Lecture 20

CS 170

- NP Completeness
- Reductions

Sanjam Garg.

Search problems

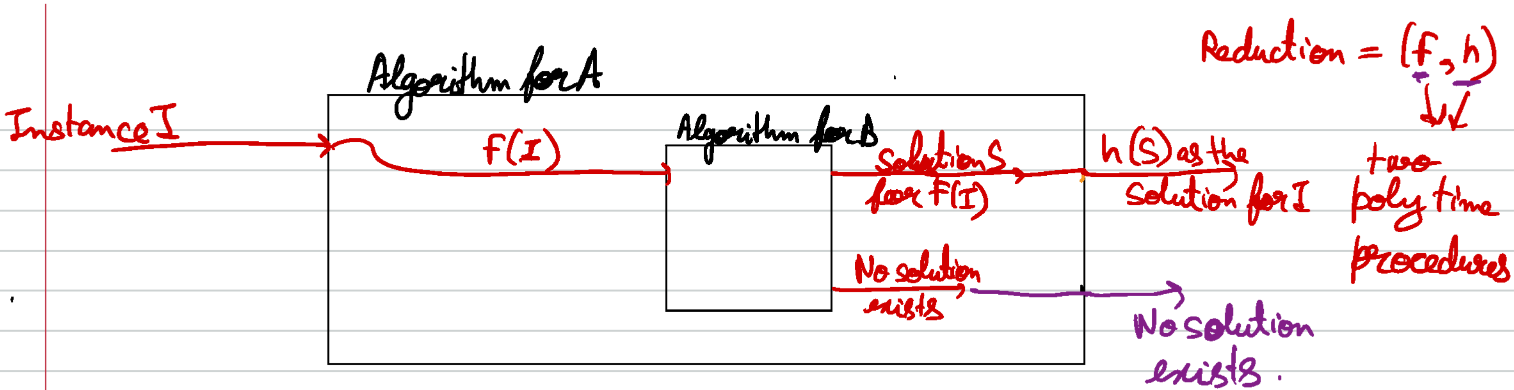
A search problem is specified by an algorithm VERIFY that takes two inputs, an instance I and a proposed solution S and runs in time polynomial in $|I|$.

We say that S is a solution to I if $\text{VERIFY}(I, S) = 1$

P : Class of search problems where we can **find** a solution in polynomial in $|I|$ time.

NP : Class of all search problems, i.e. the class of all problems where we can **verify** a solution in polynomial time

$P \subseteq NP$



1) Running time: f & h run in time polynomial in $|I|$
2) If B outputs S as a solution to $f(I)$ (under problem B) then $h(S)$ is a solution to I (under problem A)
3) If B outputs "no solution exists" then no solution to I exists either.

↳ if I has a solution then $f(I)$ also has a solution.

Composition of Reductions.

Lemma: If $A \xrightarrow{f_{AB}\ h_{AB}} B$ & $B \xrightarrow{f_{BC}\ h_{BC}} C$ then $A \to C$.

Proof: $f_{AC}(I) = f_{BC}(f_{AB}(I))$ $\qquad h_{AC}(S) = h_{AB}(h_{BC}(S))$

(s,t)-Rudrata Path $\longrightarrow$ Rudrata Cycle

(s,t)-Rudrata Path

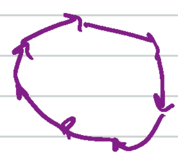
Input: $G = (V, E), s, t$

Solution: A path starting at s and ending at t that visits each vertex

Rudrata Cycle

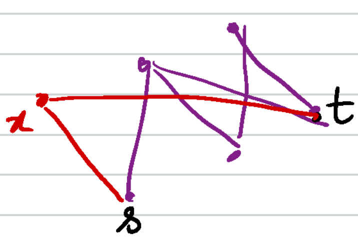
Input: $G = (V, E)$

Solution: a cycle that visits each vertex exactly once.



$f(G, s, t) = G'$ $\qquad G' = (V', E')$ $\qquad V' = V \cup \{x\}$

$E' = E \cup \{(x,s), (x,t)\}$

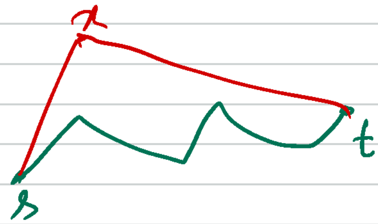


$h(\underset{\substack{\uparrow \\ \text{RC in } G'}}{C}) = C - \{(x,s), (x,t)\}$

1) Runtime of f & h

2) If S is a RC in G' then h(S) is a RP-(s,t) in G.

3) If G has a (s,t)-RP then G' has a RC.



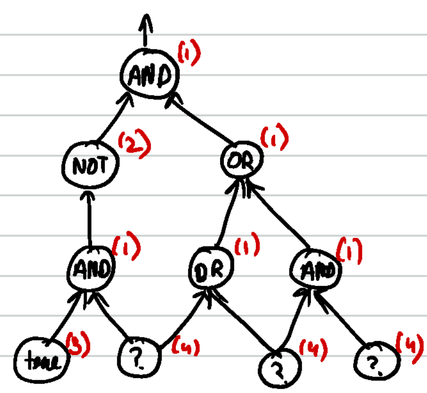
Circuit SAT

Instance: a boolean circuit C → A DAG with 5 kinds of gates

1) AND & OR gates of indegree 2
2) NOT gate of indegree 1
3) known input gates
4) unknown input gates.

Solution: an assignment to unknown input gates s.t. the output gate outputs true

Lemma: Circuit SAT $\in$ NP



Circuit SAT $\longrightarrow$ SAT

Circuit SAT

Instance: a boolean circuit C

Solution: an assignment to unknown input gates s.t. the out put gate outputs true

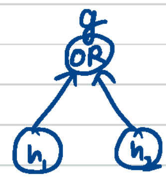
SAT

Instance: Formula ϕ

Solution: Assignment $S: \{x_1 \dots x_n\} \to \{T, F\}$

$f(C) \to$ $\forall$ gate in the circuit C we will introduce a variable g

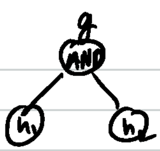
$\phi \to$ true gate $\downarrow$ (g) false gate $\downarrow$ $(\bar{g})$



$h_1 \Rightarrow g$ $\quad (g \vee \bar{h}_1)$

$h_2 \Rightarrow g \quad \to \quad (g \vee \bar{h}_2)$

$g \Rightarrow h_1 \vee h_2 \quad (h_1 \vee h_2 \vee \bar{g})$



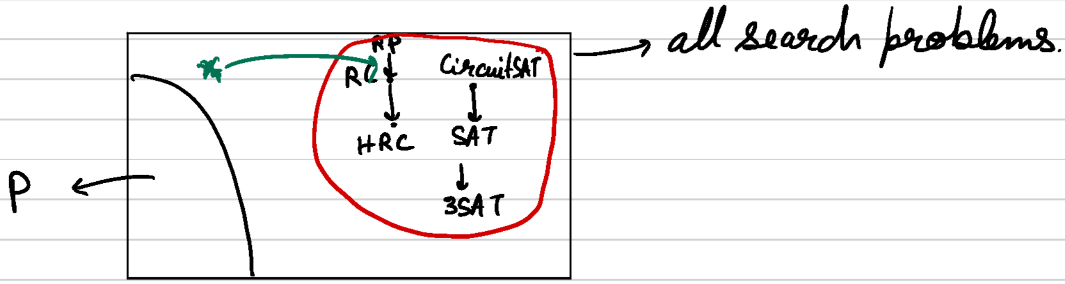
$g \Rightarrow h_1 \qquad (h_1 \vee \bar{g})$ $\qquad (g)$

$g \Rightarrow h_2 \quad \to \quad (h_2 \vee \bar{g})$

$h_1 \wedge h_2 \Rightarrow g \qquad (g \vee \bar{h}_1 \vee \bar{h}_2)$

1. polytime
2. $h(S) = S|_{\text{the unknown input gates}}$
3. if C has a solution then so does ϕ

What have we seen so far?



NP- completeness

A search problem is NP-complete if all other search problems reduce to it.

Lemma: $\forall A \in NP$ $\quad A \to$ circuit SAT $\to$ SAT $\to$ 3SAT

Proof: $\text{VERIFY}_A(I_A, S_A) = 0/1 \longrightarrow$ poly time algo in $|I_A|$

$$C_{\text{VERIFY}_A, I_A}(w) = \text{VERIFY}_A(I_A, w)$$

$f(I_A) = C_{\text{VERIFY}_A, I_A}$

$h(S) = S$

1. f & h are poly time
2. S is a solution to CircuitSAT then S is also a solution to A
3. if A has a solution then so does $C_{\text{verify}_{A}, I_A}$

3SAT $\longrightarrow$ Independent Set

Instance: Formula ϕ on variable $x_1 \dots x_m$

Solution: A satisfying assignment

Instance: $G = (V, E)$, g

Solution: $S \subseteq V$ s.t. $|S| = g$ & $\forall u, v \in S$ we have $(u,v) \notin E$

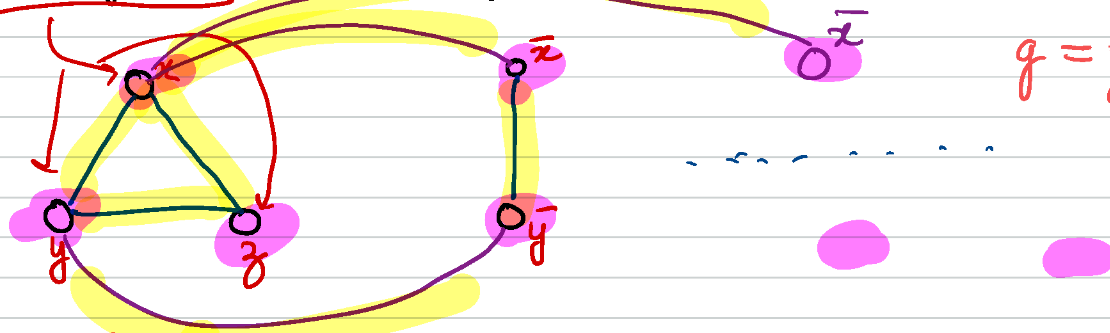
wlog $\rightarrow \phi$ each clause has more than one variable.

(x) ↳ true $(\bar{y})$ ↳ false

$$\phi = \underbrace{(x \vee y \vee z)} \wedge (\bar{x} \vee \bar{y}) \wedge \dots\dots$$

F

$G =$



$g = \#$ of clauses.

$G = (V, E)$

① polytime

② I in G of size g then we can construct a satisfying assignment for ϕ (h does)

③ if there is a satisfying assignment for $\phi \longrightarrow$ an IS in G

SAT IS

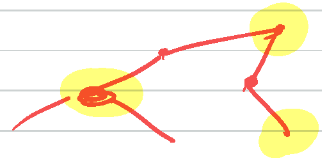
Independent Set $\longrightarrow$ Vertex Cover

Instance : $G=(V,E)$, g

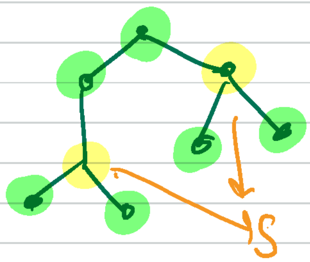
Solution : $S \subseteq V$ s.t. $|S| = g$ & $\forall\, u,v \in S$ $(u,v) \notin E$

Instance : $G=(V,E)$, b

Solution : $S \subseteq V$ s.t. $|S| = b$ & $\forall (u,v) \in E$ either $u \in S$ or $v \in S$

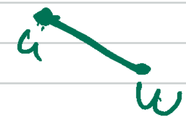


$$f(G, g) = G, \underbrace{|V| - g}_{b=}$$



$V \setminus S \longrightarrow$

S is IS then $\forall\, u,v \in S$ $(u,v) \notin E$



u or w is in $V \setminus S$

$h(S) = V \setminus S$

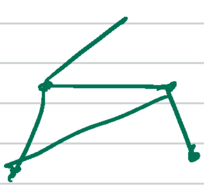
Independent Set $\longrightarrow$ Clique

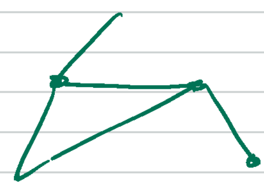
Instance : $G=(V,E)$, g

Solution : $S \subseteq V$ s.t. $|S| = g$ & $\forall u,v \in S$ we have $(u,v) \notin E$

Instance : $G=(V,E)$, g

Solution : $S \subseteq V$ s.t. $|S| = g$ & $u,v \in S$ $(u,v) \in E$ $u \neq v$





(S, E') $E' \subseteq E$ | where both vertices in S

(S, E') $E' \subseteq E$ | both vertices in S

$$F(G=(V,E), g) = (G'=(V,E'), g)$$

$$E' = V \times V \setminus E$$