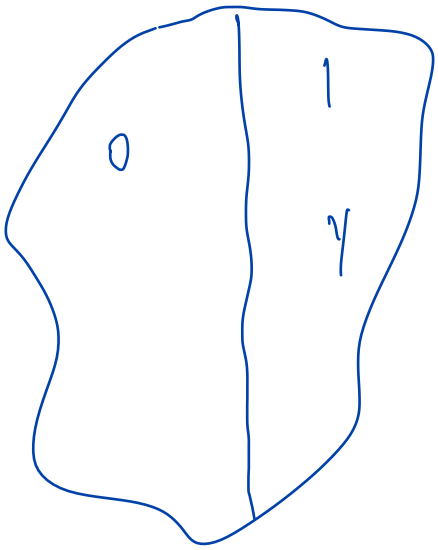
May 3

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

Y = set of all inputs with output 1



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

Given an algo. A, we will 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: $z \stackrel{?}{\in} Y$

↳ 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 input

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

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

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

Y

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

subset $S \subseteq V$ of size k

verifier B: $B(G, k, S) \to$ True if S is an IS of size $\ge k$

→ False o.w.

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

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

Y $\quad$ z

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

verifier B: Evaluate the 3-SAT formula on the assignment V

Def: $Y \in NP$ if $\exists$ an efficient verification process for Y (by efficient 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, $B(z,t) = \text{False}$

$IS \in NP$; $3\text{-SAT} \in NP$; $VC \in NP$ ↳ ex.

Claim: $P \subseteq NP$

Pf idea: Say $Y \in P \Rightarrow \exists$ a poly time alg A for Y

Verifier $B(z,t) = A(z)$