Lecture 7

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

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"

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

behavior:

unlucky + saw reject every time

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

$\geq 1 - \frac{1}{2^k}$

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

$\therefore$ error probability $\leq 2^{-k}$ (1-sided error)

2) "2-point sampling"

idea: use p.i. samples instead

assumption: given $\mathcal{H}$, family of p.i. fctns each one mapping $[2^{k+2}] \to \{0,1\}^{|R|}$
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

  if $h = ax+b \bmod p$
  e.g. $r_1 = a+b \bmod p$
  $r_2 = 2a+b \bmod p$
  $\vdots$

- output "REJECT"

random bits used: $O(k+|R|)$ ☺
runtime: $O(2^k \times$ time for $A)$ ☹ (but doesn't depend on n)

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

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

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

terms in sum

q

$E[\sigma(r_i)] = Pr[\text{Accept}]$

if $x \in L$ expect to see $\geq \frac{1}{2}$ "accept"
what is probability you don't see any?

Two useful lemmas:

<u>Chebyshev's ‡:</u> X r.v.

$E[X] = \mu$

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

<u>Pairwise Independence Tail ‡:</u>

$X_1 \cdots X_t$ 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. $Pr[\text{"REJECT"}]$

this can happen if $\frac{Y}{q}=0$ or if $\frac{Y}{q} \geq 2E[\frac{Y}{q}]$

via calculation

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

$$\leq Pr\Big[\Big|\tfrac{Y}{q} - \underbrace{E[\tfrac{Y}{q}]}_{\mu = 1/2}\Big| \geq \underbrace{E[\tfrac{Y}{q}]}_{\text{choosing } \varepsilon = 1/2}\Big]$$

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

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

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

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

⇑ 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")

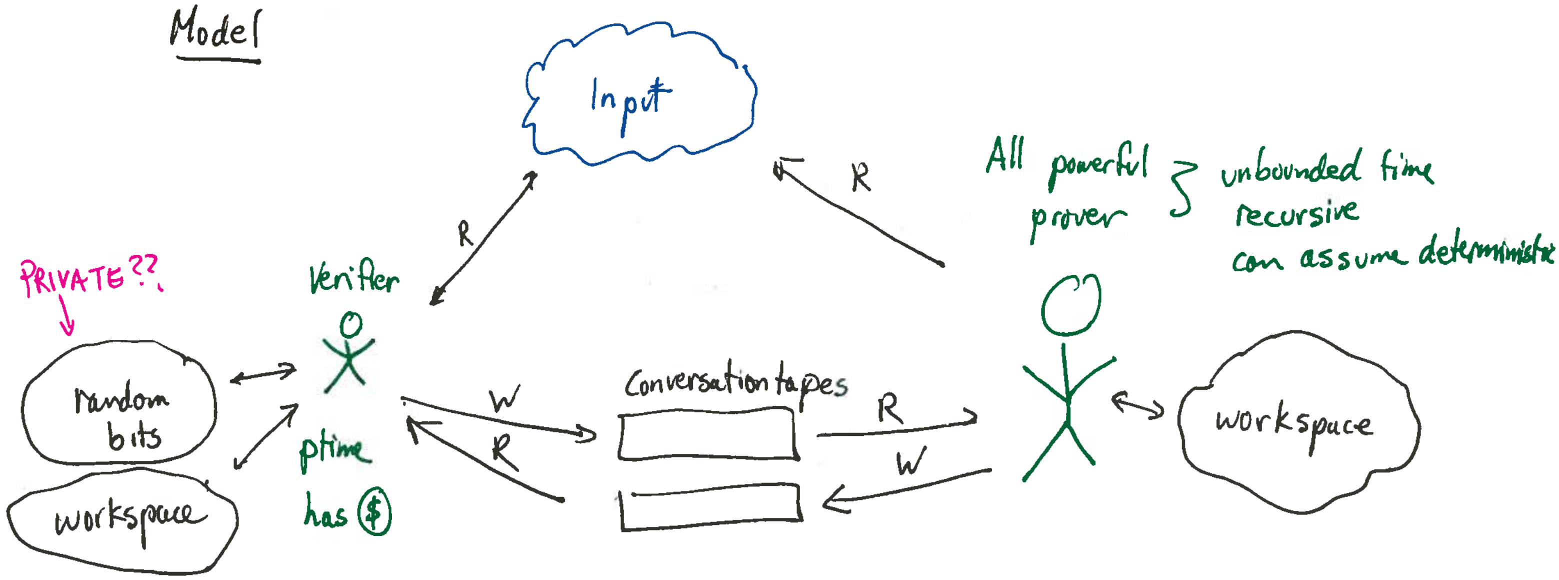
IP:

generalization of NP:

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

what if require that P follows protocol?

for crypto setting, useless!

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

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

turns out $IP = PSPACE$

<u>Today</u> [Goldwasser Sipser]

Protocol in which P can convince V that size of set S is "big".

Only need that $\forall x \in S$, can verify that x is in S in poly time

V can figure it out?
P can give V a proof?
P can interactively prove to V
All are good

Let $S_\phi = \{x \mid x$ satisfies $\phi\}$

<u>Note</u> given x, V can check that x satisfies ϕ

<u>Claim</u> exist protocol st. on input ϕ

- if $|S_\phi| > K$ + if V,P follow protocol then $Pr[V \text{ accepts}] \geq 2/3$
- if $|S_\phi| < \frac{K}{\Delta}$ + if V follows protocol then $Pr[V \text{ accepts}] < 1/3$

What is Δ? Assume $\Delta = 4$

- no requirement on P
- V will not accept even if P cheats!
- important for crypto

Why interesting?

Can use to show # random strings which cause algorithm $\mathcal{A}$ to accept on input x $\geq 2/3$

Used to show "public coin" model $\approx$ "private coin" model

ie. can prove same set of statements.

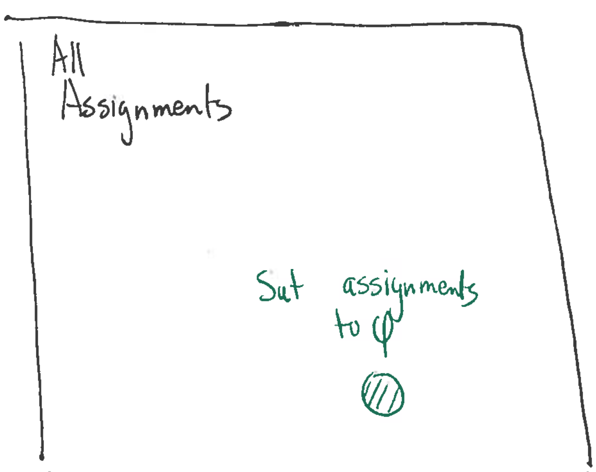
First idea Random sampling

Repeat ? times:

V picks random assignment x + evaluates $\phi(x)$

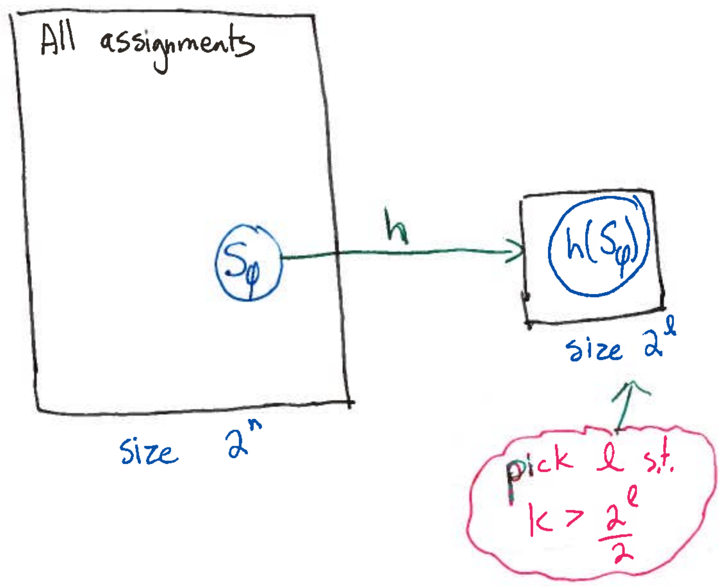
Outputs $\dfrac{\text{\# satisfied } x\text{'s}}{\text{total \# repetitions}}$

Needs $\Omega\left(\dfrac{\text{\# total assignments}}{\text{\# satisfying assignments}}\right)$ ← could be $\Omega(2^n)$



Problem: what if S_ϕ is very small compared to set of all assignments?

Fix: Universal Hashing



need:

1. $|h(S_\varphi)| \approx |S_\varphi|$
2. $\frac{|h(S_\varphi)|}{2^\ell}$ is $\frac{1}{\text{poly}(n)}$
   (in our case, constant)
3. h computable in poly time

Protocol: { For distinguishing set size k from set size ? }

Given H, collection of p.i. fctns mapping $\{0,1\}^n \to \{0,1\}^\ell$

1. V picks $h \in_R H$
2. $V \to P$: h
3. $P \to V$: $x \in S_\varphi$ s.t. $h(x) = 0^\ell$
4. V accepts iff $x \in S_\varphi$

Idea: hope: $h(S_\varphi)$ fills a "random" portion of range

Case 1 $|S_\varphi| > k$: hopefully $|h(S_\varphi)| \approx k$ so 0^ℓ hit with $\geq \frac{1}{2}$? reasonable probability
& all powerful P can find preimage in S_φ

Case 2 $|S_\varphi| < \frac{k}{\Delta}$: $|h(S_\varphi)| < \frac{k}{\Delta}$ so less likely 0^ℓ hit because V will detect
P can't send fake preimage

Recall H is p.i. family of hash fctns if

$$\forall\, x,y \in \{0,1\}^n \;\&\; \forall\, a,b \in \{0,1\}^\ell$$

$$\Pr_{h\in H}[\, h(x)=a \;\&\; h(y)=b \,] = 2^{-2\ell}$$

Lemma H is p.i., $U \subseteq \{0,1\}^n$, $a = \frac{|U|}{2^\ell}$

then $a - \frac{a^2}{2} \le \Pr_h[0^\ell \in h(U)] \le a$

if $U \equiv S_\varphi$ would be fraction mapped to if h maps U 1-1

Pf.

RHS:

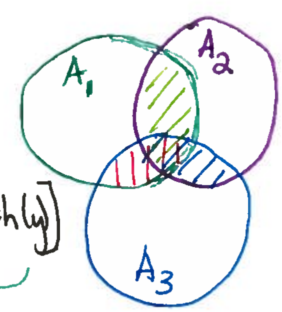
$\forall x \quad \Pr_h[0^\ell = h(x)] = 2^{-\ell}$ since H is p.i.

so $\Pr_h[0^\ell \in h(U)] \le \sum_{x\in U} \Pr[0^\ell = h(x)] = \frac{|U|}{2^\ell} = a$

union bnd

LHS:

$$\Pr[\cup A_i] \ge \sum_i \Pr[A_i] - \sum_{i\ne j} \Pr[A_i \cap A_j]$$



$$\Pr_h[0^\ell \in h(U)] \ge \sum_{x\in U} \underbrace{\Pr[0^\ell = h(x)]}_{2^{-\ell}} - \sum_{x\ne y\in U} \underbrace{\Pr[0^\ell = h(x) = h(y)]}_{2^{-2\ell}}$$

pairwise indep!

$$= \frac{|U|}{2^\ell} - \binom{|U|}{2}\frac{1}{2^{2\ell}} \ge \frac{|U|}{2^\ell} - \frac{|U|^2}{2}\cdot\frac{1}{2^{2\ell}}$$

$$\ge a - \frac{a^2}{2} \quad \blacksquare$$

Finishing up:

Pick ℓ s.t. $2^{\ell-1} \le k \le 2^{\ell}$. let $a = \frac{|h(S_\varphi)|}{2^{\ell}}$

if $|S_\varphi| > k$ then $a \ge 1/2$

so $\Pr[0^{\ell} \in h(S_\varphi)] \ge a - \frac{a^2}{2} \ge 3/8$

if $|S_\varphi| < \frac{k}{\Delta}$ then $a < \frac{\frac{k}{\Delta}}{2^{\ell}} < \frac{1}{\Delta}$

So $\Pr[0^{\ell} \in h(S_\varphi)] \le \frac{1}{\Delta}$

(Picking $\Delta = 4$ $\Rightarrow$) $\le \frac{1}{4}$

If repeat $O(\log 1/\beta)$ times,

Chernoff $\Rightarrow$ with prob $\ge 1-\beta$

if $|S_\varphi| > k$ then P is successful $\ge 3/8 - o(1)$ of the repetitions

if $|S_\varphi| < \frac{k}{\Delta}$ then P is successful $\le 1/4 + o(1)$ of the repetitions.

Can improve so that $\Delta = 1-\varepsilon$.

HOW???

Idea for general Thm:

i.e. $IP_{\substack{\text{private}\\\text{coins}}} = IP_{\substack{\text{public}\\\text{coins}}}$

argue that l.b. protocol can be used to show that size of accepting region probability mass is large.

(need that can verify a conversation/random coin to be in accept region)