Computational Complexity

Mohammad Mahmoody

Session 26
April 2014

The formal definition of class **IP**

Definition 8.6 *(Probabilistic verifiers and the class* **IP***)* For an integer $k \geq 1$ (that may depend on the input length), we say that a language L is in $\mathbf{IP}[k]$ if there is a probabilistic polynomial-time Turing machine V that can have a k-round interaction with a function $P:\{0,1\}^* \to \{0,1\}^*$ such that

$$\text{(Completeness)} \qquad x \in L \Rightarrow \exists P \Pr[\mathtt{out}_V\langle V, P\rangle(x) = 1] = 1$$

$$\text{(Soundness)} \qquad x \notin L \Rightarrow \forall P \Pr[\mathtt{out}_V\langle V, P\rangle(x) = 1] \leq 1/3$$

where all probabilities are over the choice of r.

We define $\mathbf{IP} = \cup_{c \geq 1} \mathbf{IP}[n^c]$.

Some Points

- The definition is not symmetric (just like NP)
  If $x \notin L$ then there is no honest prover strategy defined
- Honest Prover (defined for $x \in L$) can be assumed to be deterministic (sends what maximizes verifier's accept probability)
- If zero-error (deterministic verifier) → $L \in NP$
- 1/3 is called soundness error:

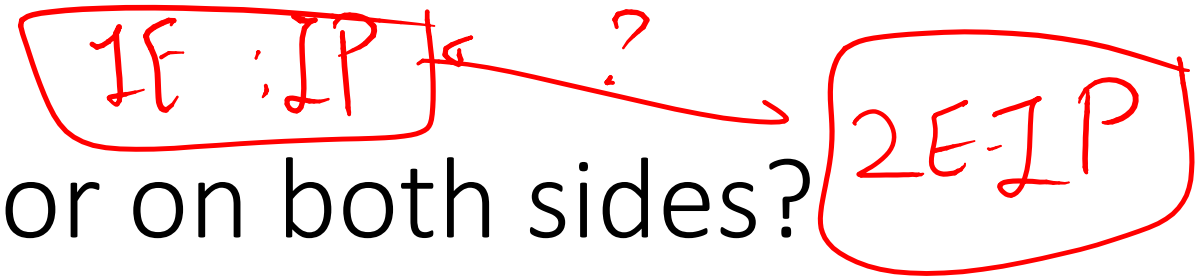
Computationally unbounded.

$SAT \in NP \subseteq IP$

Prover → w → Verifier (x, w)

(Completeness)	$x \in L \Rightarrow \exists P \Pr[\text{out}_V\langle V, P\rangle(x) = 1] \geq 2/3$
(Soundness)	$x \notin L \Rightarrow \forall P \Pr[\text{out}_V\langle V, P\rangle(x) = 1] \leq 1/3$

= 1



Why not allowing error on both sides?

- Recall: It is not known whether $\mathbf{RP} \overset{?}{=} \mathbf{BPP}$

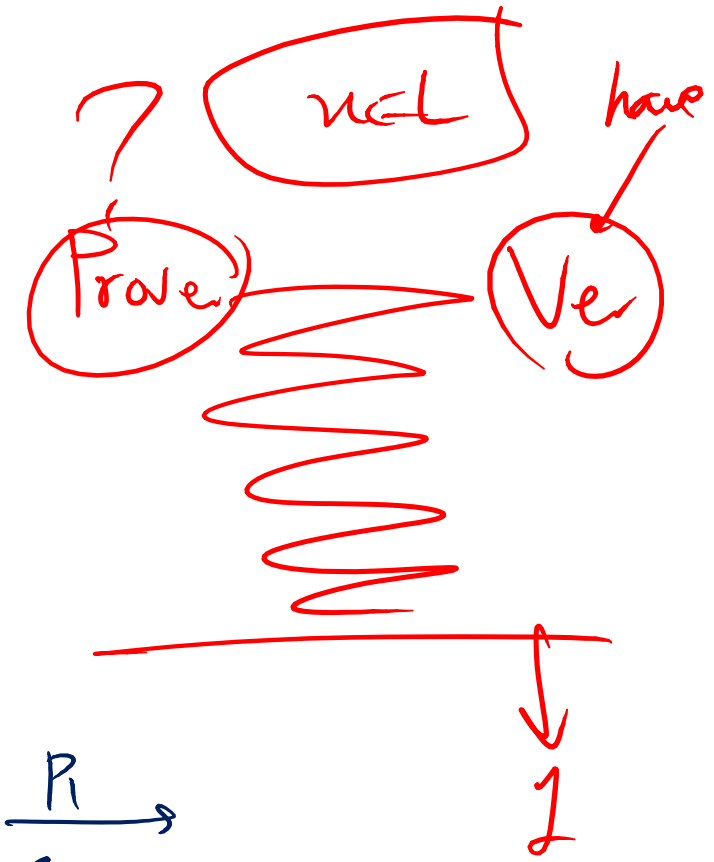
- However: the following two give the same class $\mathbf{IP}$

$$\begin{aligned} &\text{(Completeness)} && x \in L \Rightarrow \exists P \Pr[\mathtt{out}_V\langle V, P\rangle(x) = 1] = 1 \\ &\text{(Soundness)} && x \notin L \Rightarrow \forall P \Pr[\mathtt{out}_V\langle V, P\rangle(x) = 1] \leq 1/3 \end{aligned}$$

$$\begin{aligned} &\text{(Completeness)} && x \in L \Rightarrow \exists P \Pr[\mathtt{out}_V\langle V, P\rangle(x) = 1] \geq 2/3 \\ &\text{(Soundness)} && x \notin L \Rightarrow \forall P \Pr[\mathtt{out}_V\langle V, P\rangle(x) = 1] \leq 1/3 \end{aligned}$$

Shamir's Theorem: IP = PSPACE

- **IP ⊆ PSPACE**



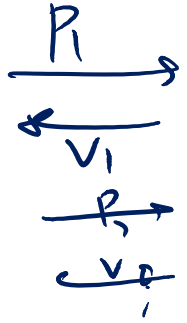
$L \in IP$

if $x \in L \rightarrow$ Prover $P_r[\text{Ver accep}] = 1$

if $x \notin L \rightarrow \forall P \rightarrow P[V \text{ accep}] \leq \frac{1}{3}$

find programp $P_r(x)$ that maximizes $P_r[\text{Ver accep}]$

time & spaces



given x run $P_r \leftrightarrow^{x} \text{Ver}$ and see if Ver accepts?

IP = PSPACE

- **PSPACE ⊆ IP**

- Note: even showing TAUTOLOGY ⊆ **IP** is highly nontrivial!

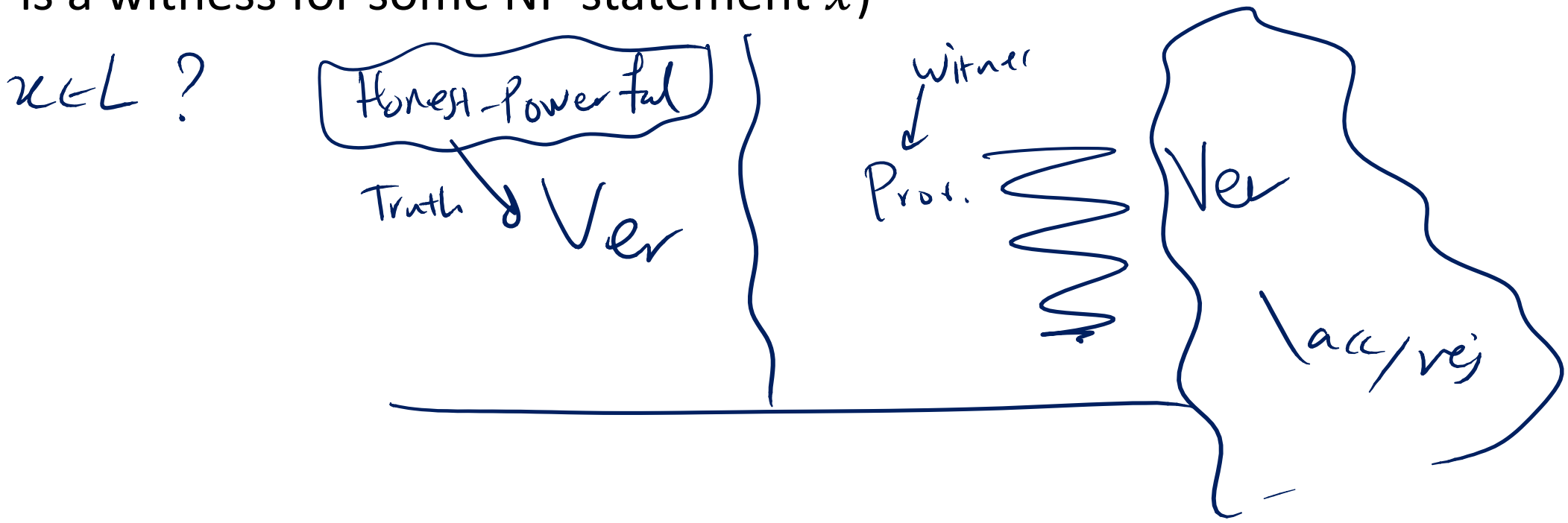
- Idea: write a CNF formula ϕ as a polynomial $p_\phi(\cdot)$ such that $p_\phi(\vec{b})$ is 1 iff $\phi(\vec{b}) = 1$ then Prover proves the value of

Arithmatization.

$$\sum_{b_1 \in \{0,1\}} \sum_{b_2 \in \{0,1\}} \cdots \sum_{b_n \in \{0,1\}} P_\phi(b_1, \ldots, b_n)$$

Another magic of interaction: Zero-Knowledge Proofs

- You know a secret w that could be "verified" and you want to sell it (w is a witness for some NP statement x)



$GI : (G_1, G_2) \in GI$ iff $G_1 \equiv G_2$ $\quad f : V_{G_1} \longrightarrow V_{G_2}$

$(x,y) \in E_{G_1}$ iff $(f(x), f(y)) \in E_{G_2}$

Prover $\quad G_1 \overset{\text{clair}}{\equiv} G_2 \quad$ Ver

Complet- $x \in L \Longrightarrow$ Ver accept $\longleftarrow$ Zero knowledge.

Sound. $x \notin L \longrightarrow$ Ver reject

Prove $G_2 \equiv H \equiv G_1$

H

Ver

b

f : map H to G_b

$G_1 \not\equiv G_2$

$\forall H \; \exists b$

$G_b \not\equiv H$

$\rightarrow Pr[\text{Ver ask } b] = \frac{1}{2}$