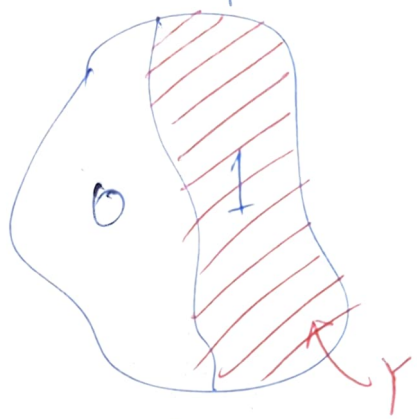
Dec 1

Recall: Problem Y with output in {0,1} / {F,T} / {No, Yes}

≡ Y is the subset of inputs where the output is 1

{ if $w \notin Y \Rightarrow$ output on $w = 0$ }



Algorithmic ~~version~~ Q: Given an input w, is $w \in Y$?

{ Ex $w = G, k$ Y = set of all (G,k) s.t. G has an IS of size $\geq k$ } (IS)

Def: Given an alg A & input w, $A(w) \in \{0,1\}$ as A's output on w.

Def: An algo solves Y if $\forall$ inputs w $A(w) = 1 \iff w \in Y$

Recall: A is poly time if $\forall$ inputs w, $A(w)$ can be computed in $\text{poly}(|w|)$ time. $|w| = N$ $\text{poly}(N) = N^c$ for some constant c.

DEF: $\mathcal{P}$: set of all problems that can be solved by a poly time algo A.

Q: Is the shortest path problem in $\mathcal{P}$

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

NO: since the output is not in {0,1}

↳ i/p: G, s, t, k o/p: TRUE $\iff \exists$ an s-t path of cost $\leq k$.

Efficient verification (book: certifications)

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

(1) B takes as input w, t & output $B(w,t) \in \{0,1\}$ (input: w, witness: t)

(2) B runs in time poly($|w|$) (t doesn't appear here)

(3) $w \in Y \iff \exists$ a witness / string t s.t
   (i) $|t| \leq$ poly($|w|$) AND
   (ii) $B(w,t) = 1$

Intuition: If G has an IS of size $\geq k$ $\Rightarrow \exists$ an IS $\forall$ size $= k$.

Ex: $Y = IS$ i/p: $w = G, k$

Witness: $S \subseteq V$ of size $|S| = k$

Claim1: $\exists$ an efficient verifier

verifier $B(w, t)$ (w: G, k; t: S) Idea: check if S is an IS

→ $B_{IS}(G, k, S)$

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

} poly(N)

Claim2: G has an IS of size $\geq k \iff \exists$ a witness $S \subseteq V$ s.t $B_{IS}(G, k, S) = 1$

DEF: $Y \in NP$ if $\exists$ an efficient verifier B_Y for Y.

[unpack the def]

$Y \in NP$ iff $\forall$ inputs w:

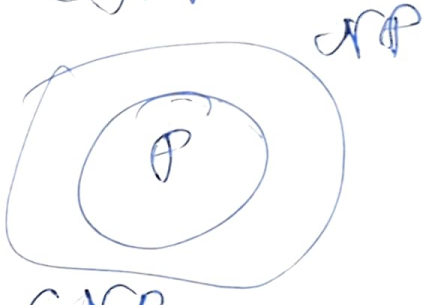
(i) $w \in Y \Rightarrow \exists$ a witness t s.t. $|t| \leq \text{poly}(|w|)$ & $B_Y(w,t) = 1$

(ii) $w \notin Y \Rightarrow \nexists$ witness t s.t. $|t| \leq \text{poly}(|w|)$ $B_Y(w,t) = 0$

Q: Is $\in NP$ ✓ **Ex:** $VC \in NP$

Big Q: $P \stackrel{?}{=} NP$

Claim: $P \subseteq NP$



Pf: $Y \in P$ . . . $\Rightarrow Y \in NP$

↳ $\exists$ a poly time algo A that solves Y s.t. $A(w) = 1 \Leftrightarrow w \in Y$

Show: $Y \in NP$

Goal: $\exists$ an efficient verifier B_Y

$B_Y(w,t)$
return $A(w)$

$\Rightarrow \forall$ witness t, $B(w,t) = A(w)$

$\Rightarrow Y \in NP$ ∎