Lecture 3: Feynman-Kitaev concluded, and BQP-completeness

Sept 11, 2025 *TF: Yeongwoo Hwang, Tina Zhang*

1 Hamiltonian recap

A Hamiltonian is a Hermitian operator that plays a central role in quantum mechanics. Viewed as an observable, it measures the energy of a physical system. This perspective ties it to the classical notion of a constraint satisfaction problem: the energy of a configuration counts the number of constraints that configuration violates.

We will typically work with "local Hamiltonians",

$$H = \sum_i H_i,$$

where each operator H_i is Hermitian and *local*, in that it acts only $O(1)$ qubits (or qudits, if we work with higher-dimensional particles) in our system. Each operator H_i is called a "local term" of the Hamiltonian. In the last class, you saw an alternate definition of this:

$$H = \sum_\alpha \beta_\alpha P_\alpha,$$

where the strings α index Paulis of weight $O(1)$, and $\beta_\alpha \in \mathbb{R}$. It is a simple exercise to show that any Hamiltonian in the former form can be written in the latter form, using the fact that the Paulis form a basis for the space of matrices.

As remarked above, we can turn any classical CSP into a Hamiltonian. E.g. let's take 2SAT: we can turn a clause $(x \vee y)$ into a Hamiltonian term acting on two qubits, whose matrix representation is the diagonal matrix

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

This assigns an energy penalty of 1 to the single unsatisfying computational basis string, and zero energy penalty to all the others.

2 Local Hamiltonian problem is QMA-complete

Here, we will see that the local Hamiltonian problem is QMA-complete. That is, we will provide a reduction from any computation problem P in QMA to a local Hamiltonian problem, by appealing to P's verification circuit. One such circuit is depicted in Figure 1. The main statement we will show is the following:

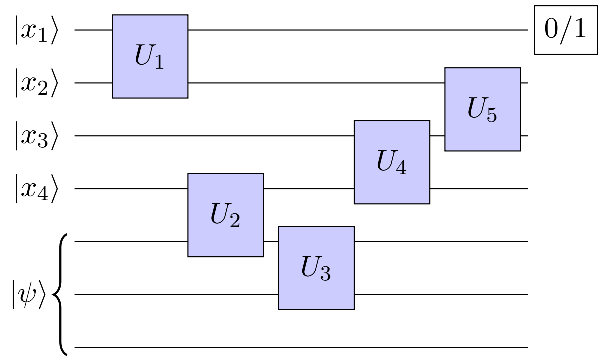

Figure 1: A quantum circuit used by the verifier in a QMA protocol. The ancilla register is abbreviated. Input is $|x\rangle$ and the prover sends $|\psi\rangle$. Without loss of generality, we can assume that at each time step, a two qubit gate is applied. The circuit involves $T = \text{poly}(|x|)$ gates. At the last step, a qubit O is measured in the $\{|0\rangle, |1\rangle\}$ basis.

Theorem 2.1. *There is a local Hamiltonian H such that the following holds for the circuit in Figure 1. Suppose there is a state $|\psi\rangle$ which ensures that the probability to output 1 is at least $1 - e^{-\Theta(|x|)}$. Then the ground energy of H is $O\left(e^{-\Theta(|x|)}\right)$. If the probability to output 1 is at most $e^{-\Theta(|x|)}$ for all $|\psi\rangle$, then the ground energy of H is at least $\Omega\left(\frac{1}{T^3}\right)$.*

Proof. We will use the Feynman-Kitaev clock construction. Recall the Feynman-Kitaev Hamiltonian. Introducing a "clock" Hilbert space $\mathcal{H}_C$ of dimension $T+1$ and consider the Hamiltonian

$$H = H_{init} + H_{prop} + H_{out},$$

where

$$\begin{aligned}
H_{init} &= |0\rangle\langle 0|_C \otimes \left(\sum_i \frac{\mathbb{1} - (-1)^{x_i} Z_i}{2} \right), \\
H_{prop} &= \sum_{t=0}^{T-1} \Big(|t\rangle\langle t|_C \otimes \mathbb{1} + |t+1\rangle\langle t+1|_C \otimes \mathbb{1} - |t\rangle\langle t+1| \otimes U_{t+1}^\dagger - |t+1\rangle\langle t| \otimes U_{t+1} \Big), \\
H_{out} &= |0\rangle\langle 0|_O \otimes |T\rangle\langle T|_C \,.
\end{aligned} \tag{1}$$

Note that H_{out} gives a penalty if the output is not 1 at the time step T. See Figure 2 for a depiction.

We will first analyze the properties of the Hamiltonian and then prove the main theorem.

Claim 2.2. The ground space of $H_{init} + H_{prop}$ is spanned by the history states, for all possible witnesses $|\psi\rangle$:

$$\text{span}\left\{ \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle_C \otimes (U_t U_{t-1} \dots U_1 U_0 |x\rangle \otimes |\psi\rangle) \,\middle|\, \forall\, |\psi\rangle \right\}, \tag{2}$$

where $U_0 = \mathbb{1}$. Any quantum state $|\theta\rangle$ orthogonal to the ground space has energy (also called the spectral gap) $\Omega\left(\frac{1}{T^2}\right)$ with respect to $H_{init} + H_{prop}$.

Proof sketch. What is H_{prop} doing? Let's build some intuition by focusing on a single term

$$H_{prop,t} = |t\rangle\langle t|_C \otimes \mathbb{1} + |t+1\rangle\langle t+1|_C \otimes \mathbb{1} - |t\rangle\langle t+1| \otimes U_{t+1}^\dagger - |t+1\rangle\langle t| \otimes U_{t+1}. \tag{3}$$

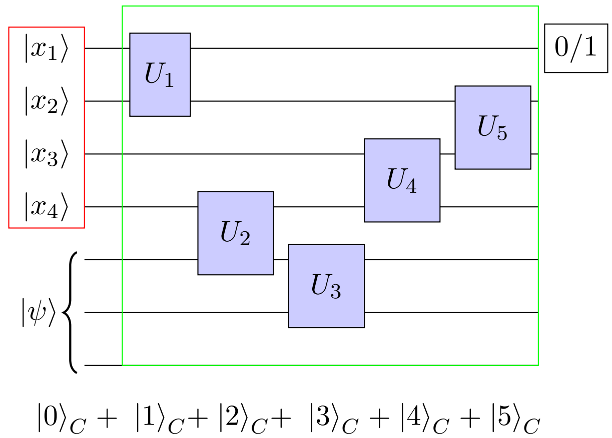

Figure 2: History state for the quantum circuit depicted in Figure 1. The Hamiltonian term H_{init} (red) gives penalty if the input is not $|x\rangle$. The H_{prop} (green) gives penalty if the computation does not follow the quantum circuit.

On the clock register, the action of $H_{prop,t}$ is restricted to a 2-dimensional subspace span$\{|t\rangle, |t+1\rangle\}$. With this in mind, we can re-write it as

$$H_{prop,t} = \begin{pmatrix} I & -U_t^\dagger \\ -U_t & I \end{pmatrix}. \tag{4}$$

We can show by direct calculation that $H/2$ is a projection, and its kernel can be written as span$\{\frac{1}{\sqrt{2}}(|t\rangle |\psi\rangle + |t+1\rangle U_t |\psi\rangle)\}$. Inspired by the expression of the kernel, we can also view $H_{prop,t}$ in a rotated basis. Let

$$R_t = |t\rangle\langle t| \otimes I + |t+1\rangle\langle t+1| \otimes U_t^\dagger = \begin{pmatrix} I & 0 \\ 0 & U_t^\dagger \end{pmatrix}. \tag{5}$$

Then we have

$$R_t \cdot \frac{H}{2} \cdot R_t^\dagger = |-\rangle\langle -| \otimes I. \tag{6}$$

That is, in this rotated basis $H_{prop,t}$ is enforcing a uniform superposition on the clock register.

We can generalize this rotation to the entire H_{prop}. Consider the unitary

$$R = \sum_{t=0}^{T} |t\rangle\langle t|_C \otimes U_0^\dagger U_1^\dagger U_2^\dagger \dots U_t^\dagger. \tag{7}$$

Similar to the above calculation, we can show that

$$R(H_{init} + H_{prop})R^\dagger = H_{init} + \tilde{H}_{prop}, \tag{8}$$

where

$$\tilde{H}_{prop} = \sum_{t=0}^{T-1} \underbrace{\Big(|t\rangle\langle t|_C + |t+1\rangle\langle t+1|_C - |t+1\rangle\langle t|_C - |t\rangle\langle t+1|_C \Big)}_{2|-\rangle\langle -| \text{ acting on span}\{|t\rangle, |t+1\rangle\}}. \tag{9}$$

$\tilde{H}_{prop}$ only acts nontrivially on the clock register, and it's easy to see that its unique ground state is

$$|\Omega\rangle_C = \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle_C .$$

Now, if there is a state that is in the common zero-eigenspace of H_{init} and $\tilde{H}_{prop}$, that state must be of the form $|\Omega\rangle_C \otimes |\text{else}\rangle$. Combining this fact with the expression of H_{init}, we conclude that the input register must be $|x\rangle$. Overall, the ground space of $H_{init} + \tilde{H}_{prop}$ can be completely characterized as

$$\text{span}\left\{ \frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle_C \otimes |x\rangle \otimes |\psi\rangle \,\middle|\, \forall\, |\psi\rangle \right\}. \tag{10}$$

Applying $R^\dagger$ to the above expression gives Eq. (2).

In order to lower bound the energy of any state orthogonal to the ground space, we can again focus on the Hamiltonian in the rotated basis $H_{init} + \tilde{H}_{prop}$. Note that there is a way to interpret $\tilde{H}_{prop}$ as a random walk on a line, which has a spectral gap of $\Omega\left(\frac{1}{T^2}\right)$. The spectral gap of H_{init} is 1. It can be argued that the overall spectral gap is the minimum of the two, as stated in the claim. Full details can be found in Section 5 of this survey. $\square$

Completeness. Now, we show the first part of Theorem 2.1. Suppose there is a state $|\psi\rangle$ such that probability of output 1 is at least $1 - e^{-\Theta(|x|)}$, or equivalently, the probability of output 0 is at most $e^{-\Theta(|x|)}$. Consider the history state $\frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle_C \otimes (U_t U_{t-1} \ldots U_1 U_0 |x\rangle \otimes |\psi\rangle)$. Since its energy with $H_{init} + H_{prop}$ is already 0, we just need to show that its energy with H_{out} is small too. Consider

$$\begin{aligned}
&\left(\frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} \langle t|_C \otimes \left(\langle x| \otimes \langle\psi| U_0^\dagger \ldots U_t^\dagger\right)\right) H_{out} \left(\frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle_C \otimes (U_t U_{t-1} \ldots U_1 U_0 |x\rangle \otimes |\psi\rangle)\right) \\
&= \frac{1}{T+1} \left(\langle x| \otimes \langle\psi| U_0^\dagger U_1^\dagger \ldots U_T^\dagger\right) |0\rangle\langle 0|_O \left(U_T U_{t-1} \ldots U_1 U_0 |x\rangle \otimes |\psi\rangle\right) \\
&= \frac{\Pr[output = 0]}{T+1} \leq \frac{e^{-\Theta(|x|)}}{T+1},
\end{aligned}$$

where the first equality uses the fact that only $t = T$ counts in H_{out}. Thus, the ground energy of $H_{in} + H_{out} + H_{prop}$ is less than $\frac{e^{-\Theta(|x|)}}{T+1}$.

Soundness. Next, we show that if the probability to output 0 is at least $1 - e^{-\Theta(|x|)}$ for all $|\psi\rangle$, then the ground energy of $H_{in} + H_{out} + H_{prop}$ is larger than $\Omega\left(\frac{1}{T^3}\right)$. We will give a sketch and the full proof can be found in Section 5 of this survey. Suppose a quantum state $|\omega\rangle$ has energy at least $\frac{1}{100T^3}$ with respect to $H_{init} + H_{prop}$, then we are done (as the energy of any state with respect to H_{out} is non-negative). So lets assume that the energy of $|\omega\rangle$ is at most $\frac{1}{100T^3}$ with respect to $H_{init} + H_{prop}$. Then from Claim 2.2, $|\omega\rangle$ can't be orthogonal to the ground space of $H_{init} + H_{prop}$. In fact, we can argue that the fidelity of $|\omega\rangle$ with some state of the form $\frac{1}{\sqrt{T+1}} \sum_{t=0}^{T} |t\rangle_C \otimes (U_t U_{t-1} \ldots U_1 U_0 |x\rangle \otimes |\psi\rangle)$ must be at least $1 - \frac{1}{100T}$. This means that the energy difference between the two states with respect to H_{out} is at most $\frac{1}{100T}$. Now consider the energy:

$$\left(\frac{1}{\sqrt{T+1}}\sum_{t=0}^{T}\langle t|_C \otimes \left(\langle x| \otimes \langle \psi| U_0^\dagger \ldots U_t^\dagger\right)\right) H_{out} \left(\frac{1}{\sqrt{T+1}}\sum_{t=0}^{T}|t\rangle_C \otimes (U_t U_{t-1} \ldots U_1 U_0 |x\rangle \otimes |\psi\rangle)\right)$$
$$= \frac{1}{T+1}\left(\langle x| \otimes \langle \psi| U_0^\dagger U_1^\dagger \ldots U_T^\dagger\right) |0\rangle\langle 0|_O \left(U_T \ldots U_1 U_0 |x\rangle \otimes |\psi\rangle\right)$$
$$= \frac{\Pr[output = 0]}{T+1} \geq \frac{1-e^{-\Theta(|x|)}}{T+1} \geq \frac{1}{2T}.$$

Thus the energy $\langle\omega| H_{out} |\omega\rangle \geq \frac{1}{2T} - \frac{1}{100T} = \Omega(\frac{1}{T})$. Thus, the theorem concludes. $\square$

Locality. The astute reader will have noticed that the Hamiltonian we constructed is *not* necessarily local if expressed in terms of qubits. This is because of the clock states: a term $|t+1\rangle\langle t|_C$, if the clock states are encoded in qubits using a binary encoding, can have locality up to $O(\log T)$. The way around this used by Kitaev is to encode the clock in *unary* using T qubits.

$$\begin{aligned}
|0\rangle_C &= |000\ldots 0\rangle \\
|1\rangle_C &= |100\ldots 0\rangle \\
|2\rangle_C &= |110\ldots 0\rangle \\
&\ldots \\
|T\rangle_C &= |111\ldots 1\rangle .
\end{aligned}$$

A propagation term $|t+1\rangle\langle t|$ can now be encoded as a three-local operator:

$$|t+1\rangle\langle t|_C \mapsto I_{1,\ldots,t-1} \otimes |110\rangle\langle 100|_{t,t+1,t+2} \otimes I_{t+3,\ldots,T}.$$

Now, if we do this, we have the problem that not all possible states of the clock qubits are valid unary encodings of some time. We need to rule out the "bad" clock states. This we can do with some additional "format" terms in the Hamiltonian, that force the state to be a unary encoding, by placing an energy penalty on a 1 following a 0:

$$H_{\text{format}} = \sum_t |01\rangle\langle 01|_{t,t+1} .$$

It can be checked that the Hamiltonian does not mix good with bad clock states, and that all bad clock states incur a penalty of at least 1, so the ground energy in the NO case is still $\Omega(1/T^3)$ as desired. (See Kitaev, Shen, and Vyalyi, Chapter 14 for all the gory details.)

3 Hamiltonians and dynamics

Behold the Schrödinger equation:

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H(t)|\psi(t)\rangle . \tag{11}$$

If H is independent of time, this has a simple solution:

$$|\psi(t)\rangle = e^{-iHt/\hbar}|\psi(0)\rangle . \tag{12}$$

Up till now, we have studied only the "static" properties of the Hamiltonian, namely the *ground state* and its ground energy. We have shown that these ground states can encode the results of quantum computations. But what about "dynamic" properties of the Hamiltonian? Could the time-evolution of H encode a computation as well?

In fact, this is the question that Feynman asked back in the 80s, and to answer which he invented the clock construction. What Feynman showed is essentially the following theorem:

Theorem 3.1. *Let V be a quantum circuit on n qubits with $T = \mathrm{poly}(n)$ gates that we are promised either accepts or rejects with high probability, and let H_V be the associated Feynman-Kitaev Hamiltonian (with a little twist). Then there is an efficiently preparable initial state $|\psi_0\rangle$ such that we can determine whether V accepts or rejects by preparing $\mathrm{poly}(n)$ copies of*

$$e^{-iH_V T} |\psi_0\rangle ,$$

measuring them in the standard basis, and doing efficient post-processing.

Informally, the theorem is saying that "time evolution is BQP-hard". We won't prove this here but will give a sketch of why it is true. Essentially, the key fact that's used to prove this is that the propagation Hamiltonian (after the Kitaev basis change has been performed) describes particle freely moving along the line of clock states $0, \ldots, T$. To see this, imagine that the clock space is actually *infinite* dimensional, with integer times going from $-\infty$ to $+\infty$. Here, instead of propagating in *time*, we are instead propagating in *space*. The propagation Hamiltonian can be written as

$$H_{\text{prop}} = \sum_{x=-\infty}^{\infty} |x\rangle \left(2\langle x| - \langle x-1| - \langle x+1|\right) \tag{13}$$

$$|\psi\rangle = \sum_x \psi(x) |x\rangle \tag{14}$$

$$H_{\text{prop}} |\psi\rangle = \sum_x (2\psi(x) - \psi(x-1) - \psi(x+1)) |x\rangle . \tag{15}$$

Now, if you squint at this, this is actually the *discrete Laplacian* of ψ

$$\partial_x \psi(x) = \psi(x+1) - \psi(x) \tag{16}$$

$$\partial_x^\dagger \psi(x) = \psi(x-1) - \psi(x) \tag{17}$$

$$\begin{aligned} \Delta\psi(x) &= \partial_x^\dagger \partial_x \psi(x) && (18)\\ &= \partial_x \psi(x-1) - \partial_x \psi(x) && (19)\\ &= \psi(x) - \psi(x-1) - \psi(x+1) + \psi(x) && (20)\\ &= 2\psi(x) - \psi(x-1) - \psi(x+1). && (21) \end{aligned}$$

So we can wave our hands and think about the *continuum limit*

$$H_{\text{prop}} = -\partial_x^2.$$

It's easy to see that this Hamiltonian has plane wave eigenstates

$$\begin{aligned}
\left|\hat{k}\right\rangle &= \sum_x e^{ikx} \left|x\right\rangle \\
H\left|\hat{k}\right\rangle &= \sum_x k^2 e^{ikx} \left|x\right\rangle = k^2 \left|\hat{k}\right\rangle \\
e^{-iHt}\left|\hat{k}\right\rangle &= e^{-ik^2 t} \left|\hat{k}\right\rangle \\
&= \sum_x e^{i(kx-k^2 t)} \left|x\right\rangle .
\end{aligned}$$

This is a plane wave moving to the right with speed k. If we prepare a wave packet, it's group velocity is 2. So intuitively we have the following:

- First, pad the circuit V with identity gates at either end.
- Next, prepare $|\psi_0\rangle$ to be a wavepacket state concentrated in the clock register around the "runway" of initial timesteps where the circuit has identity gates, in tensor product with the all-zeros state on the computational register.
- Evolve for time $T/2$. Then the wavepacket's center will be around the final time. It will be highly spread out though.
- Measure: if we get a clock state in the final time range, then read off the answer to the computation. Otherwise, discard the measurement outcome. This is why we need poly(n) copies of our state.