Sp 2014

Lecture 4

- p.i. random bits to reduce error
- Random bits for Interactive proofs
    - IP
    - Graph $\ncong$

Using Pairwise Independence to reduce error

Setting:

Given RP algorithm $\mathcal{A}$

- if $x \in L$ $\Pr_R[\mathcal{A}$ on input x, random bits R, outputs ACCEPT$] > 1/2$
- if $x \notin L$ " $= 0$

How can we reduce error?

1) Repeat $\mathcal{A}$ k times
use new random bits each time
if ever see "ACCEPT" then output "ACCEPT"
else output "REJECT"

$\Big\}$ Uses $O(k \cdot |R|)$ random bits

behavior:

if $x \in L$ $\Pr[\text{"ACCEPT"}] \geq 1 - (1 - 1/2)^k$
$\geq 1 - \frac{1}{2^k}$

if $x \notin L$ $\Pr[\text{"ACCEPT"}] = 0$

$\therefore$ error probability $\leq 2^{-k}$

2) "2-point sampling"

idea: use p.i. samples instead

assumption: given $\mathcal{H}$, family of p.i. fctns mapping $\{0,1\}^{k+2} \to \{0,1\}^{|R|}$
st. can pick random $h \in \mathcal{H}$ with $O(k+|R|)$ random bits
+ poly $(k, |R|)$ time

Sampling algorithm

- pick $h \in_R \mathcal{H}$
- for $i = 1 .. 2^{k+2}$

  $r_i \leftarrow h(i)$

  if $\mathcal{A}(x, r_i) =$ "ACCEPT" output "ACCEPT" + halt
- output "REJECT"

random bits used: $O(k+|R|)$

behavior:

if $x \notin L$, $\Pr[\text{ACCEPT}] = 0$

if $x \in L$:

will misclassify if never see r_i st. $\mathcal{A}(x, r_i) =$ "ACCEPT"

let $c(r_i) = \begin{cases} 0 & \text{if } \mathcal{A}(x, r_i) = \text{"REJECT"} \\ 1 & \text{o.w.} \end{cases}$ ← $\mathcal{A}$ correct!

let $Y = \sum_{i=1}^{q=2^{k+2}} c(r_i)$

$$E\left[\frac{Y}{q}\right] \geq \frac{2^{k+2}}{2^{k+2}} \cdot \frac{1}{2} = \frac{1}{2}$$

Two useful lemmas:

Chebyshev's ≠: X r.v.

$E[X] = \mu$

$\Pr[|X-\mu| \geq \varepsilon] \leq \frac{Var[X]}{\varepsilon^2}$

Pairwise Independence Tail ≠:

$X_1 \cdots X_t$ p.i. r.v.'s in $[0,1]$

$X = \frac{\sum X_i}{t}$

$\mu = E[X]$

then $\Pr[|X-\mu| \geq \varepsilon] \leq \frac{1}{t\varepsilon^2}$

---

what is $\Pr[\frac{Y}{q} = 0]$? i.e. $\Pr[\text{"REJECT"}]$

$$\Pr[\text{"REJECT"}] = \Pr[\tfrac{Y}{q} = 0]$$

$$\leq \Pr\Big[\Big|\frac{Y}{q} - \overbrace{E[\tfrac{Y}{q}]}^{\mu}\Big| \geq \underbrace{E[\tfrac{Y}{q}]}_{\varepsilon}\Big]$$

$$\leq \frac{1}{q \cdot (\frac{1}{2})^2}$$

$$= 2^{-(k+2)} \cdot 4 = 2^{-k}$$

so, $O(k+|R|)$ random bits give $\leq 2^{-k}$ prob error

Note: runtime is still $O(2^k \cdot T_A(n))$

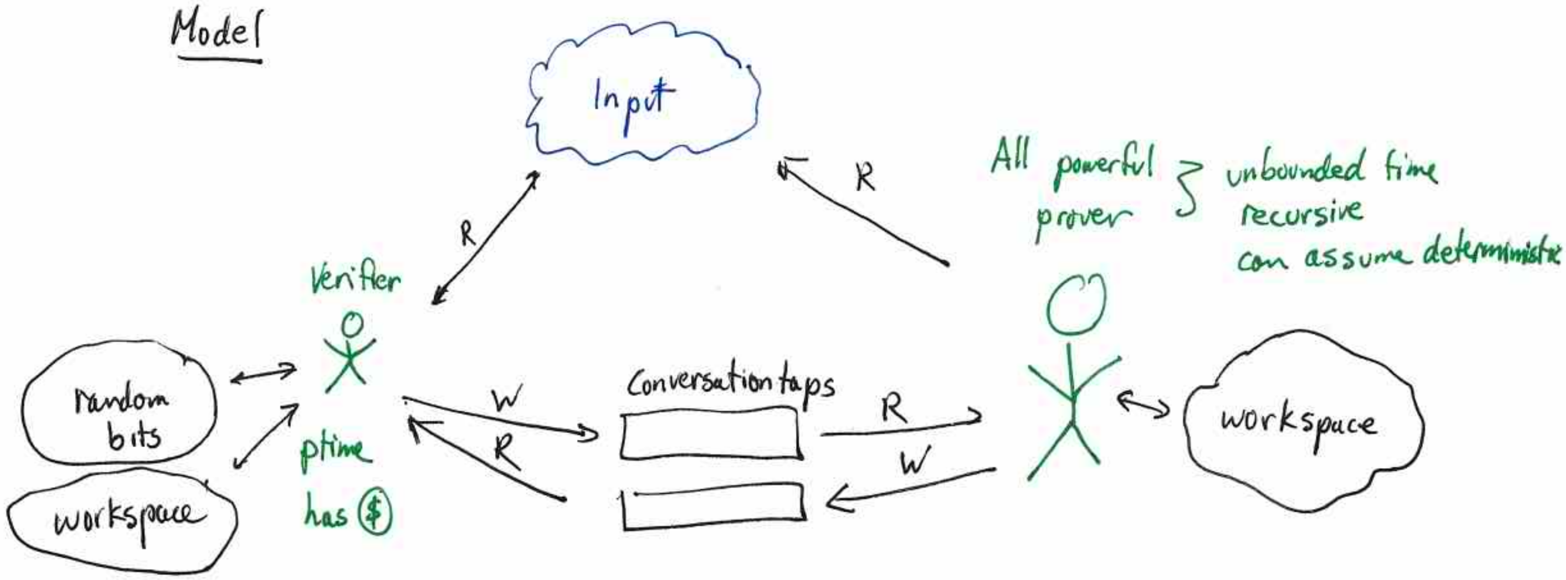
Interactive Proofs

NP = all decision problems for which "Yes" answers can be verified in ptime by a deterministic TM ("verifier")

IP: generalization of NP:

- short proofs $\Rightarrow$ short interactive proofs
  "conversations that convince"

Model



def "Interactive Proof Systems" (IPS) [Goldwasser Micali Rackoff]

for language L is protocol s.t.

- if V, P follow protocol & $x \in L$ then $\Pr_{V\text{'s coins}}[V \text{ accepts } x] \geq \frac{2}{3}$
- if V follows protocol & $x \notin L$ then (no matter what P does) $\Pr_{V\text{'s coins}}[V \text{ rejects } x] \geq 2/3$

<u>def</u> IP $= \{L \mid L$ has IPS$\}$

<u>Note:</u> Clearly $NP \subseteq IP$

turns out that $IP = PSPACE$!

Graph Isomorphism (GI)

<u>Input</u> G, H

<u>Output</u> is $G \cong H$? (i.e. $\exists\, \pi$ st. $(u,v) \in E_G$ iff $(\pi(u), \pi(v)) \in E_H$?)

<u>NOTE</u>: $GI \in NP \Rightarrow GI \in IP$

GI not Known to be in P

Graph Non-Isomorphism (GNI)

<u>Input</u> G, H

<u>Output</u> is $G \ncong H$?

<u>Note</u>: GNI not Known to be in P <u>or</u> NP

but is in IP! [Goldreich Micali Wigderson]

IP Protocol for graph $\ncong$:

<u>Input</u> G, H

<u>Protocol</u> Do $O(1)$ times:

- V computes G' : random permutation of G
  H' : " " " H

- V flips coin
  H: sends (G, G') to P
  T: sends (G, H') to P

- $P \to V$: $\cong / \ncong$

-

V flip	P response	V output
H	$\cong$	continue
H	$\ncong$	fail & halt
T	$\cong$	fail & halt
T	$\ncong$	continue

not same as $\notin L$ unless V follows protocol

Output "ACCEPT"

Proof of correctness

- if $G \not\cong H$, P can figure out coin toss & always answer correctly } here we use that P has unbounded time

- if $G \cong H$,
  - distribution of V's msgs are identical under H/T
  - since P deterministic wlog

    let $q \equiv$ fraction of random permutations π s.t. Prover $(G, \pi(G)) = $ "$\not\cong$"

    $$\Pr[\text{fail in round } i] = \frac{1}{2} \cdot q + \frac{1}{2}(1-q) = 1/2$$

    prob V flips H & expect $\cong$

    Prob V picks π s.t. P answers $\not\cong$

    prob V flips T & expect $\not\cong$

    Prob V picks π s.t. P answers $\cong$

<u>Note</u> V's random perm & coin flips must be hidden, or P could <u>cheat</u>!