Lecture 2

The circuit-to-Hamiltonian construction

Scribe: Thomas Vidick

The Local Hamiltonian problem

Now that the class QMA is defined, we would like to identify some problems that are in QMA or complete for it. One such problem is the Local Hamiltonian (henceforth abbreviated as LH) problem. The $k-\mathrm{LH}$ problem is the quantum analog of $k-\mathrm{CSP}$. The n variables in a $k-\mathrm{CSP}$ correspond to n qubits in a $k-\mathrm{LH}$. The m constraints each acting on at most k variables in a $k-\mathrm{CSP}$ correspond to m Hamiltonians each measuring at most k qubits in a $k-\mathrm{LH}$.

Definition 2.1. An instance of $k-\mathrm{LH}$ is given by a collection of m Hamiltonians H_j ($H_j = H_j^\dagger$) such that $H_j \in \mathrm{L}\left(\mathbb{C}^{2^k}\right)$ and $\|H_j\| \le 1$. The total *"energy"* is specified by the Hamiltonian $H = \frac{1}{m}\sum_{j=1}^m H_j$.[1]

Definition 2.2. (The Local Hamiltonian Problem) Given an instance of $k-\mathrm{LH}$ and real parameters $a < b$, the Local Hamiltonian problem, written as $k\mathrm{LH}_{a,b}$, is to decide between the following two cases:

- *(YES):* $\exists |\psi\rangle \in \mathbb{C}^{2^n}$, $\||\psi\rangle\| = 1$, such that $\langle\psi|H|\psi\rangle \le a$
- *(NO):* $\forall |\psi\rangle \in \mathbb{C}^{2^n}$, $\||\psi\rangle\| = 1$, $\langle\psi|H|\psi\rangle \ge b$

Note that this is a promise problem, i.e. to solve $k\mathrm{LH}_{a,b}$ it is enough to give the correct answer, YES or NO, on Hamiltonians that satisfy the promise that their total energy is either at most a or at least b.

Example 2.3. 3SAT is an instance of $3\mathrm{LH}_{0,1}$. Let there be n qubits corresponding to the n variables of the 3SAT formula. We will define a Hamiltonian H_j for every clause C_j in the 3SAT formula. Intuitively, H_j can be thought as the *energy* or *penalty* that is imposed if the clause C_j is not satisfied by a setting of the variables. For every clause $C_j = x_a \vee \overline{x_b} \vee x_c$, the Hamiltonian $H_j = |0\rangle\langle 0|_a \otimes |1\rangle\langle 1|_b \otimes |0\rangle\langle 0|_c \otimes \mathrm{Id}$ evaluates to 1 iff the constraint C_j isn't satisfied. The completeness is straightforward, and for soundness, expanding the state as a linear combination of the 2^n n-bit strings, it is easy to see that in case of an unsatisfiable formula, since at least one clause will be unsatisfied by any assignment, no state can lead to less than energy 1 on average.

[1]Here and elsewhere, it is implicit that H_j acts on a designated subset of k qubits, and is the identity outside of those qubits.

2.1 QMA-completeness of the Local Hamiltonian problem

Our main result today is the following theorem.

Theorem 2.4. *(Kempe-Kitaev-Regev)* $2\mathrm{LH}_{a,b}$ *is* QMA*-complete for some* $a = 2^{-\operatorname{poly}(n)}$ *and* $b = 1/\operatorname{poly}(n)$.

The first result along these lines came from Kitaev, who showed that $5 - \mathrm{LH}$ is QMA-complete. We first show a slightly weaker version of the theorem, which contains the key ideas:

Theorem 2.5. *(Kitaev) There exists* $a = 2^{-\operatorname{poly}(n)}$, $b = 1/\operatorname{poly}(n)$ *and* $k = O(\log n)$ *such that* $k\mathrm{LH}_{a,b}$ *is QMA-complete.*

Note that the statement has two parts: firstly,that $k\mathrm{LH}_{a,b} \in \mathrm{QMA}$, and secondly, that $k\mathrm{LH}_{a,b}$ is QMA-hard, i.e. any problem in QMA reduces to $k - \mathrm{LH}$. In the proof, we show both parts in turn.

Proof. **(i)** Assume we are given an instance of $k\mathrm{LH}_{a,b}$. Here n denotes the number of qubits in the LH instance. We will show that the Local Hamiltonian problem on this instance can be solved in QMA. The input x to the QMA algorithm A that converts $x \to C_x$ will consist of the description of each of the Hamiltonians in the LH instance. The algorithm A works as follows: it first selects a uniformly random $1 \le j \le m$. It then measures the witness according to the POVM $\{(\mathrm{Id} + H_j)/2, (\mathrm{Id} - H_j)/2\}$. It rejects if the outcome of the measurement is $(\mathrm{Id} + H_j)/2$. Note that this is a well-defined POVM due to the assumption that $\|H_j\| \le 1$. Now,

$$\begin{aligned}
Pr(C_x \text{ rejects}) &= \sum_{j=1}^{m} \Pr(\text{Measurement outcome is } (\mathrm{Id} + H_j)/2) \cdot \Pr(H_j \text{ is chosen}) \\
&= \frac{1}{m} \sum_{j=1}^{m} \langle \psi | \frac{\mathrm{Id} + H_j}{2} | \psi \rangle \\
&= \frac{1}{2} \big(1 + \langle \psi | H | \psi \rangle \big) \ .
\end{aligned}$$

Since either one of the case holds $\exists \psi, \langle \psi | H | \psi \rangle \le a$ or $\forall \psi, \langle \psi | H | \psi \rangle \ge b$, it implies that the circuit C_x accepts with probability at least $\frac{1}{2} - \frac{a}{2m}$ for some $|\psi\rangle$, or accepts with probability at most $\frac{1}{2} - \frac{b}{2m}$ for all $|\psi\rangle$. Further, as long as $b - a \in \frac{1}{O(\operatorname{poly}|x|)}$, the gap between the two cases can be amplified (as described in Exercise1.1).

(ii) For this part, we need to show that every $L \in \mathrm{QMA}$ can be reduced to an instance of kLH for some $k = O(\log n)$. We will construct a $O(\log n)$-local Hamiltonian H_x such that the following holds:

- *(Completeness):* If $\exists \phi$ such that $\Pr(C_x \text{ accepts } \phi) \ge 1 - \epsilon$, then $\exists \psi, \langle \psi | H_x | \psi \rangle \le \epsilon$
- *(Soundness):* If $\forall \phi$, $\Pr(C_x \text{ accepts } \phi) \le \epsilon$, then $\forall \psi, \langle \psi | H_x | \psi \rangle \ge \frac{3}{4} - \epsilon$

To see the difficulty in doing this, consider first the classical Cook-Levin reduction of a circuit to 3SAT. If the input variables to the circuit are x_1 to x_n, and without loss of generality, if only one gate acts at every "stage" and there are T stages, one can introduce auxiliary variables $x_{i,j}$, where $1 \le i \le n$ and $1 \le j \le T$, such that $x_{i,j}$ denotes the value in the i'th wire at the j'th stage. The constraints that are introduced are so as to make sure that the values of the variables are consistent with the applied gates. For instance, if an OR gate acts on $x_{1,5}$ and $x_{2,5}$ and gives the output on $x_{2,6}$, we add the constraint $x_{2,6} = x_{1,5} \vee x_{2,5}$, and so on (the constraints can further easily be converted to constraints on 3 variables, giving a 3SAT expression).

Can the same thing be done in the quantum case? Consider a quantum circuit $C_x = U_T ... U_1$, with n input qubits x_i, and such that the unitaries U_j act on at most 2 qubits at every stage. We shall create a Hamiltonian that will give an energy penalty if any of the constraints are violated. Since all input qubits are in the $|0\rangle$ state and the output needs to be in the $|0\rangle_1$ state, two of the Hamiltonians are simple:

$$H_{in} = \sum_{i=1}^{n} |1\rangle\langle 1|_i \otimes \mathrm{Id} , \qquad H_{out} = |0\rangle\langle 0|_1 \otimes \mathrm{Id} ,$$

where here the input qubits from $i = 1$ to n correspond to the ancilla qubits initialized to $|0^n\rangle$ by the circuit C_x. Further, we should introduce constraints of the form $|\psi_j\rangle = U_j \otimes \mathrm{Id}\, |\psi_{j-1}\rangle$, where $|\psi_j\rangle$ is a (quantum) variable describing the state of all the qubits at the j-th state of the circuit. Unfortunately it is not clear at all how to implement such a contraint with a *local* Hamiltonian! For instance, if $|\psi_1\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$ and $|\psi_2\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle - |1^n\rangle)$ then one can in fact show that no local measurement acting on $< n$ qubits will be able to distinguish (at all, even with small success probability) between these two states. Indeed, observe that if we measure any qubit in $|\psi_1\rangle$ or $|\psi_2\rangle$ then it will be 0 or 1 with equal probability in *both* cases. To expand this observation into a formal argument for the local indistinguishability of the two states we'd need to get into the formalism of *density matrices*, which are used to describe the *reduced* state of a quantum vector on a subset of its qubits; we will return to this topic later.

Since "juxtapositions" of quantum states cannot be compared locally, the main idea instead is to use *superpositions* of the two states. If we were given access to the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle|\psi_1\rangle + |1\rangle|\psi_2\rangle)$, we could apply a Hadamard transformation ($|0\rangle \to |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|1\rangle \to |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$) on the first qubit, and then make a measurement of the first qubit. One can verify that the probability of obtaining the outcome $|0\rangle$ is exactly $1/4\| |\psi_1\rangle + |\psi_2\rangle \|^2$, and the probability of obtaining the outcome $|1\rangle$ is exactly $1/4\| |\psi_1\rangle - |\psi_2\rangle \|^2$, giving us a very precise way to compare the two states.

We now describe Kitaev's construction of a local Hamiltonian.

Kitaev's Construction: For intuition, we first describe the "ideal witness" that we would like the ground state of the local Hamiltonian to be:

$$|\psi\rangle = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} (U_t U_{t-1} ... U_1 |0_n\rangle \otimes |\phi\rangle) \otimes |t\rangle_c , \tag{2.1}$$

where $|\phi\rangle$ is a witness that maximizes the probability of C_x accepting. $|\psi\rangle$ is a uniform superposition over the state of the circuits at each stage $j = 0, \ldots, T$. The superposition is indexed by the states $|t\rangle$ of the "clock", which keeps track of the number of unitaries that have been applied so far. This idea, of replacing a time-dependent unitary evolution by a time-independent Hamiltonian, goes back to Feynman.

The local Hamiltonian can be decomposed in three parts. The first two are straightforward and almost exactly as introduced earlier:

$$H_{in} = \sum_{i=1}^{n} |1\rangle\langle 1|_i \otimes \mathrm{Id} \otimes |0\rangle\langle 0|_c , \qquad H_{out} = |1\rangle\langle 1|_1 \otimes \mathrm{Id} \otimes |T\rangle\langle T|_c .$$

The third part is the *propagation* Hamiltonian

$$H_{prop} = \sum_{t=1}^{T} H_{prop,t} ,$$

where

$$H_{prop,t} = \frac{1}{2}\big(\, \mathrm{Id} \otimes |t\rangle\langle t|_c + \mathrm{Id} \otimes |t-1\rangle\langle t-1|_c - U_t \otimes |t\rangle\langle t-1|_c - U_t^\dagger \otimes |t-1\rangle\langle t|_c \big) \ .$$

Finally, we let the Hamiltonian H in our LH instance be as follows:

$$H = J_{in} H_{in} + (T+1) H_{out} + J_{prop} H_{prop} \ ,$$

where J_{in} and J_{prop} are positive integer weights that will be assigned later. Since T, the number of gates in the circuit C_x, is polynomial in n, this gives a Hamiltonian acting on $O(\log\ n)$ qubits.

Completeness: Assume there is some state $|\phi\rangle$ such that $\Pr(C_x \text{ accepts } |0_n\rangle \otimes |\phi\rangle) \geq 1-\epsilon$. We let our state $|\psi\rangle$ be the ideal state as in (2.1). Note that $\langle\psi|H_{in}|\psi\rangle = 0$ since for $t = 0$, none of the inputs is in the $|1\rangle$ state which will make the first term corresponding to the ancilla bits in $|\psi\rangle$ above 0, and for all other values of t, the term corresponding to the clock will become 0.

Also, $\langle\psi|H_{prop}|\psi\rangle = 0$, since all other terms except the corresponding terms for the $t-1$ and t times cancel out, which further cancel out as follows:

$$\begin{aligned} H_{prop,t}|\psi\rangle &= \frac{1}{2\sqrt{T+1}}\Big(\mathrm{Id} \otimes |t\rangle\langle t|_c + \mathrm{Id} \otimes |t-1\rangle\langle t-1|_c - U_t \otimes |t\rangle\langle t-1|_c - U_t^\dagger \otimes |t-1\rangle\langle t|_c\Big) \\ &\quad .\,(U_t ... U_1|0_n\rangle \otimes |\phi\rangle \otimes |t\rangle + U_{t-1}...U_1|0_n\rangle \otimes |\phi\rangle \otimes |t-1\rangle) \\ &= \frac{1}{2\sqrt{T+1}}\big((U_t...U_1|0_n\rangle \otimes |\phi\rangle \otimes |t\rangle + U_{t-1}...U_1|0_n\rangle \otimes |\phi\rangle \otimes |t-1\rangle \\ &\quad - U_t...U_1|0_n\rangle \otimes |\phi\rangle \otimes |t\rangle - U_t^\dagger U_t U_{t-1}...U_1|0_n\rangle \otimes |\phi\rangle \otimes |t-1\rangle\big) \\ &= 0\ . \end{aligned}$$

Thus,

$$\begin{aligned} \langle\psi|H|\psi\rangle &= \langle\psi|(T+1)H_{out}|\psi\rangle \\ &= (T+1)\cdot\frac{1}{(\sqrt{T+1})^2}\|\Pi_1^{|1\rangle} U_T...U_1|0\rangle \otimes |\phi\rangle\|_2^2 \\ &= Pr(C_x \text{ rejects } |0\rangle \otimes |\phi\rangle) \\ &\leq \epsilon\ , \end{aligned} \tag{2.2}$$

as claimed.

Soundness: Before we can analyze the soundness, we will need an important lemma:

Lemma 2.6. *(Projection Lemma, Kempe-Kitaev-Regev): Let $H = H_1 + H_2$, where H, H_1, H_2 are Hermitian positive semidefinite. Let S be the null-space of H_2 and assume $\lambda_{min}(H_2|_{S^\perp}) \geq J > 2\|H_1\|$, where $\|\cdot\|$ denotes the operator norm, the largest singular value. Then*

$$\lambda_{min}(H_1|_S) - \frac{\|H_1\|^2}{J - 2\|H_1\|} \leq \lambda_{min}(H) \leq \lambda_{min}(H_1|_S)$$

Proof. RHS: Let $|v\rangle$ be an eigenvector associated with the smallest eigenvalue of $H_1|_S$. Thus,

$$\begin{aligned} \langle v|H|v\rangle &= \langle v|H_1|v\rangle + \langle v|H_2|v\rangle \\ &= \langle v|H_1|v\rangle + 0 \\ \lambda_{min}(H) &\leq \langle v|H|v\rangle = \langle v|H_1|v\rangle = \lambda_{min}(H_1|_S) \end{aligned}$$

LHS: Let $|v\rangle$ be an eigenvector corresponding to the smallest eigenvalue of H. Expand $|v\rangle = \alpha_1|v_1\rangle + \alpha_2|v_2\rangle$, where $|v_1\rangle \in S$, $|v_2\rangle \in S^\perp$, $\alpha_1, \alpha_2 \in \mathbb{R}$ (which we can always assume by multiplying $|v_1\rangle$ and $|v_2\rangle$ by a complex phase if necessary), and $|\alpha_1|^2 + |\alpha_2|^2 = 1$. Thus,

$$\langle v|H_2|v\rangle = 0 + |\alpha_2|^2\langle v_2|H_2|v_2\rangle \geq |\alpha_2|^2 J$$

where we used the condition given in the lemma for the inequality. Also,

$$\begin{aligned}\langle v|H_1|v\rangle &= (1-|\alpha_2|^2)\langle v_1|H_1|v_1\rangle + |\alpha_2|^2\langle v_2|H_1|v_2\rangle + 2Re(\alpha_1\alpha_2\langle v_1|H_1|v_2\rangle) \\ &\geq \langle v_1|H_1|v_1\rangle - |\alpha_2|^2\|H_1\| + |\alpha_2|^2(-\|H_1\|) + 2\alpha_2(-\|H_1\|)\end{aligned}$$

Hence,

$$\begin{aligned}\langle v|H|v\rangle &= \langle v|H_1|v\rangle + \langle v|H_2|v\rangle \\ &\geq \langle v_1|H_1|v_1\rangle - |\alpha_2|^2\|H_1\| - |\alpha_2|^2\|H_1\| - 2\alpha_2\|H_1\| + |\alpha_2|^2 J\end{aligned}$$

This quantity is minimized by setting $|\alpha_2| = \dfrac{\|H_1\|}{J - 2\|H_1\|}$. Substituting this value gives the required inequality.

□

We will also use the following claim, whose proof is left as an exercise (hint: observe that H_{prop} can be brought into a simple tridiagonal form by an appropriate change of basis).

Claim 2.7. *The smallest non-zero eigenvalue of H_{prop} is at least c/T^2 for some $c > 0$.*

We conclude our soundness analysis by showing how the *Projection Lemma* can be used to get the claimed bound. Let S_{prop} be the null-space of H_{prop}. Using the claim above we get that $\lambda_{min}(H_{prop}|_{S_{prop}^\perp}) \geq c/T^2$. Let $H_1 = J_{in}H_{in} + (T+1)H_{out}$ and $H_2 = J_{prop}H_{prop}$. Thus, $\lambda_{min}(H_2 = J_{prop}H_{prop}|_{S_{prop}^\perp}) \geq cJ_{prop}/T^2$. Moreover, since $\|H_1\| \leq (T+1)\|H_{out}\| + J_{in}\|H_{in}\| \leq T+1+J_{in}(n+q) \leq poly(n)$ if $J_{in} = poly(n)$, we can let $J_{prop} = T^2 J_{in}/c = poly(n)$ and satisfy all the conditions required to apply the Projection Lemma. Further, we can choose J_{prop} large enough so that the result is the following lower bound on the minimum eigenvalue of H:

$$\lambda_{min}(H) \geq \lambda_{min}(H_1|_{S_{prop}}) - \frac{1}{8}.$$

Now we apply the Projection Lemma again to find a lower bound on $\lambda_{min}(H_1|_{S_{prop}})$. Assume all further arguments are restricted to the space S_{prop}. Let $S_{in} \subseteq S_{prop}$ be the null-space of H_{in} inside S_{prop}. Now let $H_1 = (T+1)H_{out}|_{S_{prop}}$ and $H_2 = J_{in}H_{in}|_{S_{prop}}$. Using a similar argument as the previous case we can apply the Projection Lemma again and get

$$\lambda_{min}\left(J_{in}H_{in}|_{S_{prop}} + (T+1)H_{out}|_{S_{prop}}\right) \geq \lambda_{min}(H_{out}|_{S_{in}}) - \frac{1}{8}.$$

But note that by the same calculation as in (2.2), $\lambda_{min}((T+1)H_{out}|_{S_{in}})$ is precisely the probability with which the circuit C_x rejects the state $|0_n\rangle \otimes |\phi\rangle$, which we assumed to be at least $1-\epsilon$. Thus, we get that,

$$\lambda_{min}(H) \geq \lambda_{min}(H_{out}|_{S_{in}}) - \frac{1}{8} - \frac{1}{8} \geq 1 - \epsilon - \frac{1}{4} = \frac{3}{4} - \epsilon$$

as claimed. □

So far the construction we gave only shows QMA-hardness of $k-\text{LH}$ for $k=\Omega(\log n)$. To go down to hardness for 2-local Hamiltonians we take three steps.

The first step consists in representing the clock in unary, using T qubits and states $|0\cdots 00\rangle$ for time 0, $|0\cdots 01\rangle$ for time 1, up to $|1\cdots 11\rangle$ for time T. In this case, controlling on a time t for the clock can be done by looking only at qubits $t-1$, t and $t+1$ and verifying that their state is $|011\rangle$. This leads to a 5-local Hamiltonian, with the largest terms being those from the propagation Hamiltonian, which act on 2 computation qubits and 3 clock qubits. The only added difficulty is that there exists some ill-formed clock terms. To penalize those we introduce an additional "clock" Hamiltonian $H_{clock}=\sum_t |10\rangle\langle 10|_{t,t-1}$, which ensures that clock states are always formed of a continuous sequence of 0, followed by a continuous sequence of 1. The analysis follows by an additional application of the projection lemma to restrict to the subspace of valid clock states.

To obtain a 3-local Hamiltonian one replaces the propagation Hamiltonian by a new form,

$$H'_{prop,t}=\frac{1}{2}\big(\,\text{Id}\otimes|10\rangle\langle 10|_{t,t+1}+\text{Id}\otimes|10\rangle\langle 10|_{t-1,t}-U_t\otimes|1\rangle\langle 0|_t-U_t^{\dagger}\otimes|0\rangle\langle 1|_t\big)\ .$$

This is now indeed 3-local. Without going into details, the key observation is that if Π_{clock} is the projection on valid clock states, then $\Pi_{clock}H'_{prop,t}\Pi_{clock}=H_{prop,t}$. Another application of the projection lemma (again!) then allows one to complete the analysis.

Finally, to obtain a 2-local Hamiltonian one needs a somewhat more involved use of the projection lemma, having recourse to "third-order perturbation theory". We will discuss this in the next lecture.