# Ph/CS 219A
# Quantum Computation

## Lecture 18. QMA-completeness of the local Hamiltonian problem

Last time we saw how a quantum computer can efficiently simulate time evolution governed by a local Hamiltonian, and can also efficiently estimate energy eigenvalues of a local Hamiltonian, for energy eigenstates that can be efficiently prepared.

We expect, though, that for some local Hamiltonians preparing particular energy eigenstates (like ground states) is hard even for a quantum computer. In fact, something analogous is true even for classical systems --- preparing the ground state of a classical *spin glass* is known to be NP-hard in general. For quantum local Hamiltonians, preparing the ground states is QMA-hard, hence even harder than the classical case, if (as we expect) QMA is strictly larger than NP.

Is this a roadblock to efficient simulation of the physical world using quantum computers? Perhaps not; if a quantum computer cannot prepare the ground state, it is likely that no naturally occurring process can solve the state preparation problem either!

*Updated Chapter 6 Lecture Notes have been posted on the course website. This lecture aligns with Sec. 6.10 of Chapter 6. Problems Set 4 is due on December 4.*

# 3-SAT is NP-complete

It can be NP-hard to find the ground state of a classical local Hamiltonian (“spin glass”). Nature cannot solve it in polynomial time, and neither can we.

Problem in NP, instance *x*. Is there are witness *y* accepted by verifier circuit V(*x*,*y*)?

1) Any problem in NP reduces to CIRCUIT-SAT (CIRCUIT-SAT is NP-complete).
2) CIRCUIT-SAT reduces to 3-SAT (3-SAT is NP-complete)
3) 3-SAT reduces to computing the ground-state energy of a classical 3-local Hamiltonian to constant accuracy.
4) MAX 2-SAT is NP-hard, reduces to computing ground-state energy of classical 2-local Hamiltonian to constant accuracy.
5) Still NP-hard if the Hamiltonian is geometrically local in 2 or more dimensions (“real spin glasses”).

$k-\mathrm{SAT\ Problem}:$

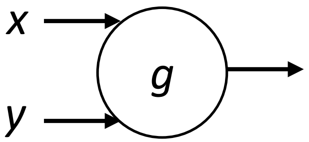
Boolean formula $f = \wedge_a C_a$, clause $C_a$ depends on $k$ variables.

$\mathrm{SAT}(f) = 1$ iff $f(x) = 1$ (all clauses satisfied) for some $x$.

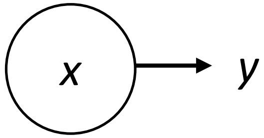
Reduction of CIRCUIT-SAT to 3-SAT: Given circuit *C*, find Boolean formula *R(C)* such that there is an input accepted by *C* iff there is a satisfying assignment for the formula *R(C)*.

# 3-SAT is NP-complete

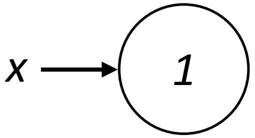
Reduction of CIRCUIT-SAT to 3-SAT: Given circuit *C*, find Boolean formula *R(C)* such that there is an input accepted by *C* iff there is a satisfying assignment for the formula *R(C)*.




$C_g(x,y,z) = 1 \text{ iff } \; z = g(x,y).$ Checks that gate *g* is executed correctly.




$C_x(y) = 1 \text{ iff } \; y = x.$ Checks that input bit is correct.



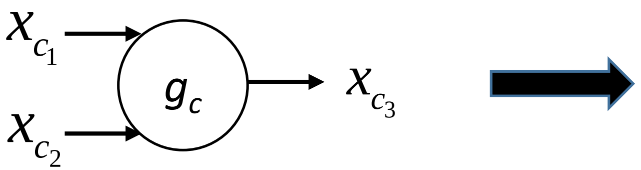

$C_1(x) = 1 \text{ iff } \; x = 1.$ Checks that answer bit is one.

Variables are input bits and output bits to each gate in the circuit *C*. The formula *R(C)* contains a clause corresponding to each gate (number of clauses = poly(*n*)), which evaluates to true if the gate is executed correctly.

The witness for the 3-SAT formula is an assignment that satisfies all clauses, including the clause that checks the answer bit to verify the input is accepted --- a *history* of the entire computation that can be checked *locally*. 3-SAT because 2→1 gates are universal.

# 3-SAT as a Hamiltonian

Finding the minimum energy of a 3-local classical Hamiltonian is NP-hard:




$$H(x)=\sum_c H_c(x_{c_1},x_{c_2},x_{c_3}),\quad H_c=0 \text{ if true},\quad H_c=1 \text{ if false}$$

$$\Rightarrow\quad \min_x H(x)=0 \text{ iff } \exists \text{ satisfying assignment, else } \min_x H(x)\geq 1.$$

Ising spin-glass. NP-hard in $D \geq 2$ spatial dimensions. Cf. MAX 2-SAT.

$$H=-\sum_{\langle ij\rangle} J_{ij}Z_iZ_j-\sum_i h_iZ_i,\quad Z_i\in\{-1,1\},\quad J_{ij}\in\{-1,0,1\},\quad h_i\in\{-1,0,1\},\quad \langle i,j\rangle \text{ denotes nearest neighbors.}$$

Antiferromagnetic edges ($J$ = -1) and local magnetic field cause *frustration*. There are many local minima of the energy, so the global minimum may be hard to find.

For a quantum local Hamiltonian problem, finding the ground state may be even more difficult, because different terms in the Hamiltonian may fail to commute with one another, further compounding the frustration.

Indeed, while the classical problem is NP-hard, the quantum problem is QMA-hard, hence even harder than the classical problem if (as expected), QMA $\neq$ NP.

# Quantum *k*-local Hamiltonian problem

*k*-local Hamiltonian: a sum of terms, each with bounded operator norm and acting on $\leq k$ qubits.

$$H = \sum_a H_a, \quad H_a \text{ acts on } \leq k \text{ qubits}, \quad \|H_a\| \leq h.$$

Promise: Ground-state energy $E_0$ satisfies either $E_0 \leq E_{\text{low}}$, or $E_0 > E_{\text{high}}$, where $E_{\text{high}} - E_{\text{low}} > 1/\text{poly}(n)$.

$$f(H) = \begin{cases} 1 & \text{if } E_0 \leq E_{\text{low}}, \\ 0 & \text{if } E_0 > E_{\text{high}}. \end{cases}$$

Finding the ground state energy $E_0$ to accuracy 1/poly(*n*) would suffice to solve the problem.

We wish to show that 5-local Hamiltonian is a QMA-complete problem:
(1) *k*-local Hamiltonian is in QMA.
(2) Any problem in QMA reduces to 5-local Hamiltonian.
(Can be improved to geometrically local 2-local Hamiltonian, but we won't show that today.)

Idea (following the classical case):
A problem in QMA has a quantum verifier circuit, which for instance *x* accepts some quantum witness iff *x* is in language *L*.

We'll construct a local Hamiltonian *H*, that checks each gate of this quantum circuit. The witness is the ground state of *H,* which has low energy iff the verifier circuit accepts the witness with high probability.

# History state

We wish to show that 5-local Hamiltonian is a QMA-complete problem:
(1) *k*-local Hamiltonian is in QMA.
(2) Any problem in QMA reduces to 5-local Hamiltonian.

We already showed part (1) in the previous lecture. The quantum witness is the ground state of the local Hamiltonian *H*. We have seen that a size poly(*n*) quantum circuit can measure the energy of a local Hamiltonian to accuracy 1/poly(*n*).

For part (2). Merlin provides a quantum state that encodes the *history* of the verifier computation that accepts the witness for the QMA problem. We will construct a Hamiltonian *H* that checks the history: the history state is a low energy state of *H* if and only if the history is valid and accepts the witness.

History state:

$$|\eta\rangle = \frac{1}{\sqrt{T+1}}\sum_{t=0}^{T}|\psi(t)\rangle\otimes|t\rangle, \quad |\psi(t)\rangle = (U_t U_{t-1}..U_1)|\psi_{\text{witness}}\rangle.$$

The “clock” $|t\rangle$ keeps track of “time”: the quantum gate $U_t$ is applied at step $t$.

Local Hamiltonian:

$$H = H_{\text{in}} + H_{\text{out}} + H_{\text{prop}} + H_{\text{clock}}$$

$H_{\text{in}}$ fixes input bits (other than witness), $H_{\text{out}}$ checks answer bit, $H_{\text{clock}}$ enforces encoding of clock, $H_{\text{prop}}$ penalizes incorrect quantum gates.

# Spectrum of $H_{\text{prop}}$

$$|\eta\rangle = \frac{1}{\sqrt{T+1}}\sum_{t=0}^{T}|\psi(t)\rangle\otimes|t\rangle, \quad |\psi(t)\rangle = (U_t U_{t-1}\ldots U_1)|\psi_{\text{witness}}\rangle, \quad H = H_{\text{in}} + H_{\text{out}} + H_{\text{prop}} + H_{\text{clock}}.$$

$$H_{\text{prop}} = \sum_{t=1}^{T} H_{\text{prop}}(t), \quad H_{\text{prop}}(t) = \frac{1}{2}\Big(I\otimes|t\rangle\langle t| + I\otimes|t-1\rangle\langle t-1| - U_t\otimes|t\rangle\langle t-1| - U_t^\dagger\otimes|t-1\rangle\langle t|\Big).$$

$$H_{\text{prop}} :|\psi(t-1)\rangle\otimes|t-1\rangle \mapsto \frac{1}{2}\big(|\psi(t-1)\rangle\otimes|t-1\rangle - U_t|\psi(t-1)\rangle\otimes|t\rangle + \ldots\big),$$

$$H_{\text{prop}} :|\psi(t)\rangle\otimes|t\rangle \mapsto \frac{1}{2}\Big(|\psi(t)\rangle\otimes|t\rangle - U_t^\dagger|\psi(t)\rangle\otimes|t-1\rangle + \ldots\Big).$$

Cancellation:

$H_{\text{prop}}|\eta\rangle = 0$ if $|\eta\rangle$ is a valid history state.

All other energy eigenstates of $H_{\text{prop}}$ have positive energy. Make a unitary change of basis:

$$V = \sum_{t=0}^{T} U_t U_{t-1}\cdots U_1\otimes|t\rangle\langle t| \quad \Rightarrow \quad H'_{\text{prop}} = V^\dagger H_{\text{prop}} V = \sum_{t=1}^{T}\frac{1}{2}\Big(|t\rangle\langle t| + |t-1\rangle\langle t-1| - |t\rangle\langle t-1| - |t-1\rangle\langle t|\Big).$$

Easy to diagonalize (details in notes):

$$|\psi_k\rangle = \sum_{t=0}^{T}\cos\left(\omega_k\left(t+\frac{1}{2}\right)\right)|t\rangle, \quad \omega_k = \frac{\pi}{T+1}k \text{ for } k\in\{0,1,2,..,T\}, \quad E_k = 2\sin^2\omega_k$$

$$\Rightarrow \quad E_1 - E_0 = 2\sin^2\left(\frac{\pi}{2(T+1)}\right) \approx \frac{\pi^2}{2(T+1)^2} = \frac{1}{\text{poly}(n)}.$$

# Checking the answer bit

$$|\eta\rangle = \frac{1}{\sqrt{T+1}}\sum_{t=0}^{T}|\psi(t)\rangle\otimes|t\rangle, \quad |\psi(t)\rangle = (U_t U_{t-1}\ldots U_1)|\psi_{\text{witness}}\rangle, \quad H = H_{\text{in}} + H_{\text{out}} + H_{\text{prop}} + H_{\text{clock}}$$

$$H_{\text{out}} = (|0\rangle\langle 0|)^{(\text{output})}\otimes I^{(\text{else})}\otimes(|T\rangle\langle T|)^{(\text{clock})}.$$

Penalty if the answer bit at time $T$ is 0 instead of 1.

If the verifier accepts with probability 1-$\varepsilon$:

$$E_0 \le \langle\eta|H_{\text{out}}|\eta\rangle = \frac{\varepsilon}{T+1}.$$

(We could make this a constant (not dependent on $T$) by padding the history with $\approx T$ additional time steps in which answer stays fixed.)

Furthermore, we can make $\varepsilon$ very small by amplifying, checking multiple copies of the witness.

Now $H = H_1 + H_2$, where $H_1 = H_{\text{in}} + H_{\text{out}}$, $H_2 = H_{\text{prop}}$ (ignore clock Hamiltonian for now).
Both $H_1$ and $H_2$ are nonnegative, and both have null vectors (eigenstates with zero eigenvalue).
These null spaces do not align perfectly if $\varepsilon > 0$ --- a valid history that is accepted with probability = one would be in both null spaces.

Gap for $H_1 = 1$, gap for $H_2 = 2\sin^2(\pi^2/(T+1)^2)$.

From bound on expectation $H_1$ of for states in the null space of $H_2$, we can bound expectation of $H$:

$$E_0 \ge 4\sin^2\left(\frac{\pi}{2(T+1)}\right)\times\frac{1}{4}\left(\frac{1-\sqrt{\varepsilon}}{T+1}\right) \ge \sin^2\left(\frac{\pi}{2(T+1)}\right)\times\left(\frac{1-\sqrt{\varepsilon}}{T+1}\right) \ge \text{constant}\times\frac{1-\sqrt{\varepsilon}}{(T+1)^3} = \frac{1-\sqrt{\varepsilon}}{\text{poly}(n)}$$

for acceptance probability $\varepsilon$ (details in notes).

# Encoding the clock

"Unary" encoding with $T$ qubits: $|t=0\rangle = |000..0\rangle, \quad |t=1\rangle = |100..0\rangle, \quad |t=2\rangle = |110..0\rangle, \quad |t=3\rangle = |1110\ldots0\rangle, \ldots$

Penalize clock states where a 1 follows a 0: $H_{\text{clock}} = \sum_{i=1}^{T-1} \left(|01\rangle\langle 01|\right)_{i,i+1}.$

Acting on validly encoded clock states:

$$|t\rangle\langle t| = (|10\rangle\langle 10|)_{t,t+1}, \quad |t\rangle\langle t-1| = (|110\rangle\langle 100|)_{t-1,t,t+1}, \quad |t-1\rangle\langle t| = (|100\rangle\langle 110|)_{t-1,t,t+1}.$$

(2-local and 3-local). Therefore $H_{\text{prop}}$ is 5-local: $U_t \otimes |t\rangle\langle t-1| + h.c.$ acts on 5 qubits, and

$H = H_{\text{in}} + H_{\text{out}} + H_{\text{prop}} + H_{\text{clock}}$ is 5-local; estimating its ground state energy to 1/poly(n) accuracy is QMA-hard.

We can make it geometrically nonlocal by encoding the clock more cleverly, and with further tricks we can show that the 2-local Hamiltonian problem is QMA-complete, for geometrically local 2D qubit systems, or for geometrically local 1D chains of higher dimensional systems.

Not only that, but for *translation-invariant* geometrically local quantum systems in 1D, whether the spectral gap (energy gap between ground state and first excited state) tends to zero as the system size get large is a *Turing undecidable* problem!

# Other Courses

Ph/CS 219B next term. Professor Kitaev. (Some years we do 219C, too.)

CS/Ph 120 Quantum cryptography.

APh/Ph 138AB Quantum hardware and techniques.

APh/ME 201 Physics on near-term quantum computers.

Special topics classes.

Quantum Science and Engineering (QSE) minor.