COL863: Quantum Computation and Information

Ragesh Jaiswal, CSE, IIT Delhi

Quantum Computation: Quantum circuits

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: $E(U_m U_{m-1} ... U_1, V_m V_{m-1} ... V_1) \leq \sum_{j=1}^{m} E(U_j, V_j)$.

Claim 1

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

- Claim 1(a): The $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$ gate is (upto a global phase factor) a rotation by $\pi/4$ around the $\hat{z}$ axis on the Block sphere.
- Claim 1(b): The operation HTH is a rotation by $\pi/4$ around the $\hat{x}$ axis on the Bloch sphere.
- Claim 1(c): Composing T and HTH gives (upto a global phase):

$$e^{-i\frac{\pi}{8}Z} e^{-i\frac{\pi}{8}X} = \cos^2\frac{\pi}{8}I - i\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right]\sin\frac{\pi}{8}$$

which may be interpreted as rotation of the Bloch sphere about an axis along $\vec{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$ with unit vector $\hat{n}$ by an angle θ that satisfies $\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}$. Moreover θ is an irrational multiple of 2π.

Claim 1

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

- Claim 1(c): Composing T and HTH gives (upto a global phase):

$$e^{-i\frac{\pi}{8}Z}e^{-i\frac{\pi}{8}X} = \cos^2\frac{\pi}{8}I - i\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right]\sin\frac{\pi}{8}$$

  which may be interpreted as rotation of the Bloch sphere about an axis along $\vec{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$ with unit vector $\hat{n}$ by an angle θ that satisfies $\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}$. Moreover θ is an irrational multiple of 2π.
- Claim 1(d): For any α and $\varepsilon > 0$, there exists a positive integer n such that $E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)^n) < \varepsilon/3$.
  (*In simpler terms, $R_{\hat{n}}(\alpha)$ can be approximated to arbitrary accuracy by repeated application of $R_{\hat{n}}(\theta)$.*)
  - Uses the lemma that $E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\alpha+\beta)) = |1 - e^{i\beta/2}|$.

Claim 1

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

- Claim 1(c): Composing T and HTH gives (upto a global phase): $e^{-i\frac{\pi}{8}Z}e^{-i\frac{\pi}{8}X} = \cos^2\frac{\pi}{8}I - i\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right]\sin\frac{\pi}{8}$, which may be interpreted as rotation of the Bloch sphere about an axis along $\vec{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$ with unit vector $\hat{n}$ by an angle θ that satisfies $\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}$. Moreover θ is an irrational multiple of 2π.
- Claim 1(d): For any α and $\varepsilon > 0$, there exists a positive integer n such that $E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)^n) < \varepsilon/3$.
- Claim 1(e): For any α, $HR_{\hat{n}}(\alpha)H = R_{\hat{m}}(\alpha)$ where $\hat{m}$ is a unit vector in the direction $(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$.

Claim 1

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

- Claim 1(c): Composing T and HTH gives (upto a global phase): $e^{-i\frac{\pi}{8}Z}e^{-i\frac{\pi}{8}X} = \cos^2\frac{\pi}{8}I - i\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right]\sin\frac{\pi}{8}$, which may be interpreted as rotation of the Bloch sphere about an axis along $\vec{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$ with unit vector $\hat{n}$ by an angle θ that satisfies $\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}$. Moreover θ is an irrational multiple of 2π.
- Claim 1(d): For any α and $\varepsilon > 0$, there exists a positive integer n such that $E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)^n) < \varepsilon/3$.
- Claim 1(e): For any α, $HR_{\hat{n}}(\alpha)H = R_{\hat{m}}(\alpha)$ where $\hat{m}$ is a unit vector in the direction $(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$.
- Claim 1(f): An arbitrary single qubit unitary operator U (upto a global phase) may be written as

$$U = R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta).$$

Claim 1

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

- Claim 1(c): Composing T and HTH gives (upto a global phase): $e^{-i\frac{\pi}{8}Z}e^{-i\frac{\pi}{8}X} = \cos^2\frac{\pi}{8}I - i\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right]\sin\frac{\pi}{8}$, which may be interpreted as rotation of the Bloch sphere about an axis along $\vec{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$ with unit vector $\hat{n}$ by an angle θ that satisfies $\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}$. Moreover θ is an irrational multiple of 2π.
- Claim 1(d): For any α and $\varepsilon > 0$, there exists a positive integer n such that $E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)^n) < \varepsilon/3$.
- Claim 1(e): For any α, $HR_{\hat{n}}(\alpha)H = R_{\hat{m}}(\alpha)$ where $\hat{m}$ is a unit vector in the direction $(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$.
- Claim 1(f): An arbitrary single qubit unitary operator U (upto a global phase) may be written as $U = R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta)$.
- Claim 1(g): For any $\varepsilon > 0$, there exists positive integers n_1, n_2, n_3 such that:

$$E(U, R_{\hat{n}}(\theta)^{n_1} H R_{\hat{n}}(\theta)^{n_2} H R_{\hat{n}}(\theta)^{n_3}) < \varepsilon.$$

Claim 1

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

- Claim 1(c): Composing T and HTH gives (upto a global phase): $e^{-i\frac{\pi}{8}Z}e^{-i\frac{\pi}{8}X} = \cos^2\frac{\pi}{8}I - i\left[\cos\frac{\pi}{8}(X+Z) + \sin\frac{\pi}{8}Y\right]\sin\frac{\pi}{8}$, which may be interpreted as rotation of the Bloch sphere about an axis along $\vec{n} = (\cos\frac{\pi}{8}, \sin\frac{\pi}{8}, \cos\frac{\pi}{8})$ with unit vector $\hat{n}$ by an angle θ that satisfies $\cos\frac{\theta}{2} = \cos^2\frac{\pi}{8}$. Moreover θ is an irrational multiple of 2π.
- Claim 1(d): For any α and $\varepsilon > 0$, there exists a positive integer n such that $E(R_{\hat{n}}(\alpha), R_{\hat{n}}(\theta)^n) < \varepsilon/3$.
- Claim 1(e): For any α, $HR_{\hat{n}}(\alpha)H = R_{\hat{m}}(\alpha)$ where $\hat{m}$ is a unit vector in the direction $(\cos\frac{\pi}{8}, -\sin\frac{\pi}{8}, \cos\frac{\pi}{8})$.
- Claim 1(f): An arbitrary single qubit unitary operator U (upto a global phase) may be written as $U = R_{\hat{n}}(\beta)R_{\hat{m}}(\gamma)R_{\hat{n}}(\delta)$.
- Claim 1(g): For any $\varepsilon > 0$, there exists positive integers n_1, n_2, n_3 such that: $E(U, R_{\hat{n}}(\theta)^{n_1}HR_{\hat{n}}(\theta)^{n_2}HR_{\hat{n}}(\theta)^{n_3}) < \varepsilon$.
  - Question: What is the dependence of n_1, n_2, n_3 in terms of the error parameter ε?

Claim 1

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

- Question: What is the complexity of this approximate construction in the worst case?

Theorem (Solovay-Kitaev Theorem)

An arbitrary single qubit gate may be approximated to an accuracy ε using $O(\log^c(1/\varepsilon))$ gates from our discrete set, where $c \approx 2$ is a small constant.

Claim 1

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

- Question: What is the complexity of this approximate construction in the worst case?

Theorem (Solovay-Kitaev Theorem)

An arbitrary single qubit gate may be approximated to an accuracy ε using $O(\log^c(1/\varepsilon))$ gates from our discrete set, where $c \approx 2$ is a small constant.

- Corollary: A circuit containing m `CNOT` and single qubit unitary operations can be approximated to accuracy ε using $O(m \log^c(m/\varepsilon))$ gates from our discrete set.

Claim

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

- Question: Given a unitary transformation U on n qubits, does there always exist a circuit of size polynomial in n approximating U?

Claim

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

- Question: Given a unitary transformation U on n qubits, does there always exist a circuit of size polynomial in n approximating U? No

Theorem

Suppose we have g different types of gates each acting on at most f qubits. In this setup, if any unitary operation on n qubits can be approximated to within ε accuracy using m gates, then $m = \Omega\left(\frac{2^n \log 1/\varepsilon}{\log n}\right)$.

Theorem

Suppose we have g different types of gates each acting on at most f qubits. In this setup, if any unitary operation on n qubits can be approximated to within ε accuracy using m gates, then $m = \Omega\left(\frac{2^n \log 1/\varepsilon}{\log n}\right)$.

Proof sketch

- The proof is by a covering argument.
- Claim 1: A arbitrary state $|\psi\rangle$ can be thought of as a point on the surface of a unit ball in 2^{n+1} dimensions. That is, a point on the $(2^{n+1} - 1)$-sphere with unit radius.

Theorem

Suppose we have g different types of gates each acting on at most f qubits. In this setup, if any unitary operation on n qubits can be approximated to within ε accuracy using m gates, then $m = \Omega\left(\frac{2^n \log 1/\varepsilon}{\log n}\right)$.

Proof sketch

- The proof is by a covering argument.
- Claim 1: A arbitrary state $|\psi\rangle$ can be thought of as a point on the surface of a unit ball in 2^{n+1} dimensions. That is, a point on the $(2^{n+1} - 1)$-sphere with unit radius.
- Fact from Geometry: The surface area of radius ε near $|\psi\rangle$ is approximately same as the volume of a $(2^{n+1} - 2)$-sphere of radius ε.
- Claim 2: The number of patches required to cover state space is $\Omega\left(\frac{1}{\varepsilon^{2^{n+1}-1}}\right)$.

Theorem

Suppose we have g different types of gates each acting on at most f qubits. In this setup, if any unitary operation on n qubits can be approximated to within ε accuracy using m gates, then $m = \Omega\left(\frac{2^n \log 1/\varepsilon}{\log n}\right)$.

Proof sketch

- The proof is by a covering argument.
- Claim 1: A arbitrary state $|\psi\rangle$ can be thought of as a point on the surface of a unit ball in 2^{n+1} dimensions. That is, a point on the $(2^{n+1} - 1)$-sphere with unit radius.
- Fact from Geometry: The surface area of radius ε near $|\psi\rangle$ is approximately same as the volume of a $(2^{n+1} - 2)$-sphere of radius ε.
- Claim 2: The number of patches required to cover state space is $\Omega\left(\frac{1}{\varepsilon^{2^{n+1}-1}}\right)$.
- Claim 3: The number of patches we can hit with m gates is $O(n^{fmg})$.
- Combining claims 2 and 3, we get the statement of the theorem. □

End