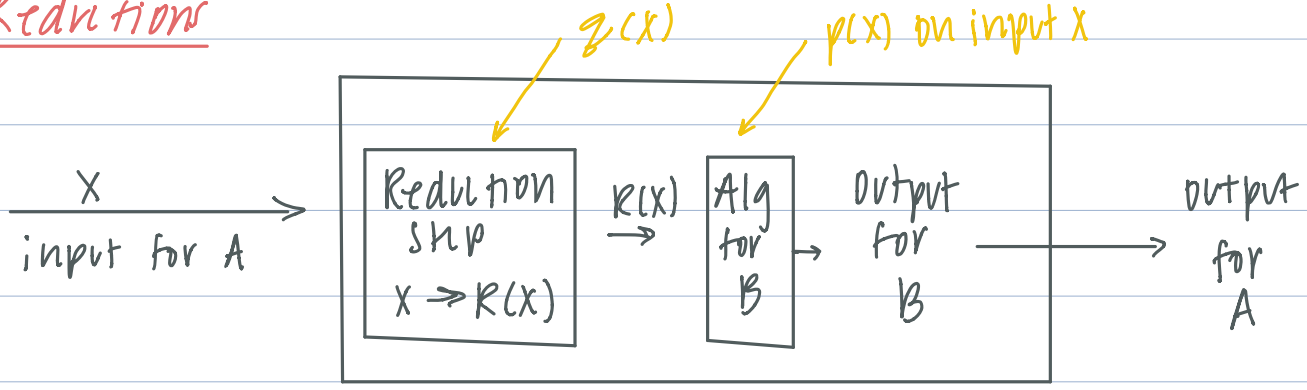
CS 124 Lecture 20 Mon, April 13, 2020

~ NP and Review ~

P = Poly-time = class of yes/no problems s.t. ∃ an algorithm A and a positive int k s.t. A solves the problem in time $O(n^k)$

Reductions



p(x) is poly ∴ B ∈ P

Time for A: $q(x) + p(|R(x)|) \rightarrow A \in P$.

★ $A \leq_p B$ if I can solve B, I can solve A
if A can't be solved in poly-time, neither can B

NP

Things I can "verify" in poly-time
class of yes/no problems s.t. if answer is yes, there is a short certificate that verifies it.

EX: For input X, there is a certificate (or hint) of length p(x) where p(x) is a polynomial.
There's a poly-time algorithm that takes as input X, hint(X) and returns YES if the answer is yes, NO otherwise.

* not symmetric → cannot hint NO

3SAT

Certificate: truth assignment

Algorithm: check the truth assignment

Composite

Certificate: factor

Algorithm: division algorithm

co-NP

Similar definition to NP but show NO instead of YES.

NP-Complete

"Hardest" (Reduction) set of problems?

- Are in NP
- All other problems reduce to it ← single problem at level

X is NPC if $\forall Y \in NP$ s.t. $Y \leq_p X$ and $X \in NP$

$A \leq_p B \leq_p C$ given B is NPC, C is NPC

$A \leq_p C$

Circuit-SAT

Cook's Theorem

Given a boolean circuit w/ some input values classified, is there a way to set the rest of the inputs so output

is true?

✓ In NP

- checking algo (can implement in poly-sized circuit)

  Inputs: original input to problem, corresponding certificate

  The Q: Is there a hint for Alg A ≡ Are there hint inputs s.t. the circuit outputs true

Circuit SAT $\leq_p$ 3-SAT would show Circuit SAT is NPC

Circuit C as input (known and unknown inputs w/ $\neg, \wedge, \vee$)

variable for each gate and each input

- if input is known: (X) if true, $(\bar{X})$ if false
- if input is unknown: free variable
- OR gate: $(\bar{y} \vee x) \wedge (\bar{z} \vee x) \wedge (\bar{x} \vee y \vee z)$

- AND gate: $(\bar{x} \vee y) \wedge (\bar{x} \vee z) \wedge (\bar{y} \vee \bar{z} \vee x)$
- NOT gate: $(\bar{x} \vee \bar{y}) \wedge (x \vee y)$

- output gate: (z)

Claim: Circuit has unknown inputs yielding true $\Longleftrightarrow$ 3SAT formula is satisfiable

3SAT $\leq_p$ Int Linear Program

* 3 sat formula to LP

$X \longrightarrow X$

$\bar{X} \longrightarrow 1 - X$

clauses → constraints

$(X \vee \bar{y} \vee z) \rightarrow X + (1-y) + (1-z) \geq 1$

1 = true, 0 = false all variables: $0 \le x \le 1$

optimize anything

Claim: ∃ solution to ILP $\iff$ 3SAT formula is satisfiable.

ILP $\in$ NP: certificate is simply values that satisfy constraints

3SAT $\le_p$ ISET

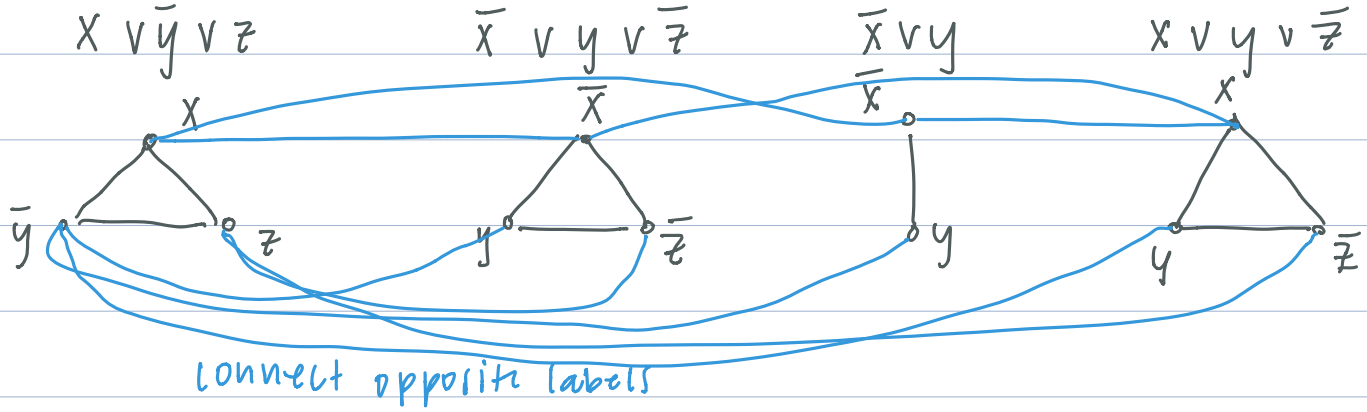
Independent set problem:

$G = (V, E)$ $S \subseteq V$ is an iset if $\forall (u,v) \in E$,

both u and v are not $\in S$.

Is there an independent set of size $\ge k$?

★ Gadgets to encode parts of the problem



Claim: if 3 SAT is solvable, ∃ ISET of size k = # clauses

- Pick one vertex from each clause that is true

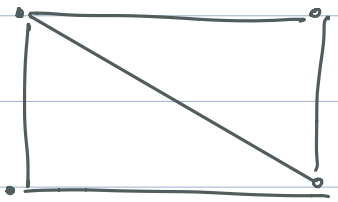
If ∃ ISET of size |clauses| then ∃ satisfying assignment for 3SAT

- at least one vertex per clause
- set vertex to true
- set remaining variables to arbitrary values

ISET $\leq_p$ VERTEX COVER

Vertex cover S for graph $G = (V, E)$ is a subset of vertices so that $\forall (u,v) \in E$ $u \in S$ or $v \in S$ or both

Is there a VC of size $\leq k$.



C is vertex cover, V-C is ISET

S is ISET, $\forall (u,v) \in E$, $u \in S$ or $v \in S$ or neither $\in S \rightarrow \forall (u,v)$ $v \in V-S$, $u \in V-S$ or both $\in V-S \rightarrow V-S$ is Vertex cover

ISET $\leq_p$ CLIQUE

Clique is FC set of vertices (subgraph of graph that is a clique of size $\geq k$)

Flip edges (connect vertices that are not connected and disconnect vertices that are connected).

Claim: Clique in G $\Leftrightarrow$ ISET in G' (complement of G)
of size $\geq k$ of size $\geq k$

P $\stackrel{?}{=}$ NP

checking and finding solutions are equally difficult
Find a poly-solution for a single NPC problem $\rightarrow$ solution for all of them