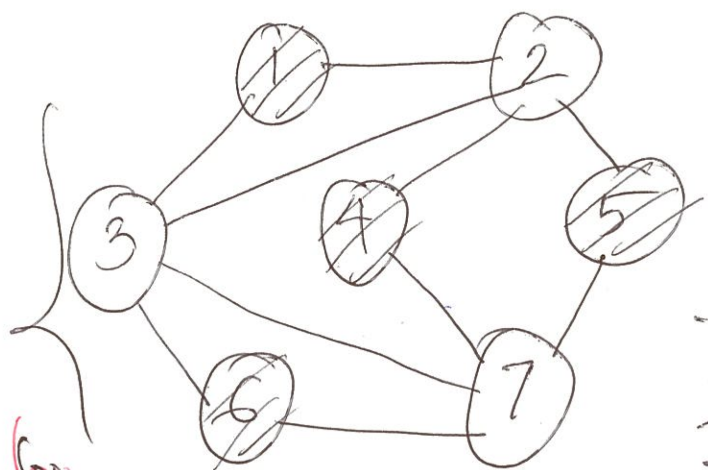
Nov 25

Problem: Independent Set (IS) problem.

$G = (V, E)$

Def: An IS of G is a subset $S \subseteq V$ s.t there is NO edge between ANY distinct pairs of vertices in S



G_0

$\{1,4\}$ ✓

$\{3,7\}$ ✗ $\{1,4,7\}$ ✗

$\{3,4,5\}$ ✓

$\{1,4,5,6\}$ ✓

Formal Problem **decision problem**

Input: $G = (V, E)$ $|V| = n$ $+$ $0 \le k \le n$

Output: TRUE/1 $\Longleftrightarrow$ G has an IS of size $\ge k$

Ex: $G_0, 2$ ✓ $G_0, 3$ ✓ $G_0, 4$ ✓ $G_0, 5$ ✗

Note: Subset of an IS is also an IS

Problem 2: ~~Veet~~ Vertex Cover (VC)

Def: A VC ~~is a~~ of $G = (V, E)$, ~~C~~ $C \subseteq V$ s.t ALL edges in E has atleast 1 end point in C.

Ex: G_0 $\{1,2,3,4,5,6,7\}$ ✓ $\{1,2,3,4,5,6\}$ ✓

$\{1,2,6,7\}$ ✓ $\{2,3,7\}$ ✓ $\{1,7\}$ ✗ $\{1\}$ ✗

Formal problem: input: $G = (V, E)$ $0 \le k \le n$

O/P: TRUE $\iff$ G has a VC of size $\le k$

Ex: $G_0; 6$ ✓ $G_0; 5$ ✓ $G_0; 4$ ✓ $G_0; 3$ ✓ $G_0; 2$ ✗

later

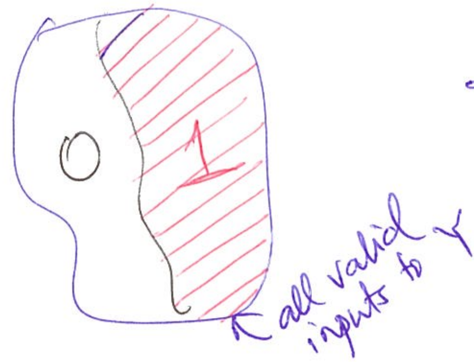
THM: $IS \le_p VC$ and $VC \le_p IS$

Lemma: Let $G = (V, E)$. $S \subseteq V$ is an IS iff $V \setminus S$ is a VC.

Recall: ~~We consider~~ Problem Y with Binary output $\{0,1\}$ / $\{F,T\}$ / $\{No, Yes\}$

$\Rightarrow$ Y is the subset of inputs where the answer is 1.

{ if $w \notin Y$ then the output should be 0 }



Algorithmic Q: Given an input w is $w \overset{?}{\in} Y$

Ex: $w = G; k$ $\overset{IS}{Y}$ = set of all pairs (G, k) s.t. G has an IS of size $\ge k$.

Def: Given an algo A, input w, we denote the output of running A on w as $A(w) \in \{0,1\}$

Def: An algo solves a problem Y if $\forall$ inputs w,

$A(w) = 1 \iff w \in Y$

Recall: A is polytime algo if for all inputs w, $A(w)$ can be computed in $\mathrm{poly}(|w|) = |w|^{O(1)}$ time.

N

Def: P is the set of all problems than can be solved by a polytime algo

Q: Is the shortest path problem in P?

(i/p: G, s, t o/p: length of a shortest s-t path)

Binary: i/p: $G, s, t; k$ o/p: Yes $\iff$ $\exists$ a shortest st path of length $\leq k$.

Efficient verification (book: certification)

Q: $w \overset{?}{\in} Y$ Ex: Y is IS, $w = G;k$

Def: A certificate/witness is a string that supports the claim that $w \in Y$

Def: B is an efficient verifier for Y if

(i) B takes as input (w, t) & ~~exp~~ output $B(w,t) \in \{0,1\}$

input → w, witness → t

(ii) B runs in time $\text{poly}(|w|)$ note no $|t|$!

(iii) $w \in Y \iff \exists$ a poly sized witness t s.t. $|t| \leq \text{poly}(|w|)$

$$B(w,t) = 1$$

(a) $w \in Y \Rightarrow \exists$ a poly sized witness t s.t. $B(w,t)=1$

(b) $w \notin Y \Rightarrow \forall$ poly sized witness t $B(w,t)=0$

Ex: $Y = \text{IS}$ $w = (G, k)$ Intuition S is an IS of size $= k$

witness: $S \subseteq V$ s.t. $|S| = k$

Claim 1: $\exists$ an efficient verifier

$B_{IS}(\underbrace{G, k}_{=w}; \underbrace{S}_{=t})$

0. If $|S| \neq k$ return 0
1. If $\forall u \neq w \in S$ if $(u,w) \notin E$ return 1 else return 0   poly(n)

Claim 2: G has an IS of size $k \iff \exists S \subseteq V$ s.t. $B_{IS}(G,k,S) = 1$

<u>DEF:</u> $Y \in NP$ if $\exists$ an efficient verifier B_Y for Y.

$\equiv$

$Y \in NP$ iff $\forall$ input w

(i) $w \in Y \Rightarrow \exists$ a polysized witness t s.t. $B_Y(w,t) = 1$

(ii) $w \notin Y \Rightarrow \forall$ ______________________

$B_Y(w,t) = 0$

<u>Q:</u> $IS \overset{?}{\in} NP$ ✓

<u>Ex:</u> $VC \overset{?}{\in} NP$

<u>Big Q:</u> $P \overset{?}{=} NP$

<u>Claim:</u> $P \subseteq NP$