LECTURE 14

Note Title 4/1/2007

TODAY: Interactive Proofs

- AM
- IP
- IP $\subseteq$ PSPACE ...

Classical Notion of Proof $\approx$ NP

Theorem: $T \in \Sigma^*$

Proof: $\Pi \in \Sigma^*$

Π proves T if $V(T, \Pi) = 1$.

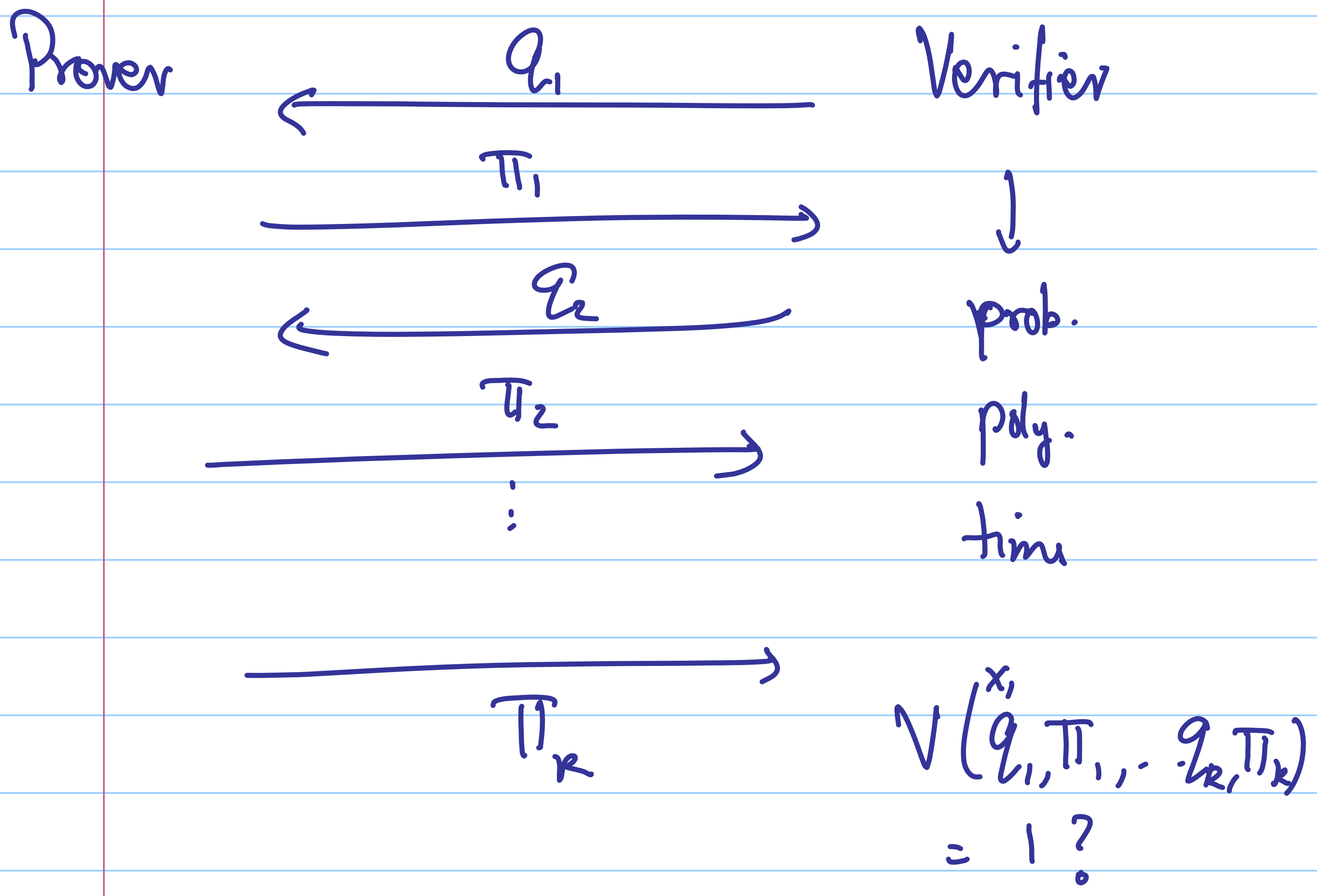
$|\Pi| = |T|^{O(1)}$ & V polytime

$\Rightarrow$ "True-Theorem" in NP.

Interactive Proofs :

- Arose in context of cryptography;
- How do you prove X while keeping Y secret (modulo truth of X) ?
- E.g. I am allowed to access account
  "madhu@mit.edu"
  without revealing & my password is
  "blah-blah"
- Interactive proofs different from non-interacti
  ones.

Model



$L \in IP$ if $\exists\ \underset{\uparrow}{Q}, \underset{\uparrow}{V}$

prob. poly time s.t.

for $q_i = Q(x, \pi_1 \dots \pi_{i-1}, R, i)$

$x \in L \Rightarrow \exists P$ s.t. $V(x, \pi_1 \dots \pi_k, R) = 1$

w.p. $\geq c(n)$

$x \notin L \Rightarrow \forall P$ - - - $< s(n)$

$$\pi_i = P(x, q_1 .. q_i).$$

Related notion

Arthur-Merlin Proofs [Babai]

Motivation: some number-theoretic problems don't appear NP-hard.

$L \in NP$

$\bar{L}$ not quite in NP

but close ...

Formally: $\bar{L} \in AM$ ...

$$\begin{tikzcd} \text{Merlin} \arrow[rr, shift right, "\pi_1"'] & & \text{Arthur} \arrow[ll, shift right, "q_1"'] \end{tikzcd}$$

$x \in L$ ---

Historical Issues

1. Coins of Verifier $\underset{\substack{\uparrow \\ (\text{AM})}}{\text{public}}$ or $\underset{\substack{\uparrow \\ (\text{IP})}}{\text{private}}$

   [Goldwasser - Sipser] : Can convert private to public .

2. Error : one-sided or two-sided

   [Goldreich Mansour ?] : Can assume one-sided

3. # Rounds : Constant ? (→ associated with AM)

   Poly ? (IP).

Constant ⇒ 2 rounds.

[GMR] $IP \subseteq PSPACE$

[GMW] $GNI \in IP$; $GNI \in AM$

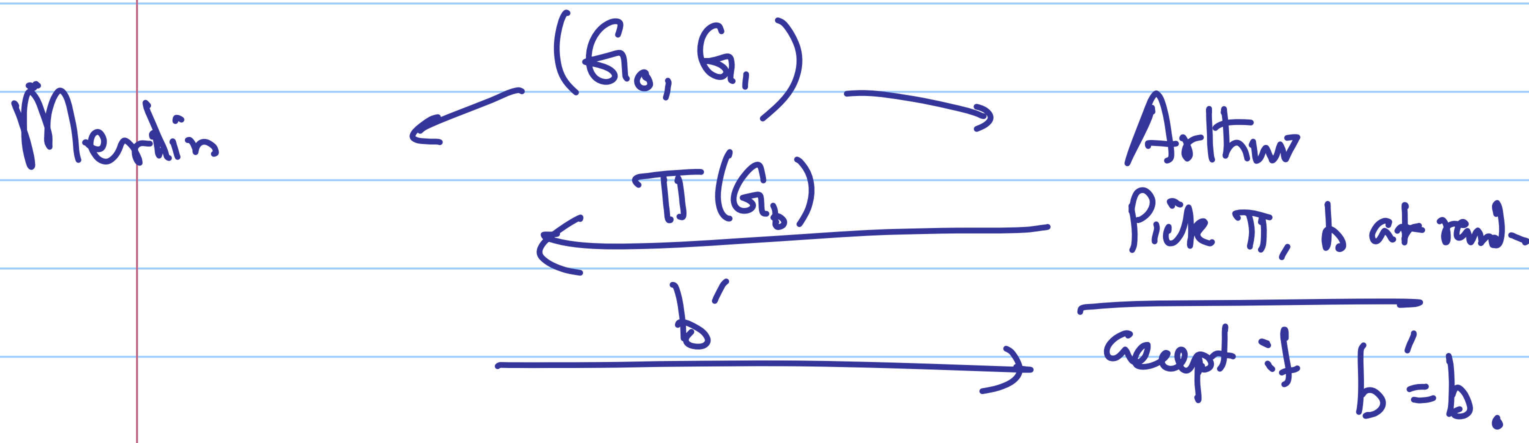
Complexity Classes from IP

$NP \subseteq MA \subseteq AM \subseteq IP \overset{\circ}{=} IP(poly) \subseteq PSPACE$.

↑ prob. verifier

Example:

$GNI \subseteq AM$:



1. IP $\subseteq$ PSPACE.

Proof Idea:

Key Concept: Optimal Prover

- $P^*(x, q_1, \pi_1, q_2, \pi_2, \ldots q_i)$:

  determines "optimal" answer to q_i, given history $x, q_1, \pi_1 \cdots q_{i-1}, \pi_{i-1}$.

- Prob $(x, q_1 \ldots q_i, \pi_i)$:

  computes prob. acceptance given history $x, q_1 \ldots q_i, \pi_i$.

  using P^* for answers to future questions.

- Gives big computation tree of max & avg. nodes ...
- Can be computed in PSPACE.

One-Sided Error? Public Coins?

Easy in poly rounds [Kilian]

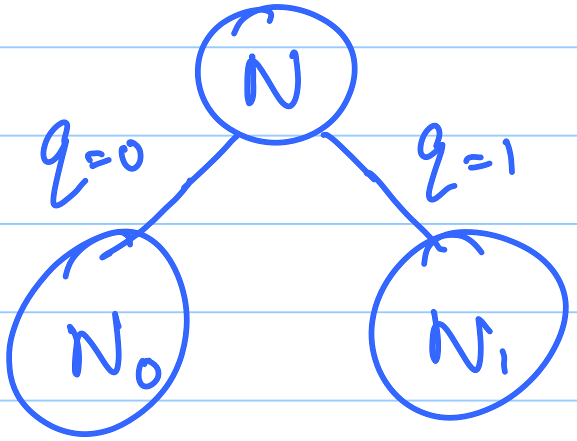
Idea: Assume questions binary; & random coins revealed at end;

∴ So fixing optimal prover P^*; Verifier's view is a tree & he wants to know how many paths accepts

$$V \longrightarrow V'$$

arbitrary

public-coin
one-sided ...



V': wants to know how many accepting paths at root.

P': sends # N to V'.
also for two children.

V': picks q with prob. $\frac{N_q}{N}$ (if $N = N_0 + N_1$)

Analysis: Suppose prover claims $N' > N$

Then (inductively) caught w.p. $1 - \frac{N}{N'}$

Proof: Prob. Catching

$$= \left(1 - \frac{N_0}{N_0'}\right) \cdot \frac{N_0'}{N'}$$

$$+ \left(1 - \frac{N_1}{N_1'}\right) \frac{N_1'}{N'}$$

$$= \frac{1}{N'}\left[N_0' + N_1' - N_0 + N_1\right]$$

$$= 1 - \frac{N}{N'} \quad \textcircled{!}$$

(Should verify base case...)

Harder version : $O(1)$ -rounds.

Will show it for 2 round protocol :

Step 1: Verifier picks $R \in \{0,1\}^r$

: Computes $q = q(R, x)$

Step 2: Sends $q \rightarrow$ prover

Prover answers with $\pi = \pi(q)$

Step 3: Accept if $V(x, R, \pi) = 1$.

Want to convert this to public coin version.

[Goldwasser - Sipser]

1. Key Ingredient : Protocol for "approx. counting"

- Given : $S \subseteq \{0,1\}^n$

  "membership in S" $\in$ AM

- $|S| \geq f(n) \Rightarrow$ accept w.p. 1
- $|S| \leq \frac{f(n)}{?} \Rightarrow$ accept w.p. $\leq \frac{1}{2}$

2. Use above to prove that for fixed (q,a)

$$S_{(q,a)} = \{ R \mid q(R) = q \text{ \& } V(x,R,a) \text{ accepts} \}$$

is large.

3. Can use above to prove

$$\sum S_{q,a} \text{ is large.}$$

Protocol for approx. Counting

Verifier V':

- Picks $h: \{0,1\}^r \to 2 \cdot [f(n)]$
- Asks for R s.t. "$R \in S$" & "$h(R) = ?$" ← to be fixed later

$$V' \xrightarrow{\quad h \quad} P'$$

P': Picks shifts $s_1 \dots s_t$

$t = O(\log(f(n)))$.

$$\xleftarrow{\quad s_1 \dots s_t \quad}$$

$$V' \xrightarrow{\quad y \quad}$$

Now P' proves to V' that
$\exists\, R \in S$ (2 proves this)
s.t. $h(R \oplus S_i) = y$ for some i.

[Combines [Valiant-Vazirani]
& [Lauteman-Sipser]]

* * *

Similar proofs yield

$$IP[k] \subseteq AM[O(k)] \subseteq AM\left[\frac{O(k)}{c}\right] \quad \forall c.$$

$$AM[O(1)] = AM[2] = BP\cdot\exists \; ..$$