Lecture 8

More applications of pairwise independence

- reducing error

- 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 $\forall x, y$

$xa+b \mod q$

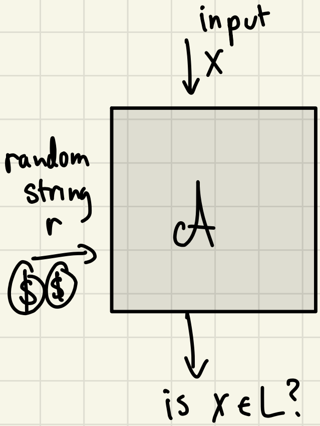
& $ya+b \mod q$

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



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?

Old way:

repeat $\mathcal{A}$ k times with <u>new</u> random bits each time

- if ever see "accept" then output "accept"
- else output "reject"

$\Big\}$ $O(k \cdot r)$ random bits

behavior:

$x \in L$: $\Pr[\text{accept}] \geq 1 - (1 - \frac{1}{2})^k \geq 1 - \frac{1}{2^k}$

$x \notin L$: $\Pr[\text{accept}] = 0$ $\quad \therefore$ conf error $< 2^{-k}$

1-sided error

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. $\mathcal{A}(x, r_i) =$ "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

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

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

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

so if $x \in L$ expect to see $\geq 1/2$ "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

$$\shortparallel$$

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

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

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

t is $= q = 2^{k+2}$ $\longrightarrow$ $= \dfrac{1}{q \cdot \left(\frac{1}{2}\right)^2}$

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

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

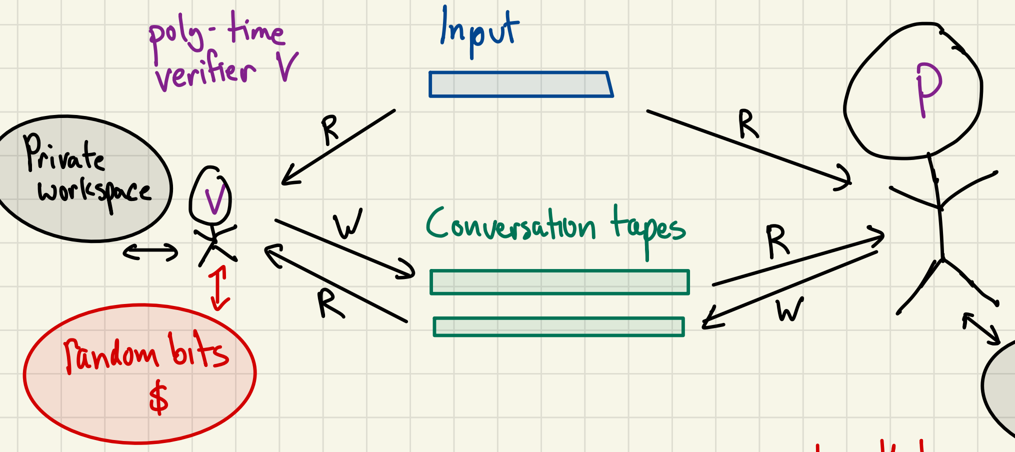
If you can't, you will get it right with prob $\frac{1}{2}$

$\Rightarrow$ 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

"All-powerful" Prover P: unbounded time but recursive ↑ e.g. can't solve halting problem



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)

def. [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) $x \in L \iff$ 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 $IP = PSPACE$

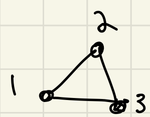
protocol involves several rounds of interaction
between P & V

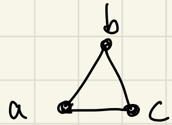
Graph Isomorphism

Given graphs G & H, are they isomorphic?

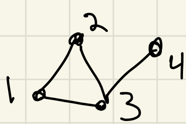
$\pi : V_G \to V_H$ is isomorphism if satisfies

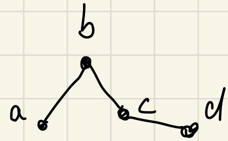
$$(u,v) \in E_G \text{ iff } (\pi(u), \pi(v)) \in E_H$$



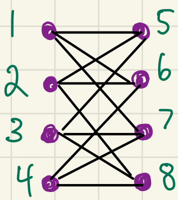


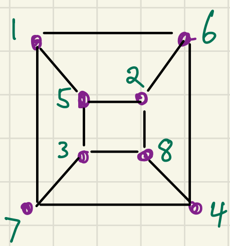
yes!





no!





yes!

"quasi-poly"

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

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 $G_1 \not\cong G_2$:

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 $G_1 \not\cong G_2$, 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]

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

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 $S_\phi = \{x \mid x$ 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 $\Delta = 4$