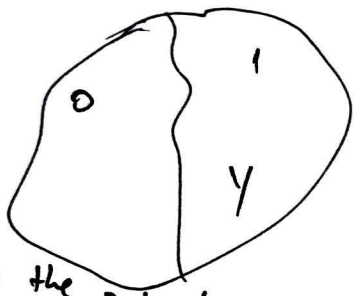
May 1

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

$\Rightarrow Z \leq_p X$

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

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



Algorithmic problem: Given input z, $z \overset{?}{\in} Y$

Given an algo A, we will ~~[illegible]~~ use $A(z) \in \{0,1\}$ to denote the output

→ Algo A solves/computes the problem Y

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

→ 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 alg.

Efficient verification (called certification in book)

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

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

B → efficient verifier for Y if

① B runs in time poly $(|z|)$ & takes z & t as its input

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

$z \in Y \iff \exists$ a string/witness t $|t| \leq p(|z|)$

and $B(z,t) = \text{True}$

→ Independent set $\{G=(V,E), k\} = z$

Y

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 of size $\geq k$
→ False o.w.

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

→ 3-SAT : 3-SAT formula on $X = \{x_1, \dots x_n\}$

Y z

(Ex. $x_1 \vee x_2$)

witness v: $X \to \{0,1\}$

→ witness $(1,1)$

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 input

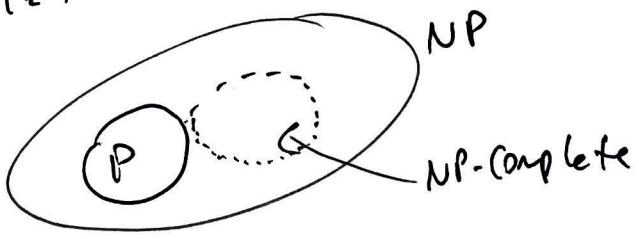
$z \in Y \Rightarrow \exists$ a witness t s.t. $B(z,t) = \text{True}$

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

IS $\in NP$; 3-SAT $\in NP$; UC $\in NP$ ↖ ex.

Claim 2: $P \subseteq NP$ Say $Y \in P \Rightarrow \exists$ 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

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

(as $X \in P$)

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

Lemma 1: Y is NP-Complete + $X \in NP$

If $Y \leq_p X \Rightarrow X$ 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: UC is NP-Complete

IS $\leq_p$ UC