COL863: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

Quantum Computation: Quantum circuits

- 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 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

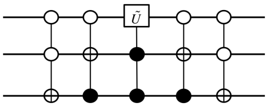
An arbitrary two-level unitary operator may be expressed exactly using using single qubit and `CNOT` gates.

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

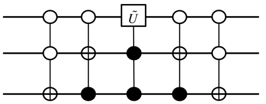
An arbitrary two-level unitary operator may be expressed exactly using using single qubit and CNOT gates.

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

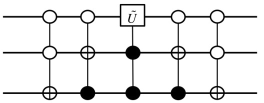
An arbitrary unitary operator may be expressed **exactly** using single qubit and `CNOT` gates.

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 $|111\rangle$: $|000\rangle \rightarrow |001\rangle \rightarrow |011\rangle \rightarrow |111\rangle$.
- 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? $O(n^2 4^n)$ 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 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, 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, 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, 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: $E(U_m U_{m-1} ... U_1, V_m V_{m-1} ... V_1) \leq \sum_{j=1}^{m} E(U_j, V_j)$.

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