Lecture 22:

Pseudorandomness &

Unpredictability

Another notion of randomness?

Unpredictability

Def. $X = X_1 \cdots X_n$ is "next bit unpredictable"

if $\forall$ ppt P, $\exists$ negligible fctn $\varepsilon(n)$

s.t. $\Pr_{X,\, i \in_R [n],\, \text{coins of } P} [P(X_1 \cdots X_{i-1}) = X_i] \leq \frac{1}{2} + \varepsilon(n)$

Note:

X uniform $\Rightarrow \varepsilon = 0$

X statistically close to uniform $\Rightarrow \varepsilon(n)$ negligible

i.e. ε-close for ε negligible

X indistinguishable from uniform $\Rightarrow \varepsilon(n)$ negligible
(by ppt)

since: "predict next bit" is a statistical test

if can pass $\Rightarrow$ can distinguish from uniform

what about other direction?

Cool theorem: next bit unpredictability + pseudorandomness
are equivalent!!

Thm X is p.r. iff X is n.b.u.

Pf.

$\Rightarrow$ (show X not nbu $\Rightarrow$ X not p.r.)

Assume $\exists k$ s.t. $\Pr_{X,\, i \in [n],\, coins}[P(x_1 \cdots x_{i-1}) = x_i] \geq \frac{1}{2} + \frac{1}{n^k}$

then $\exists\, i$ s.t. $\Pr_{X,\, coins}[P(x_1 \cdots x_{i-1}) = x_i] \geq \frac{1}{2} + \frac{1}{n^k}$

Construct stat test T_i distinguishing X from U

statistical test T_i

$y_1 \cdots y_n \longrightarrow$

1. compute $C = P(y_1 \cdots y_{i-1})$
2. output 1 if $C = y_i$

$\longrightarrow$ P/F

PASS

$$\Pr_{y_1 \cdots y_n \in X}[T_i(y_1 \cdots y_n) = 1] \geq \frac{1}{2} + \frac{1}{n^k}$$

$$\Pr_{y_1 \cdots y_n \in U_n}[T_i(y_1 \cdots y_n) = 1] = \frac{1}{2}$$

more likely to "pass" n.b. test
$\Downarrow$
~~s~~statistical test that distinguishes

$\therefore$ X is not p.r.

$\Leftarrow$ (X not p.r. $\Rightarrow$ $\exists$ n.b. test for some i)

if X not p.r.

$\exists$ ppt T s.t. $\left| \underbrace{\Pr_{x \in X}[T(x)=1] - \Pr_{u \in U}[T(u)=1]}_{\text{wlog advantage} > 0 \text{ else, use } \overline{T}} \right| > \frac{1}{n^k}$ for infinitely many n

use hybrid argument to construct n.b. predictor:

$D_0 \equiv U \equiv u_1 \cdots u_n$

$D_1 = x_1 u_2 \cdots u_n$

$D_2 = x_1 x_2 u_3 \cdots u_n$

$\vdots$

$D_n = x_1 \cdots x_n \equiv X$

Main idea:

run statistical test

if says "pseudorandom" (i.e. outputs "1") output the bit

else, seems "not right" so output the complement of the bit some preliminary calculations:

$$\frac{1}{n^k} < \Pr_{x \in D_n}[T(x)=1] - \Pr_{x \in D_0}[T(x)=1]$$

$$= \sum_{i=1}^{n} \Pr_{x \in D_i}[T(x)=1] - \Pr_{x \in D_{i-1}}[T(x)=1] \qquad \text{telescoping}$$

divide by n:

$$\frac{1}{n^{k+1}} < \frac{1}{n} \sum_{i=1}^{n} \Pr_{x \in D_i}[T(x)=1] - \Pr_{x \in D_{i-1}}[T(x)=1]$$

so:

$$\exists\, i \text{ s.t. } \Pr_{x \in D_i}[T(x)=1] - \Pr_{x \in D_{i-1}}[T(x)=1] \geq \frac{1}{n^{k+1}}$$

so define next bit predictor for this i:

n.b.p. for i:

$P(x_1 \cdots x_{i-1})$:

1. choose $u_i \cdots u_n \in_R \{0,1\}^{n-i}$
2. $b \leftarrow T(x_1 \cdots x_{i-1} u_i \cdots u_n)$
3. if $b=1$ output u_i ← u_i seems right ie. $x_1 \ldots x_{i-1} u_i \ldots u_n$ looks like output of PRG

   else output $\overline{u}_i$

Note: $P(x_1 \cdots x_{i-1}) = x_i$ iff $b=1$ & $u_i = x_i$ (T passes u_i)

or $b=0$ & $\overline{u}_i = x_i$ (T fails u_i)

$$\Pr[\underbrace{P(x_1 \cdots x_{i-1}) = x_i}_{\text{event "}*\text{"}}] = \Pr[* \mid u_i = x_i] \cdot \underbrace{\Pr[u_i = x_i]}_{=1/2} + \Pr[* \mid u_i \neq x_i] \cdot \underbrace{\Pr[u_i \neq x_i]}_{=1/2}$$

$$= \frac{1}{2} \cdot \Big[\Pr[b = 1 \mid u_i = x_i] + \Pr[b = 0 \mid u_i \neq x_i]\Big]$$

T "passes" T "fails"

$$= 1 - \Pr[b = 1 \mid u_i \neq x_i]$$

$$= \frac{1}{2}\Big[1 + \Pr[T(x_1 \cdots x_{i-1} x_i u_{i+1} \cdots u_n) = 1] - \Pr[T(x_1 \cdots x_{i-1} \overline{x}_i u_{i+1} \cdots u_n) = 1]\Big]$$

a c

add + subtract b →

$$= \frac{1}{2} + \frac{1}{2}\Big[\Pr[T(\underbrace{x_1 \cdots x_{i-1} x_i u_{i+1} \cdots u_n}_{D_i}) = 1] - \Pr[T(\underbrace{x_1 \cdots x_{i-1} u_i u_{i+1} \cdots u_n}_{D_{i-1}}) = 1]\Big]$$

$$+ \underbrace{\frac{1}{2}\Big[\Pr[T(x_1 \cdots x_{i-1} u_i u_{i+1} \cdots u_n) = 1] - \Pr[T(x_1 \cdots x_{i-1} \overline{x}_i u_{i+1} \cdots u_n) = 1]\Big]}_{\text{what is this?}}$$

b c

what is this?
see ** calculation – it = a – b !

$$\geq \frac{1}{2} + \frac{1}{2} \cdot 2 \cdot \frac{1}{n^{k+1}} = \frac{1}{2} + \frac{1}{n^{k+1}}$$

**:

$$\Pr[T(x_1 \cdots x_{i-1} u_i \cdots u_n) = 1] = \frac{\Pr[T(x_1 \cdots x_i u_{i+1} \cdots u_n) = 1] + \Pr[T(x_1 \cdots \overline{x}_i u_{i+1} \cdots u_n) = 1]}{2}$$

$$b = \frac{a + c}{2} \Rightarrow a - b = b - c$$

Curious Note:

Since order of bits irrelevant for PRG statistical test T, order of bits irrelevant for prediction.
so $b_1 \cdots b_n$ hard for n.b. test $\Rightarrow$ $b_n \cdots b_1$ hard for n.b. test.

How do we construct PRG's

want to use "computational hardness"
will start with 1-way functions.

def. f is 1-way if
1) f computable in deterministic ptime
2) $\forall$ ppt A, $\exists$ negligible $\varepsilon(n)$
st. $\forall n$ big enough

$$\Pr_{x,\text{ coins of } A}\left[A(f(x)) \in \underbrace{f^{-1}(f(x))}_{\text{any inverse of } f(x)}\right] \leq \varepsilon(n)$$

notes:
1) A ptime in n, not just $|f(x)|$ (which might be small)
2) don't need to find "right" inverse - just some inverse

Why is this good? We have candidates!

1) $f(x,y) = x \cdot y$ factoring
2) $f_{m,e}(x) = x^e \bmod m$ RSA $m = pq$
3) $f_m(x) = x^2 \bmod m$ Rabin's fctn (square roots mod m)
4) $f_{p,g}(x) = g^x \bmod p$ discrete log

For PRGs to exist, 1-way fctns must exist:

<u>Claim</u> $f: \{0,1\}^n \to \{0,1\}^{2n}$ PRG $\Rightarrow$ f is o.w.

<u>idea</u> if f not o.w.

$\exists$ inverter algorithm which sometimes works

use it to give statistical test on PRG output

(i.e. output "1" if finds inverse)

- sometimes works on PRG output
- almost never works on truly random bits

But do 1-way fctns imply existence of PRG's?

Yes, but much harder to prove...

<u>Thm</u> [HILL] 1-way fctn exist $\Rightarrow$ PRG's exist

so PRGs exist $\Updownarrow$ 1-w.f.'s exist!

here, a weaker result

<u>Thm</u> 1-way permutations exist $\Rightarrow$ PRG's exist

fctn that is 1-1 + onto
so preimages are unique