Lecture 9

More applications of pairwise independence

- reducing randomness in amplification

- Interactive proofs.

  IP

  Graph $\not\cong$

  Public coins vs. private coins

Last time:

define pairwise independence

show how to extend m truly random bits

into $n \gg m$ pairwise indep random bits

e.g. q prime

pick random $a, b \in \{0 . \, q-1\}$

output

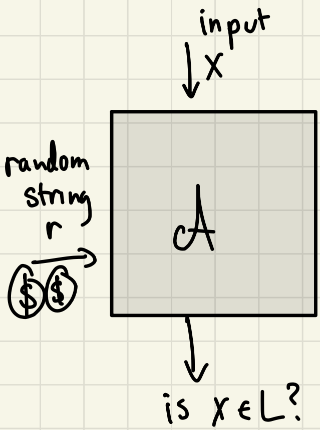
$$\left.\begin{array}{r} b \mod q \\ a+b \mod q \\ 2a+b \mod q \\ 3a+b \mod q \\ \vdots \end{array}\right\}$$

not independent but $\forall x, y$ $xa+b \mod q$ & $ya+b \mod q$ are unif distrib. in $\mathbb{Z}_q \times \mathbb{Z}_q$

$h_{a,b}(x) = ax + b \mod q$

family of fctns $\mathcal{H} = \{ h_{a,b} \mid a, b \in \mathbb{Z}_q \}$

Using Pairwise Independence to Reduce Error in Amplification



Given RP algorithm $\mathcal{A}$:

- if $x \in L$ $\Pr_r[\mathcal{A}(x, r)] = \text{accept}] > 1/2$
- if $x \notin L$ $\Pr_r[\mathcal{A}(x, r)] = \text{accept}] = 0$

How to reduce confidence error to $< 2^{-k}$?

<u>Method</u>	<u>#random bits used</u>
1) run k times on independent bits & output "$x \in L$" if see 1 & "$x \notin L$" o.w.	$k \cdot r$
2) use random walks to choose bits	$r + O(k)$ ← best in terms of runtime & # bits
3) today: use pairwise independence	$O(r+k)$ ↑ simpler analysis?

2-point sampling

idea use pairwise indep choices of random strings

assumption given $\mathcal{H}$, family of p.i. fctns

each $h \in \mathcal{H}$ maps $[2^{k+2}] \to \{0,1\}^r$

can pick random $h \in \mathcal{H}$ with $O(k+r)$ random bits & poly(k,r) time

we didn't show this

Sampling algorithm:

only place randomness is used

- 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"

if $h = ax+b \bmod p$

then $r_1 = a+b \bmod p$

$r_2 = 2a+b \bmod p$

$r_3 = 3a+b \bmod p$

$\vdots$

random bits used:

from assumption on $\mathcal{A}$

$$O(k + r)$$ ☺

runtime: $O(2^k \times \text{time for } \mathcal{A})$ ☹ but doesn't depend on n

behavior:

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

if $x \in L$,

will misclassify if <u>never</u> see

r_i s.t. $\mathcal{A}(x, r_i) = \text{"Accept"}$

let $\sigma(r_i) = \begin{cases} 0 & \text{if } \mathcal{A}(x, r_i) = \text{"reject"} \\ 1 & \text{o.w.} \end{cases}$ incorrect / correct

$$E[\sigma(r_i)] = \Pr[\sigma(r_i) = 1] = \Pr[\text{accept}] \geq \tfrac{1}{2}$$

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

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

so if $x \in L$ expect to see $\geq \frac{1}{2}$ "accepts". What is probability you don't see <u>any</u>? i.e. $\Pr[Y = 0]$?

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

Back to our analysis:

What is $\Pr[Y=0]$? ← only way we output wrong answer

$$\Pr[Y=0] = \Pr\left[\frac{Y}{q}=0\right]?$$

why $\leq$? absolute value can be $\geq 1/2$ if $Y/q = 0$ or if $Y/q \geq 2 \cdot E[Y/q]$

$$\text{Note} \quad \Pr\left[\frac{Y}{q}=0\right] \leq \Pr\left[\left|\frac{Y}{q} - \underbrace{E\left[\frac{Y}{q}\right]}_{\underbrace{\mu}_{\mu \text{ is } \geq 1/2}}\right| \geq \underbrace{E[Y/q]}_{\underbrace{\varepsilon}_{\text{choose } \varepsilon = 1/2}}\right]$$

t is $= q = 2^{k+2}$

$$= \frac{1}{q \cdot \left(\frac{1}{2}\right)^2}$$

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

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

note: runtime is $\underbrace{O(2^k \cdot T_A(n))}_{\text{bad?}}$ ☹

but doesn't depend on n. ☺

Another setting in which k-wise independence is useful:

Interactive Proofs

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

IP:

generalization of NP

Short proofs $\Longrightarrow$ short interactive proofs

"Conversations that convince"

The Pepsi Challenge (1975)

How to prove you can tell the difference:

Do K times:

- we toss coin (& don't show it to you)
  - H: we give you Pepsi
  - T: we give you Coke
- you taste & tell us which one

If you get it right K times, I'll believe you

why?

If you can tell difference, you will always get it right

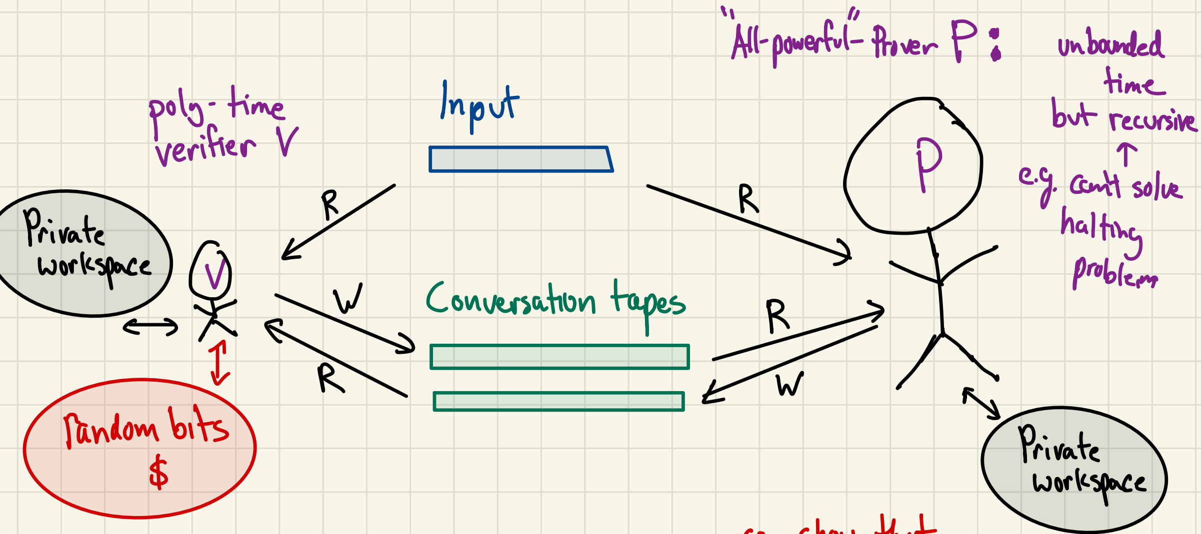
If you can't, you will get it right with prob $\frac{1}{2}$

$\Rightarrow$ prob you are right all K times $= \frac{1}{2^K}$

So, if you get it right K times,

you know or are very lucky!

IP Model



Private??

can show that "all-powerful" prover doesn't need random coins

(i.e. anything it can do with coins, it can also do without coins)

<u>def.</u> [Goldwasser Micali Rackoff]

An Interactive Proof System (IPS) for language L is protocol s.t.

- if $x \in L$ & both V, P follow protocol then

$$\Pr_{V\text{'s coins}}[V \text{ accepts } x] \geq 2/3$$

- if $x \notin L$ & V follows protocol then (no matter what P does)

$$\Pr_{V\text{'s coins}}[V \text{ rejects } x] \geq 2/3$$

So, if $x \in L$, P can "convince" V of that fact

+ if $x \notin L$, even if P tries to cheat it cannot convince V to accept.

why interesting?

Example 1 Cryptography

assume (1) L is a hard language to compute

+ (2) $x \in L \Leftrightarrow$ P is "the bank"

- P can convince V to trust it if it really is the bank
- no impostor can convince V to trust it

(leads to further notions such as zero-knowledge...)

For more take a crypto class!

Example 2 Complexity

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

Clearly $NP \subseteq IP$

To show $x \in L$ for L in NP

- P constructs NP-proof & sends to V
- V verifies the proof

for $x \notin L$, there is no proof that would convince V

turns out

Thm $IP = PSPACE$

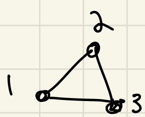
protocol involves several rounds of interaction between P & V

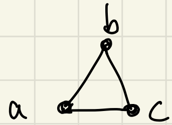
Graph Isomorphism

Given graphs G & H, are they isomorphic?

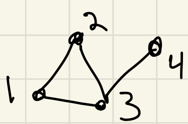
$\pi : V_G \to V_H$ is isomorphism if satisfies

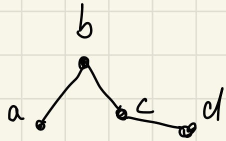
$(u,v) \in E_G$ iff $(\pi(u), \pi(v)) \in E_H$



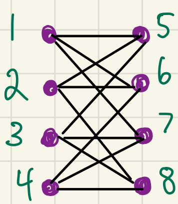


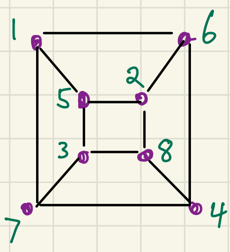
yes!





no!





yes!

Is Graph $\cong$ in P? we don't know. recently $O(n^{\text{polylog} n})$ "quasi-poly"

so unlikely to be NP-complete

Example of problem that has interesting interactive proof:

- Graph Isomorphism $\in NP$

- $\overline{\text{Graph Isomorphism}} \in NP$? (yes if $GI \in P$, but we don't know this)

but $\overline{GI} \in IP$:

Proving $G_1 \ncong G_2$:

Protocol:

repeat k times
- Verifier picks $c \in \{1,2\}$ randomly
- Verifier picks random relabeling of nodes in G_c + sends new adjacency matrix to P
- P guesses c

Why does it work?

if $G_1 \ncong G_2$, P (who has unbounded computation) can guess correctly every time

if $G_1 \cong G_2$, P needs to guess coin flips correctly each time, can do this with prob $\leq 1/2^k$

Question: do V's coins need to be private?

in this example, if P saw V's choice, it could cheat

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

$$IP_{\substack{\text{private}\\ \text{coins}}} = IP_{\substack{\text{public}\\ \text{coins}}}$$

GS's Answer: NO!
anything that has protocol with private coins also has (possibly different) protocol with public coins.

today we will see a <u>building</u> <u>block</u> for theorem:

<u>Informally</u>:
- Given set S s.t. $S \in IP$ ← interesting even if $S \in P$
- Protocol in which P can convince V that size of set S is "big"

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

(note $S_\phi \in P$)

<u>Claim</u> $\exists$ protocol s.t. 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 ← even if P cheats!
  then $\Pr[V \text{ accepts}] < 1/3$

for now assume $\Delta = 4$

Note:

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

First idea Random Sampling

Repeat ? times:

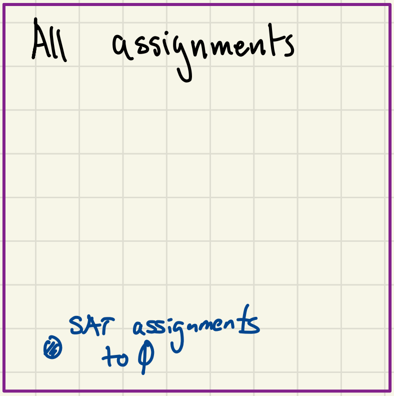
V picks random assignment x + evaluates $\varphi(x)$

Output $\dfrac{\text{\# satisfying } x\text{'s}}{\text{total \# repetitions}}$

how many repetitions?

$$\Omega\left(\frac{\text{\# total assignments}}{\text{\# satisfying assignments}}\right)$$

could be $\Omega(2^n)$



Problem;
what if S_ϕ is small?

Fix : Universal hashing

Recall:

Family of fctns $\mathcal{H} = \{h_1, h_2 \dots\}$

for $h_i : [N] \to [M]$ is

"pairwise independent" if

when $h \in_u \mathcal{H}$

(1) $\forall x \in [N], \quad h(x) \in_u [M]$

any locn x is mapped uniformly

(2) $\forall x_1 \neq x_2 \in [N], \; (h(x_1), h(x_2)) \in_u [M]^2$

any pair of locns $x_1 \neq x_2$ mapped uniformly & independently

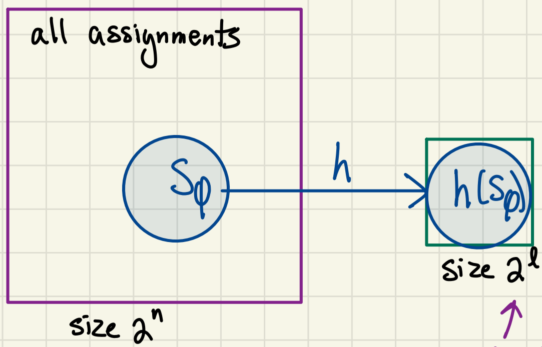
equivalently:

$\forall x_1 \neq x_2 \in [N]$

$\forall y_1, y_2 \in [M]$

$$\Pr_{h \in \mathcal{H}}[h(x_1) = y_1 \;\&\; h(x_2) = y_2] = \frac{1}{M^2}$$

How does it help?



pick ℓ s.t.

$$2^\ell > k \geq \frac{2^\ell}{2}$$

Need:

1. $|h(S_\varphi)| \approx |S_\varphi|$
2. h computable in poly time

idea

- Clearly $|h(S_\varphi)| \leq |S_\varphi|$
- hopefully $|h(S_\varphi)|$ is not too much smaller than $|S_\varphi|$

this is a very nice property of p.i. hash fctns.

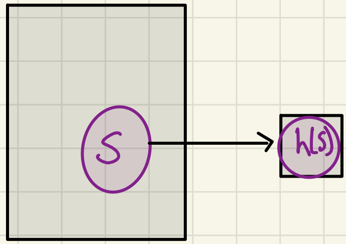
(we will show that whp $|h(S_\varphi)| > \frac{|S_\varphi|}{\Delta}$)

$\Rightarrow$ if ℓ s.t. 2^ℓ is roughly $|h(S_\varphi)|$

then most of $1..2^\ell$ gets mapped to by $h(S_\varphi)$

(uses that $\mathcal{H}$ is p.i.)

A comment about p.i. hash fctns



typical use:

- map set S into smaller "space"
- good for storage, reducing size of "names" of elements ...
- need property of $\underbrace{\text{"few collisions"}}$

since collisions cause problems, so need to minimize
(e.g. in hash tables, collisions ⇒ chaining length)

- here "few collisions" ⇒ $|h(S)|$ is not too much smaller than $|S|$

Why is that good?

- pick any pt in range, say 0^ℓ
- if h(S) big, it will probably hit 0^ℓ

uses that h(x) is unif dist

Protocol: for distinguishing set of size K from set of size K/Δ

Given $\mathcal{H}$ (p.i. fctns mapping $\{0,1\}^n \to \{0,1\}^\ell$)

1. V picks $h \in_R \mathcal{H}$
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 "random" portion of range, so can distinguish $|h(S_\varphi)|$ large or small.

Case 1 $|S_\varphi| > K$:

hopefully $|h(S_\varphi)| \approx K$ so 0^ℓ is "hit" with reasonable ($\geq \frac{1}{2}$?) probability.

Then all-powerful P can find preimage in S_φ

Case 2 $|S_\varphi| < \frac{K}{\Delta}$:

$|h(S_\varphi)| < K/\Delta$ so less likely 0^ℓ hit.

if not hit, P can't find preimage.

If P sends V a fake preimage, V will detect.

if $U \equiv S_\varphi$ & h maps S_φ 1-1 (which is unlikely) then a is fraction mapped to

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

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

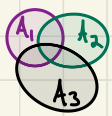
Proof

RHS:

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

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

LHS: $\Pr[\cup A_i] \underset{\uparrow\ \text{inclusion exclusion}}{\ge} \sum_i \Pr[A_i] - \sum_{i \ne j} \Pr[A_i \cap A_j]$



for $A_x \equiv$ "$0^\ell \in h(x)$":

$$\Pr_{h \in \mathcal{H}}[0^\ell \in h(U)] \ge \sum_{x \in U} \underbrace{\Pr[0^\ell = h(x)]}_{2^{-\ell}} - \sum_{x \ne y \in U} \underbrace{\Pr[0^\ell = h(x) = h(y)]}_{2^{-2\ell} \text{ if pairwise indep}}$$

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

$$\ge a - a^2/2$$

∎

Finishing up:

Pick ℓ s.t. $2^{\ell-1} \le k \le 2^{\ell}$

let $a = \dfrac{|S_\varphi|}{2^\ell}$

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

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

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

assumption on k

so $\Pr[0^\ell \in h(S_\varphi)] \le a < \dfrac{1}{\Delta}$

e.g. picking $\Delta = 4$ gives

$\le 1/4$

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

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

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

if $|S_\varphi| \le \dfrac{k}{4}$ then P is successful $\le 1/4 + o(1)$ of repetitions

Comments

- Can improve so $\delta = 1 - \varepsilon$ (how??)
- Can use same idea to prove

$$IP_{\substack{\text{private}\\\text{coins}}} = IP_{\substack{\text{public}\\\text{coins}}}$$

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

(need that V can verify a conversation/random coin flips transcripts falls into accept region).