CMSC 858L: Quantum Complexity

Instructor: Daniel Gottesman

Spring 2023

16 LOCAL HAMILTONIAN continued

16.1 References

For QMA-completeness of the 5-LOCAL HAMILTONIAN problem, see chapter 14 of Kitaev, Shen, and Vyalyi, *Classical and Quantum Computation*. For QMA-completeness of the 3-LOCAL HAMILTONIAN problem, see Kempe and Regev, "3-Local Hamiltonian is QMA-complete," quant-ph/0302079. For QMA-completeness of the 2-LOCAL HAMILTONIAN problem, see Kempe, Kitaev, and Regev, "The Complexity of the Local Hamiltonian Problem," quant-ph/0406180.

16.2 Kitaev Lemma

Last time we proved that $O(\log n)$-LOCAL HAMILTONIAN is QMA-complete except for one lemma:

Lemma 1. *Let K_1, K_2 be positive semi-definite operators with no shared 0 eigenstates and suppose that all eigenstates of both K_1 and K_2 with nonzero eigenvalue have eigenvalue at least v. Let θ be the minimum angle between $|\psi_1\rangle$ and $|\psi_2\rangle$ where $|\psi_i\rangle$ is an eigenstate of K_i with eigenvalue 0. Then*

$$\langle\phi|(K_1+K_2)|\phi\rangle \geq 2v\sin^2\theta/2 \tag{1}$$

for all state $|\phi\rangle$.

Proof of lemma. Let $|\phi\rangle$ be an arbitrary state and let Π_i be a projector onto the 0 eigenvalue space of K_i. Then

$$\langle\phi|(K_1+K_2)|\phi\rangle \geq v\langle\phi|[(I-\Pi_1)+(I-\Pi_2)]|\phi\rangle = (2-\langle\phi|(\Pi_1+\Pi_2)|\phi\rangle)v. \tag{2}$$

We wish to upper bound $\langle\phi|(\Pi_1+\Pi_2)|\phi\rangle$.

Let us focus on $|\phi\rangle$ which is an eigenstate of $\Pi_1+\Pi_2$, $(\Pi_1+\Pi_2)|\phi\rangle = \lambda|\phi\rangle$. We can write $|\phi\rangle$ as

$$|\phi\rangle = \alpha_i|\eta_i\rangle + \beta_i|\xi_i\rangle \tag{3}$$

for $i=1,2$, $|\eta_i\rangle$ in subspace projected on by Π_i, and $|\xi_i\rangle$ a state orthogonal to the subspace projected on by Π_i. Then

$$\langle\phi|(\Pi_1+\Pi_2)|\phi\rangle = |\alpha_1|^2 + |\alpha_2|^2 = \lambda. \tag{4}$$

We also have

$$\begin{aligned}
\lambda^2 &= (\langle\phi|(\Pi_1+\Pi_2))((\Pi_1+\Pi_2)|\phi\rangle) && (5)\\
&= (\alpha_1^*\langle\eta_1| + \alpha_2^*\langle\eta_2|)(\alpha_1|\eta_1\rangle + \alpha_2|\eta_2\rangle) && (6)\\
&= |\alpha_1|^2 + |\alpha_2|^2 + 2\mathrm{Re}(\alpha_1^*\alpha_2\langle\eta_1|\eta_2\rangle) && (7)\\
&= \lambda + 2\mathrm{Re}(\alpha_1^*\alpha_2\langle\eta_1|\eta_2\rangle). && (8)
\end{aligned}$$

Now, we know that

$$|\langle\eta_1|\eta_2\rangle| \leq \cos\theta, \tag{9}$$

since θ is the minimum angle between 0 eigenvectors of K_1 and K_2. Thus,

$$\lambda^2 - \lambda \leq 2|\alpha_1\alpha_2|\cos\theta \leq (|\alpha_1|^2 + |\alpha_2|^2)\cos\theta = \lambda\cos\theta. \tag{10}$$

That is,

$$\lambda \leq 1 + \cos\theta. \tag{11}$$

Plugging this back into eq. (**??**), we find

$$\langle\phi|(K_1 + K_2)|\phi\rangle \geq (1 - \cos\theta)v = 2v\sin^2\theta/2. \tag{12}$$

□

16.3 Completeness of 5-LOCAL HAMILTONIAN

Recall that for $O(\log n)$-LOCAL HAMILTONIAN, we had a Hamiltonain $H = H_P + H_i + H_f$, where H_P enforces the ground state to be a history state $\sum_t |\psi_t\rangle|t\rangle$ for the checking circuit, H_i enforces the $t = 0$ terms to have correctly initialized ancillas, and H_f gives an energy penalty if the final $t = T$ time is not an accepting state for the check circuit.

The $O(\log n)$ size of the terms in the previous result come purely from the clock. If we can find a better way to encode the clock so that we can identify the time specified by the clock using only a few qubits, we can instead show the completeness of k-LOCAL HAMILTONIAN with constant k.

For instance, we could encode the clock in unary. This is of course a very inefficient way of storing it, but the maximum time T is still polynomial in n, so the number of qubits needed for a unary clock encoding is acceptable. Then the time 0 is $00\ldots0$, time 1 is $10\ldots0$, and time T is $11\ldots1$. The advantage of this encoding is that time t is $1\ldots10\ldots0$, beginning with t 1's, which always differs from the encoding of time $t-1$ in only one place, the tth bit, which is 1 for t and 0 for time $t-1$.

In the Hamiltonian above, we had terms involving $|t\rangle\langle t-1|$. We might want to replace this by just a single qubit operator $\langle 1||0\rangle$ on the tth qubit. Indeed, this will convert the time $t-1$ to time t, as desired. Unfortunately, it will also convert time s (for $s < t-1$) to something that is not a valid time encoding, so using this replacement will have undesireable side effects. Instead, we need an operator that acts *only* on the times t and $t-1$. The thing that singles out those two times is that they have a 1 at the $(t-1)$th place and a 0 at the $(t+1)$th place; they are the only two times that have those two properties. Thus, if we replace $|t\rangle\langle t-1|$ by $|110\rangle\langle 100|$ for qubits $t-1$, t, and $t+1$, this will only convert time $t-1$ to time t and have no effect on other times. (We might be tempted to just use $|11\rangle\langle 10|$ for qubits $t-1$ and t, but to keep the Hamiltonian hermitian, we need to include also the adjoint of this $|10\rangle\langle 11|$, which will convert any time greater than t into some invalid time encoding.)

Similarly, we can replace $|t\rangle\langle t|$ with $|10\rangle\langle 10|$ on qubits t and $t+1$. Once we have done this everywhere in H_P, we can immediately see that history states using the new time encoding are once again ground states for the new H_P. We can similarly revise H_i and H_f. All terms of these Hamiltonians are now 5-local.

However, closer examination will reveal that $H_P + H_i + H_f$ has 0 energy states that are not history states. In particular, any state where the clock qubits are not in a valid clock encoding, such as $|\psi\rangle|00100\ldots0\rangle$, will not activate any of the terms of H_P, H_i, or H_f, and so have 0 energy. The solution is straightforward: We need an additional constraint term in the Hamiltonian which forces the clock to be in a valid encoding. One property of valid clock encodings is that they never have a 1 to the right of a 0. Any state that is not a valid clock encoding, on the other hand, does have a 1 to the right of a 0. Thus, if we have a Hamiltonian

$$H_C = \sum_i I \otimes |01\rangle_{i,i+1}\langle 01| \tag{13}$$

(where the non-trivial action is on qubits i and $i+1$ of the clock), then the only states that have 0 energy for H_C are those with valid clock encodings.

If we consider the Hamiltonian

$$H = H_P + H_i + H_f + H_C, \tag{14}$$

the argument above for the proof of QMA-completeness of $O(\log n)$-LOCAL HAMILTONIAN shows that in a "yes" instance of L, the history state for a good witness for L has energy less than E, whereas in a "no" instance of L, any state in the subspace spanned by states with valid clock encodings has energy at least $E+\Delta$. We also note that any state in the subspace spanned by states with invalid clock encodings has energy at least 1 (due to H_C), which is greater than $E+\Delta$. The Hamiltonian preserves these two subspaces, so any state which is a superposition over the two of them will have energy at least as big as the lesser energy $E+\Delta$. This proves:

Theorem 1. 5-*LOCAL HAMILTONIAN is QMA-complete.*

16.4 Completeness of 2-LOCAL HAMILTONIAN

5-LOCAL HAMILTONIANS are still rather complicated. Can we work with simpler Hamiltonians? By improving our clock construction further, we can prove the completeness of 3-LOCAL HAMILTONIANS (although I will skip most details of the proof). For instance, we could still use a unary clock encoding $|11\cdots10\cdots0\rangle$ but then terms of H_P will simply be

$$\frac{1}{2}\left[I\otimes(|10\rangle_{t,t+1}\langle 10|+|10\rangle_{t-1,t}\langle 10|)-U_t\otimes|1\rangle_t\langle 0|-U_t^\dagger\otimes|0\rangle_t\langle 1|\right], \tag{15}$$

where the subscript indicates which clock qubits are addressed. In particular, the terms with a U involve only the tth clock qubit, changing it from 0 to 1 (or from 1 to 0 for $U^\dagger$). This is just a 3-LOCAL HAMILTONIAN.

But hold on, this H_P will involve transitions between valid clock encodings and invalid clock encodings, for instance time 1 $|100\cdots0\rangle$ could transition to $|100010\cdots0\rangle$. But we still have the H_C term, so this invalid encoding will have an energy penalty. The Hamiltonian then becomes *frustrated*, meaning it is not possible to satisfy all Hamiltonian terms at once, and the ground states won't have 0 energy even when we are reducing from a problem where the witness is accepted with 100% probability. The actual ground states will be some compromise between satisfying the modified H_P term and the H_C term. In particular, if we increase the relative strength of H_C compared to the other terms, then the lowest energy states will have to come very close to satisfying H_C and thus have a valid clock encoding. Within this large component of the ground state, the only relevant transitions are ones between consecutive valid clock encodings, and each is associated with doing the appropriate gate U_t. Therefore, the ground state will be close to a valid history state for the circuit, as required.

But this approach will not work for 2-LOCAL HAMILTONIAN, since U_t itself is already 2-local, and we then don't have any room to tie it to advancing the clock. Instead, we use another trick, known as *perturbation theory gadgets*. The idea is that, given any 3-local Hamiltonian H, we can make a 2-local Hamiltonian H' that "looks like" the 3-local Hamiltonian on the low energy states.

Suppose we have a 3-qubit Hamiltonian term of H which is the product of three Paulis, which we will assume without loss of generality to be $H_{123}=X_1X_2X_3$ on qubits 1, 2, and 3. The new Hamiltonian will have the original 3 qubits but also 3 additional qubits A, B, and C to tie together the qubits 1, 2, and 3. In particular, we will have terms in H':

$$H'_{ABC}=3I-Z_AZ_B-Z_AZ_C-Z_BZ_C. \tag{16}$$

This will force all three qubits to be in the same state in the standard basis, either $|000\rangle_{ABC}$ or $|111\rangle_{ABC}$ (or some superposition). Then we also have a term

$$H'_{123}=X_1X_A+X_2X_B+X_3X_C. \tag{17}$$

What are the low-energy states of the sum $H'_{123}+\lambda H'_{ABC}$ when λ is large? The first priority to have low energy is to satisfy H'_{ABC} as much as possible; H'_{123} is a small perturbation. Thus, the low energy states should be close to superpositions of $|000\rangle_{ABC}$ and $|111\rangle_{ABC}$. But within this subspace, states that do a better job of satisfying H'_{123} will be lower energy than ones which don't. However, a single term of H'_{123} applied to such a state will give us a state that violates H'_{ABC}, so is severely penalized. However, there are

terms $X_1X_AX_2X_BX_3X_C$ that are the product of 3 terms of H'_{123} that respect H'_{ABC} and so are allowed in the low-energy subspace. But notice: this term includes $X_1X_2X_3$, the original term H_{123} from H! The best attempt to satisfy H'_{123} within the low-energy space of H'_{ABC} is to simulate the H_{123} term.

One can show that by replacing each 3-local product term in H with a 2-local Hamiltonian using these perturbation theory gadgets, the resulting Hamiltonian has low-energy states which map to the low-energy states of H. This in turn shows that it is possible to reduce 3-LOCAL HAMILTONIAN to 2-LOCAL HAMILTONIAN, which must also be QMA-complete.

Naturally, 1-LOCAL HAMILTONIAN is not going to be QMA-complete. It is just a sum of single-qubit terms, and each can be separately diagonalized in constant time. The ground state will just be a tensor product of the ground states of the single-qubit Hamiltonians, and therefore the ground state energy can be easily computed in P.

Note, though, that more general Hamiltonians which are a sum of commuting terms are not necessarily easy, although probably they are not QMA-complete. For one thing, k-SAT can be phrased as a commuting Hamiltonian where each clause can be enforced through a diagonal Hamiltonian term on k qubits. Thus, commuting Hamiltonians are NP-hard. However, it's not even clear that the general k-local commuting Hamiltonian problem is in NP. (This is an open problem.) Again, all terms of the Hamiltonian can be simultaneously diagonalized, but the eigenstates might be highly entangled states. (For instance, stabilizer states, which we saw earlier, are eigenstates of commuting Hamiltonians formed from their stabilizers.) Therefore, classically specifying a single one of these to be the witness might be difficult.

In general, when dealing with Hamiltonian complexity, one can consider different kinds of Hamiltonians as we have seen above. The single-qubit (or single-qudit) Hamiltonians are essentially trivial. Then commuting Hamiltonians are more complicated but still easier to deal with than the non-commuting but unfrustrated Hamiltonians (as in the $O(\log n)$-LOCAL HAMILTONIAN and 5-LOCAL HAMILTONIAN problems), which in turn are easier to deal with than general frustrated Hamiltonians, as with the 3-LOCAL HAMILTONIAN and 2-LOCAL HAMILTONIAN problems. That is, it is easier to prove things about the "less complicated" Hamiltonian types on this list; but of course looking at a wider range of possible Hamiltonians may enable you to find examples that have some particular interesting property.