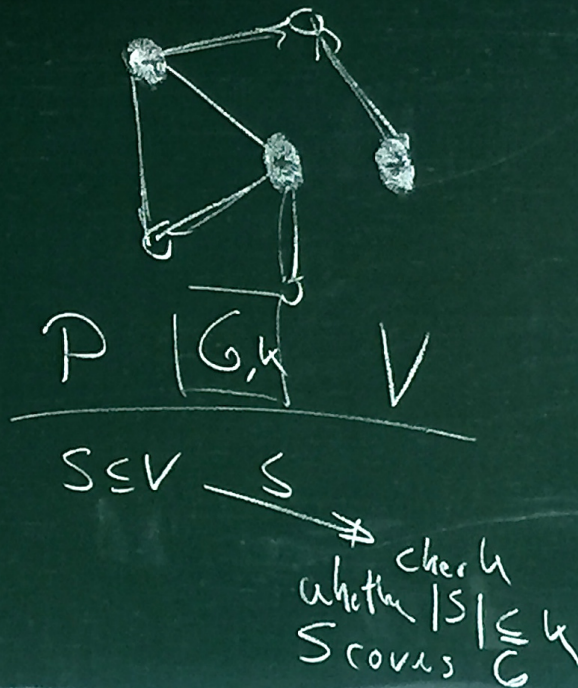


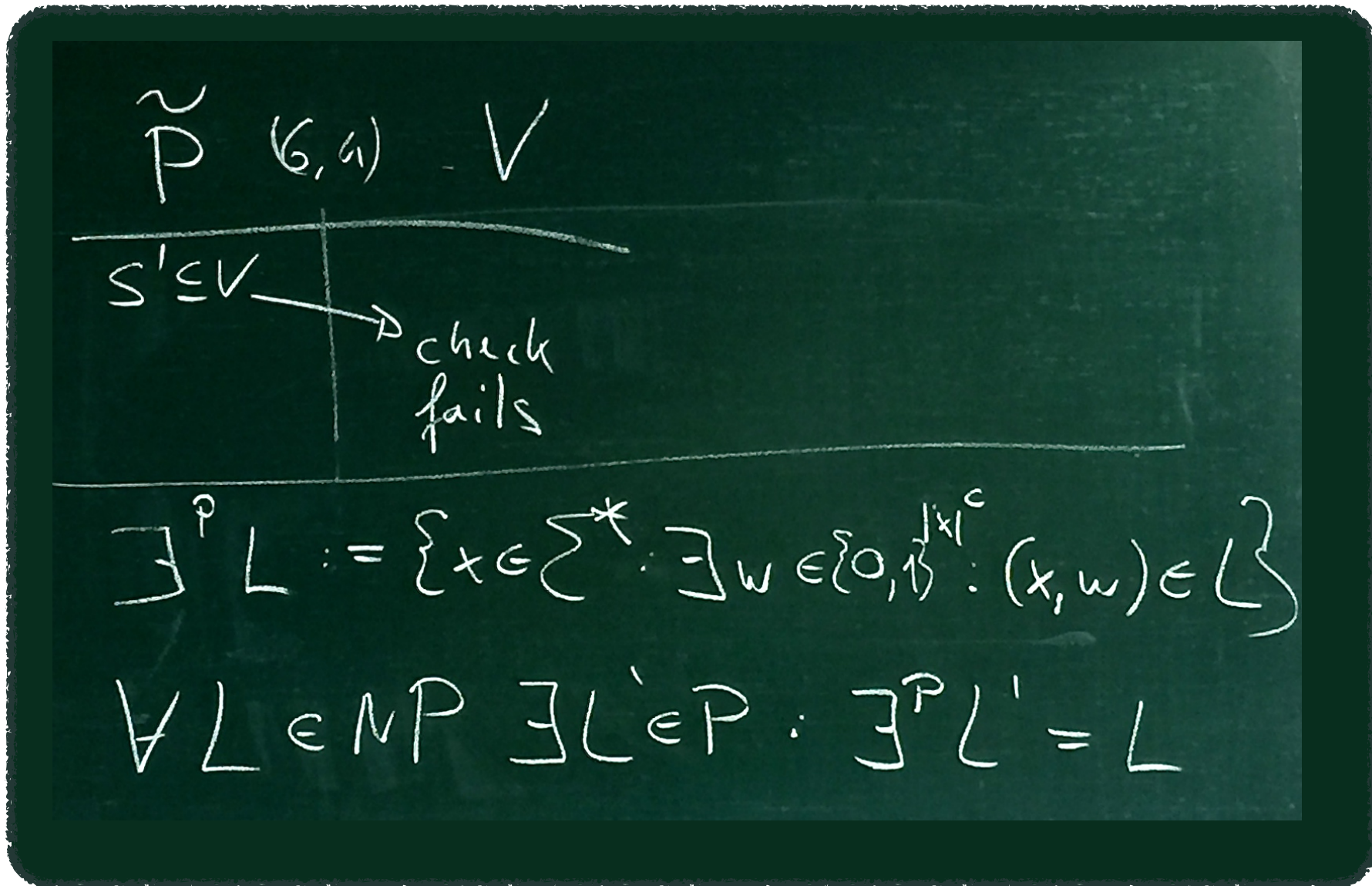
17 Interactive Proof Systems

Interactive Proof Systems

NP · set of problems with easy proofs

Vertex Cover = $\{ (G, k) \mid$
 $\# \text{ nodes to cover the graph} \leq k \}$





$\tilde{P} (G, A) - V$

$S' \subseteq V$

\rightarrow check fails

$\exists^P L := \{x \in \Sigma^* : \exists w \in \{0,1\}^{|x|^c} : (x,w) \in L\}$

$\forall L \in NP \exists L' \in P : \exists P' L' = L$

Observation

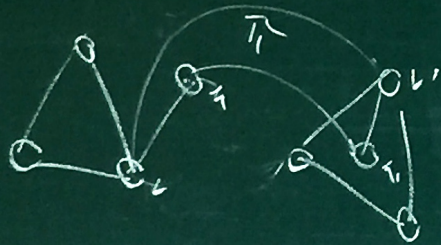
- A prover can convince a poly time bounded verifier that $x \in L$, $\forall x \in L \in NP$
- cannot convince if $x \notin L$

17 Interactive Proof Systems

$ISO = \{(G, H) \mid \text{graphs } G, H \text{ are isomorphic}\}$

$G \cong H$: bijective function: $\pi: V(G) \rightarrow V(H)$

$(u, v) \in E(G) \Leftrightarrow (\pi(u), \pi(v)) \in E(H)$



$P \quad (G, H) \quad V$

$\xrightarrow{\pi}$

check that π is bijective

 $\forall u, v \in V(G)$

$(u, v) \in E(G)$

$\Leftrightarrow (\pi(u), \pi(v)) \in E(H)$

17 Interactive Proof Systems

NON-ISO := $\{(G, H) \mid G \not\equiv H\}$

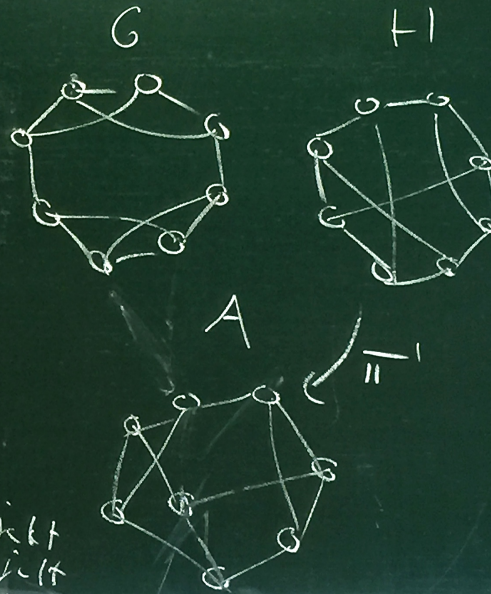
P (G, H) V

Choose two random permutations $\pi, \pi' : V \rightarrow V$

if $A \approx G$ $\leftarrow A_1 = \begin{cases} \pi(G) & \text{with prob. } 1/2 \\ \pi'(H) & \text{"} \end{cases}$
 Send G

else if $A \approx H$ \leftarrow Send H

if a) and $B \neq G$ then reject
 else if b) and $B \neq H$ then reject



$v_2 \in \{0, 1\}$ with prob. $1/2$

$A_2 = \begin{cases} \pi(G) & \text{if } v_2 = 0 \\ \pi(H) & \text{if } v_2 = 1 \end{cases}$

if $A_2 \approx G$ \leftarrow $G = B_2$
 if $A_2 \approx H$ \leftarrow $H = B_2$

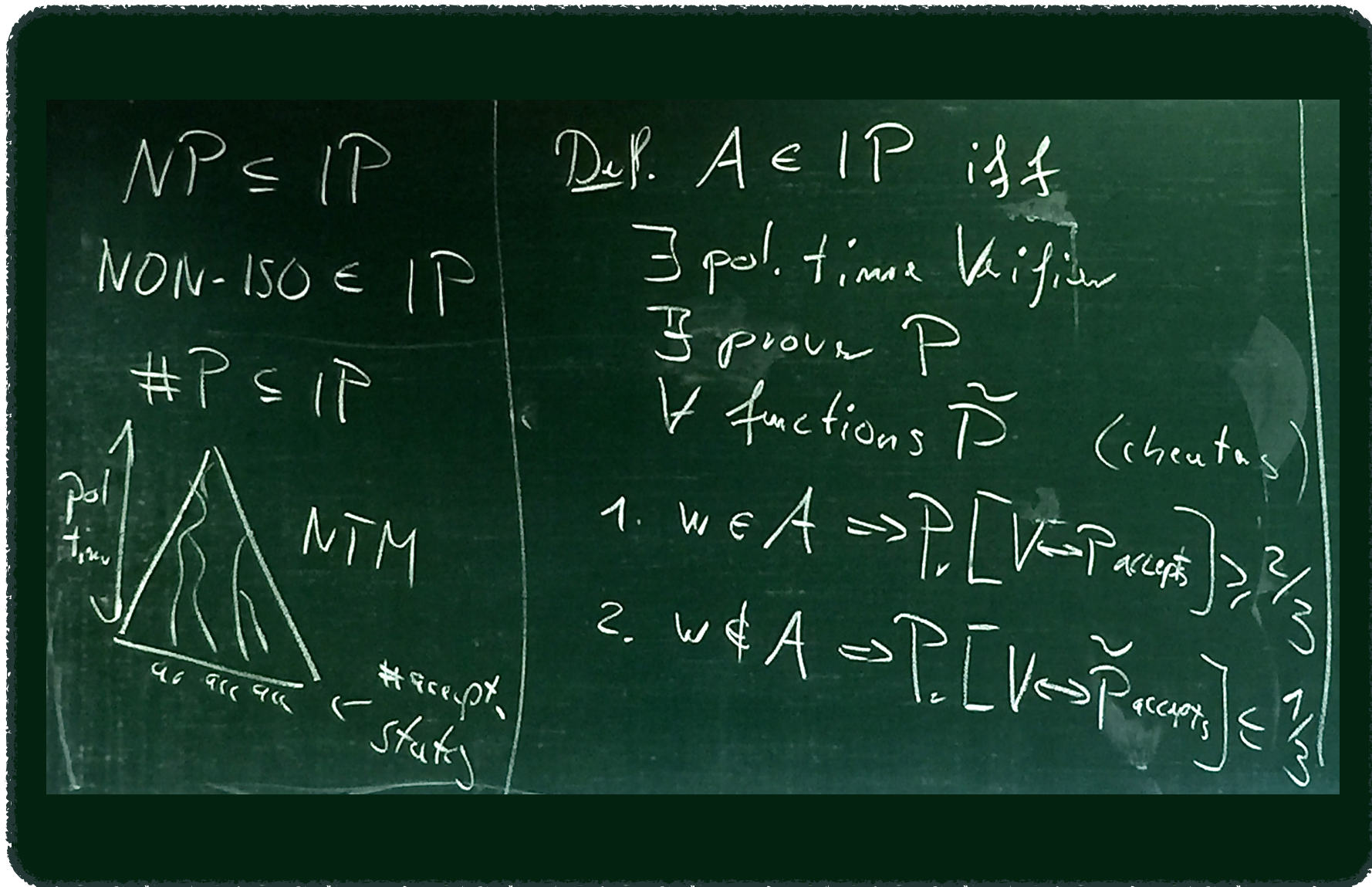
if $(v_2 = 0)$ and $G \neq B_2$ then reject
 else if $(v_2 = 1)$ and $B_2 \neq H$ reject
 else accept

17 Interactive Proof Systems

$L \in IP$

<p><u>Prover</u></p> <ul style="list-style-type: none"> - input $x \in L$ - messages sent so far m <p>output $P(x, m_1, m_2, \dots, m_i)$</p> <p>$P$ is not bounded</p> <p>i is even</p>	<p><u>Verifier</u></p> <ul style="list-style-type: none"> - input $x \in \Sigma^*$ - random bits $r_k \in \{0,1\}^*$ - messages sent so far m <p>output $V(x, r_1, \dots, r_m, m_1, \dots, m_i)$</p> <p>$i$ is odd or accept</p> <p>V is $x ^{O(1)}$ or reject</p> <p>- time bounded</p>
---	---

17 Interactive Proof Systems



$NP \subseteq IP$
 $NON-ISO \in IP$
 $\#P \subseteq IP$

pol. time
 NTM
 #accept. strings

Def. $A \in IP$ iff
 \exists pol. time verifier
 \exists prover P
 \forall functions \tilde{P} (cheaters)

- $w \in A \Rightarrow \Pr[V \leftrightarrow P \text{ accepts}] \geq \frac{2}{3}$
- $w \notin A \Rightarrow \Pr[V \leftrightarrow \tilde{P} \text{ accepts}] \leq \frac{1}{3}$

17 Interactive Proof Systems

IP = PSPACE

Theorem $IP \subseteq PSPACE$

Proof $A \in IP$; "we know" V in V
 - prover is too hard to compute

$$\text{if } x \in A \Rightarrow P_A \geq \frac{2}{3}$$

$$\text{if } x \notin A \Rightarrow P_A \leq \frac{1}{3}$$

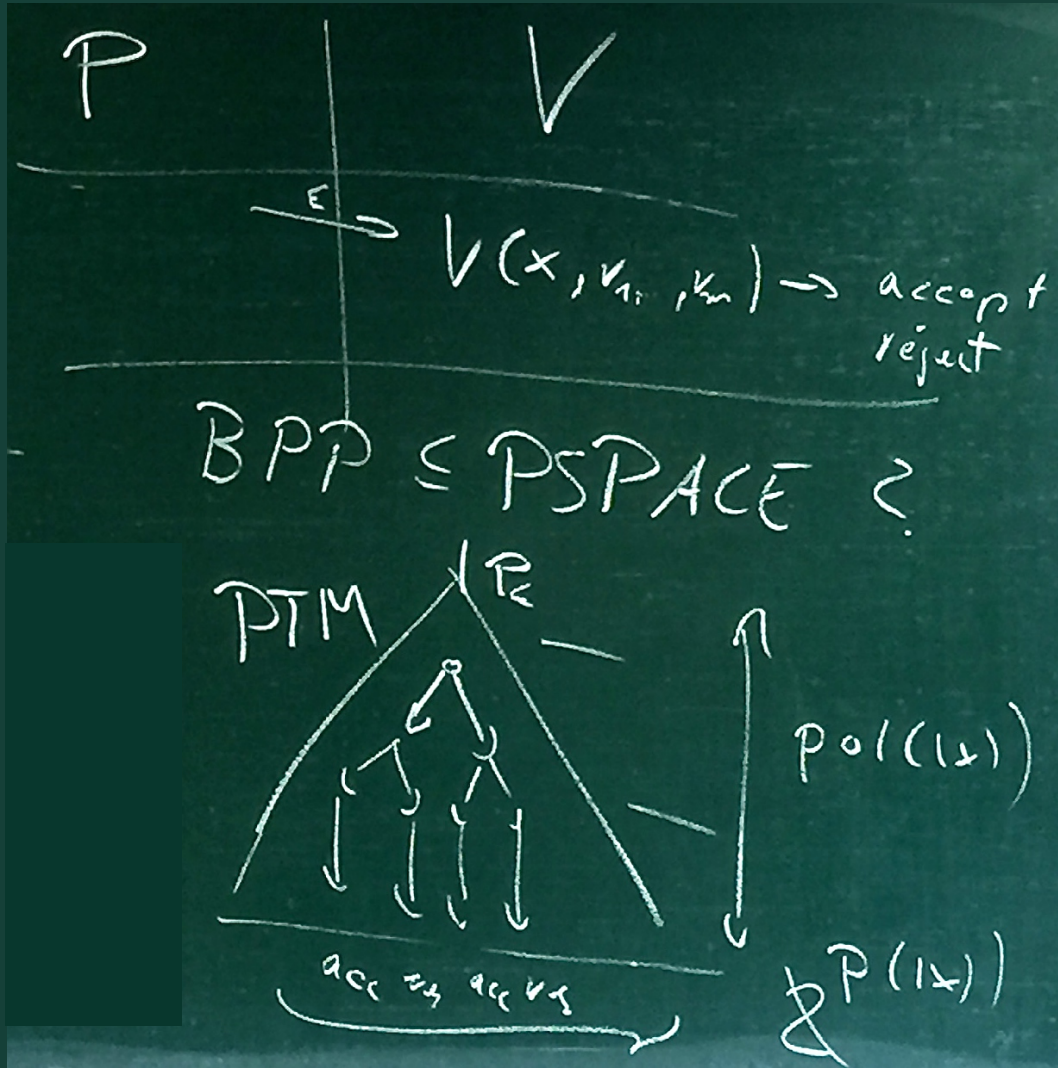
consider

$$P_A = \max_{\text{all } \tilde{P}} P_{\tilde{P}} [V \leftrightarrow \tilde{P} \text{ accepts}]$$

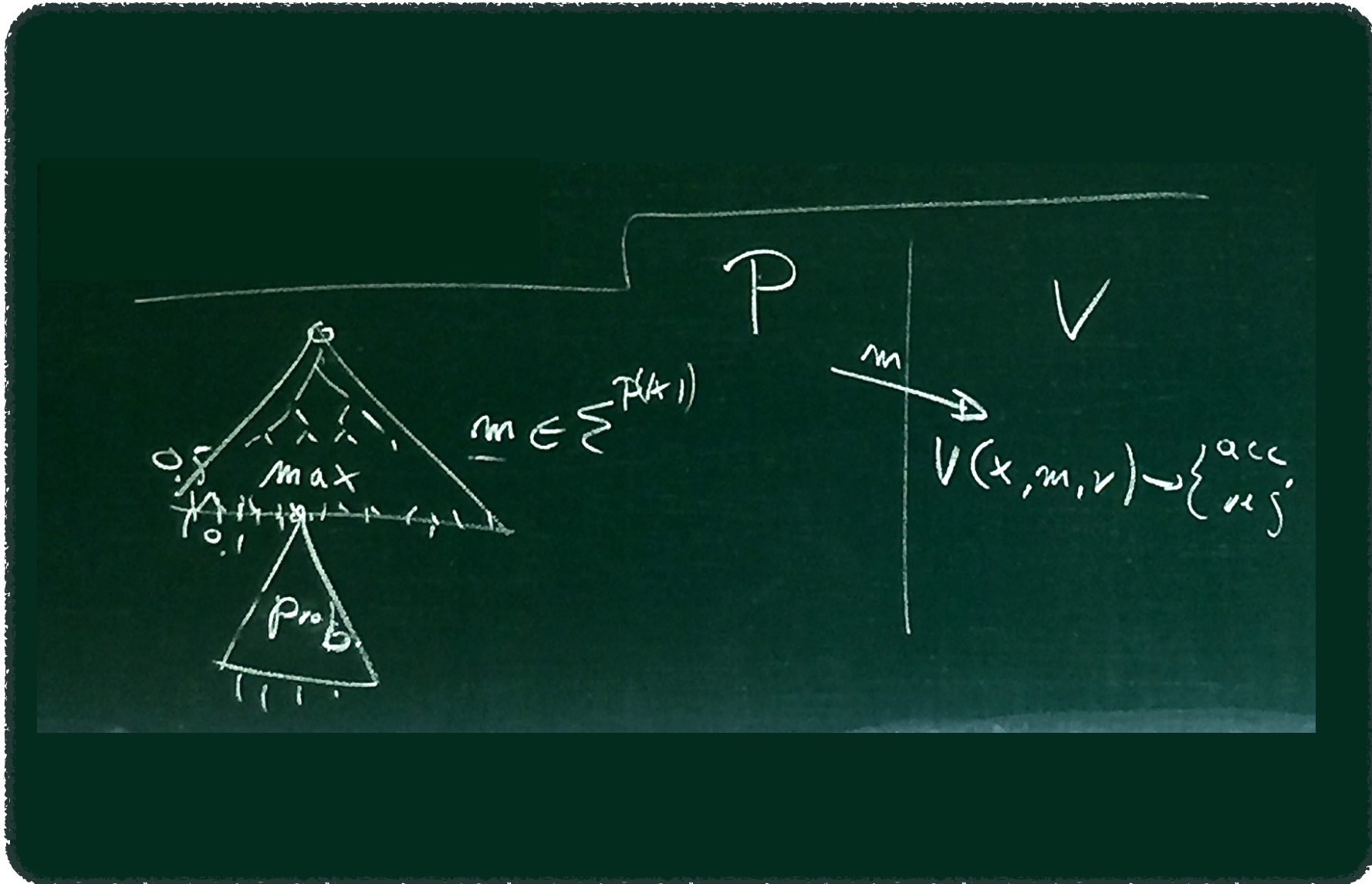
on input x

compute P_A

17 Interactive Proof Systems



17 Interactive Proof Systems



17 Interactive Proof Systems

