Lecture 4

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

Using Pairwise Independence to reduce error

Setting:

Given RP algorithm A

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

How can we reduce error?

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

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

behavior:

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

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

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

2pt.:

2) "2-point sampling"

idea: use p.i. samples instead

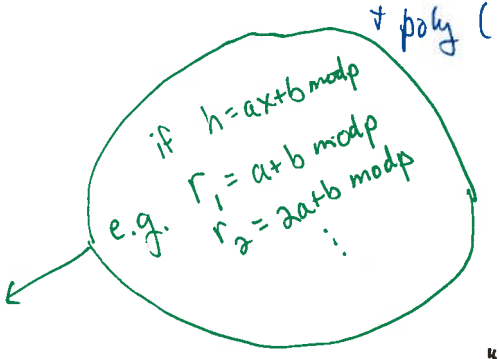
assumption: given $\mathcal{H}$, family of p.i. fctns (each one) mapping $[2^{k+2}] \to \{0,1\}$ s.t. can pick random $h \in \mathcal{H}$ with $O(k+|R|)$ random bits + poly $(k, |R|)$ time

Sampling algorithm

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

  $r_i \leftarrow h(i)$

  if $A(x, r_i)$ = "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 s.t. $A(x, r_i) =$ "ACCEPT"

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

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

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

← if $x \in L$ expect to see $> \frac{1}{2}$ "0"s what is probability you don't see any

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 $[0,r]$

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

$\mu = E[X]$

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

---

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

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

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

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

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

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

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

↑ bad, but doesn't depend on n

Interactive Proofs

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

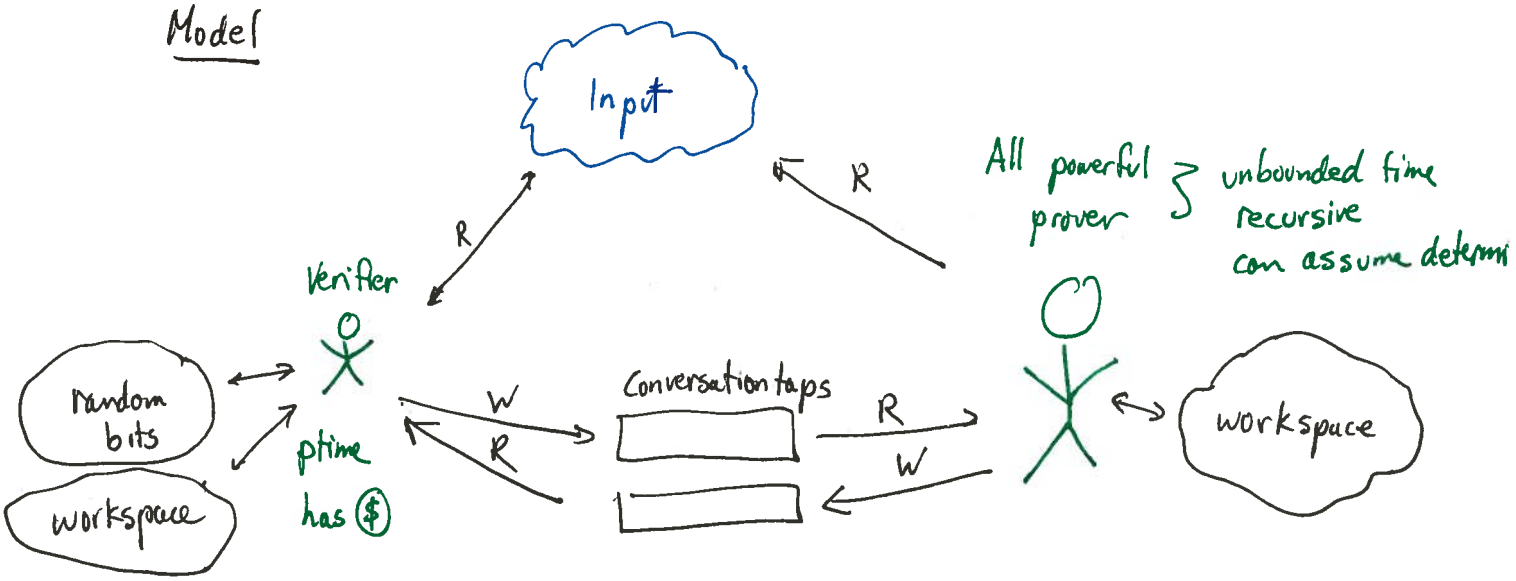
IP:

generalization of NP:

- short proofs ⇒ 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) $\Pr_{V\text{'s coins}}[V \text{ rejects } X] \geq 2/3$

def $IP = \{L \mid L \text{ has IPs}\}$

Note: Clearly $NP \subseteq IP$

turns out that $IP = PSPACE$!

Graph Isomorphism (GI)

Input G, H

Output is $G \cong H$? (i.e. $\exists \pi$ s.t. $(u,v) \in E_G$ if $(\pi(u), \pi(v)) \in E_H$

NOTE: $GI \in NP \Rightarrow GI \in IP$

GI not known to be in P (though is now known to be in quasi-P [Babai])

Graph Non-Isomorphism (GNI)

Input G, H

Output is $G \neq H$?

Note: GNI not known to be in P or NP

but is in IP! [Goldreich Micali Wigderson]

IP Protocol for graph $\not\cong$:

Input G, H

Protocol 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 → V: $\cong$ / $\not\cong$

V flip	P response
H	$\cong$
H	$\not\cong$
T	$\cong$
T	$\not\cong$

V output
continue
fail + halt
fail + halt
continue

} not same as $\not\in L$ 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 $(G, \pi(G)) = "\not\cong"$

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

- $\frac{1}{2}$: prob V flips H & expect $\cong$
- q: Prob V picks π s.t. P answers $\not\cong$
- $\frac{1}{2}$: prob V flips T & expect $\not\cong$
- $(1-q)$: Prob V picks π s.t. P answers $\cong$

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