LECTURE 16 (March 18^{th})

TODAY Local Hamiltonian Problem

Recall the complexity class QMA : Language $L \in QMA$ if $\exists$ an efficient quantum verifier V

$x \in L \Rightarrow \exists$ quantum proof $|\pi\rangle$ s.t. $\mathbb{P}[V(x, |\pi\rangle) \text{ accepts}] \geq 2/3$

$x \notin L \Rightarrow \forall$ proofs $|\pi\rangle$ s.t. $\mathbb{P}[V(x, |\pi\rangle) \text{ accepts}] \leq 1/3$

What interesting problems are in QMA? What's a complete problem for QMA?

- Of course, $NP \subseteq QMA$. What about problems beyond NP?
- Group non-membership : Given elements $h, g_1, \dots, g_k$ of a finite but exponentially-sized group G determine if h is not in the subgroup generated by $g_1, \dots, g_k$

  Note that the complement problem is in NP

  It turns out that this problem is in QMA (shown by Watrous)
  We will not cover this here

• k-local Hamiltonian Problem

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

Note that we write $A \preceq B$ to mean that $B - A$ is positive semidefinite which also implies that the i^{th} eigenvalue of $B \geq$ i^{th} eigenvalue of A

Thus, $0 \preceq H_i \preceq \mathbb{I} \Rightarrow$ all eigenvalues of H_i are in $[0,1]$

Example $H_i = O \otimes \mathbb{I}$ where O acts on qubits 1 & 2 and $\mathbb{I}$ acts on other $n-2$ qubits

The Hamiltonian H is defined to be the sum $H = \sum_{i=1}^{m} H_i$

Since each H_i can be described by a constant-sized matrix, # bits needed to describe $H = \text{poly}(n)$

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)

The local Hamiltonian problem corresponds to estimating the minimum eigenvalue called the ground energy up to a $\frac{1}{\text{poly}(n)}$ precision

The minimum eigenvector is called the ground state of the Hamiltonian

This captures a lot of problems relevant to quantum physics and chemistry

Each local term H_i can be thought of as a local constraints in terms of an energy penalty
For example,

if $H_1 = \mathbb{I}_2 - |00\rangle\langle 00|$ acting on qubits 1 and 2

then $\langle\psi| H_1 |\psi\rangle = 0$ if $|\psi\rangle = |00\rangle \otimes |\phi\rangle$
$\langle\psi| H_1 |\psi\rangle > 0$ otherwise

To minimize the energy penalty for H_1, $|\psi\rangle$ needs to of the form $|00\rangle \otimes |\phi\rangle$

In-class Exercise Express 3SAT as a Local Hamiltonian problem

This exercise also shows that 3-LH is NP-hard

We will prove the following result

Theorem (Kitaev) 5-Local Hamiltonian is QMA-complete with $b - a = \frac{1}{\text{poly}(n)}$

Remark In fact, 2-Local Hamiltonian is already QMA-complete but we will not prove this here

This can be considered a quantum analog of the Cook-Levin theorem which says that 3-SAT is NP-complete

The proof of the Cook-Levin theorem proceeds by encoding the steps of the NP-verifier as a 3-SAT formula. The proof here will proceed by encoding the steps of the quantum verifier as a local Hamiltonian term

Proof of Membership

Proof Let $H = \sum_{i=1}^{m} H_i$ be the k-local Hamiltonian

In the accept case, $\lambda_{min}(H) \leq a$
In the reject case, $\lambda_{min}(H) \geq b$

Given a witness $|\pi\rangle$, can we efficiently estimate $\langle\pi|H|\pi\rangle$ upto $1/\text{poly}(n)$ precision?

Consider a local term $H_i = h_i \otimes \mathbb{I}$ where h_i is $2^k \times 2^k$ psd matrix

Diagonalizing $h_i = \sum_j \lambda_{ij} P_{ij}$ where P_{ij} is the projector on eigenspace of h_i with eigenvalue λ_{ij}

Note that $\sum_j P_{ij} = I$, so $\{P_{ij}\}_j$ form a projective measurement

Therefore, $$\langle \pi | H_i | \pi \rangle = \sum_j \lambda_{ij} \underbrace{\langle \pi | P_{ij} \otimes \mathbb{I} | \pi \rangle}$$

$:= \mathbf{P}$[obtaining outcome j by measuring $|\pi\rangle$ with POVM $\{P_{ij}\}_j$]

Since $\{P_{ij}\}_j$ only acts on $O(1)$ qubits, this can be efficiently performed on a quantum computer

= Average of λ_{ij}'s under the distribution on outcomes j obtained by measuring $|\pi\rangle$ under POVM $\{P_{ij}\}_j$

This suggests the following quantum verifier that takes in $T = \mathrm{poly}(n)$ copies of $|\pi\rangle$

- Repeat the following T times :

  $\boxed{1}$ Pick a random Hamiltonian term H_i

  $\boxed{2}$ Measure a fresh copy of $|\pi\rangle$ with POVM $\{P_{ij}\}_j$.
  If we obtain outcome j, set $X_t = m\lambda_{ij}$

- If $\frac{1}{T}\sum_{t=1}^{T} X_t \leq a$, output accept o/w reject

ACCEPT CASE ($\lambda_{min}(H) \leq a$)   Witness $= |\psi\rangle^{\otimes T}$ where $|\psi\rangle$ is the ground state of H and $T = \mathrm{poly}(n)$

$$\text{Then, } \mathbb{E}[X_t] = \frac{1}{m}\sum_{i=1}^{m}\sum_j \langle \psi | P_{ij} \otimes \mathbb{I} | \psi \rangle \cdot m\lambda_{ij}$$

$$= \langle \psi | H | \psi \rangle \leq a$$

$\Rightarrow$ Since each X_t is independent and at most 1, concentration bounds imply that the empirical average $\frac{1}{T}\sum_t X_t$ is close to the true value

REJECT case
$(\lambda_{min}(H) \geq b)$

No witness $|\pi\rangle \in (\mathbb{C}^n)^{\otimes T}$ should work

If $|\pi\rangle$ was a tensor product state, X_t's are independent and $\mathbb{E}[X_t] \geq b$ so, concentration bounds still imply that $\frac{1}{T}\sum X_t$ is close

As we have seen before in the context of QMA amplification, entangled proofs $|\pi\rangle$ can only be worse

Proof of Completeness

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

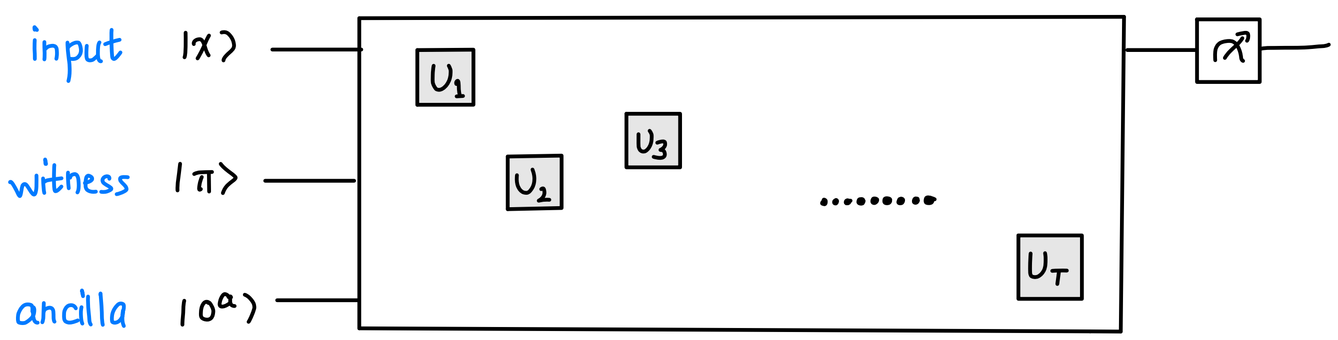
Proof Let $L \in$ QMA and V be the efficient quantum verifier for L

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

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

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

Let the verifier V be given by



where U_i's are single or two-qubit gates, $T = \text{poly}(n)$
and the acceptance probability of verifier is $1 - 2^{-\text{poly}(n)}$
which we can assume by amplification

Let us first construct a k-Local Hamiltonian H
where $k = O(\log T)$ instead of $O(1)$

The ground states of Hamiltonian H are the history states

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

where

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

we will call this snapshot state at time t

with $|\pi^*\rangle$ being a proof that maximizes $\mathbb{P}[\, V|x\rangle|\pi\rangle|0\rangle^a \text{ accepts}]$

$|t\rangle$ is a $(\log T)$ qubit register that stores which snapshot we record

Moreover, If $x \in L \implies \lambda_{min}(H) \le \exp(-n)$
If $x \notin L \implies \lambda_{min}(H) \geq \frac{c}{T^3}$ for some constant c.

Note that we keep the execution history of the verifier as a superposition

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

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

Evolution Each consecutive snapshot satisfies
$$|\Omega_t\rangle = U_t |\Omega_{t-1}\rangle$$

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

If we had a quantum state $|\Omega\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle \otimes |\Omega_t\rangle$

satisfying all of these constraints, then we could conclude that $\exists$ a state $|\pi\rangle$ s.t. if we executed Verifier on $|x\rangle \otimes |\pi\rangle \otimes |0^a\rangle$ it would accept whp, thus certifying that $x \in L$

What do the Hamiltonian terms look like? Let's divide our qubits into different registers

- C = clock register with $O(\log T)$ qubits
- X = initial input register
- P = initial proof register
- A = ancillas

For the start check, we need to ensure that X register of $|\Omega_0\rangle$ is in the $|x\rangle$ state and that A register are $|0^a\rangle$

We can enforce the $|x\rangle$ part by using

$$H_i^{(x)} = |0\rangle\langle 0|_c \otimes |\bar{x}_i\rangle\langle \bar{x}_i|_{X,i} \quad \text{for } i = 1, \dots n$$

where $|0\rangle\langle 0|_c$ is the projector on clock state being $|0\rangle$
and $|\bar{x}_i\rangle\langle \bar{x}_i|_{X_i}$ projector on the i^{th} qubit of X being in $|\bar{x}_i\rangle$ state

What this term says that either the clock register is not $|0\rangle$ in which case we don't care about this term or if the clock register is $|0\rangle$, then to minimize the energy the i^{th} qubit of X_i better be in the state $|x_i\rangle$

Similarly, to enforce the ancillas,

$$H_i^{(A)} = |0\rangle\langle 0|_c \otimes |1\rangle\langle 1|_{A,i}$$

The END check is also simple. Just add the term

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

The evolution checks will ensure that the computation evolves correctly between every time t and $t+1$

We will see them and complete the analysis in the next lecture