Assignments 60%  
Final project 40%

Resources: Course website  
Slack

Lecture 1  
① Q. circuit model (review)  
② Amplitude Amplification

Quantum circuit model

Hilbert space of n qubits: $\mathbb{C}^2 \otimes^n$  
Computational basis $\{|x\rangle: x \in \{0,1\}^n\}$

Suppose $U$ is 1-qubit unitary

While $U_i \overset{\text{def}}{=} \underbrace{I \otimes I \otimes \cdots \otimes I}_{i-1} \otimes U \otimes I \otimes \cdots \otimes I_{n-i}$

Also for 2-qubit gates, e.g. $\text{CNOT}_{12} = \text{CNOT} \otimes \underbrace{I \otimes \cdots \otimes I}_{n-2}$
A gate set \( G \) is a set of allowed \( n \)-qubit gates.

**Ex 1:**

\[
G_A = \{ \text{CNOT}_{ij} : i \neq j, \ i, j \in [n] \} \cup \{ U_i : U \in U(2), i \in [n] \}
\]

**Ex 2:**

"Clifford + T"

\[
G_B = \{ \text{CNOT}_{ij} : i \neq j, \ i, j \in [n] \} \cup \{ H_i : 1 \leq i \leq n \} \cup \{ T_i : 1 \leq i \leq n \}
\]

\[
H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad T = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{pmatrix}
\]

Informally, \( G_B = \{ \text{CNOT}, H, T \} \)

A q. circuit over a gate set \( G \) is a seq. of gates \( U^1, U^2, \ldots, U^n \in G \)

Specifically, unitary

\[
U = U^n U^{n-1} \cdots U^2 U^1
\]
A gate set \( \mathcal{G} \) is universal if

\[
\forall \epsilon > 0 \text{ and any } n\text{-qubit unitary } U \exists m > 0 \text{ and } U_1, U_2, \ldots, U_m \in \mathcal{G}
\]

such that

\[
\| U - e^{i\varphi} U^m U^{m-1} \cdots U^2 U^1 \| < \epsilon
\]

\( \varphi \in \mathbb{R} \)

Exercises: \( \mathcal{G}_A \) is universal

\( \mathcal{G}_B \) is universal
Translation between gate sets

Suppose \( U = U^m U^{m-1} \cdots U^1 \) \( U^i \in G^- \)

\( V = V^m V^{m-1} \cdots V^1 \) \( V^i \) a product of gates in \( G^- \)

Think \( V^i \approx U^i \)

Claim: \( \| U - V \| \leq \sum_{j=1}^{m} \| U^j - V^j \| \)

Proof: Induction on \( m \)

Base case \( m = 1 \) trivial

Now suppose true for \( m - 1 \)

\[
\| U - V \| = \| (U^m - V^m) U^{m-1} \cdots U^1 + (V^m U^{m-1} \cdots U^1) \|
\]

\[
= \| (U^m - V^m) U^{m-1} \cdots U^1 \| + \| (V^m U^{m-1} \cdots U^1) \|
\]

\[
\leq \| U^m - V^m \| + \| U^{m-1} \cdots U^1 - V^{m-1} \cdots V^1 \|
\]

\[
\leq \| U^m - V^m \| + \sum_{j=1}^{m-1} \| U^j - V^j \| \quad \text{inductive hypothesis}
\]

Corollary: \( \| U - V \| \leq \epsilon \) if \( \| U^j - V^j \| \leq \epsilon / m \) for all \( j \) suffices to approx gates in \( G^- \)
Thm [Solovay–Kitaev]

Let $G$ be a universal gate set for $d$-qubits where $d = o(n)$. Suppose $G$ has the property that $V \in G \Rightarrow V^* \in G$.

Let $U \in SU(2^d)$ and $\epsilon > 0$ be given. Then there is a class. alg with runtime $\text{poly} \left( \log \frac{1}{\epsilon} \right)$ which outputs a sequence

$$U_1, U_2, \ldots, U_m \in G \quad m = \text{poly} \left( \log \frac{1}{\epsilon} \right)$$

such that

$$\| U - U_m U_{m-1} \ldots U_1 e^{i\phi} \| < \epsilon$$

Combining claim + thm: overhead for translating $m$-gate circuit using some gate set $G$ (with gates on $o(n)$ qubits) into another universal gate set $G'$

$$\text{cost} = O \left( \text{poly} \left( \log \frac{m}{\epsilon} \right) \right)$$

polynomial speedups preserved.
Amplitude Amplification [Brassard, Hoyer, Mosca, Tapp 2000]

Given: $(n+1)$-qubit unitary $U$ s.t.

$$U |0^{n+1} \rangle = \sqrt{p} |\phi_+^{n+1}\rangle + \sqrt{1-p} |\phi_-^{n+1}\rangle$$

for some unknown $p \in (0,1)$

$$\|\phi_+\| = \|\phi_-\| = 1$$

Goal: prepare $|\phi_+^{n+1}\rangle$ using $U$ and $U^+$ as few times as possible.

Naive algorithm

1. Prepare $|0^{n+1}\rangle$
2. Measure $I \otimes I \otimes \cdots \otimes I$

repeat until you get $+1$ in step 2

$$\mathbb{E} \# \text{ of uses of } U \bigg| \frac{1}{p} \quad \text{not great if } p \text{ is small}$$

Thm: There is a q. alg. "AA" with expected runtime $O(\frac{1}{\sqrt{p}})$ that prepares $|\phi_+^{n+1}\rangle$. 

Remark: Includes Grover search as a special case.

function \( f : \{0,1\}^n \rightarrow \{0,1\} \)

Given an oracle that encodes \( f \)

\[ U_f |x \rangle |b \rangle = |x \rangle |b \oplus f(x) \rangle \]

Want \( x \) s.t. \( f(x) = 1 \) (if it exists)

Let \( M = \{ x : f(x) = 1 \} \)

Use AA with \( U = U_f (H^\otimes n \circ I) \)

\[ U \left| 0^{n+1} \right\rangle = \sqrt{\frac{M}{2^n}} \left( \frac{1}{\sqrt{M}} \sum_{x : f(x) = 1} |x \rangle \right) \left| 0^n \right\rangle + \sqrt{\frac{2^n - M}{2^n}} \left( \frac{1}{\sqrt{2^n - M}} \sum_{x : f(x) = 0} |x \rangle \right) \left| 0^n \right\rangle \]

\[ \rho = \frac{M}{2^n} \]

Runtime to find a solution using AA = \( O(\sqrt{\frac{2^n}{M}}) \)
Define

\[ R_B = 2(\mathbf{I} \otimes 10 \times 1) - \mathbf{I} \]

Both unitary

\[ R_A = 2\mathbf{U}10^{n+1} \times 0^{n+1} \mathbf{U}^\dagger - \mathbf{I} \]

\[ \mathbf{U} \leftarrow \cdot \ast \]

\[ \text{where } \mathbf{U} \text{ use of } \mathbf{U}, \mathbf{U}^\dagger \]

Lemma

\[ (R_A R_B)^j \mathbf{U}10^{n+1} > = \sin((2j+1)\Theta_p) \mathbf{1}\theta_j > 117 \]

+ \[ \cos((2j+1)\Theta_p) \mathbf{1}\theta_j > 107 \]

where \[ \Theta_p = \sin^{-1}(\sqrt{\rho}) \]

pf: Consider \[ \mathbf{V} = \text{span}\{\mathbf{1}_{\theta_j > 117}, \mathbf{1}_{\theta_j > 107}\} \]

note that \[ R_A \text{ and } R_B \text{ preserve } \mathbf{V} \]

\[ \Rightarrow \text{Since } \mathbf{U}10^{n+1} > \in \mathbf{V} \text{ so is } (R_A R_B)^j \mathbf{U}10^{n+1} > \text{ for all } j \]

Look at \[ R_A |_\mathbf{V} \quad R_B |_\mathbf{V} \]
\( R_B \) = reflection about \( \Phi_0 \geq 107 \)

\( R_A \) = reflection about \( \Omega_{10^{n+1}} = \sqrt{p} \Phi_{1/7117} + \sqrt{1-p} \Phi_{107} \)

\[ R_A R_B \] = rotation by 2\( \Phi \)

Next time
AA alg + analysis + more.