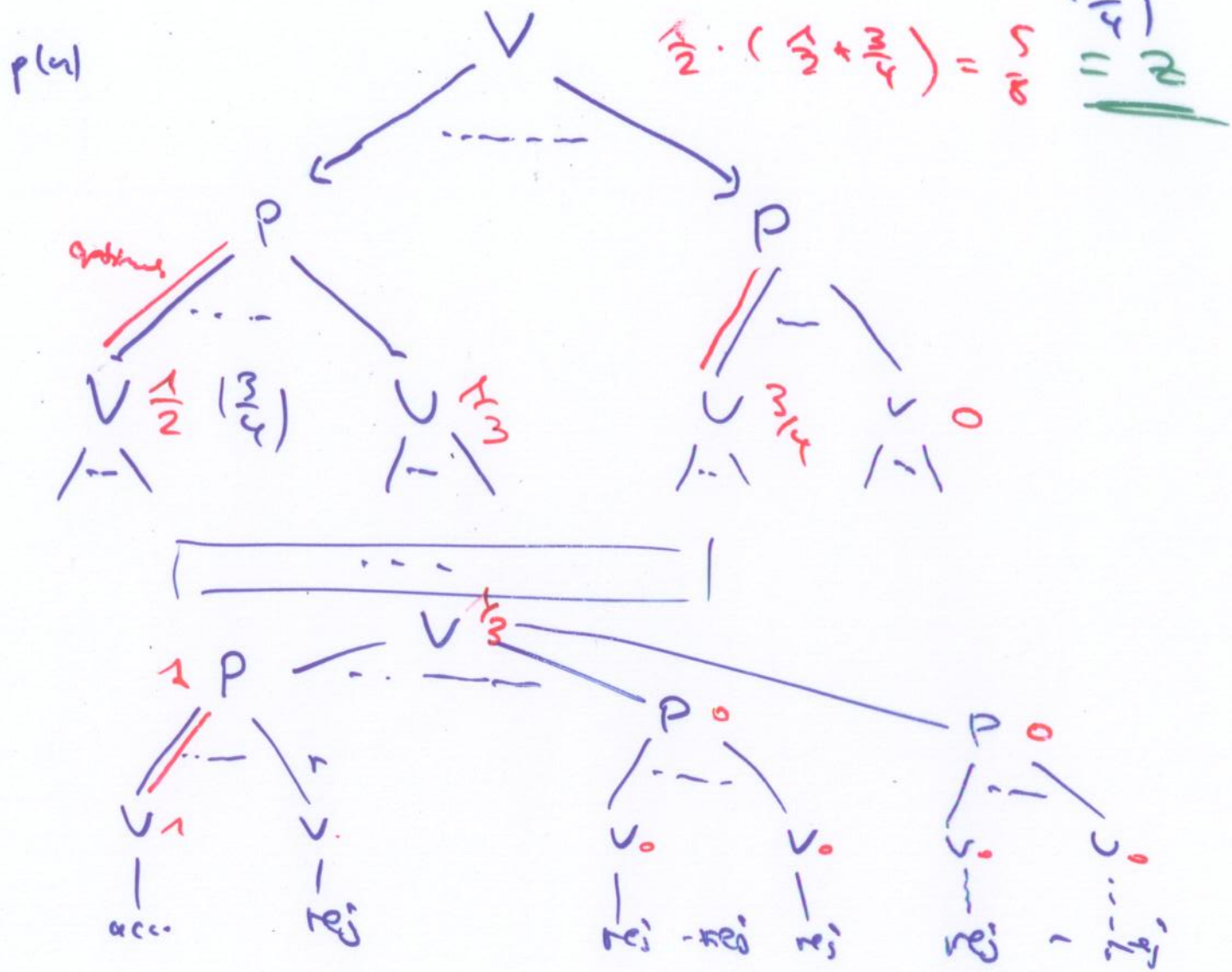
$x \in [0,1)^4$



$\frac{1}{2} \cdot \left(\frac{1}{3} + \frac{3}{4}\right) = \frac{5}{6} = \left(\frac{7}{4}\right)$

11

$\Sigma_2 SAT \ni \psi = \exists x \in \{0,1\}^n \forall y \in \{0,1\}^n . \varphi(x,y)$

$\Leftrightarrow \exists x \in \{0,1\}^n . f'(x) \in GNI$

$\overset{!}{\Leftrightarrow} \forall r \in \{0,1\}^m \exists x \in \{0,1\}^n \exists a \in \{0,1\}^{m'} : V(g(x), r, a) = 1$

decidable in Π_2
$\Rightarrow \Sigma_2 SAT \in \Pi_2$

"$\Rightarrow$": by perfect completeness

"$\Leftarrow$": if $\neg \exists x \in \{0,1\}^n . f'(x) \in GNI$

$\Rightarrow \forall x \in \{0,1\}^n . f'(x) \notin GNI$

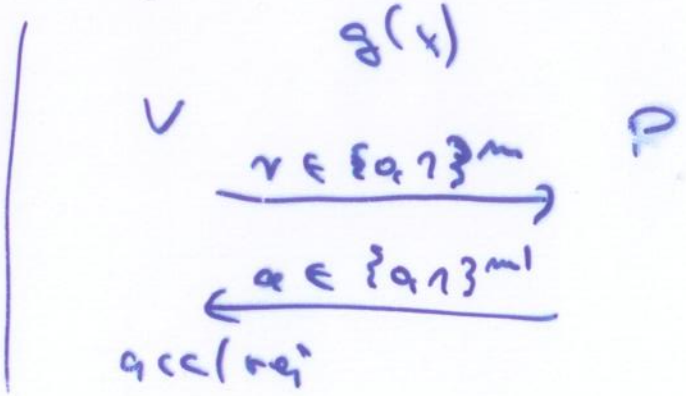
$\Rightarrow \forall x \in \{0,1\}^n$, $\forall$ provers P.

$\Pr[out_V(V,P)(f'(x)) = 1] \leq \frac{1}{2^n}$

let $Z \to \sum_{x \in \{0,1\}^n} out_V\langle V,P\rangle(f'(x))$

$E[Z] \leq$

$\Rightarrow \exists r \in \{0,1\}^m \forall x \in \{0,1\}^n \forall a \in \{0,1\}^{m'}$
$V(g(x), r, a) = 0$



Summary

13

Tricks

Chernoff bounds
hash functions
linearization
arithmetization
probabilistic arguments

Classes

BPP

AM

Protocols

socks
Goldwasser-Sipser
set lower bound protocol
envelope (graph-coloring)
priv. coin GNI

Results

IP = PSPACE
error reduction
GNI ∈ AM(2)
IP[k] = AM(k+2)
public coins = private coins
coNP-compl. ⇒ hierarchy collapses

Definitions

perfect completeness
zero knowledge