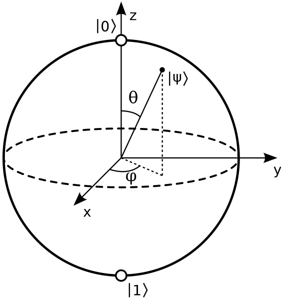
COL863: Quantum Computation and Information

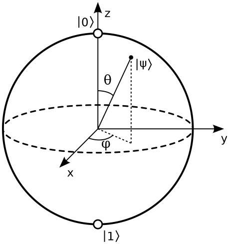
Ragesh Jaiswal, CSE, IIT Delhi

Quantum Computation: Quantum circuits

- Single qubit gates are 2×2 unitary matrices. Some of the important gates are:
  - Pauli matrices: $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
  - Hadamard gate: $H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.
  - Phase gate: $S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$.
  - $\pi/8$ gate: $T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
- Simplification: A qubit $\alpha |0\rangle + \beta |1\rangle$ may be represented as $\cos\frac{\theta}{2} |0\rangle + e^{i\psi} \sin\frac{\theta}{2} |1\rangle$. So, any tuple (θ, ψ) represents a qubit.
- This has a nice visualisation in terms of Bloch sphere.



- Single qubit gates are 2×2 unitary matrices. Some of the important gates are:
  - Pauli matrices: $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
  - Hadamard gate: $H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.
  - Phase gate: $S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$.
  - $\pi/8$ gate: $T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
- Simplification: A qubit $\alpha |0\rangle + \beta |1\rangle$ may be represented as $\cos\frac{\theta}{2} |0\rangle + e^{i\psi} \sin\frac{\theta}{2} |1\rangle$. So, any tuple (θ, ψ) represents a qubit.
- This has a nice visualisation in terms of Bloch sphere.



- The vector $(\cos\psi \sin\theta, \sin\psi \sin\theta, \cos\theta)$ is called the Bloch vector.

- Single qubit gates are 2×2 unitary matrices. Some of the important gates are:
  - Pauli matrices: $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
  - Hadamard gate: $H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.
  - Phase gate: $S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$.
  - $\pi/8$ gate: $T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
- Pauli matrices give rise to three useful classes of unitary matrices when they are exponentiated, the rotational operators about the $\hat{x}$, $\hat{y}$, and $\hat{z}$ axis.

$$R_x(\theta) \equiv e^{-i\theta X/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} X = \begin{bmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_y(\theta) \equiv e^{-i\theta Y/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Y = \begin{bmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{bmatrix}$$

$$R_z(\theta) \equiv e^{-i\theta Z/2} = \cos\frac{\theta}{2} I - i \sin\frac{\theta}{2} Z = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix}$$

- Single qubit gates are 2×2 unitary matrices. Some of the important gates are:
  - Pauli matrices: $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
  - Hadamard gate: $H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.
  - Phase gate: $S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$.
  - $\pi/8$ gate: $T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
- A few useful results:
  - Let $\hat{n} = (n_x, n_y, n_z)$ be a real unit vector. The rotation by θ about the $\hat{n}$ axis is given by

$$R_{\hat{n}}(\theta) \equiv e^{-i\frac{\theta}{2}(\hat{n}\cdot\vec{\sigma})} = \cos\frac{\theta}{2} I - i\sin\frac{\theta}{2}(n_x X + n_y Y + n_z Z),$$

    where $\vec{\sigma}$ denotes the vector (X, Y, Z).
  - Theorem: Suppose U is a unitary operator on a single qubit. Then there exist real numbers α, β, γ, and δ such that $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.

Theorem

Suppose U is a unitary operator on a single qubit. Then there exist real numbers α, β, γ, and δ such that $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.

Proof sketch

There are real numbers $\alpha, \beta, \gamma, \delta$ such that:

$$U = \begin{bmatrix} e^{i(\alpha - \beta/2 - \delta/2)} \cos \frac{\gamma}{2} & -e^{i(\alpha - \beta/2 + \delta/2)} \sin \frac{\gamma}{2} \\ e^{i(\alpha + \beta/2 - \delta/2)} \sin \frac{\gamma}{2} & e^{i(\alpha + \beta/2 + \delta/2)} \cos \frac{\gamma}{2} \end{bmatrix}$$

Now one just needs to verify that the RHS matches $e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.

Theorem

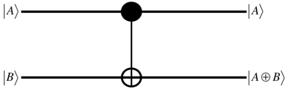
Suppose U is a unitary operator on a single qubit. Then there exist real numbers α, β, γ, and δ such that $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.

Theoerm

Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha} AXBXC$, where α is some overall phase factor.

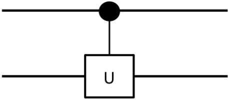
- Single qubit gates are 2×2 unitary matrices. Some of the important gates are:
  - Pauli matrices: $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
  - Hadamard gate: $H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.
  - Phase gate: $S \equiv \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$.
  - $\pi/8$ gate: $T \equiv \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$
- Summary:
  - The above matrices are fundamental entities that define general classes of single-qubit unitary gates such that any single-qubit unitary gate can be represented in terms of these gates.

- The simplest two-qubit gate is the Controlled-NOT or `CNOT` gate:

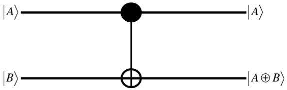


with matrix representation $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$. The top qubit is called the control qubit and the bottom qubit is called the target qubit.

- Another simple two-qubit gate is the Controlled-U gate:

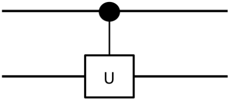


- The simplest two-qubit gate is the Controlled-NOT or CNOT gate:



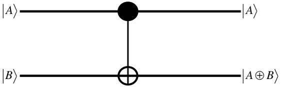
with matrix representation $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$. The top qubit is called the control qubit and the bottom qubit is called the target qubit.

- Another simple two-qubit gate is the Controlled-U gate:



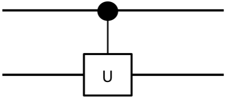
- Some exercises:
    - Build a CNOT gate from one Controlled-Z gate and two Hadamard gates.

- The simplest two-qubit gate is the Controlled-NOT or `CNOT` gate:

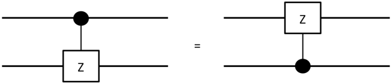


with matrix representation $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$. The top qubit is called the control qubit and the bottom qubit is called the target qubit.

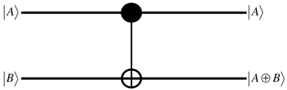
- Another simple two-qubit gate is the Controlled-U gate:



- Some exercises:
  - Build a `CNOT` gate from one Controlled-Z gate and two Hadamard gates.
  - Show that:

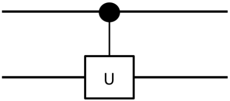


- The simplest two-qubit gate is the Controlled-NOT or `CNOT` gate:

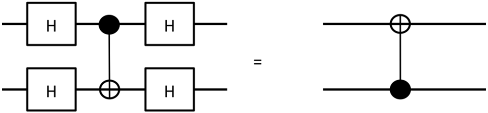


with matrix representation $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$. The top qubit is called the control qubit and the bottom qubit is called the target qubit.

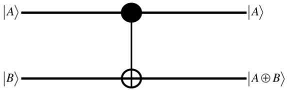
- Another simple two-qubit gate is the Controlled-U gate:



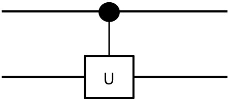
- Some exercises:
  - Show that:



- The simplest two-qubit gate is the Controlled-NOT or `CNOT` gate:



  with matrix representation $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$. The top qubit is called the control qubit and the bottom qubit is called the target qubit.
- Another simple two-qubit gate is the Controlled-U gate:



Question

For a single qubit U, can we implement Controlled-U gate using only `CNOT` and single-qubit gates?

Question

For a single qubit U, can we implement Controlled-U gate using only `CNOT` and single-qubit gates?

Theoerm

Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha} AXBXC$, where α is some overall phase factor.

Theoerm

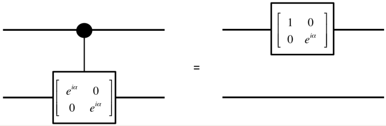
Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha} AXBXC$, where α is some overall phase factor.

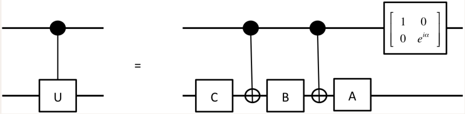
Question

For a single qubit U, can we implement Controlled-U gate using only CNOT and single-qubit gates? Yes

Construction sketch

The construction follows from the following circuit equivalences.





Question

For a single qubit U, can we implement Controlled-U gate using only `CNOT` and single-qubit gates? Yes

Question

For a single qubit U, can we implement Controlled-U gate with two control qubits using only `CNOT` and single-qubit gates?

Question

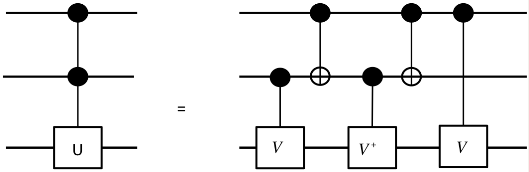
For a single qubit U, can we implement Controlled-U gate using only CNOT and single-qubit gates? Yes

Question

For a single qubit U, can we implement Controlled-U gate with two control qubits using only CNOT and single-qubit gates? Yes

Construction sketch

The construction follows from the following circuit equivalence.



Here V is such that $V^2 = U$.

Question

For a single qubit U, can we implement Controlled-U gate using only `CNOT` and single-qubit gates? Yes

Question

For a single qubit U, can we implement Controlled-U gate with two control qubits using only `CNOT` and single-qubit gates? Yes

Question

For a single qubit U, can we implement Controlled-U gate with n control qubits using only `CNOT` and single-qubit gates?

Question

For a single qubit U, can we implement Controlled-U gate using only CNOT and single-qubit gates? Yes

Question

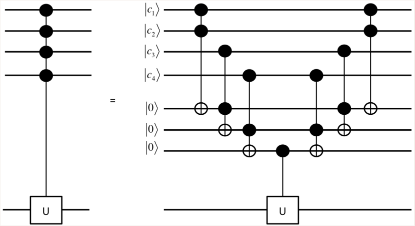
For a single qubit U, can we implement Controlled-U gate with two control qubits using only CNOT and single-qubit gates? Yes

Question

For a single qubit U, can we implement Controlled-U gate with n control qubits using only CNOT and single-qubit gates? Yes using ancilla qubits

Construction sketch

An example construction with $n = 4$.



Quantum Circuit
Controlled operations

- A few other gates and circuit identities:

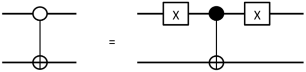
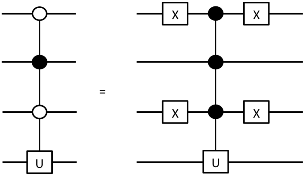
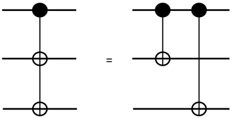


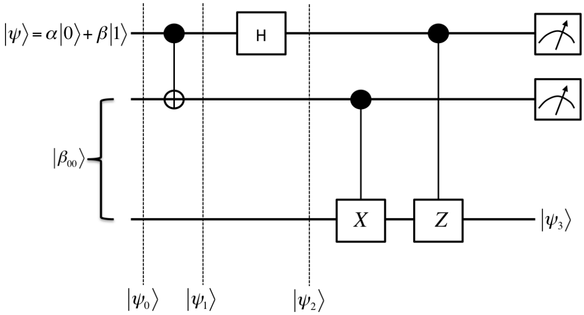
Figure: `NOT` gate applied to the target qubit conditional on the control qubit being 0.





Principle of deferred measurements

Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit, then the clasically controlled operations can be replaced by conditional quantum operations.



Principle of deferred measurements

Measurements can always be moved from an intermediate stage of a quantum circuit to the end of the circuit; if the measurement results are used at any stage of the circuit, then the clasically 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.

- Exercise: Suppose ρ is the density matrix describing a two qubit system. Suppose we perform a projective measurement in the computational basis of the second qubit. Let $P_0 = I \otimes |0\rangle\langle 0|$ and $P_1 = I \otimes |1\rangle\langle 1|$ be the projectors onto the $|0\rangle$ and $|1\rangle$ states of the second qubit, respectively. Let ρ' be the density matrix which would be assigned to the system after the measurement by an observer who did not learn the measurement result. Show that

$$\rho' = P_0 \rho P_0 + P_1 \rho P_1.$$

Also show that the reduced density matrix for the first qubit is not affected by the measurement, that is, $tr_2(\rho) = tr_2(\rho')$.

End