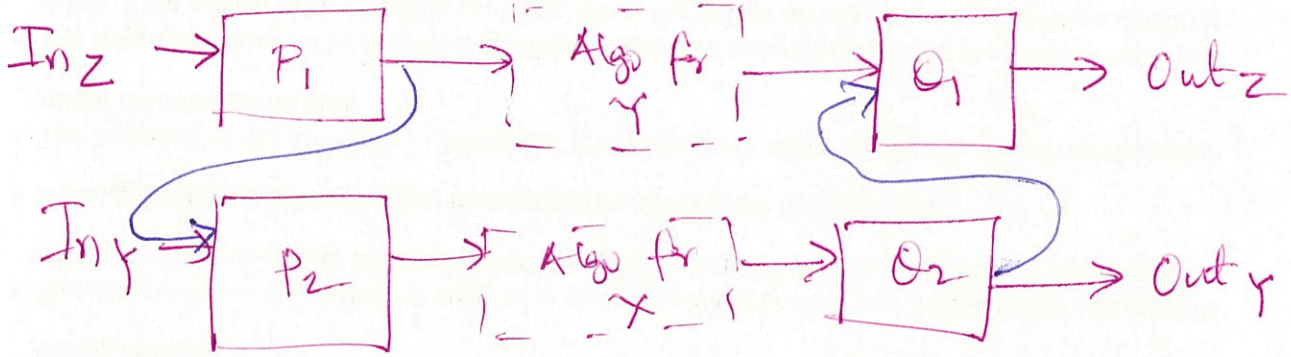
Dec 3

Claim 1: $\leq_p$ is transitive

$Z \leq_p Y$ and $Y \leq_p X$

$\Rightarrow$ $Z \leq_p X$

Pf:



Recall: Problem Y with output $\{0,1\}$

$\equiv$ Y is a subset of inputs with output 1.

Algorithmic problem Given an input w, is $w \stackrel{?}{\in} Y$

Eg: $w \equiv \Phi$ 3-SAT formula

$Y \equiv$ set of all satisfiable 3-SAT formula.

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

Def: An algo A solves a problem Y

$\forall$ input w, $A(w) = 1 \iff w \in Y$

Recall: A is poly-time algo if $\forall$ inputs A(w) is computed in poly $(|w|)$ size

($|w|$ ↖ size of w)

poly $(N) = N^c$ for some constant c.

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

Is the shortest path problem (i/p: $G=(V,E)$ ce Vee no -ve cycle s,t

Technically: Boolean / decision version of SP ⟶ o/p: cost of shortest s-t path)

i/p: k

o/p: ∃ an s-t path of cost $\leq k$.

Efficient verification (book: certification)

Q: Is $w \overset{?}{\in} Y$

Eg: $Y \equiv$ 3-SAT

w is Φ

↳ A certificate / witness t for $w \in Y$. t is an assignment

Def: B is an efficient verifier for Y if

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

(2) B runs in time poly ($|w|$)

(3) $w \in Y \iff \exists$ a string / witness t s.t

(i) $|t| \leq$ poly ($|w|$) AND (ii) $B(w,t)=1$

Claim 2: 3-SAT (Y) has an efficient verifier

witness (t): $\varphi : X \to \{0,1\}$ ← poly time

3-SAT formula Φ (w) on $X=\{x_1,\dots,x_n\}$

Verifier (B): check if Φ on assignment φ gives 1 or 0

Claim 3: Independent set

$|S|=k$

t: witness: $S \subseteq V$

w: $G=(V,E)$; k

o/p: 1 if G has an IS $S \subseteq V$ of size $\geq k$

Verifier: B: ∀ $u \neq v \in S$ check if $(u,v) \in E$ ↳ output 1 $\iff (u,v) \notin E$

poly time

no edges between S ∀ $u \neq v$.

→ Above examples, notion of witness are "obvious"
NOT always: E.g. PRIMES has an efficient verifier.

DEF: $Y \in \mathcal{NP}$ if $\exists$ an efficient verifier B for Y

s.t $\forall$ inputs w: $|t| \leq \text{poly}(|w|)$

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

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

IS $\in \mathcal{NP}$, 3-SAT $\in \mathcal{NP}$; VC $\in \mathcal{NP}$ (Ex.)

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

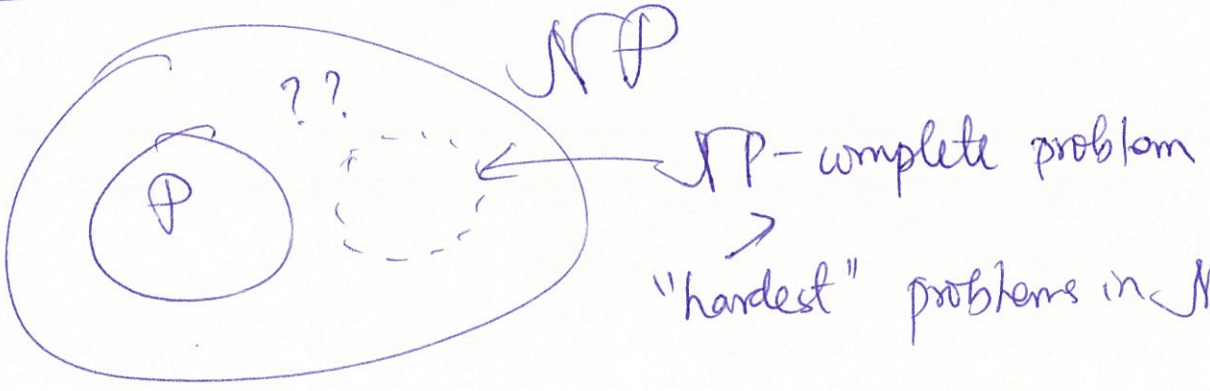
Claim 4: $\mathcal{P} \subseteq \mathcal{NP}$

Pf: $Y \in \mathcal{P} \Rightarrow \exists$ an alg A s.t $A(w) = 1 \iff w \in Y$

Show: Y has an efficient verifier

$B(w,t) = A(w)$ ∎

→ $P \stackrel{?}{=} \mathcal{NP} \equiv \mathcal{NP} \subseteq \mathcal{P}$



Def: X is NP-complete IF

(1) $X \in NP$

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

Lemma 1: Let X be an NP-complete problem

If $X \in P \Rightarrow P = NP$

THM 1: 3-SAT is NP-complete (see book)

Lemma 2: Let Y be NP-complete. $X \in NP$

If $Y \leq_p X \Rightarrow X$ is NP-complete.