COL863: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

Quantum Computation: Quantum circuits

Quantum Circuit
Controlled operations

Theoerm

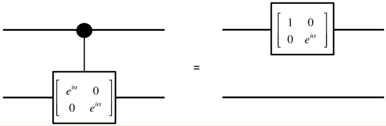
Suppose U is a unitary gate on a single qubit. Then there exist unitary operators A, B, C on a single qubit such that $ABC = I$ and $U = e^{i\alpha}AXBXC$, where α is some overall phase factor.

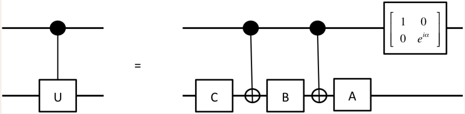
Question

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

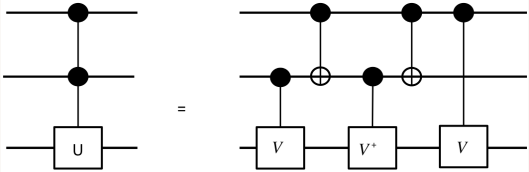
For a single qubit U, can we implement Controlled-U gate using only `CNOT` and single-qubit gates? Yes

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

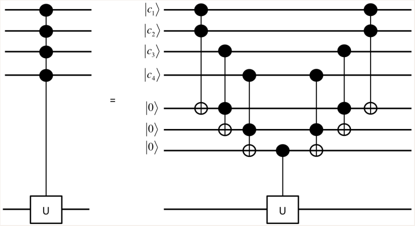
For a single qubit U, can we implement Controlled-U gate with two control qubits using only CNOT and single-qubit gates? Yes

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 $n = 4$.



- A few other gates and circuit identities:

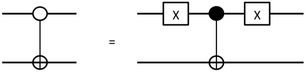
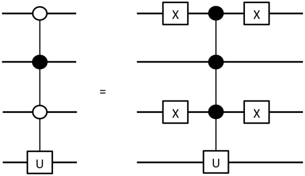
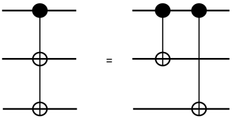


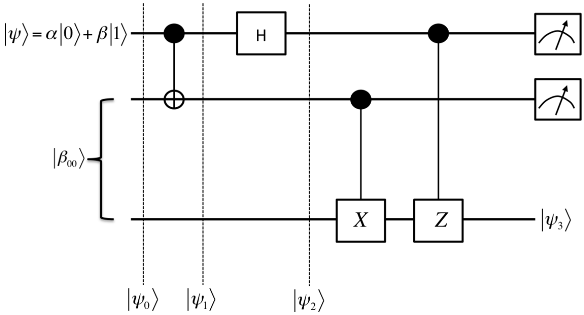
Figure: NOT gate applied to the target qubit conditional on the control qubit being 0.





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, $tr_2(\rho) = tr_2(\rho')$.

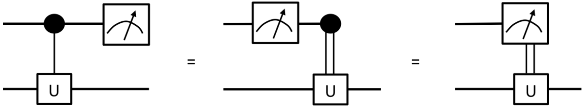
Principle of deferred measurements

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: Show that measurement commutes with control.



- 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, phase, `CNOT`, and $\pi/8$ gates.

Claim

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

Proof sketch

- Claim 1: A single qubit operation may be **approximated** to arbitrary accuracy using the Hadamard, phase, 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 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 which require 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 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 staring 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 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

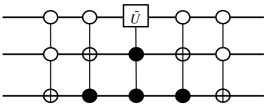
An arbitrary two-level unitary operator may be expressed exactly using using single qubit and CNOT gates.

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

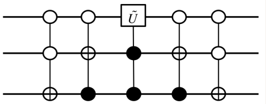
An arbitrary two-level unitary operator may be expressed exactly using using single qubit and CNOT gates.

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 willl be required in the entire construction?

Claim 2

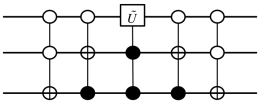
An arbitrary unitary operator may be expressed **exactly** using single qubit and CNOT gates.

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 $|111\rangle$: $|000\rangle \to |001\rangle \to |011\rangle \to |111\rangle$.
- Construction:



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

Claim

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

Proof sketch

- Claim 1: A single qubit operation may be **approximated** to arbitrary accuracy using the Hadamard, phase, 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 using single qubit and CNOT gates.

- A discrete set of gates cannot be used to implement an arbitrary unitary operation.
- However, it may be possible to approximate any unitary gate using a discrete set of gates.

Claim 1

A single qubit operation may be **approximated** to arbitrary accuracy using the Hadamard, phase, and $\pi/8$ gates.

- We first need to define a notion of approximating a unitary operation.
- Let U and V be unitary operators on the same state space.
  - U denotes the target unitary operator that we would like to implement.
  - V is the operator that is actually implemented.
- The error (w.r.t. implementing V instead of U) is defined as

$$E(U, V) \equiv \max_{|\psi\rangle} ||(U - V)|\psi\rangle||$$

- Question: Why is the above a reasonable notion of error when implementing V instead of U?

Claim 1

A single qubit operation may be **approximated** to arbitrary accuracy using the Hadamard, phase, and $\pi/8$ gates.

- The error (w.r.t. implementing V instead of U) is defined as

$$E(U, V) \equiv \max_{|\psi\rangle} ||(U - V)\,|\psi\rangle\,||$$

Claim 1.1

Suppose we wish to implement a quantum circuit with m gates $U_1, ..., U_m$. However, we can only implement $V_1, ..., V_m$. The difference in probabilities of a measurement outcome will be at most a tolerance $\Delta > 0$ given that $\forall j, E(U_j, V_j) \leq \frac{\Delta}{2m}$.

Claim 1

A single qubit operation may be **approximated** to arbitrary accuracy using the Hadamard, phase, and $\pi/8$ gates.

- The error (w.r.t. implementing V instead of U) is defined as

$$E(U, V) \equiv \max_{|\psi\rangle} ||(U - V)\,|\psi\rangle\,||$$

Claim 1.1

Suppose we wish to implement a quantum circuit with m gates $U_1, ..., U_m$. However, we can only implement $V_1, ..., V_m$. The difference in probabilities of a measurement outcome will be at most a tolerance $\Delta > 0$ given that $\forall j, E(U_j, V_j) \leq \frac{\Delta}{2m}$.

Proof sketch

- Claim 1.1.1: For any POVM element M let P_U and P_V denote the probabilities for measuring this element when U and V are used respectively. Then $|P_U - P_V| \leq 2 \cdot E(U, V)$.
- Claim 1.1.2: $E(U_m U_{m-1} ... U_1, V_m V_{m-1} ... V_1) \leq \sum_{j=1}^{m} E(U_j, V_j)$.

End