Lecture 20

7 APR 2014

Begin by recalling the definition of QMA. Just as the Cook-Levin theorem & the theory of NP-completeness are cornerstones of computational complexity theory, we would like to establish a natural promise problem which is complete for QMA.

Such a problem is called "Local Hamiltonian", which has an appealing physical interpretation.

the problem is: Suppose that we have a "succinct" (p(n) bits) representation of a "large" Hamiltonian H acting on n qubits, what is the smallest eigenvalue of H?

Might think that you could just

diagonalize H, but it is a $2^n \times 2^n$ matrix, whereas the input is specified as poly(n) bits. So this naive approach would require exponential time.

Def'n: Say that H (hermitian operator acting on n qubits) is a k-local Hamiltonian if it can be written as

$$H = \sum_{j=1}^{r} H_j$$

where $\{H_j\}_{j=1}^{r}$ is a collection of local Hamiltonian terms, such that each H_j acts non-trivially on some subset $S_j \subseteq [n]$ of at most k qubits & satisfies $0 \leq H_j \leq$

(Convention is that each H_j acts as identity on all qubits in the set $[n] \setminus S_j$.)

We can now define the k-Local Hamiltonian promise problem:

Input: A k-Local Hamiltonian

1) H acting on n qubits, specified as a collection of local Hamiltonian terms $\{H_j\}_{j=1}^{r}$ (each is a $2^k \times 2^k$ matrix)

2) poly-time computable threshold parameters $a > b \geq 0$ such that $a - b \geq \frac{1}{q}$ where $q \in \text{poly}$

Decide whether

YES: $\lambda_{min}(H) \leq b$

NO: $\lambda_{min}(H) \geq a$

The complexity parameter is $\underset{\substack{\uparrow \\ \text{\# of bits} \\ \text{needed to} \\ \text{specify } H.}}{\langle H \rangle}$

As shown in Hwk. 1, k-LH generalizes MAX-k-CSP
↑
(constraint satisfaction problem)

MAX-k-CSP has as input r Boolean functions $c_i : \{0,1\}^k \to \{0,1\}$ where each c_i acts on k out of n bits. Question is then what is the largest # of clauses c_i that we can satisfy w/ a Boolean assignment to the n bits?

We can easily embed this as an instance of k-LH. For each clause c_i, define a diagonal $2^k \times 2^k$ matrix H_{c_i} such that $H_{c_i}(m,m) = 0$ if binary rep. of m is a satisfying assignment & otherwise let $H_{c_i}(m,m) = 1$. Idea is to give an *energy penalty* for failing assignments.

This construction implies that the optimal value of Max-k-CSP corresponds to the minimum eigenvalue of H.

We would like to show now that k-LH is a QMA-complete quantum constraint satisfaction problem.

The quantum Cook-Levin theorem proved by Kitaev is that k-LH is QMA-complete for $k \geq 5$.

1st part: Let us show that k-LH is in QMA. So the prover should provide a quantum witness state (or "quantum proof") that the verifier can use to decide whether to accept or reject.

Recall that the prover is always trying to make the verifier accept, so the verifier has to employ some procedure to reduce the probability of being fooled.

Let us begin by supposing that we have a YES instance. So in this case, the prover can provide a state of eigenvalue smaller than b. (He can just send the ground state of the Hamiltonian.)

Let $|n\rangle$ denote the ground state & let λ be its eigenvalue, so that $\lambda \leq b$.

Suppose to begin with that each term in the Hamiltonian is a projector, so that $H_j = |\phi_j\rangle\langle\phi_j|$ for some state $|\phi_j\rangle$

then consider that

$$f = \langle x | H | x \rangle = \sum_{j=1}^{r} \langle x | H_j | x \rangle$$

$$= \langle x | \left(\sum_{j=1}^{r} |\phi_j\rangle\langle\phi_j| \right) | x \rangle$$

$$= \sum_{j=1}^{r} |\langle x | \phi_j \rangle|^2$$

$$\Rightarrow \quad \frac{f}{r} = \frac{1}{r} \sum_{j=1}^{r} |\langle x | \phi_j \rangle|^2 \quad (*)$$

Observe that $|\langle x|\phi_j\rangle|^2$ is the probability of getting $|\phi_j\rangle$ when measuring $\{|\phi_j\rangle\langle\phi_j|,$
$I^{\otimes n} - |\phi_j\rangle\langle\phi_j|$

Since $|\phi_j\rangle\langle\phi_j|$ acts on a constant # of qubits, a circuit to implement this measurement takes constant time

Also $(*)$ means that we can interpret $\frac{f}{r}$ as the probability of getting a "0" after picking j unif @ random from $\{1, \ldots, r\}$ + measuring $\{|\phi_j\rangle\langle\phi_j|, I^{\otimes n} - |\phi_j\rangle\langle\phi_j|$

So this gives a simple verification procedure for the verifier:

1) Pick j unif @ random from $\{1, \dots, r\}$

2) measure $|n\rangle$ w/ $\{|\phi_j\rangle\langle\phi_j|, I^{\otimes n} - |\phi_j\rangle\langle\phi_j|\}$

3) reject if outcome is $|\phi_j\rangle\langle\phi_j|$, accept if outcome is $I - |\phi\rangle\langle\phi_j|$

(ideal ground state should be as orthogonal to all $|\phi_j\rangle$ as possible)

probability for accepting is

$$\Pr\{\text{accept}\} = \sum_{j=1}^{r} \Pr\{j\} \Pr\{\text{accept} | j\}$$

$$= \frac{1}{r} \sum_{j=1}^{r} \langle n | \left(I - |\phi_j\rangle\langle\phi_j| \right) |n\rangle$$

$$= 1 - \frac{1}{r} \sum_{j=1}^{r} |\langle n | \phi_j \rangle|^2$$

$$= 1 - \frac{\langle n | H | n \rangle}{r}$$

$$= 1 - \frac{\lambda}{r} \geq 1 - \frac{b}{r}$$

On the other hand, if we have a NO instance, then the acceptance probability of this verification procedure is

$$1 - \frac{1}{r} \langle n | H | n \rangle \qquad (**)$$

but here we have the promise that $\langle n | H | n \rangle \geq a$ so that

$$(**) \leq 1 - \frac{a}{r}$$

So, to summarize, for a YES instance acceptance prob. is $\geq 1 - \frac{b}{r}$ + for a NO instance, it is $\leq 1 - \frac{a}{r}$

the gap between these is

$$1 - \frac{b}{r} - \left(1 - \frac{a}{r}\right) = \frac{a-b}{r} \geq \frac{1}{\text{poly}}$$

So, by QMA error reduction, we can amplify this gap to be arbitrarily large (exp. close to extremes)

Idea for general H_j is a generalization of this construction.

For this case H_j can be written w/ a spectral decomposition of the form

$$H_j = \sum_{i=1}^{\dim(H_j)} w_{i,j} \, |\phi_{i,j}\rangle\langle\phi_{i,j}|$$

We need a trick which allows us to "toss a coin" w/ probability of heads $1 - \langle n|H_i|n\rangle$.

To this end, add a single qubit to the system. We can then apply a unitary transformation

$$U_j |\phi_{ij}\rangle|0\rangle = |\phi_{ij}\rangle\left(\sqrt{w_{ij}}\,|0\rangle + \sqrt{1-w_{ij}}\,|1\rangle\right)$$

(Again, this is a constant sized unitary.)

Can prove that picking j unif@ random from $\{1,\dots,r\}$, applying U_j, & measuring $|1\rangle$ has probability

$$1 - \frac{1}{r}\langle n|H|n\rangle$$

rewrite $|n\rangle$ in the eigenbasis of H_j as

$$|n\rangle = \sum_i \alpha_i |\phi_{ij}\rangle$$

So if we perform U_j on $|n\rangle$ ~~measure~~ the result is

$$U_j|n\rangle|0\rangle = \sum_i \alpha_i U_j |\phi_{ij}\rangle|0\rangle$$

$$= \sum_i \alpha_i |\phi_{ij}\rangle\left(\sqrt{w_{ij}}\,|0\rangle + \sqrt{1-w_{ij}}\,|1\rangle\right)$$

the projection onto $|1\rangle\langle 1|$ is then

$$\sum_i \alpha_i \sqrt{1-w_{ij}}\,|\phi_{ij}\rangle|1\rangle$$

so that the probability of getting one is

$$\sum_{i',i} \alpha_{i'}^{*} \sqrt{1-w_{i'j}}\,\alpha_i \sqrt{1-w_{ij}}\,\langle \phi_{i'j}|\phi_{ij}\rangle$$

$$= \sum_i |\alpha_i|^2 (1-w_{ij}) = 1 - \langle n|H_j|n\rangle$$

Then the procedure gives acceptance prob. $1 - \frac{1}{r}\langle n|H|n\rangle$

Idea to show hardness for QMA:

Recall from the Cook-Levin theorem that we showed a reduction from any decision problem in NP to 3-SAT. 1st step was to show that Circuit-SAT reduces to 3-SAT. Next we show that there is a circuit which encodes the entire computation of the Turing machine as local consistency checks (thus shows that computation is local).

So prover can send an assignment of many variables that encode the history of the computation & verifier can check whether the assignment is valid.

Naive Idea for a quantum generalization:

If promise problem A is in QMA, for $x \in A_{yes}$, $\exists$ a quantum witness state $|\psi\rangle$ & a circuit consisting of two-qubit gates that will accept w/ high probability ;

& for $x \in A_{no}$, $\forall$ witness states the circuit rejects.

Idea would be for prover to send the history of the computation

$$|\psi\rangle|x\rangle, \; U_1|\psi\rangle|x\rangle, \; U_2U_1|\psi\rangle|x\rangle, \; \ldots, \; U_L \cdots U_2U_1|\psi\rangle|x\rangle$$

& verifier could check locally whether this is a valid history, by using local Hamiltonian terms to penalize invalid histories.

But there is a big problem w/ this: prover does not have to send a product state

Suppose $U_1 = I$

so that 1st two registers should be in the same state

$|\alpha\rangle = |\psi\rangle|x\rangle$, $|\psi\rangle|x\rangle = |\beta\rangle$

But ~~there are many~~ the prover can entangle the registers so that they appear similar locally but are very different ~~both~~ globally.

Consider instead the superposition

$$\frac{1}{\sqrt{2}}\left(|0\rangle|\alpha\rangle + |1\rangle|\beta\rangle\right)$$

By looking at just the 1st qubit, we can learn a lot about whether $|\alpha\rangle$ & $|\beta\rangle$ are the same or different, So the idea instead will be for the prover ~~to~~ send a history state:

$$|\eta\rangle = \frac{1}{\sqrt{L+1}} \sum_{\ell=0}^{L} U_\ell \cdots U_1 |\psi\rangle|x\rangle|\ell\rangle$$