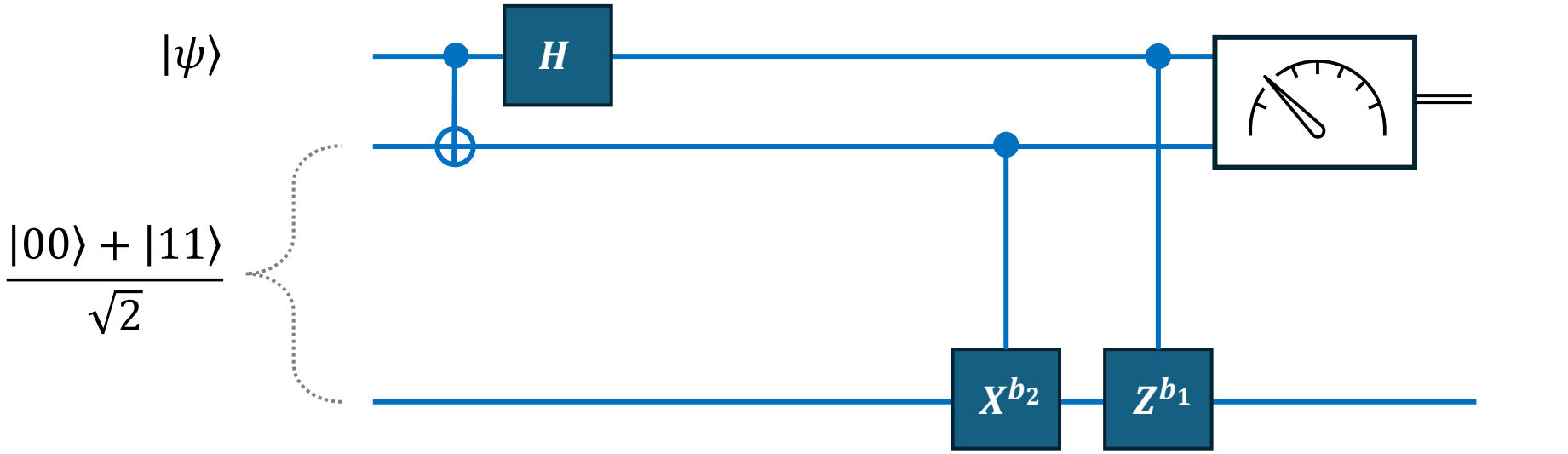
- Two principles about measurement
  - Principle of **Deferred Measurement**
  - Principle of **Implicit Measurement**

Measurement

- Two principles about measurement
  - Principle of Deferred Measurement
  - Principle of Implicit Measurement
- **Any quantum algorithm can be modeled purely with unitaries**
  - Even for *classical-quantum hybrid* algorithms!

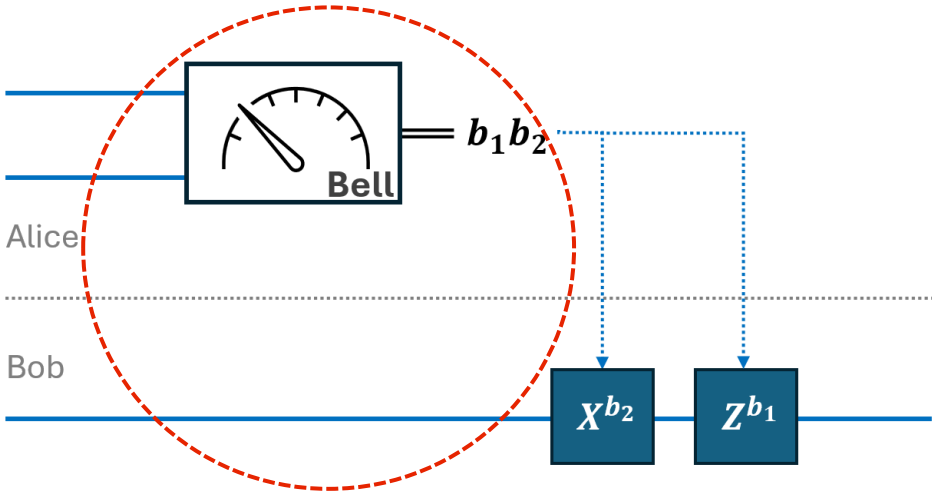
Measurement

- **Exercise: Quantum Teleportation**



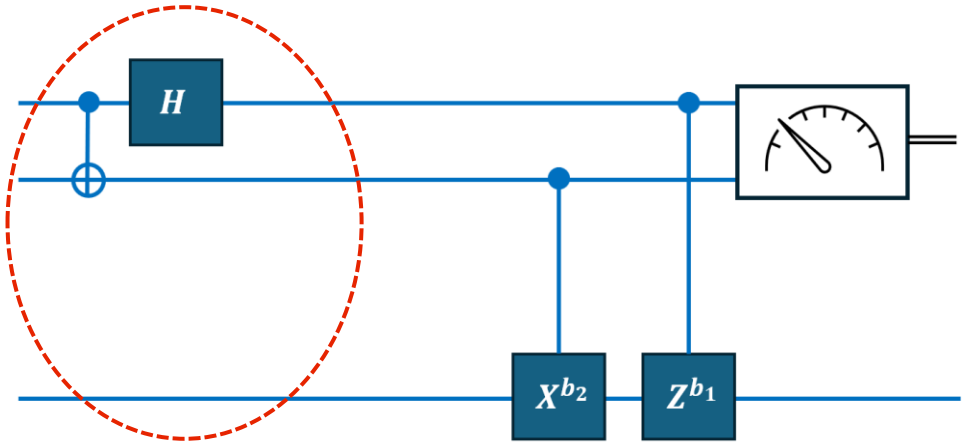
Total states: $|\phi_0\rangle$ $|\phi_1\rangle$ $|\phi_2\rangle$

Measurement

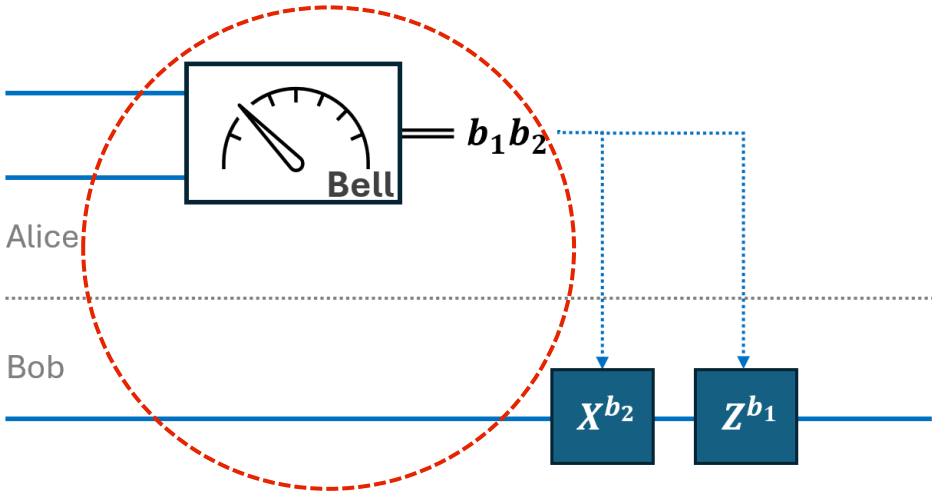


Not invertible

Invertible



Measurement

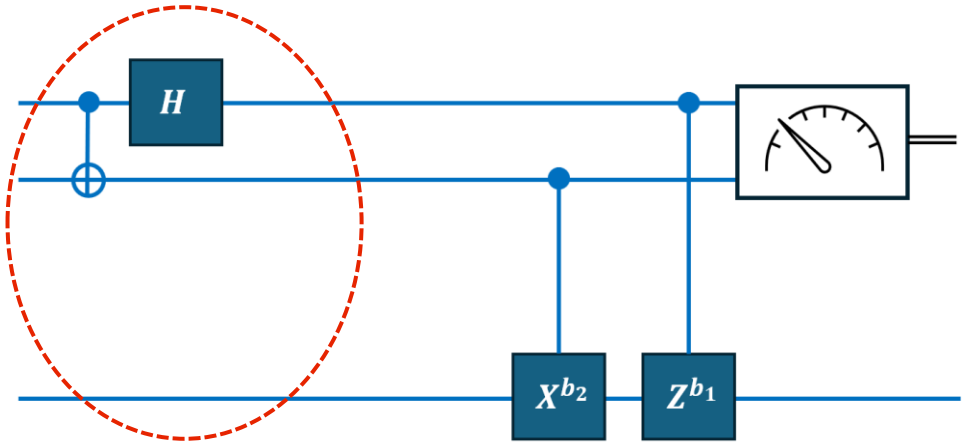


Not invertible

Extract information

No information extraction

Invertible



Next Week

- Next two or three weeks:
  - **Quantum Fourier Transformation**
  - **Order Finding**, and its application to **Factoring and Discrete Logarithm**

Reference

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