$\boxed{\text{Nov 25}}$

Claim: $Z \le_p Y$ and $Y \le_p X$

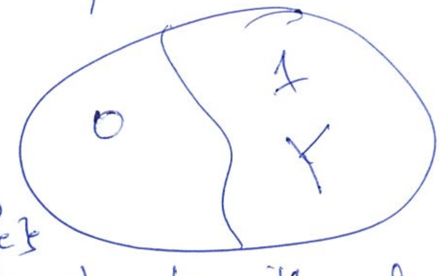
$\Rightarrow Z \le_p X$

Recall: We have defined Y with $\{0,1\}$ output.

$\equiv$ Y = set of all inputs with output 1

Algorithmic problem: Given input z,

$z \overset{?}{\in} Y$ $\in \{\text{True}, \text{False}\}$



Given an algo A, we will use $A(z)$ to denote it's output.

$\rightarrow$ Algo A solves/computes the problem Y.

$\forall$ inputs z $\quad A(z) = \text{True} \iff z \in Y$

$\rightarrow$ A is poly time if on all inputs z, it takes poly($|z|$) steps.

P: set of problems that can be solved by a poly-time algo.

Efficient verification (called certification in book)

Q: $z \overset{?}{\in} Y$

$\hookrightarrow$ a certificate/witness t for $z \in Y$

B ~~P~~ $\rightarrow$ ~~efficient~~ efficient verifier for Y if

(1) B~~P~~ runs in ~~p~~ time poly($|z|$) & ~~takes~~ z & t as it's input.

(2) $\exists$ a poly time function p s.t.

$z \in Y \iff$ $\exists$ a string/witness t $|t| \le \text{poly}(|z|)$ and B~~P~~$(z, t) = \text{True}$.

→ $\underbrace{\text{Independent set}}_{Y}$ $\{G = (V, E); k\} = Z$

witness to the claim that G has an IS of size $\geq k$,

subset $S \subseteq V$ of size k

verifier B: $B(G, k, S)$ → True if S is an IS

→ False o/w

poly time as check if $\forall$ $u \neq w \in S$ $(u, w) \notin E$

→ $\underbrace{\text{3-SAT}}_{Y}$: $\underbrace{\text{3-SAT formula}}_{Z}$ on $X = \{x_1, \dots, x_n\}$ (Ex: $(x_1 \vee x_2)$)

Witness: $v: X \to \{0, 1\}$ with $(1, 1)$

verifier B: Evaluate the 3-SAT formula on the assignment v.

Def: $Y \in NP$ if $\exists$ an efficient verification process for Y. ← verifier B

→ Let z be an i/p

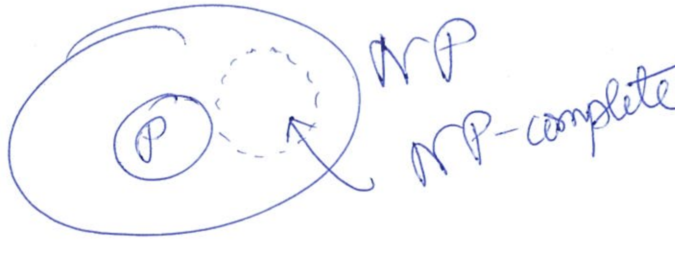
$z \in Y \implies \exists$ witness t s.t. $B(z, t) = \text{True}$

$z \notin Y \implies \forall$ witness t $B(z, t) = \text{False}$.

$IS \in NP$; $3\text{-SAT} \in NP$; $VC \in NP$ ← Ex.

Claim 2: $P \subseteq NP$ Say $Y \in P \implies \exists$ a poly-time algo A for Y

Pf idea: Verifier $B(z, t) = A(z)$



NP-complete problems: "Hardest" problems in NP

Def: X is NP-complete if

(1) $X \in NP$

(2) $\forall Y \in NP$, $Y \leq_p X$

Lemma: Let X be an NP-complete problem.

$\exists$ a poly time algo for X $\iff P = NP$

Pf: $\Rightarrow$: As X is NP-complete

$\forall Y \in NP$, $Y \leq_p X$

$\Rightarrow Y \in P$

as $X \in P$

$\Leftarrow$: ~~Pf~~ $P = NP \Rightarrow$ X has a poly time algo as $X \in NP$.

Lemma 1: Y ~~be~~ is NP-complete + $X \in NP$.

~~Pf~~ $Y \leq_p X \Rightarrow$ X is also NP-complete.

Pf: (book)

THM 1: 3-SAT is NP-complete.

COR 1: IS is NP-complete.

(as 3-SAT $\leq_p$ IS)

COR 2: VC is NP-complete.

$IS \leq_p VC$