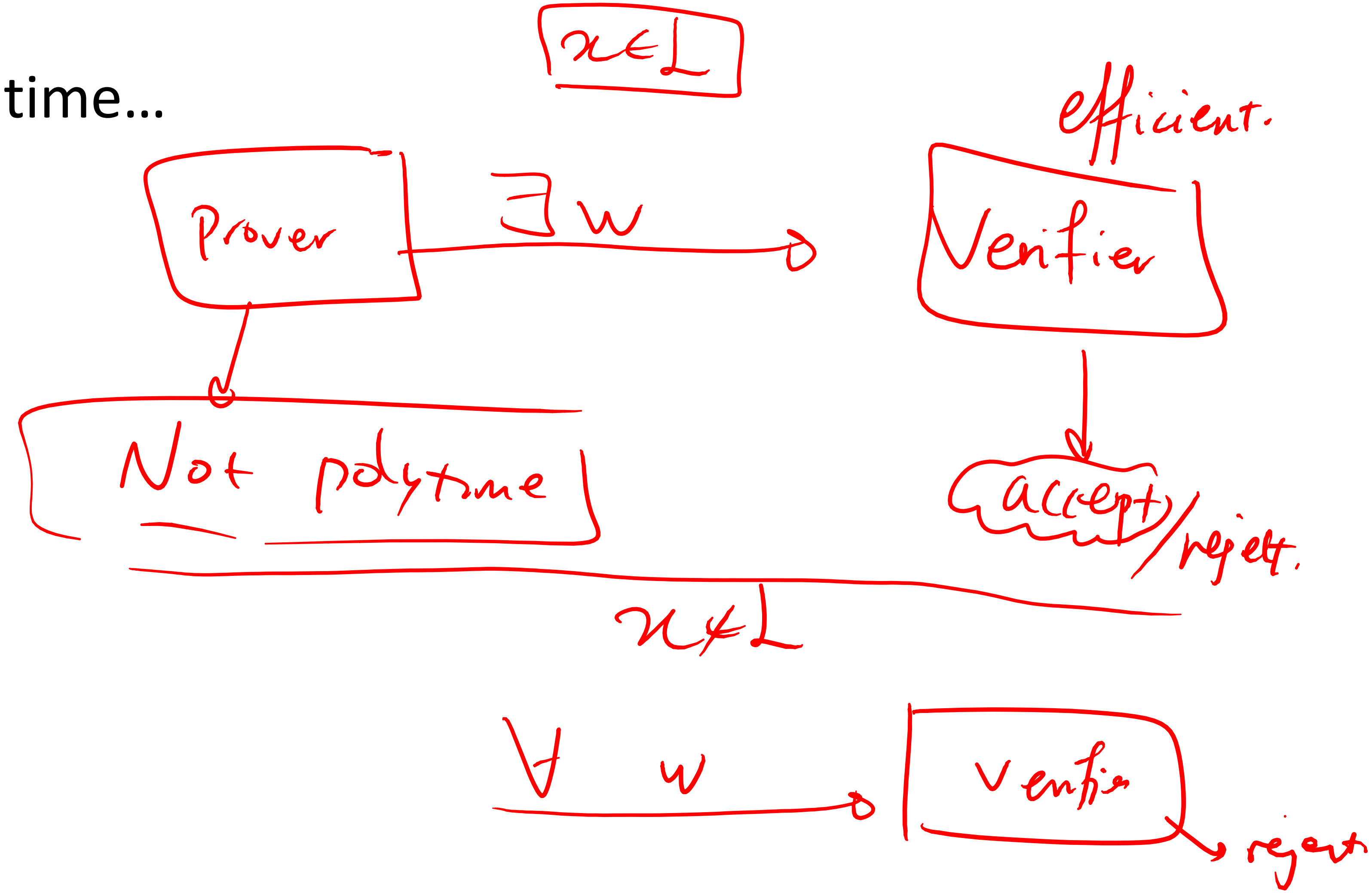
Computational Complexity

Mohammad Mahmoody

Session 24
April 2014

Interactive Proofs – Revising notion of “proof”

- Recalling **NP** one more time…



Allowing interaction (interrogation)

- Coke vs. Pepsi

if you right, $\boxed{\text{convinced always}}$

if coke = pepsi $\Longrightarrow \Pr[\text{convinced}] \leq \frac{1}{2}$

claim: coke $\neq$ pepsi

You prover.

challenge $\in_R$ {coke, pepsi}

identify challenge.

Moni: Verifier

- Informal Definition:
  IP = class of "problems" whose solution can be proved interactively

Graph Non-Isomorphism

$GI : L : \{ (G_1, G_2) \mid G_1 \equiv G_2 \}$

$GI \in NP$

- It is not known whether GNI $\overset{?}{\in}$ **NP** or not... but we show GNI ∈ **IP**

Prover

Claim: $G_1 \not\equiv G_2$

Verifier

H'

Choose $H \in \{G_1, G_2\}$

relabel nodes of H at random

get H'

b

$G_b \equiv H'$

✓ If prover Correct in claim ⟹ verifier accepts.

★ prover is lying

H''s distribution is independent of choice of H ⟹ prover can guess b w.p. $\leq \frac{1}{2}$

$$\Pr[E_1 \wedge E_2] = \Pr[E_1] \cdot \Pr[E_2 | E_1]$$

Can we decrease the "error" ?

P_1 We have a 2-message interactive protocol to GNI

Completeness: if $x \in GNI \Longrightarrow$ honest prover convinces verifier

Soundness: if $x \notin GNI$ $(G_1 \equiv G_2)$ $\Longrightarrow$ for any prover: Verifier rejects w.p. $1-(\frac{1}{2})$ ← err

Protocol 2: Prover $\boxed{P_1}$ if verifier accept run $\boxed{P_1}$ again

Verifier: accept iff both executions lead to accept.

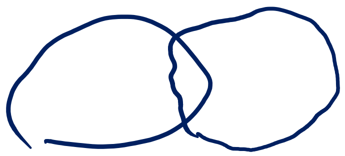
Completeness: if $x \in GNI \to$ Verifier accepts both executions

Soundness: $x \notin GNI$

$$\Pr[acc_1 \wedge acc_2] = \Pr[acc_1] \cdot \Pr[acc_2 | acc_1]$$

Is randomness of the verifier really helpful?

Definition 8.3 *(Deterministic proof systems)* We say that a language L has a *k-round deterministic interactive proof system* if there's a ~~deterministic~~ TM V that on input $x, a_1, \ldots, a_i$ runs in time polynomial in $|x|$, and can have a k-round interaction with any function P such that



Why dIP is not interesting?

$NP \subseteq dIP$

$NP = dIP$

transcript is witness

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