Lecture 17

Nov 19 , 2025

Proving local Hamiltonian is QMA-hard:

Given input circuit $C = g_T \cdots g_1$ acting on n qubit input, m ancilla.

Construct a local Ham H and quantities (a, b),

1. $\exists |\psi\rangle$ s.t. $C(|\psi\rangle)$ accepts w pr $\geq 1 - \epsilon$,

   then $\exists |\varphi\rangle$ s.t. $\langle \varphi | H | \varphi \rangle \leq a$

2. $\forall |\psi\rangle$, $C(|\psi\rangle)$ accepts w pr $\leq \epsilon$,

   then $\forall |\varphi\rangle$, $\langle \varphi | H | \varphi \rangle \geq b$.

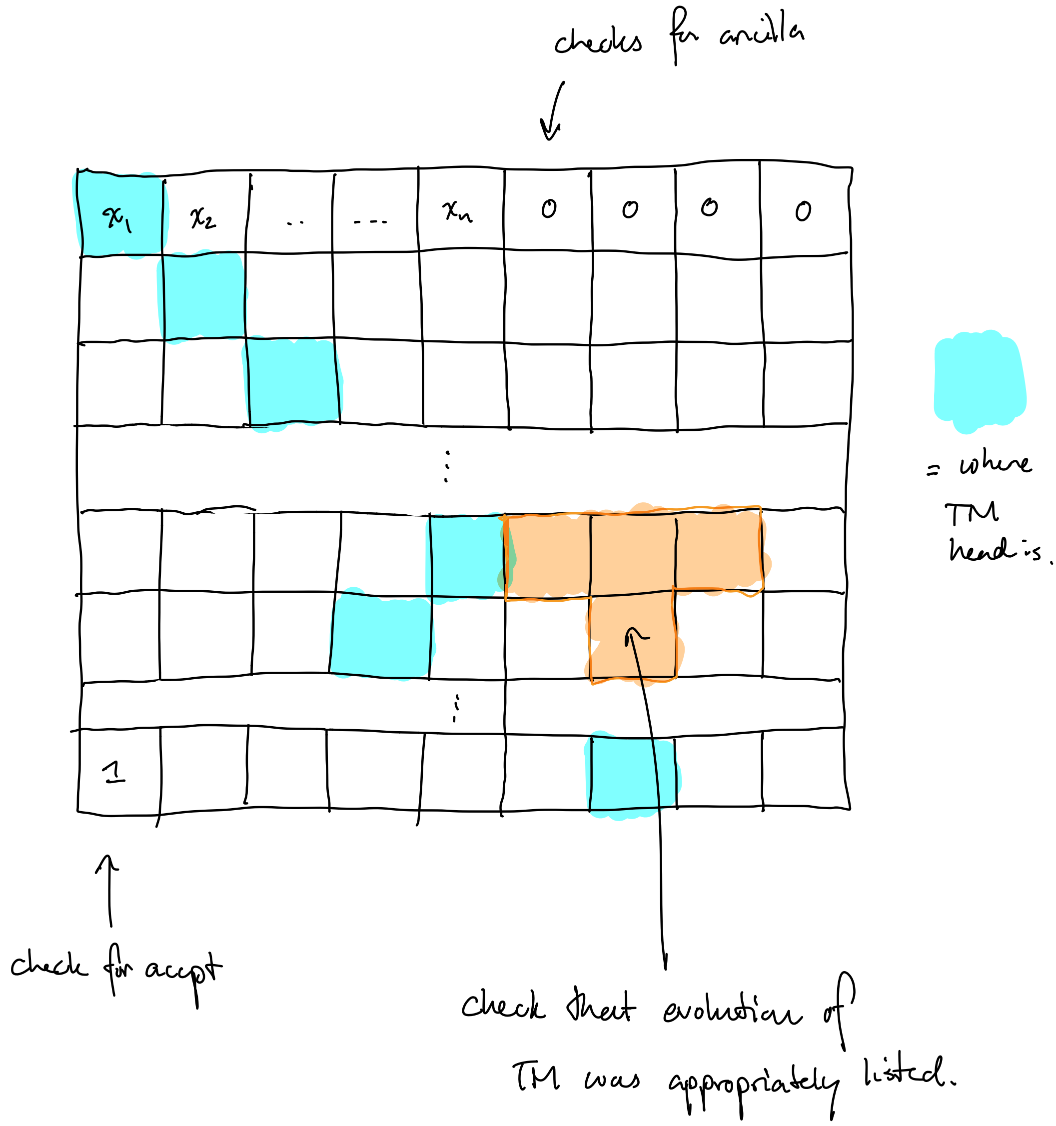
In class, we will only prove that $\underbrace{O(\log n)}_{\sim k}$-LH is QMA-hard.

HW will include problem for proving 5-local hardness.

Quantum analog of the Cook-Levin theorem proving that 3-SAT is NP-complete.

Cook-Levin Tableau Review:

given classical computation of T time steps using total space S, write a $T \cdot S$ tableau with the state of the machine at time t in row t.



Can we construct the same for quantum comp.?

Consider a circuit $C = g_T \cdots g_1$. Can we create a table with rows

$$|\psi_0\rangle = |\psi_{\text{witness}}\rangle \otimes |0^m\rangle$$

$$|\psi_1\rangle = g_1 |\psi_0\rangle$$

$$|\psi_2\rangle = g_2 g_1 |\psi_0\rangle = g_2 |\psi_1\rangle$$

$$\vdots$$

$$|\psi_T\rangle = C|\psi_0\rangle .$$

Why does this not work? Local checks cannot verify the evolutions.

<u>Ex</u>. $|\psi_t\rangle = \dfrac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$ and $g_{t+1} = Z_1$.

Then $|\psi_{t+1}\rangle = \dfrac{|0^n\rangle - |1^n\rangle}{\sqrt{2}}$.

Whereas if $g_{t+1} = \mathbb{1}$, then $|\psi_{t+1}\rangle = \dfrac{|0^n\rangle + |1^n\rangle}{\sqrt{2}}$.

<u>Claim</u> Any $k \leq (n-1)$ reduced density matrix of $\dfrac{|0^n\rangle \pm |1^n\rangle}{\sqrt{2}}$ is

$$\frac{1}{2}\left(|0^k\rangle\langle 0^k| + |1^k\rangle\langle 1^k|\right).$$

So a check differentiating if $g_{t+1} = Z_2$ vs. $\mathbb{1}$ must be non-local if it can distinguish

$$|\psi_t\rangle \otimes |\psi_{t+1}\rangle \text{ from } |\psi_t\rangle \otimes |\psi_t\rangle$$

$$g_t = Z_1 . \qquad\qquad g_t = \mathbb{1}$$

We need a better solution that can detect global changes that occur from local gates.

Let's create a $O(\log n)$-local Hamiltonian whose ground states are of the form $\frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes |\psi_t\rangle$ ← state register

time register

t expressed in $\lceil \log(T+1) \rceil$ bits

and $|\psi_t\rangle = g_t \cdots g_1 |\psi_0\rangle$ (all related).

In order to write out the Ham. let's first understand

$$h = \frac{|1\rangle\langle 1| \otimes \mathbb{1} - |1\rangle\langle 0| \otimes U - |0\rangle\langle 1| \otimes U^\dagger + |0\rangle\langle 0| \otimes \mathbb{1}}{2}$$

$$h = \frac{1}{2}\begin{pmatrix} \mathbb{1} & -\mathcal{U}^\dagger \\ -\mathcal{U} & \mathbb{1} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} -\mathcal{U}^\dagger \\ \mathbb{1} \end{pmatrix}\begin{pmatrix} -\mathcal{U} & \mathbb{1} \end{pmatrix}$$

Then $\langle\psi|h|\psi\rangle$ for $h = |0\rangle|\psi_0\rangle + |1\rangle|\psi_1\rangle$ $\leftarrow$ unnormalized eqns.

$$\frac{1}{2}\begin{pmatrix} \langle\psi_0| & \langle\psi_1| \end{pmatrix}\begin{pmatrix} \mathbb{1} & -\mathcal{U}^\dagger \\ -\mathcal{U} & \mathbb{1} \end{pmatrix}\begin{pmatrix} |\psi_0\rangle \\ |\psi_1\rangle \end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix} \langle\psi_0| & \langle\psi_1| \end{pmatrix}\begin{pmatrix} |\psi_0\rangle - \mathcal{U}^\dagger|\psi_1\rangle \\ -\mathcal{U}|\psi_0\rangle + |\psi_1\rangle \end{pmatrix}$$

$$= \frac{1}{2}\left(\langle\psi_0|\psi_0\rangle - \langle\psi_0|\mathcal{U}^\dagger|\psi_1\rangle - \langle\psi_1|\mathcal{U}^\dagger|\psi_0\rangle + \langle\psi_1|\psi_1\rangle\right)$$

$$= \frac{1}{2}\left\| |\psi_1\rangle - \mathcal{U}|\psi_0\rangle \right\|^2 .$$

h measures distance from states of the form

$$\frac{1}{\sqrt{2}}|0\rangle|\psi_0\rangle + \frac{1}{\sqrt{2}}|1\rangle\mathcal{U}|\psi_0\rangle.$$

where $|\psi_0\rangle$ is of norm 1.

Alternate proof of fact:

Let $V = |1\rangle\langle 1| \otimes U + |0\rangle\langle 0| \otimes \mathbb{1}$

$V^\dagger = |1\rangle\langle 1| \otimes U^\dagger + |0\rangle\langle 0| \otimes \mathbb{1}$

$$V^\dagger h V = \frac{|1\rangle\langle 1| \otimes \mathbb{1} - |1\rangle\langle 0| \otimes \mathbb{1} - |0\rangle\langle 1| \otimes \mathbb{1} + |0\rangle\langle 0| \otimes \mathbb{1}}{2}$$

$$= |-\rangle\langle -| \otimes \mathbb{1}.$$

So groundstates of $V^\dagger h V$ are states of the form

$|+\rangle \otimes |\psi_0\rangle$.

and $V^\dagger h V$ is a projector. So groundstates of h

are states of the form $V|+\rangle \otimes |\psi_0\rangle$

$$= \frac{1}{\sqrt{2}}\left(|0\rangle|\psi_0\rangle + |1\rangle U|\psi_0\rangle\right).$$

Apply this intuition to general Hamiltonian circuit

$$h_t = \frac{1}{2}\left(|t\rangle\langle t| \otimes \mathbb{1} - |t\rangle\langle t-1| \otimes g_t - |t-1\rangle\langle t| \otimes g_t^\dagger + |t-1\rangle\langle t-1| \otimes \mathbb{1}\right)$$

Each term h_t acts on time register + 2 extra qubits def. by g_t.

Same calculation will tell us that for $|\psi\rangle = \sum_t |t\rangle|\psi_t\rangle$

that

$$\langle\psi|h_t|\psi\rangle = \left\| \, |\psi_t\rangle - g_t|\psi_{t-1}\rangle \, \right\|^2 .$$

But how do all the pieces act together? Analyze a rotation.

$$V = \sum_{t=0}^{T} |t\rangle\langle t| \otimes g_t \cdots g_1$$

$$V^\dagger = \sum_{t=0}^{T} |t\rangle\langle t| \otimes g_1^\dagger \cdots g_t^\dagger .$$

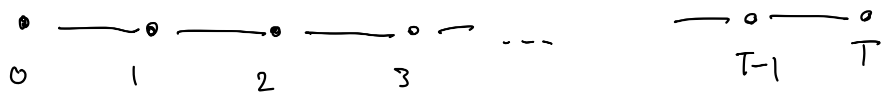
$$V^\dagger h_t V = \frac{1}{2}\Big(|t\rangle\langle t| \otimes \mathbb{1} - |t-1\rangle\langle t| \otimes \mathbb{1} - |t\rangle\langle t-1| \otimes \mathbb{1} + |t-1\rangle\langle t-1| \otimes \mathbb{1} \Big)$$

$$= \frac{1}{\sqrt{2}}\big(|t\rangle - |t-1\rangle\big)\frac{1}{\sqrt{2}}\big(\langle t| - \langle t-1|\big) \otimes \mathbb{1} .$$

So, $V^\dagger\left(\sum_{t=1}^{T} h_t\right)V =$

$$\frac{1}{2}\begin{pmatrix} 1 & -1 & & & \\ -1 & 2 & -1 & & \\ & \ddots & \ddots & \ddots & \\ & & -1 & 2 & -1 \\ & & & -1 & 1 \end{pmatrix} \otimes \mathbb{1} .$$

This is a special matrix. It is the Laplacian of a line graph and also a circulant matrix. (also tri-diagonal)



$\lambda_0 = 0$, eigenvector $|\Psi_0\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes |\psi_0\rangle$ ← for any $|\psi_0\rangle$

$\lambda_1 \geq \frac{c}{T^2}$ ← exercise / intuition from graph mixing time.

So, removing rotation by V:

$$H_{prop} = \sum_{t=0}^{T} h_t$$ is a Hamiltonian with

ground-energy $= 0$, groundstates of the form $\underbrace{\frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes g_t \cdots g_1 |\psi_0\rangle}_{\text{known as a history state}}$

for any state $|\psi_0\rangle$

highly degenerate groundspace.

and first non-zero energy of $\geq c/T^2$.

Therefore, $H_{prop} \geq \frac{c}{T^2}(\mathbb{1} - \Pi_{prop})$

projector onto span of history states

Next: Adding checks for ancilla and output and computing overall eigenvalues to make sure cheating provers are detected.

History states just check evolution of the computation

To check output of computation, we want a term that checks that when the time register is set to T, the first qubit is in the $|1\rangle$ state.

$$H_{out} = |T\rangle\langle T|_{time} \otimes |0\rangle\langle 0|_1$$

Penalizes being time T and first qubit = 0.

To check input, we need to make sure that all the ancilla registers of the computation were set to $|0\rangle$.

$$H_{in} = \sum_{j=1}^{m} |0\rangle\langle 0|_{time} \otimes |1\rangle\langle 1|_{ancilla(j)}$$

$H_{out} + H_{in}$ is a commuting Hamiltonian meaning every pair of local terms commute.

Each local term is a projector. So $H_{out} + H_{in}$ has an integer spectrum.

$$H_{out} + H_{in} \geq \left(\mathbb{1} - \Pi_{inout}\right)$$

projector onto passing all in & out checks.

<u>Claim</u> $H = H_{prop} + H_{out} + H_{in}$ suffices as a Ham.

Intuition: Let $|\psi\rangle = \sum_{t=0}^{T} |t\rangle|\varphi_t\rangle$ ← unnormalized.

so $\| |\psi\rangle \| = 1 \Rightarrow \sum_{t=0}^{T} \| |\varphi_t\rangle \|^2$

h_t gives energy $\quad \| |\varphi_t\rangle - g_t |\varphi_{t-1}\rangle \|^2$

H_{in} gives energy $\quad \sum_{j=1}^{m} \| \langle 1|_{ancilla(j)} |\varphi_0\rangle \|^2$

H_{out} gives energy $\quad \| \langle 0|_1 |\varphi_T\rangle \|^2$

Recall $$V = \sum_{t=0}^{T} |t\rangle\langle t| \otimes g_t \cdots g_1 .$$

Let $$|\mu\rangle = V^\dagger |\psi\rangle = \sum_t |t\rangle |\mu_t\rangle$$

where $|\mu_t\rangle = g_1^\dagger \cdots g_t^\dagger |\psi_t\rangle$.

Then

h_t gives energy $$\| |\mu_t\rangle - |\mu_{t-1}\rangle \|^2$$

H_{in} gives energy $$\sum_{j=1}^{m} \| \langle 1|_{ancilla(j)} |\mu_0\rangle \|^2$$

H_{out} gives energy $$\| \langle 0|_1 C |\mu_T\rangle \|^2$$

If satisfiable then $\exists$ good choice $|\mu\rangle$ for all $|\mu_0\rangle \dots |\mu_t\rangle$.

When unsatisfiable, in order for H_{in} and H_{out}

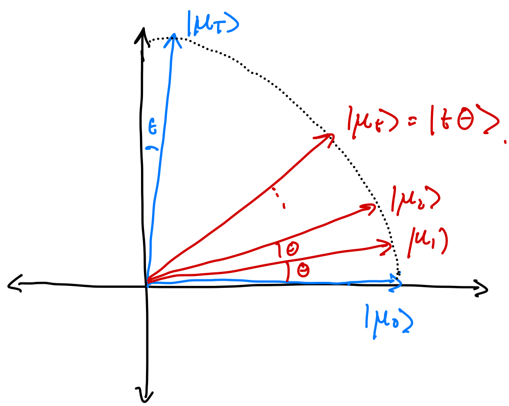
energy to be small ... $|\mu_0\rangle$ and $|\mu_T\rangle$ are orthogonal.

For intuition only: The following is not the lowest energy state.

Cartoon: $|\mu_0\rangle = |0\rangle$ and $|\mu_1\rangle \approx |1\rangle$ in some 2D space

(can be formal due to Jordan's lemma)

Then ideal $|\mu_t\rangle$ would be $|t\theta\rangle$ for $\theta = \frac{\pi}{2T}$ to minimize H_{prop} energy.



Then $\langle\psi|H|\psi\rangle$

$$= \langle\mu|V^\dagger H V|\mu\rangle$$

$$\leq \langle\mu|V^\dagger h_t V|\mu\rangle$$

$$= T \cdot \sin^2\theta$$

$$= O\left(\frac{1}{T}\right).$$

We will prove a lower bound of $\Omega\left(\frac{1}{T^3}\right)$ in the next class.

Pf. Consider a (yes) instance of QCIRCUIT SAT.

i.e. $\exists\ |\psi\rangle$ s.t. $C(|\psi\rangle)$ accepts w pr $\geq 1-\epsilon$.

Then let $|\Psi\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes g_t \cdots g_1 |\psi, 0^m\rangle$

the History state of $|\psi\rangle$. By construction,

$\langle\Psi| H_{prop} |\Psi\rangle = 0$

$\langle\Psi| H_{in} |\Psi\rangle = 0$ $\qquad \Rightarrow \qquad \langle\Psi|H|\Psi\rangle \leq \epsilon$.

$\langle\Psi| H_{out} |\Psi\rangle \leq \epsilon$

What about a (no) instance of QCircuit SAT?

Recall the max success prob. of a QCircuit SAT instance was $\cos^2\Theta$ where Θ was the angle between $\mathbb{1}_{2^n} \otimes |0\rangle\langle 0|^m$ and $C^\dagger (|1\rangle\langle 1| \otimes \mathbb{1}_{2^{n+m-1}}) C$ projectors.

If max success prob is small ($\leq \epsilon$) then Θ is large (near $\frac{\pi}{2}$).

as $\cos^2\Theta = \epsilon$.

We want to show that $\lambda_{min}(H)$ is not super small.

Since $H_{prop} \geq \frac{c}{T^2}\left(\mathbb{1} - \Pi_{prop}\right)$

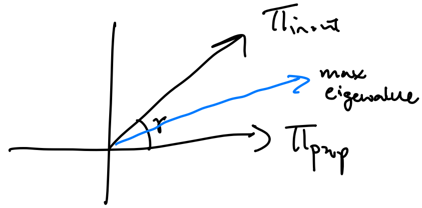
it suffices to show lower bound on:

$$\lambda_{min}\left(\frac{c}{T^2}\left(\mathbb{1}-\Pi_{prop}\right) + \left(\mathbb{1}-\Pi_{inout}\right)\right)$$

$$\gtrsim \frac{c}{T^2}\,\lambda_{min}\left(\left(\mathbb{1}-\Pi_{prop}\right)+\left(\mathbb{1}-\Pi_{inout}\right)\right)$$

$$\gtrsim \frac{c}{T^2}\left(2 - \lambda_{max}\left(\Pi_{prop}+\Pi_{inout}\right)\right)$$

$$= \frac{c}{T^2}\left(2 - 2\cos^2\frac{\gamma}{2}\right) = \frac{2c}{T^2}\sin^2\frac{\gamma}{2}.$$



where γ = angle between Π_{prop} and Π_{inout}

To do this, let's bring back

$$V = \sum_{t=0}^{\tau} |t\rangle\langle t| \otimes g_t \cdots g_1.$$

We know that

$$V^\dagger \Pi_{prop} V = \text{projector onto states} \left\{ |h_\psi\rangle := \frac{1}{\sqrt{T+1}} \sum_{t=0}^{\tau} |t\rangle \otimes |\psi\rangle \right\}$$

$$V^\dagger \Pi_{in+out} V = \left(|T\rangle\langle T| \otimes C^\dagger (|1\rangle\langle 1|_1 \otimes \mathbb{1}) C \right) \cdot$$

$$\left(|0\rangle\langle 0| \otimes \mathbb{1}_{2^m} \otimes |0^m\rangle\langle 0^m| \right)$$

terms commute.

$$\gamma = \text{angle}\left(\Pi_{prop}, \Pi_{in+out}\right) = \text{angle}\left(V^\dagger \Pi_{prop} V, V^\dagger \Pi_{in+out} V\right)$$

To calculate angle between spaces:

$$\cos^2 \gamma = \max_{|\psi\rangle} \langle h_\psi | \Pi_{in+out} | h_\psi \rangle$$

$$= \max_{|\psi\rangle} \frac{1}{T+1} \sum_{t=0}^{1} \langle t | \langle \psi | \Pi_{in+out} | t \rangle | \psi \rangle$$

$$= \max_{|\psi\rangle} \frac{T-1}{T+1} + \frac{1}{T+1} \left(\langle \psi | C^\dagger (|1\rangle\langle 1| \otimes \mathbb{1}) C | \psi \rangle + \langle \psi | \mathbb{1}_{2^m} \otimes |0^m\rangle\langle 0^m| \, |\psi\rangle \right)$$

$$= \frac{T-1}{T+1} + \frac{1}{T+1} 2 \cos^2 \frac{\theta}{2}$$

as optimal $|\psi\rangle$ is midway between projectors $C^\dagger(|1\rangle\langle 1|_1 \otimes \mathbb{1})C$

and $\mathbb{1}_{2^m} \otimes |0^m\rangle\langle 0^m|$ which are θ apart.

Recall $\sqrt{\epsilon} = \cos\theta = 2\cos^2\frac{\theta}{2} - 1 \Rightarrow$

$\Rightarrow 2\cos^2\frac{\theta}{2} = 1-\sqrt{\epsilon} \Rightarrow$

$$\cos^2\gamma = \frac{T-1}{T+1} + \frac{1}{T+1}\left(1+\sqrt{\epsilon}\right) = 1 - \frac{(1-\sqrt{\epsilon})}{T+1}.$$

$$\sin^2\frac{\gamma}{2} = \frac{1-\cos^2\gamma}{2} = \frac{1-\sqrt{\epsilon}}{2(T+1)}.$$

Therefore, $\lambda_{min}(H) \geq \frac{2c}{T^2}\left(\frac{1-\sqrt{\epsilon}}{T+1}\right) = \Omega\left(\frac{1}{T^3}\right)$

for small ϵ.

So if yes instance, $\lambda_{min}(H) \leq \epsilon$

if no instance, $\lambda_{min}(H) \gtrsim \frac{1}{T^3}$.

To complete pf of QMA-hardness, first use amplification to convert any QCIRCUITSAT problem to $(1-\epsilon, \epsilon)$ amplification for $\epsilon < \frac{1}{T^3}$. Then apply the circuit-to-Hamiltonian construction.

A more sophisticated analysis proves that no instances map to $\Omega\left(\frac{1}{T^2}\right)$.

Note that we only proved QMA-hardness for $O(\log T) = O(\log n)$ local Hamiltonians. Your homework includes a transform to 5-local Hamiltonians.

This will yield a Hamiltonian acting on $T+n+m$ qubits.

Also, we only proved it was QMA-hard to estimate $\lambda_{min}(H)$ to $\frac{1}{T^3} \sim \frac{1}{N^3}$ where N is the number of qubits in the Ham.

It may be easier to get a coarser approximation