Quantum Complexity

Quantum complexity

P,NP and friends, Hamiltonians

PHYS/CSCI 3090

Prof. Alexandra Kolla

Alexandra.Kolla@Colorado.edu
ECES 122

Prof. Graeme Smith

Graeme.Smith@Colorado.edu
JILA S326

https://home.cs.colorado.edu/~alko5368/indexCSCI3090.html

Come see us!

- Alexandra Kolla/ Graeme Smith: Friday 3:00-4:00 pm, over zoom.
- Ariel Shlosberg: Tu/Th 2:00-4:00pm, over zoom
- Steven Kordonowy: Th 11am-12pm, over zoom.
- Matteo Wilczak: Wednesday, 1-2pm, over zoom.

Today

- Take home final coming up later today/early tomorrow.

Classical Complexity

- P: is a class of languages $L \subseteq (0, 1)^*$, decidable by a poly time deterministic Turing Machine.

$P \overset{?}{\neq} NP$

max cut, vertex cover, sat, sparsest cut, ...

- NP: is a class of languages $L \subseteq (0, 1)^*$, decidable by a poly time non-deterministic Turing Machine. Also, class of languages with short certificates.

Characterization of NP

φ_1 is sat. φ_2 is not | certificate for φ_1? a sat. assign

- L is an NP language if there is a poly time algorithm V(.,.) and a polynomial p s.t.

 x∈ L ⇔

$\exists y$, |y|≤p(|x|) $and\ V(x,y)\ accepts$

input ϕ → Algo → YES if $\phi \in L_{SAT}$ / NO $\phi_1 = (x_1 \vee x_2 \vee \bar{x}_3)$

- Alternatively,

 x∈ L ⇒ $\exists y$, $\boxed{|y|\le p(|x|)}$ $and\ V(x,y)\ accepts$ $x_1, x_2, x_3 \in \{0,1\}$

L_{SAT} = Language$_{SAT}$ = {set of formulas that are satisfied}

Q: is there an assignment to x_1, x_2, x_3 s.t. $C = 1$

 x∉ L ⇒ $\forall y$, |y|≤p(|x|) $V(x,y)\ rejects$

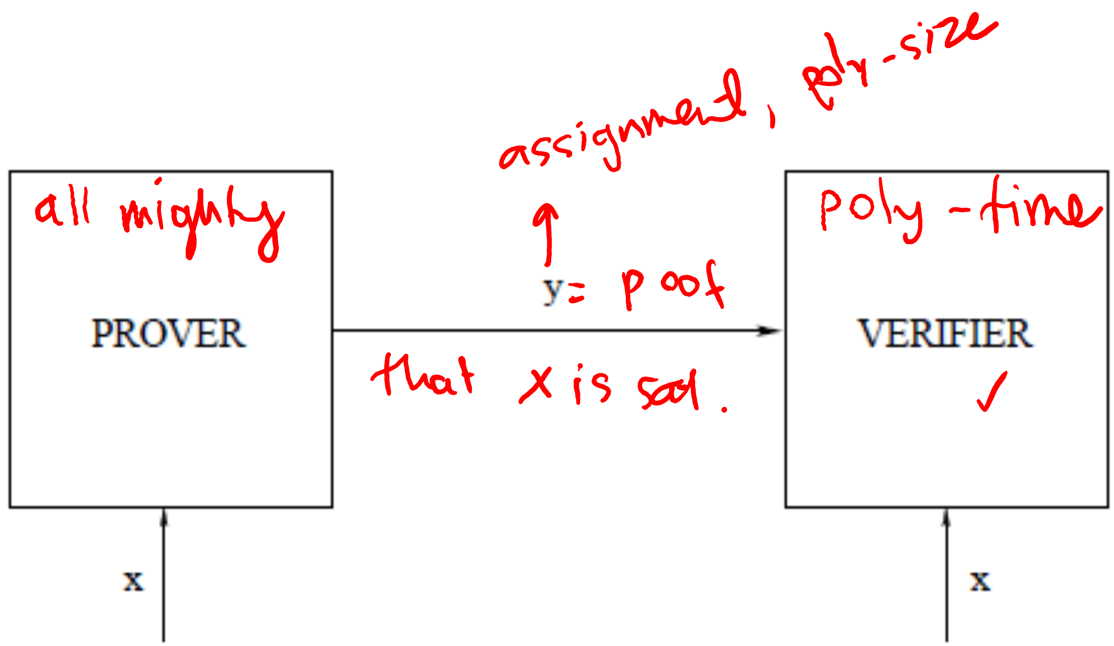
Completeness and soundness resp.

ex2: $\varphi_2 = (x_1) \wedge (\bar{x}_1)$ $\varphi_2 \notin L_{SAT}$

NP

- The class NP (non-deterministic polynomial time) contains many thousand of the most important computational problems.
- Of these problems, the vast majority are NP-complete. This means that these are the hardest problems in NP.
- By this we mean that, if anyone of them can be solved by a polynomial time algorithm, then every problem in NP can be solved by a polynomial time algorithm. The cornerstone of this theory of NP-completeness is the Cook-Levin theorem, which states that 3-SAT is NP-complete.

Prover /Verifier view of NP



X = formula, Q = $x \in L_{SAT}$?

Prover/verifier characterization of NP

- L is an NP language if there is a prover P and a poly time verifier (algorithm) V(.,.) p s.t.

$x \in L \Rightarrow$ P has strategy to convince V.

$x \notin L \Rightarrow$ P has no strategy to convince V.

- Strategy means the certificate of proof is polynomially small.

Example: 3SAT

- 3SAT (Satisfiability) definition:
- Input is a formula ϕ in 3-CNF form.
- E.g. $\phi = (x_1 \vee \overline{x_2} \vee x_{100}) \wedge (\overline{x_1} \vee x_5 \vee \overline{x_{10}}) \ldots (\overline{x_5} \vee x_1 \vee \overline{x_3}) \ldots$
- Each clause has three literals, and the formula is the "AND" of the clauses
- Q: when is the formula satisfied? $\Rightarrow$ if every c_i satisfied

$\phi = c_1 \wedge c_2 \wedge \ldots \wedge c_m$

$c_i = x_1^{(i)} \vee x_2^{(i)} \vee x_3^{(i)}$

literal = x_1 or $\overline{x_1}$

Example: 3SAT

- 3SAT (Satisfiability) definition:
- Input is a formula ϕ in 3-CNF form.
- E.g. $\phi = (x_1 \vee \overline{x_2} \vee x_{100}) \wedge (\overline{x_1} \vee x_5 \vee \overline{x_{10}}) \ldots (\overline{x_5} \vee x_1 \vee \overline{x_3}) \ldots$
- Each clause has three literals, and the formula is the “AND” of the clauses
- Q: Show that 3SAT is in NP

Example: 3SAT

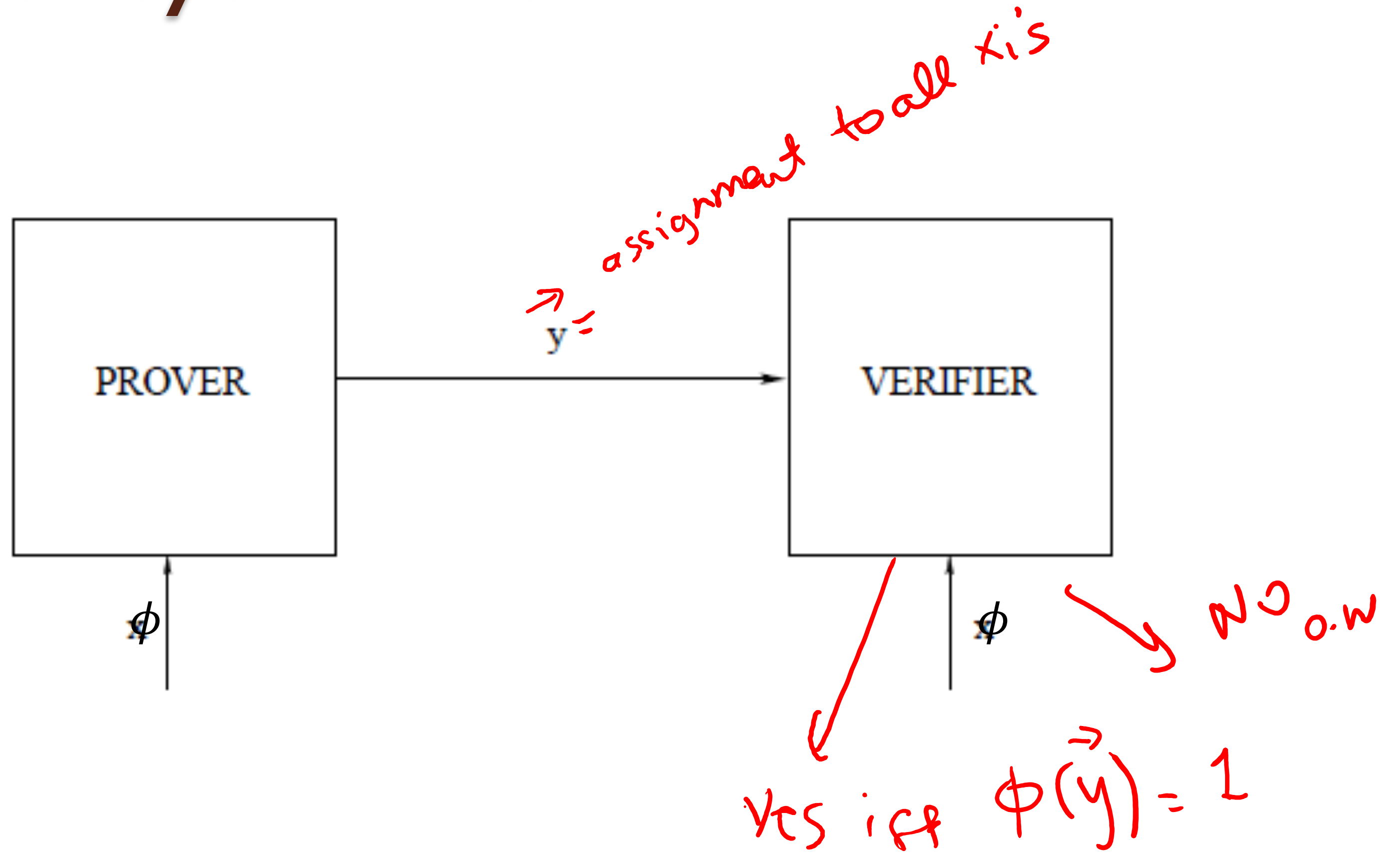
- 3SAT (Satisfiability) definition:
- Input is a formula ϕ in 3-CNF form.
- E.g. $\phi = (x_1 \vee \overline{x_2} \vee x_{100}) \wedge (\overline{x_1} \vee x_5 \vee \overline{x_{10}}) \ldots (\overline{x_5} \vee x_1 \vee \overline{x_3}) \ldots$
- Each clause has three literals, and the formula is the "AND" of the clauses
- Intuitively: 3SAT is NP-``hard"

Algo: check ~~all~~ possible assignments

$\phi \sim n$ variable)

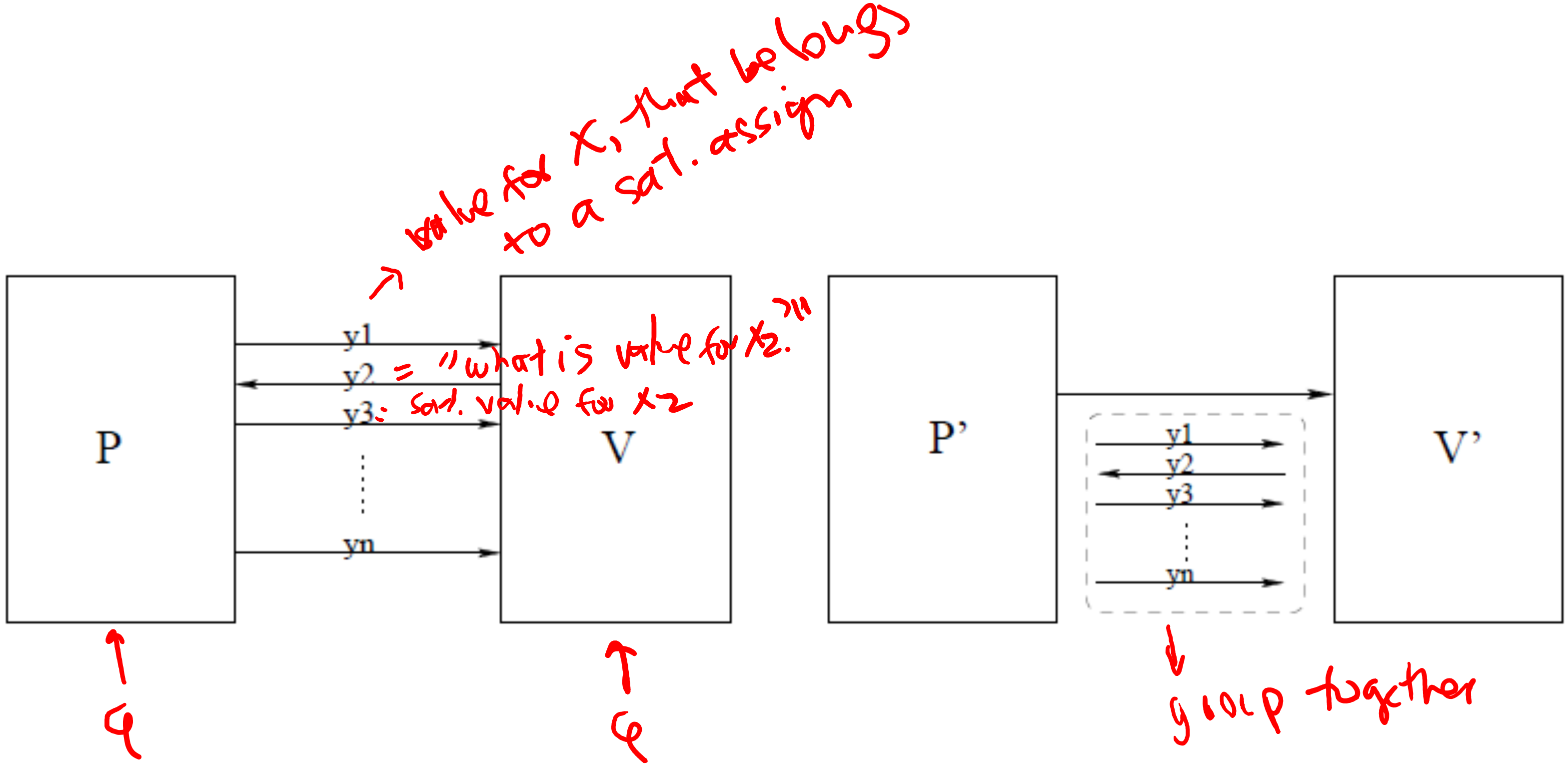
Time? 2^n exponential

Proof system for 3SAT



NP + interaction

- **Theorem**. NP+interaction =NP



NP + randomness

- **Definition**. L is in MA if there exists a probabilistic polynomial time machine V such that:

$$x \in L \Rightarrow \exists y \; Pr[V(x,y) \overset{=1}{accepts}] \geq \frac{2}{3}$$

$$x \notin L \Rightarrow \forall y \; \Pr[V(x,y) \; accepts] \leq \underset{=0}{\frac{1}{3}}$$

- It is conjectured that MA=NP.

① MA ⊇ NP ② NP ⊇ MA

- **Definition**. NP+randomness =MA

Hamiltonians

- Recall that one postulate of quantum mechanics is that the evolution of a closed quantum system is characterized by a unitary transformation. That is, the state $|\phi\rangle$ of the system at time t_1 is related to the state $|\phi'\rangle$ of the system at time t_2 by a unitary operation *U* which depends only on time t_1, t_2
- $|\phi'\rangle = U|\phi\rangle$
- Today we introduce a more refined version of this postulate, which describes the evolution of a quantum system in *continuous* time. It is stated as follows:
  The time evolution of a state of a closed quantum system is described by *Shrödinger's equation*:
- $i\frac{d|\phi\rangle}{dt} = H|\phi\rangle$
- *H* is a fixed Hermitian operator known as the Hamiltonian of the system. In specific, for an *n*-qubit system, its Hamiltonian *H* is a $2^n \times 2^n$ Hermitian matrix, i.e. $H = H^\dagger$.

Hamiltonians

- Suppose H has a spectral decomposition $H = \sum_j \lambda_j |e_j\rangle\langle e_j|$
with eigenvalues λ*j*'s and corresponding eigenvectors |*ej*⟩'s.
- The states |*ej*⟩'s are conventionally referred to as energy eigenstates, or stationary states, and λ*j* is the energy of the state |*ej*⟩.
- The lowest energy is known as the ground state energy for the system, and the corresponding energy eigenstate is known as the ground state.

$\lambda_1 < \lambda_2 \leq \lambda_3 \leq \ldots$

$|e_1\rangle$

Hamiltonians

- $H = \sum_j \lambda_j |e_j\rangle$
- Now suppose that at time t = 0 the initial state of the system is $|\phi(0)\rangle = |e_j\rangle$.
- Then a little calculus tells us that, at any time t, the system's state is given by $\boxed{|\phi(t)\rangle = e^{-i\lambda_j t}|e_j\rangle}$. So this explains why $|e\ j\rangle$ are also called stationary states: their only change in time is to acquires an overall numerical factor.

Hamiltonians

every state can be written like this

- Generally, suppose that at time $t = 0$ the initial state is $|\phi(0)\rangle = \sum_j \mu_j \left|e_j\right\rangle$, then at any time t the state of the system is given by $|\phi(t)\rangle = \mathrm{U(t)}|\phi(0)\rangle = \sum_j \mu_j e^{-i\lambda_j t} \left|e_j\right\rangle$
- Where $\mathrm{U(t)} = e^{-iHt} = \sum e^{-i\lambda_j t} \left|e_j\right\rangle\left\langle e_j\right|$

Local Hamiltonians

- Not all Hamiltonians can be easily implemented.
- The realistic Hamiltonians are local Hamiltonians.
- They are the Hamiltonian that can be written as a sum over many local interactions.

Local Hamiltonians

- Specifically, suppose for a system of *n* particles $H = \sum H_j$, where each *Hj* acts on at most a constant *c* number of particles (i.e. *Hj* = $Aj \otimes I$ for some *c*-particle operator *Aj*).
- Then we say that *H* is *c*-local.
- Such locality is quite physically reasonable, and originates in many systems from the fact that most interactions fall off with increasing distance of difference in energy.
- Local Hamiltonians and quantum circuits can (approximately) simulate each other with polynomial over- head.