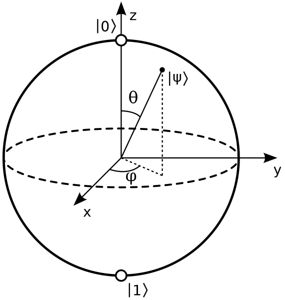
COL866: Quantum Computation and Information

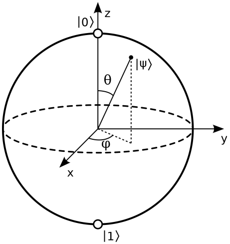
Ragesh Jaiswal, CSE, IIT Delhi

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 visualization 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

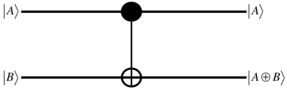
Suppose U is a unitary operator on a single qubit. Then there exist real numbers α, β, γ, and δ such that $U = e^{i\alpha} R_z(\beta) R_y(\gamma) R_z(\delta)$.

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.

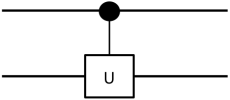
- Single qubit gates are 2×2 unitary matrices. Some of the important gates are:
  - Pauli matrices: $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, $Y \equiv \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
  - Hadamard gate: $H \equiv \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.
  - 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:

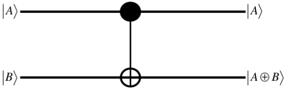


with matrix representation $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$. The top qubit is called the control qubit, and the bottom qubit is called the target qubit.

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

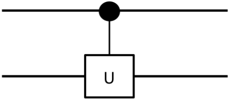


- The simplest two-qubit gate is the Controlled-NOT or `CNOT` gate:



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.

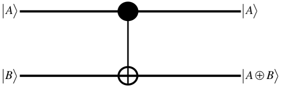
- Another simple two-qubit gate is the Controlled-U gate:



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

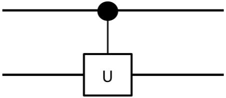
Quantum Circuit
Controlled operations

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

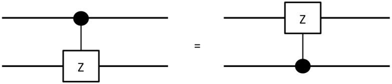


with matrix representation $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$. The top qubit is called the control qubit, and the bottom qubit is called the target qubit.

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

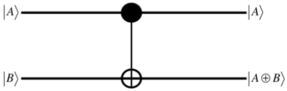


- <u>Some exercises</u>:
  - Build a `CNOT` gate from one Controlled-Z gate and two Hadamard gates.
  - Show that:



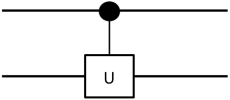
Quantum Circuit
Controlled operations

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

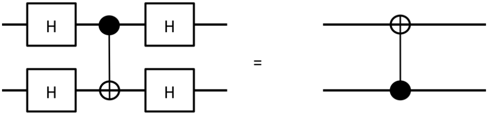


with matrix representation $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$. The top qubit is called the control qubit, and the bottom qubit is called the target qubit.

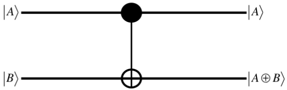
- Another simple two-qubit gate is the Controlled-U gate:



- Some exercises:
  - Show that:

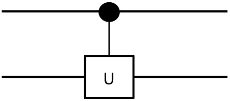


- The simplest two-qubit gate is the Controlled-NOT or `CNOT` gate:



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.

Quantum Circuit
Controlled operations

Theoerm

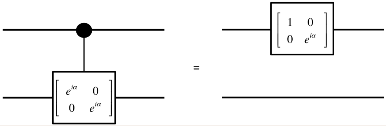
Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha} AXBXC$, where α is some overall phase factor.

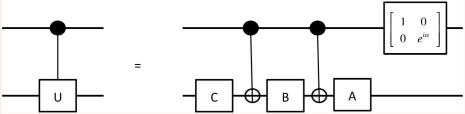
Question

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

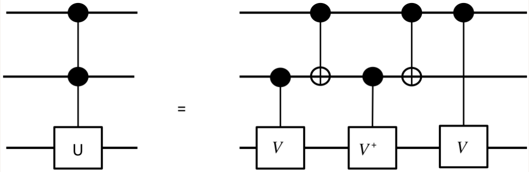
For a single qubit U, can we implement Controlled-U gate using only CNOT and single-qubit gates? Yes

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

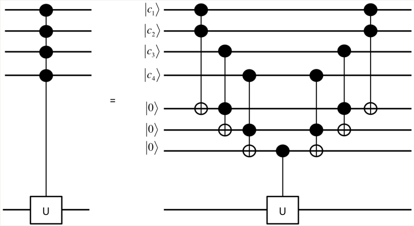
For a single qubit U, can we implement Controlled-U gate with two control qubits using only CNOT and single-qubit gates? Yes

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:

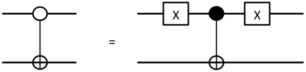
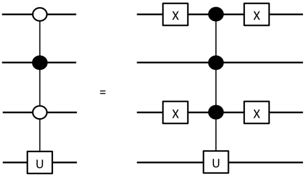
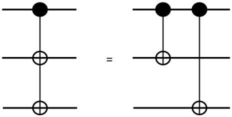


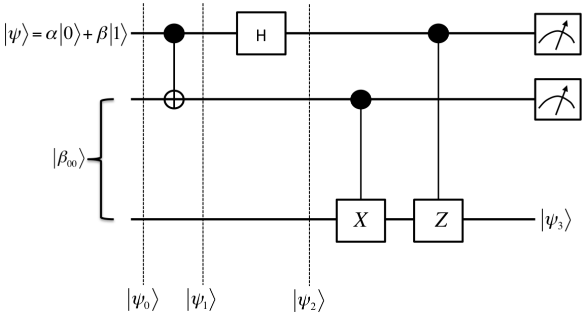
Figure: `NOT` gate applied to the target qubit conditional on the control qubit being 0.





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 classically 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 classically controlled operations can be replaced by conditional quantum operations.

Principle of implicit measurement

Without loss of generality, any unterminated quantum wires (qubits that are not measured) at the end of a quantum circuit may be assumed to be measured.

- A set of gates is said to be universal for quantum computation if **any** unitary operation may be **approximated** to arbitrary accuracy by a quantum circuit involving only those gates.

Claim

Any unitary operation can be approximated to arbitrary accuracy using Hadamard, `CNOT`, and $\pi/8$ gates.

Claim

Any unitary operation can be approximated to arbitrary accuracy using Hadamard, CNOT, and $\pi/8$ gates.

Proof sketch

- Claim 1: A single qubit operation may be **approximated** to arbitrary accuracy using the Hadamard, and $\pi/8$ gates.
- Claim 2: An arbitrary unitary operator may be expressed **exactly** using single qubit and CNOT gates.
    - Claim 2.1: An arbitrary unitary operator may be expressed **exactly** as a product of unitary operators that each acts non-trivially only on a subspace spanned by two computational basis states (such gates are called two-level gates).
    - Claim 2.2: An arbitrary two-level unitary operator may be expressed exactly using single qubit and CNOT gates.

- What about efficiency?
    - Upper-bound: Any unitary can be approximated using exponentially many gates.
    - Lower-bound: There exists a unitary operation that requires exponentially many gates to approximate.

Claim 2.1

An arbitrary unitary operator may be expressed **exactly** as a product of unitary operators that each acts non-trivially only on a subspace spanned by two computational basis states.

Proof sketch

- The main idea can be understood using a 3×3 unitary matrix:

$$U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}.$$

- We will find two-level unitary matrices U_1, U_2, U_3 such that

$$U_3 U_2 U_1 U = I \quad \text{and} \quad U = U_1^\dagger U_2^\dagger U_3^\dagger$$

Claim 2.1

An arbitrary unitary operator may be expressed **exactly** as a product of unitary operators that each acts non-trivially only on a subspace spanned by two computational basis states.

Proof sketch

- The main idea can be understood using a 3×3 unitary matrix:

$$U = \begin{bmatrix} a & d & g \\ b & e & h \\ c & f & j \end{bmatrix}.$$

- We will find two-level unitary matrices U_1, U_2, U_3 such that

$$U_3 U_2 U_1 U = I \quad \text{and} \quad U = U_1^\dagger U_2^\dagger U_3^\dagger$$

- Exercise
  - Show that any $d \times d$ unitary matrix can be written in terms of $d(d-1)/2$ two-level matrices.
  - There exists a $d \times d$ unitary matrix U which cannot be decomposed as a product of fewer than $d-1$ two-level unitary matrices.

Claim 2

An arbitrary unitary operator may be expressed **exactly** using single qubit and CNOT gates.

- Claim 2.1: An arbitrary unitary operator may be expressed **exactly** as a product of unitary operators that each acts non-trivially only on a subspace spanned by two computational basis states.
- Claim 2.2: An arbitrary two-level unitary operator may be expressed exactly using single qubit and CNOT gates.

Proof sketch

- Let U be a two-level unitary matrix on a n-qubit quantum computer.
- Let U act non-trivially on the space spanned by the computational basis states $|s\rangle$ and $|t\rangle$, where $s = s_1, ..., s_n$ and $t = t_1, ..., t_n$ are n-bit binary strings.
- Let $\tilde{U}$ be the non-trivial 2×2 submatrix of U. Note that we can think $\tilde{U}$ to be a unitary operator on a single qubit.
- We will use the gray-code connecting s and t, which is a sequence of n-bit strings starting with s and ending with t such that the subsequent strings in the sequence differ only on one bit.
- Example: $s = 101001$, $t = 110011$.

$$g_1 = 101001; g_2 = 101011; g_3 = 100011; g_4 = 110011$$

- Main idea:
  - We will design a sequence of swaps $|g_1\rangle \rightarrow |g_{m-1}\rangle, |g_2\rangle \rightarrow |g_1\rangle, |g_3\rangle \rightarrow |g_2\rangle, ..., |g_{m-1}\rangle \rightarrow |g_{m-2}\rangle$.
  - We will apply $\tilde{U}$ to the qubit that differs in g_{m-1} and g_m.
  - Swap $|g_{m-1}\rangle$ with $|g_{m-2}\rangle$, $|g_{m-2}\rangle$ with $|g_{m-3}\rangle$ and so on.

Claim 2.2

An arbitrary two-level unitary operator may be expressed exactly using single qubit and `CNOT` gates.

Example construction

- Let the two-level transformation be:

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}$$

- The gray code connecting $|000\rangle$ and $|111\rangle$:
$|000\rangle \rightarrow |001\rangle \rightarrow |011\rangle \rightarrow |111\rangle$.

Claim 2.2

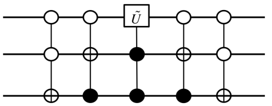
An arbitrary two-level unitary operator may be expressed exactly using single qubit and CNOT gates.

Example construction

- Let the two-level transformation be:

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}$$

- The gray code connecting $|000\rangle$ and $|111\rangle$: $|000\rangle \rightarrow |001\rangle \rightarrow |011\rangle \rightarrow |111\rangle$.
- Construction:



Claim 2.2

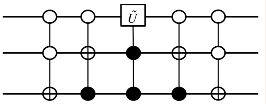
An arbitrary two-level unitary operator may be expressed exactly using single qubit and CNOT gates.

Example construction

- Let the two-level transformation be:

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}$$

- The gray code connecting $|000\rangle$ and $|111\rangle$: $|000\rangle \rightarrow |001\rangle \rightarrow |011\rangle \rightarrow |111\rangle$.
- Construction:



- Exercise
  - For an arbitrary unitary operator on an n-qubit system, how many CNOT and single qubit gate will be required in the entire construction?

Claim 2

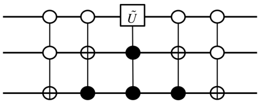
An arbitrary unitary operator may be expressed **exactly** using single qubit and `CNOT` gates.

Example construction

- Let the two-level transformation be:

$$U = \begin{bmatrix} a & 0 & 0 & 0 & 0 & 0 & 0 & c \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ b & 0 & 0 & 0 & 0 & 0 & 0 & d \end{bmatrix}$$

- The gray code connecting $|000\rangle$ and $|111\rangle$: $|000\rangle \rightarrow |001\rangle \rightarrow |011\rangle \rightarrow |111\rangle$.
- Construction:



- Exercise
  - For an arbitrary unitary operator on an n-qubit system, how many `CNOT` and single qubit gate will be required in the entire construction? $O(n^2 4^n)$ gates.

End