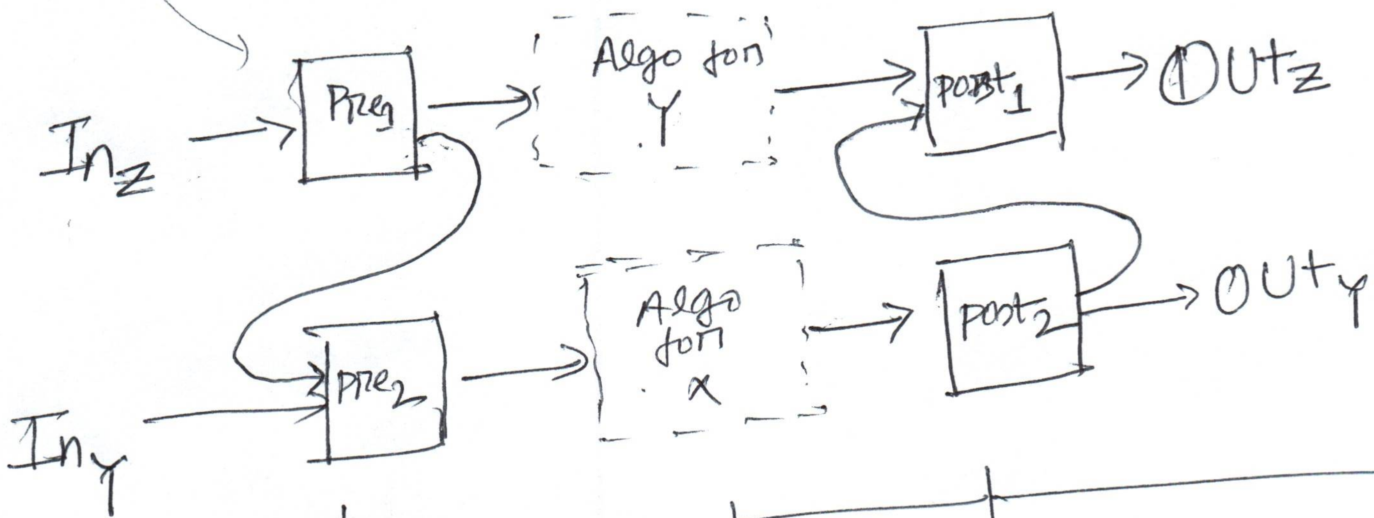
May 5

claim 1: $\le_p$ is transitive

$Z \le_p Y$ and $Y \le_p X$

$\Rightarrow Z \le_p X$



Recall: Problem Y with outputs $\in \{0,1\}$
$\equiv$ Y is a subset of inputs with output 1.

Problem: Given an input ω, is $\omega \in Y$?

Ex1: ω: $(G; K)$
Y: All G with IS of size $\geq K$

Ex2: ω: φ
Y: all satisfiable 3-SAT formulas.

Def: Given an algo A and input ω, $A(\omega) \in \{0,1\}$ denotes the output of algo A on input ω.

Def: An algo A solves a problem Y, if $\forall$ inputs ω,
$A(\omega) = 1 \Leftrightarrow \omega \in Y$.

Note: Algo A is poly-time if $A(\omega)$ is computed in poly($|\omega|$).

Def: P : Set of all problems that can be solved by a poly-time algo.

Q: Is shortest-path $\in$ P ? (I/P: G, c_e, -ve cost allowed, ~~+ve~~ No -ve cycles.
O/P: a shortest s-t path).

Decision version:

I/P: G ; K

O/P: TRUE if $\exists$ a shortest s-t path of length $\leq$ K.

$w \in Y$?

↳ we ~~m~~ need witness/certificate t.

EX1: w: (G, K)
t: $S \subseteq V$

EX2: w: 3-SAT formula φ
t: an assignment

Efficient Verification (certification)

Def: ~~An~~ B is an efficient verifier, if

(1) B takes w & t as i/p: $B(w,t) \in \{0,1\}$

(2) B runs in poly-time

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

claim 2: IS has an efficient verifier.

Y: All G that have IS of size $\geq$ K

w: (G; K)

t: $S \subseteq V$

Efficient Verifier B: ← poly-time

$\forall\ u \neq v \in S$

check if $\exists\ (u,v) \in E$

output 1 if $(u,v) \notin E\ \forall\ u \neq v \in S$

Claim 3: 3-SAT has an efficient verifier.

w: 3-SAT formula φ

t: an assignment $v: x_i \to \{0,1\}$

efficient verifier B: check if w is a satisfied/evaluates to T/1 on assignment v.

(poly-time)

Def: $Y \in NP$ if Y has an efficient verifier B for Y, s.t. $\forall$ inputs w

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

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

IS $\in$ NP ; 3-SAT $\in$ NP : VC $\in$ NP

EX

Q: $P = NP$? | $P \subseteq NP$ AND $NP \subseteq P$

<u>claim 4:</u> $P \subseteq NP$

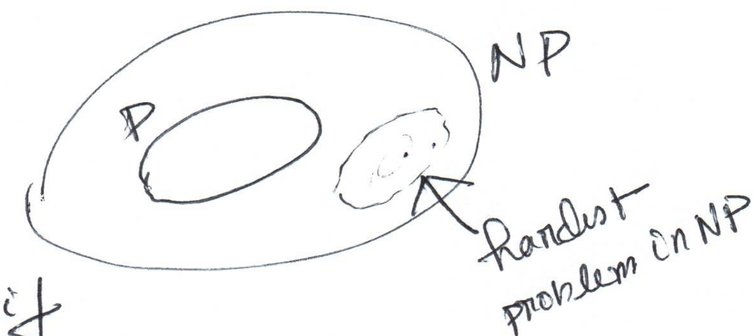
<u>Pf</u>: $Y \in P \Rightarrow \exists$ an algo A, s.t. $A(w) = 1 \Leftrightarrow w \in Y$.

show Y has an efficient verifier.

<u>Efficient verifier B:</u> $B(w, t) = A(w)$

poly-time as A is ~~poly-tim~~ poly-time.

$\Leftarrow$ $NP \subseteq P$?



<u>Def</u>: X is NP-complete if

(1) $X \in NP$

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

<u>Lemma 1:</u> let X be an NP-complete problem.

$\cancel{P}$ $X \in P \Rightarrow P = NP$.

<u>THM:</u> 3-SAT is NP-complete. (Book).

<u>Lemma 2:</u> Y is an NP problem. X is NP-complete. $X \leq_p Y \Rightarrow Y$ is NP-complete.