Lecture 21

9 APR 2014

Last time: we showed that Local Hamiltonian is in QMA.

Now, we will show that Local Ham. is QMA hard. (I.e., any problem in QMA can be reduced to LH w/ only polynomial overhead.)

#2

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 (this 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 by performing a circuit corresponding to the computation

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~~ might 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

4

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

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

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:

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

this idea for the reduction was inspired by Feynman (1985) + is known as the Feynman-Kitaev circuit-to-Hamiltonian construction. That is, Feynman proposed a way for simulating the dynamics of a quantum circuit via a Hamiltonian that acts on a <u>clock</u> register and a data register:

$$H = \sum_{t=1}^{L} H_t \qquad \text{where}$$

$$H_t = U_t \otimes |t\rangle\langle t-1| + U_t^{\dagger} \otimes |t-1\rangle\langle t|$$

(this is a local Hamiltonian)

Feynman's idea was that if you initialize the data register + the clock register to

$|\psi\rangle|0\rangle$,

after some time, this will evolve to

$U_1 |\psi\rangle|1\rangle$ & then to

$U_2 U_1 |\psi\rangle|2\rangle$ & then to

$U_t U_{t-1} \cdots U_1 |\psi\rangle|t\rangle$

so that the clock register keeps track of how far along we are in the computation. (After some time, we eventually go back...)

To see this, consider that the unitary diagonalizing H is

$$W = \sum_{t=0}^{L} U_t \cdots U_1 \otimes |t\rangle\langle t|$$

so that

$$H_{triv} = W^\dagger H W = \sum_t I \otimes \left[|t\rangle\langle t-1| + |t-1\rangle\langle t| \right]$$

which is a Hamiltonian corresponding to that of a particle moving back & forth along a 1-D line (i.e., the clock advancing and regressing)

So this means that

$$e^{iHt} |\psi\rangle|0\rangle = W W^\dagger e^{iHt} W W^\dagger |\psi\rangle|0\rangle$$
$$= W e^{iH_{triv}t} |\psi\rangle|0\rangle \rightarrow U_t \cdots U_1 |\psi\rangle|t\rangle$$

Kitaev turned Feynman's idea around as a way of ensuring that the ground state of a given Hamiltonian is equal to the history state of the circuit computation, by defining

$$H_{prop} = \sum_{t=1}^{L} H_t \quad \text{where}$$

$$H_t = -U_t \otimes |t\rangle\langle t-1| - U_t^{\dagger} \otimes |t-1\rangle\langle t| + |t\rangle\langle t| + |t-1\rangle\langle t-1|$$

so that $|\eta\rangle$ such that $\langle \eta | H_{prop} | \eta \rangle = \lambda_{min}$ is

$$|\eta\rangle = \frac{1}{\sqrt{L+1}} \sum_{t=0}^{L} U_t \cdots U_1 |\psi\rangle |t\rangle$$

To see this, consider that

~~$W^{\dagger} H_{prop} W$~~

$$W^{\dagger} H_t W = I \otimes \begin{bmatrix} |t\rangle\langle t| + |t-1\rangle\langle t-1| \\ - |t\rangle\langle t-1| - |t-1\rangle\langle t| \end{bmatrix}$$

so ~~that~~ $W^{\dagger}|\eta\rangle = |\psi\rangle \otimes \frac{1}{\sqrt{L+1}} \sum_{t=0}^{L} |t\rangle$

so this simplifies the analysis considerably, and then we just need to verify that

$$\frac{1}{\sqrt{L+1}} \sum_{t=0}^{L} |t\rangle \qquad (**)$$

is an eigenvector of

$$\sum_{t=1}^{L} |t\rangle\langle t| + |t-1\rangle\langle t-1| - |t\rangle\langle t-1| - |t-1\rangle\langle t| \qquad (*)$$

w/ eigenvalue zero. But this is a straightforward calculation & the result is that the eigenvalues of $(*)$ are

$$\lambda_k = 2(1-\cos q_k) \quad \text{where} \quad q_k = \frac{\pi k}{L+1} \quad \text{w/ } k \in \{0, \ldots, L\}$$

& $(**)$ has eigenvalue 0, so that it is the minimum among the possibilities.

So the point of this development is that H_{prop} can act as a quantum check to ensure that its ground state is equal to the history state of a given quantum circuit computation.

States orthogonal to the ground state are given an energy penalty by the Hamiltonian... (9)

In fact, this is the main idea behind a proof for the equivalence of adiabatic quantum computation & the circuit model, a point which we will return to later...

So, to complete the construction of the circuit-to-Hamiltonian reduction, we need to add two more checks:

+ think about ground state consisting of three registers:
a) witness
b) input x (ancilla)
c) clock

1) ensure that the input is legitimate ($|\psi\rangle|x\rangle$) by adding a Hamiltonian term that will penalize any states orthogonal to it:

$$H_{in} = I_p \otimes (I_A - |x\rangle\langle x|_A) \otimes |0\rangle\langle 0|_c$$

(I.e., If clock is set to zero, and ancilla is not $|x\rangle_a$, then penalize)

2) ensure that the output ~~of the~~ is on the accepting subspace by adding a Hamiltonian ~~term~~ that will penalize any states outside of the accepting subspace

$$H_{out} = \left(|0\rangle\langle 0| \otimes I_{p(n)-1}\right)_P \otimes I_A \otimes |L\rangle\langle L|_C$$

(I.e., if clock is in the final state, + decision qubit is not equal to $|1\rangle$, add an energy penalty.

So the circuit-to-Hamiltonian construction is

$$H_{in} + H_{out} + H_{prop}$$

(where H_{prop} acts on three registers)

the Hamiltonian is not quite "local" yet. (not as local as it could be)

the clock register is a qudit system + so a naive translation to qubits will not be local. H_{prop} has two-body operators acting on data registers along w/ the operators needed to advance the clock register.

same for H_{out}. can simplify H_{in} to be $I_P \otimes \left(\sum_{i=1}^{n} |1_i\rangle\langle 1_i|\right)_A \otimes |0\rangle\langle 0|_C$

but then clock register still is not quite "local

Forgetting about this for now, let's argue that this c-to-H construction gives a reduction from any QMA problem to LH. To do so, we need to show that YES instances of a QMA problem translate to YES instances of LH & that NO instances of QMA translate to NO instances of LH.

So, for a YES instance of QMA, we know that $\exists$ a unitary circuit $U_L \cdots U_1$ where each U_t acts on no more than 2 qubits & $\exists$ a quantum witness state $|\psi\rangle$ such that

$$\langle\psi|\langle x|U_1^\dagger \cdots U_L^\dagger\left(|1\rangle\langle 1|\otimes I_{p(n)+n-1}\right)U_L \cdots U_1|\psi\rangle|x\rangle \geq 1-\varepsilon$$

But this means that

$$\langle\psi|\langle x|\, U_1^\dagger \cdots U_L^\dagger\left(|0\rangle\langle 0|\otimes I_{p(n)+n-1}\right) U_L \cdots U_1|\psi\rangle|x\rangle \leq \varepsilon$$

So then from the circuit, we can specify $\{H_{in}, H_{out}, \{H_t\}_{t=1}^{L}\}$ w/ only poly overhead, so that

$$H = H_{in} + H_{out} + H_{prop}$$

The candidate for the ground state is then the history state

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

We proved already that

$\langle \eta | H_{prop} | \eta \rangle = 0$ + we can see that

$\langle \eta | H_{in} | \eta \rangle = 0$ b/c the "input" in $|\eta\rangle$ is $|x\rangle$ (legitimate)

Now, we can argue that

$\langle \eta | H_{out} | \eta \rangle \leq \frac{\varepsilon}{L+1}$ b/c the probability of rejecting a YES instance is $\leq \varepsilon$ (+ then normalization of $|\eta\rangle$ by $L+1$)

so $\langle \eta | H | \eta \rangle \leq \varepsilon / L+1$

Showing the mapping for NO instances will be the topic of next time. I.e., we will show that the minimum eigenvalue is larger than

$$\Omega\left(\frac{(1-\sqrt{\varepsilon})}{L^3}\right)$$

So if we first apply error reduction to the QMA circuit to make ε be as small as an inverse polynomial, then we get an inverse polynomial separation between

$$\frac{\varepsilon}{L+1} \quad \& \quad \frac{1-\sqrt{\varepsilon}}{L^3}$$

We need to argue how to make the Hamiltonian 5-local. Kitaev's idea was to have a unary encoding for the clock, i.e., time step t is represented as

$$|\overbrace{1,\ldots,1}^{t \text{ ones}},0,\ldots,0\rangle$$

So the operator $|t\rangle\langle t|$ now translates to $|1\rangle\langle 1|_t \otimes |0\rangle\langle 0|_{t+1}$.

Similarly $|t-1\rangle\langle t|$ is mapped to

$$|1\rangle\langle 1|_{t-1} \otimes |0\rangle\langle 1|_t \otimes |0\rangle\langle 0|_{t+1}$$

these new operations are at most 3-local

We now need to address the possibility of invalid settings of the clock (counter) since we have moved to a different space & the only allowed settings are

$$|1, \ldots, 1, 0, \ldots, 0\rangle$$

So we can penalize such invalid settings by adding the following Hamiltonian to the overall one

$$I_P \otimes I_A \otimes \sum_{t=1}^{L-1} |0\rangle\langle 0|_t \otimes |1\rangle\langle 1|_{t+1}$$

everything ends up working the same as before even w/ this new penalty.