Computational complexity theory + physics

Classical complexity theory, informal definitions:

• \( P \) = problems solvable in polynomial time on a deterministic Turing machine.
  Example: Two \( n \times n \) matrices over a constant-size finite field can be multiplied in \( O(n^{2.376}) \) time = \( \text{poly}(n) \).

• \( \mathbf{NP} \) = "nondeterministic polynomial time" = yes/no problems where each yes instance has a proof that can be verified in polynomial time (\( \text{poly} \) in the size of the problem instance/input).

Example: Is there a \( \leq n \)-page proof of claimed mathematical statement?

Example: 3-SAT: Given a formula

\[ \psi(x) = (x_1 \lor \overline{x}_1 \lor x_2) \land (x_2 \lor \overline{x}_4 \lor \overline{x}_6) \land \ldots \]

is there a boolean assignment to \( x_1, \ldots, x_n \) that satisfies all the clauses?

(Given a proof, it is easy to check, but finding the proof may be hard.)

• \( \mathbf{NP} \)-complete: hardest problems in \( \mathbf{NP} \), in a rigorous sense: for any other \( \mathbf{NP} \) problem, an instance can be turned into an instance of the \( \mathbf{NP} \)-complete problem in polynomial time.

Cook-Levin Theorem: 3-SAT is an \( \mathbf{NP} \)-complete problem.

Furthermore, Max 2-SAT is also \( \mathbf{NP} \) complete:

Given \( k \), and a formula \((x_1 \lor \overline{x}_2) \land (x_2 \lor \overline{x}_4) \land (x_3 \lor \overline{x}_1) \land \ldots\)

is there an assignment satisfying \( k \) of the clauses?

Classical condensed-matter physics also studies these constraint-satisfaction problems:

• Spin glass = weighted max 2-SAT problem with geometric locality on the constraints (frustrated magnet models)

- Survey propagation algorithm [05/02/2002] generalizes belief propagation (from statistical learning theory) — best current algorithm for random \( k \)-SAT.
Quantum complexity theory:
- BQP = "bounded-error quantum polynomial time" = problems solvable in polynomial time on a quantum computer, with error probability $\leq \frac{1}{10}$.
- QMA = like NP, problems with an efficiently verifiable proof, except the proof and verifier can both be quantum (i.e., a quantum state & a quantum computer), and error probability $\leq \frac{1}{10}$ is allowed.

conjectured relationships between these classes

classical constraint satisfaction problems $\leftrightarrow$ quantum Hamiltonian complexity
**Def.** A Hamiltonian is a Hermitian matrix, $H = H^\dagger$. Its (real) eigenvalues are called energy levels.

**Schrödinger’s equation:** The evolution of a closed quantum system is determined by a Hamiltonian $H$:

$$\frac{d}{dt} |\psi(t)\rangle = -i \ H \ |\psi(t)\rangle$$

⇒ For a time-independent Hamiltonian,

$$|\psi(t)\rangle = e^{-i \ H \ t} |\psi(0)\rangle$$

(unitary)

For an $n$-qubit system, $H$ is a $2^n \times 2^n$ matrix—difficult even to write down. But physically, two-particle interactions are most likely, motivating:

**Def.** A $k$-local Hamiltonian is the sum of Hamiltonians, each of which acts as the identity on all but at most $k$ qubits.

**Ex.:** $H = H_{12}^{(2)} \otimes I_{345} + H_{14}^{(2)} \otimes I_{235} + H_{54}^{(2)} \otimes I_{123}$ is 2-local (no geometric locality is required).
Key physics problem: Understand the evolution of (open or closed) quantum systems. (Open system = one that interacts with an environment/bath)

1. For a closed quantum system, this is very difficult!

2. For an open quantum system (evolving, e.g., according to a Lindblad equation)

\[ \dot{\rho} = -i [H, \rho] + \sum_j \left( \frac{e - \rho A_j A_j^+ - e^{+} A_j^+ A_j}{\rho A_j A_j^+ + A_j^+ A_j} \right) \]

systems empirically tend to converge (at low temperatures) to the ground state of \( H \), i.e., the lowest eigenvalue eigenvector (or at inverse temperature \( \beta \), in general to the Gibbs state \( e^{-\beta H} \))

\[ \Rightarrow \text{a more approachable problem is "just" to determine the ground space, or low-energy eigenspaces for } H \]

- A problem for which quantum information techniques have proven very useful (e.g., DMRG — matrix product states)

What if we had quantum computers?

1. Simulating the dynamics of a quantum system with a local Hamiltonian is easy (although simulation understanding)

   a. If \( H \) acts on only a constant number of qubits, it is easy to apply \( e^{i H t} \) for any \( t \) — just move into a basis in which \( H \) is diagonal, apply \( \text{diag}(e^{i \lambda s}) \), and move back

   b. Lie-Trotter formula:

   \[ \| e^{i(H_1 + H_2)t} - (e^{i H_1 t/n} e^{i H_2 t/n})^n \| = O(\| [H_1, H_2] \| t) \]

   \[ \Rightarrow \ldots \Rightarrow \text{poly}(t, \# \text{ of terms in } H, \text{ max norm of a term}) \]

   e.g.

   break the evolution into four pieces
But finding the ground state, even of a local Hamiltonian, is not easy.

Theorem [Kitaev], last time:
It is a QMA-complete problem to decide
- Given an n-qubit $5$-local Hamiltonian, and
- thresholds $a < b$ (such that $b - a > \frac{1}{n}$) for each term $|i⟩$,
- is the ground-state energy $< a$ or is it $> b$?

(If it is between $a$ and $b$, algorithm cannot do anything.)
[Note: Given a purported ground state, it is easy to check the energy is low]

⇒ It is very unlikely that quantum computers can find
- ground states, or even ground-state energies,

- not necessarily a surprise, given NP-hardness of Max 2-SAT,
- a 2-local Hamiltonian problem (in which all the terms are
diagonal in the computational basis)

- in fact, the problem is QMA-complete even for 2-local
Hamiltonians with translation-invariant interactions in
two dimensions (see Gottesman, Irani 0905.2417), and
translation-invariant 1D 2-local Hamiltonians (on $>2$-dim.
systems, not qubits) suffice for universal adiabatic
computation (initial state encodes input)

⇒ what is it that makes physical systems tractable?
(beyond locality, dimensionality, translation invariance)
Should we care?

Construction was 5-local:
- 2 qubits for the gate, 3 for the clock
- $V_4 \otimes I_{t+1}X_{t+1} + V_4^* \otimes I_{t}X_{t+1}$

- represent 1st as $\underbrace{1_1\cdots 1}_{t}\underbrace{0\cdots 0}_{t+1}$, i.e., in memory
- $I_{t+1}X_{t}$, on valid clock states, is just $1101\cdots 0_{t+1, t+2}$ elsewhere
The locality of environmental noise processes is also what lets us protect quantum data, and to compute on it!

**Example:** Recall Shor's [[9, 1, 3]] QECC:

\[ 10\rangle = (1000\rangle + 1111\rangle)(1000\rangle + 1111\rangle)(1000\rangle + 1111\rangle) \]

\[ 11\rangle = (1000\rangle - 1111\rangle)(1000\rangle - 1111\rangle)(1000\rangle - 1111\rangle) \]

distance 3 \( \Rightarrow \) corrects any one-qubit error

Say the Hamiltonian is

\[ H = H_1 + H_2 + \ldots + H_q \]

\[ = \frac{1}{\sqrt{q}} \left( \frac{1}{2} H_1 \otimes 1_{q-1} + \frac{1}{2} 1_{1} \otimes H_2 \otimes 1_{q-2} + \ldots + 1_{1,\ldots,1} \otimes H_q \right) \]

\[ U(t) = \exp(-iHt) \]

\[ = \prod_{j=1}^{q} \left( e^{-iH_1 t} \otimes 1_{q-1} \right) \]

\[ = e^{-iH_1 t} \otimes e^{-iH_2 t} \otimes \cdots \otimes e^{-iH_q t} \]

\[ = (1 - iH_1 t) \otimes (1 - iH_2 t) \otimes \cdots \otimes (1 - iH_q t) + O((t^2)) \]

\[ = 1 - iH_1 t + O((t^3)) \]

\( \Rightarrow \) (ideal) error correction fixes all the first-order errors.

In fact, if we measure the syndrome during EC, then the first error is at fourth-order probability (squared amplitude)

"Quantum Zeno effect"

Unitary/coherent EC would not help against the 2-local Hamiltonian \( H = Z_3 \otimes Z_4 \) (although the Zeno effect would still suppress it, with measurements)