LECTURE 17 (March 20th)

TODAY Local Hamiltonian Problem (part 2)
QMA(2)

RECAP

• k-local Hamiltonian Problem

Input ① m positive-semidefinite operators $H_1, \ldots, H_m$ acting on $k = O(1)$ out of n qubits and $0 \preceq H_i \preceq \mathbb{I}$ and $m = \text{poly}(n)$

② Parameters $a, b \in \mathbb{R}$ satisfying $b - a \geq \frac{1}{\text{poly}(n)}$

Decision Problem: Determine if $\lambda_{min}(H) \leq a$ OR $\lambda_{min}(H) \geq b$
(accept) (reject)

$\boxed{\text{Lemma}}$ k-LH $\in$ QMA for any $b - a \geq 1/\text{poly}(n)$

$\boxed{\text{Lemma}}$ k-Local Hamiltonian is QMA-hard for $k \geq 5$.

Together these imply that k-Local Hamiltonian is QMA-complete for $b - a \geq \frac{1}{\text{poly}(n)}$

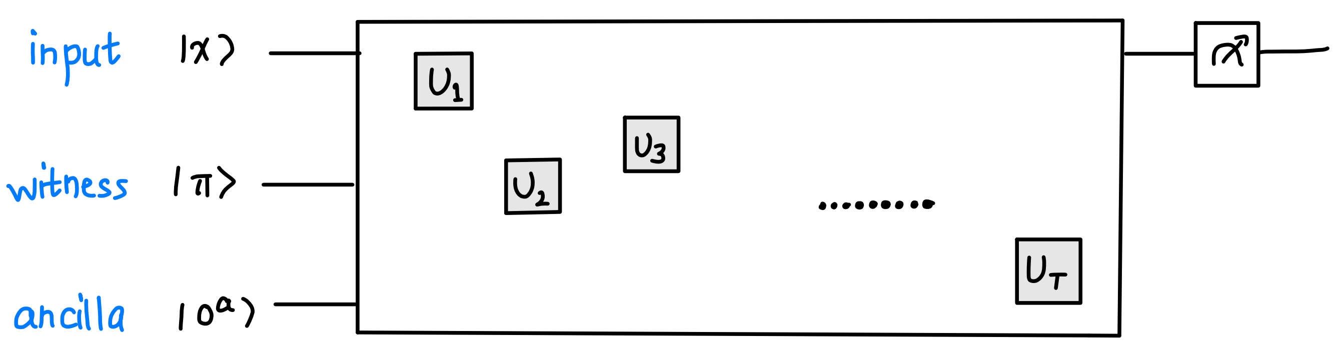
RECAP of QMA hardness proof

We will give an efficient procedure that takes an instance x of L and produces a local Hamiltonian instance such that

if $x \in L \Rightarrow \lambda_{min} \leq a$ for some $b - a = \frac{1}{\text{poly}(n)}$
if $x \notin L \Rightarrow \lambda_{min} \geq b$

We will do this by encoding each step of the verifier as a Hamiltonian term

Let the verifier V be given by



We will construct a $O(\log T)$ local Hamiltonian H whose ground states are the history states

$$|\Omega\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes |\Omega_t\rangle$$

where

$$|\Omega_t\rangle = U_t U_{t-1} \cdots\cdots U_1 (|x\rangle |\pi^*\rangle |0^a\rangle)$$

Our Hamiltonian will have local terms that enforces that the ground states correspond to the snapshots :

Start Initial snapshot $|\Omega_0\rangle = |x\rangle \otimes |\pi\rangle \otimes |0^a\rangle$ for some $|\pi\rangle$

$$H_i^{(x)} = |0\rangle\langle 0|_{\underset{\uparrow \text{clock}}{c}} \otimes |\bar{x}_i\rangle\langle\bar{x}_i|_{\underbrace{X,i}_{i^{th} \text{ qubit of } X}} \quad \text{for } i = 1, \ldots n$$

$$H_i^{(A)} = |0\rangle\langle 0|_c \otimes |1\rangle\langle 1|_{\underbrace{A,i}_{i^{th} \text{ qubit of Ancilla } A}}$$

End Measuring the first qubit of the final snapshot $|\Omega_T\rangle$ outputs 1 w.h.p.

$$H_{END} = |T\rangle\langle T|_c \otimes |0\rangle\langle 0|_{output}$$

Evolution Each consecutive snapshot satisfies

$$|\Omega_t\rangle = U_t |\Omega_{t-1}\rangle$$

The Evolution checks are more interesting

$$H^{(t\to t+1)} = \frac{1}{2}\Big(|t\rangle\langle t|_c \otimes \mathbb{I} + |t+1\rangle\langle t+1|_c \otimes \mathbb{I} - |t+1\rangle\langle t|_c \otimes U_{t+1} - |t\rangle\langle t+1| \otimes U_{t+1}^{+} \Big)$$

To make sense of these checks, let us restrict our attention to two adjacent time steps say t and $t+1$ and let $U_{t+1} = \mathbb{I}$

In this case

$$H^{(t\to t+1)} = \frac{1}{2}\Big(|t\rangle\langle t|_c \otimes \mathbb{I} + |t+1\rangle\langle t+1|_c \otimes \mathbb{I} - |t+1\rangle\langle t|_c \otimes \mathbb{I} - |t\rangle\langle t+1| \otimes \mathbb{I} \Big)$$

$$= \begin{array}{c} \\ t \\ t+1 \\ \\ \end{array} \begin{array}{c} \begin{array}{cc} t & t+1 \end{array} \\ \left[\begin{array}{cc} & \\ 1/2 & -1/2 \\ -1/2 & 1/2 \\ & \end{array}\right] \end{array} \otimes \mathbb{I}$$

$$= \left(\frac{|t\rangle - |t+1\rangle}{\sqrt{2}}\right)\left(\frac{\langle t| - \langle t+1|}{\sqrt{2}}\right) \otimes \mathbb{I}$$

If the execution was correct, we expect the history state projected to the subspace where clock register is either t or $t+1$ to be

$$\frac{1}{\sqrt{2}}|t\rangle|\Omega_t\rangle + \frac{1}{\sqrt{2}}|t+1\rangle|\Omega_t\rangle$$

$$= \frac{1}{\sqrt{2}}(|t\rangle + |t+1\rangle) \otimes |\Omega_t\rangle$$

Since we want to penalize the states that are far from the above, we can choose a term

$$\tilde{H}_{toy} = \mathbb{I} \otimes \left(\frac{|t\rangle - |t+1\rangle}{\sqrt{2}}\right)\left(\frac{\langle t| - \langle t+1|}{\sqrt{2}}\right)$$

This adds a maximal penalty to any state $\frac{|t\rangle - |t+1\rangle}{\sqrt{2}} \otimes |\Omega_t\rangle$

Note that the term $\tilde{H}_{toy}$ is exactly $H^{t\to t+1}$ when $U_{t+1} = \mathbb{I}$

The general case penalize states that are far from valid history states

You can check that

$$H^{t\to t+1} = \begin{array}{c} \\ t \\ t+1 \\ \\ \end{array} \begin{array}{c} \begin{array}{cc} t & t+1 \end{array} \\ \left[\begin{array}{cc} & \\ \frac{1}{2}\mathbb{I} & -\frac{1}{2}U_{t+1}^{\dagger} \\ -\frac{1}{2}U_{t+1} & \frac{1}{2}\mathbb{I} \\ & \end{array}\right] \end{array} = \left[\begin{array}{cc} \mathbb{I} & \\ & U_{t+1} \end{array}\right] \begin{array}{c} t \\ t+1 \end{array} \underbrace{\begin{array}{c} \begin{array}{cc} t & t+1 \end{array} \\ \left[\begin{array}{cc} \frac{1}{2}\mathbb{I} & -\frac{1}{2}\mathbb{I} \\ -\frac{1}{2}\mathbb{I} & \frac{1}{2}\mathbb{I} \end{array}\right] \end{array}}_{\text{Zeros everywhere except } t \,\&\, (t+1)\text{ st block}} \left[\begin{array}{cc} \mathbb{I} & \\ & U_{t+1}^{\dagger} \end{array}\right]$$

which is just a change of basis

Final Hamiltonian is

$$H = \sum_{i=1}^{n} H_i^{(x)} + \sum_{j=1}^{\#\text{ancillas}} H_j^{(A)} + \sum_{t=0}^{T-1} H^{(t \to t+1)} + H_{END}$$

This is called the Feynman-Kitaev construction

<u>Locality</u> $O(\log T)$ since each term acts on clock register which is $O(\log T)$ qubits and $O(1)$ other qubits

Note that the Hamiltonian terms update clock register between two adjacent times but due to carry over the Hamiltonian may need to act on $\log T$ qubits

E.g. $|0111111\rangle_c \longrightarrow |10000000\rangle_c$ needs to act on all qubits

The locality can be improved to 5 by encoding the clock in unary

$$\underset{\substack{\uparrow \\ t^{th}\text{ position}}}{0 \cdots\cdots 1 \cdots\cdots 0} = \text{clock is } t$$

Then, updating from $t \to t+1$, only corresponds to updating 3 qubits

One also needs to act some extra checks on the clock to make sure it is in unary

Analysis of the Construction

<u>Accept case</u> $(x \in L)$ Let's verify that ground energy is $\leq 2^{-n}$ in this case

Since $x \in L$, $\exists$ proof $|\pi\rangle$ s.t. V accepts w.p. $\geq 1 - 2^{-\text{poly}(n)}$

Consider the history state $|\Omega\rangle$ for V on input $|x\rangle \otimes |\pi\rangle \otimes |0^a\rangle$
Its energy is

$$\langle \Omega | H | \Omega \rangle = \sum_{i=1}^{n} \langle \Omega | H_i^{(x)} | \Omega \rangle + \sum_j \langle \Omega | H_j^{(A)} | \Omega \rangle + \sum_{t=0}^{T-1} \langle \Omega | H^{(t \to t+1)} | \Omega \rangle + \langle \Omega | H_{END} | \Omega \rangle$$

It suffices to show that the sum of all these terms is $\lesssim 2^{-n}$

Let's compute the terms. First recall that $|\Omega\rangle = \frac{1}{\sqrt{T+1}} \sum_{s=0}^{T} |s\rangle \otimes |\Omega_s\rangle$

$\boxed{1}$ $H^{(x)}$ terms

Recall that $H_i^{X} = |0\rangle\langle 0|_c \otimes |\bar{x}_i\rangle\langle \bar{x}_i|_{X,i}$

so, $\langle\Omega| H_i^{(x)} |\Omega\rangle = \frac{1}{T+1} \langle\Omega_0| \, |\bar{x}_i\rangle\langle\bar{x}_i|_{X,i} \, |\Omega_0\rangle$

since only the snapshot at time 0 matters

At time 0, the snapshot is

$$|\Omega_0\rangle = |x\rangle_X \otimes |\pi\rangle_P \otimes |0^a\rangle_A$$

So, $\langle\Omega_0| |\bar{x}_i\rangle\langle\bar{x}_i|_{X,i} |\Omega_0\rangle = 0$ since the i^{th} qubit of X in $|\Omega_0\rangle$ is in state $|x_i\rangle$

$\boxed{2}$ $H^{(A)}$ terms

Similar calculations show its zero

$\boxed{3}$ $H^{(t\to t+1)}$ terms

Fix a time t.

$$\langle\Omega| H^{(t\to t+1)} |\Omega\rangle = \frac{1}{T+1} \sum_{r,s} \langle r| \otimes \langle\Omega_r| \underbrace{\left(H^{t\to t+1} \right)}_{} |s\rangle \otimes |\Omega_s\rangle$$

$$= \frac{1}{2}|t\rangle\langle t|_c \otimes I + \frac{1}{2}|t+1\rangle\langle t+1|_c \otimes I$$
$$- \frac{1}{2}|t+1\rangle\langle t|_c \otimes U_{t+1} - \frac{1}{2}|t\rangle\langle t+1| \otimes U_{t+1}^{\dagger}$$

$$= \frac{1}{2(T+1)} \cdot \left(\begin{array}{ll} \sum_{r,s} \langle r|t\rangle\langle t|s\rangle \langle\Omega_r|\Omega_s\rangle & \to \text{first} \\ + \sum_{r,s} \langle r|t+1\rangle\langle t+1|s\rangle\langle\Omega_r|\Omega_s\rangle & \to \text{second} \\ - \sum_{r,s} \langle r|t+1\rangle\langle t|s\rangle\langle\Omega_r|U_{t+1}|\Omega_s\rangle & \to \text{third} \\ - \sum_{r,s} \langle r|t\rangle\langle t+1|s\rangle\langle\Omega_r|U_{t+1}^{\dagger}|\Omega_s\rangle & \to \text{fourth} \end{array} \right)$$

First term $= \langle\Omega_t|\Omega_t\rangle = 1$ and same for second term

Third term $= -\langle\Omega_{t+1}|U_{t+1}|\Omega_t\rangle = -1$ and same for fourth term

Overall contribution $= 0$

$\boxed{4}$ <u>H_{END} term</u> $\langle \Omega | H_{END} | \Omega \rangle = \frac{1}{T+1} \langle \Omega_T | |0\rangle\langle 0|_{out} | \Omega_T \rangle$

since only the final snapshot matters

Note that $\langle \Omega_T | |0\rangle\langle 0|_{out} | \Omega_T \rangle$ is exactly the probability that the verifier outputs 0 on input $|x\rangle \otimes |\pi\rangle \otimes |0^a\rangle$

This is at most $2^{-poly(n)}$ since Verifier errs with small probability and $x \in L$

Total energy $\langle \Omega | H | \Omega \rangle \leq 2^{-poly(n)}$

<u>Reject Case</u>
($x \notin L$)

This case is more complicated to analyze

We want to show that the energy of every state with respect to H is at least $\frac{c}{T^3}$ for some constant c

↳ This is much bigger than $2^{-poly(n)}$ since $T = poly(n)$

To gain some intuition, let us compute the energy of some history state where the proof $|\pi\rangle$ is some arbitrary proof chosen by the verifier

The calculations we did before show that the energy only comes from the last term H_{END} and equals

$$\frac{1}{T+1} \mathbb{P}[\text{ Verifier outputs 0 on } |x\rangle \otimes |\pi\rangle \otimes |0^a\rangle]$$

Since $x \notin L$, the probability is $\geq 1 - 2^{-poly(n)}$

Thus, the energy of any history state is $\Omega\left(\frac{1}{T}\right)$.

Of course, we need to show that the energy of any state (not just history states) is large

We won't cover it here but you will work through some of the steps in the exercises and you can take a look at Kitaev's paper

Thus, we have shown how instances of a QMA-problem can be converted to 5 local Hamiltonian with $b = \Omega(T^{-3})$ and $a = \exp(-n)$ where $T = poly(n)$ is the running time of the QMA verifier

To summarize

- We looked at the complexity class QMA which captures the power of poly(input-size) quantum proofs
  We also saw that $QMA_{log} = BQP$
- Error probabilities can be reduced in QMA even with a single copy of the proof
- k-Local Hamiltonian is QMA-complete with promise gap $1/poly(n)$

Beyond QMA
- Allow more (unentangled) provers → QMA(2)
- Allow interaction (and more possibly entangled) provers → MIP^* etc.
- Probabilistically Checkable Proofs → Quantum PCPs

We won't cover interactive proofs in this course

All of these have a close relation with complexity of entanglement

QMA(2)

$L \in QMA(2)$ if $\exists$ verifier s.t.

- if $x \in L \Rightarrow \exists$ a proof $|\pi\rangle \otimes |\psi\rangle$ s.t. Verifier accepts $x, |\pi\rangle \otimes |\psi\rangle$ with prob. $\geq 2/3$
- if $x \notin L \Rightarrow \forall$ proofs $|\pi\rangle \otimes |\psi\rangle$, Verifier accepts $x, |\pi\rangle \otimes |\psi\rangle$ with prob. $\leq 1/3$

Note that there are two unentangled proofs here. We don't care what the verifier does when the proofs are entangled

If we allow entangled proofs, this is same as QMA

It is easy to see that $QMA \subseteq QMA(2)$ [Why?]

One might be tempted to think that $QMA(2) \subseteq QMA$ since given a proof Arthur can verify if proof is of the form $|\pi\rangle \otimes |\psi\rangle$ and reject if not
This would imply that $QMA(2) = QMA$

Alas, Arthur can't determine if the state is a tensor product given a single (or even polynomially many) copies of the state

In its most naive formulation : there is no measurement M that accepts only unentangled states [Why ?]

In fact, unentangled states is a powerful resource and they can be used to do something that is likely not possible without.

Short Quantum Proofs for NP

Recall that $QMA_{\log} = BQP$

What about $QMA_{\sqrt{\text{input-size}}}$? Can we verify any NP-problem with a short quantum proof ?

E.g. 3-SAT $(x_1 \vee x_2 \vee \bar{x}_3) \wedge (\bar{x}_2 \vee x_4 \vee x_5) \wedge \ldots\ldots$

Is there a short quantum proof that formula is satisfiable or not?

3-COLOR Given a graph, can its vertices be colored with 3-colors so that end points of all edges have different colors?

Is there a quantum proof with $\sqrt{n}$ or $n^{0.99}$ qubits ?

We believe this is unlikely : the proof that $QMA \subseteq EXP$ would imply that if such a short quantum proof exists, then there is a $2^{\sqrt{n}}$ or $2^{cn^{0.99}}$ time classical algorithm for 3-SAT or 3-COLOR

The Exponential Time Hypothesis says that this is impossible

Exponential Time Hypothesis (Conjecture) Any deterministic algorithm for 3-SAT or 3-COLOR must take $2^{\Omega(n)}$ time

This is a strengthening of $P \neq NP$ conjecture

Despite more than 50 years of efforts, the best algorithm for 3-SAT or 3-COLOR runs in time 2^{cn} for some $c<1$.

On the other hand, a surprising result of Blier & Tapp that we will cover shows that

$\boxed{\text{NEXT TIME}}$ 3-COLOR has a QMA(2)-proof with only $O(\log n)$-qubits

Caveat: Gap between success probability is $1/\text{poly}(n)$