Complexity Classes

RP: $L \in RP$ if $\exists M$ (randomized) s.t.

1. $M(x)$ runs in time $poly(|x|)$
2. $Pr_{x,w}[M_w(x) = YES \mid x \in L] > \frac{2}{3}$ (w: coin tosses of M)
3. $Pr_{x,w}[M_w(x) = YES \mid x \notin L] = 0$

To amplify $2/3 \to 1 - \varepsilon(n)$: ($\varepsilon$: negligible)

Run M k times w/ fresh randomness.

If M outputs YES on any instance, $\therefore x \in L$

If M outputs NO on all instances, $\therefore x \notin L$

$Pr[\text{CORRECT}] = 1$

$Pr[\text{CORRECT}] = 1 - \frac{1}{3^k}$,

co-RP: $L \in$ co-RP IF $\exists M$ (RANDOMIZED) S.T.

① $M(x)$ RUNS IN TIME POLY($|x|$)

② $Pr_{x,w}[M_w(x) = \text{YES} \mid x \in L] = 1$

(w: COIN TOSSES OF M)

③ $Pr_{x,w}[M_w(x) = \text{YES} \mid x \notin L] < \frac{1}{3}$

TO AMPLIFY $2/3 \to 1 - \varepsilon(n)$:

RUN M k TIMES W/ FRESH RANDOMNESS.

IF M OUTPUTS YES ON ALL INSTANCES, $\therefore x \in L$

IF M OUTPUTS NO ON ANY INSTANCE $\therefore x \notin L$

$Pr[\text{CORRECT}] = 1 - \frac{1}{3^k}$

$Pr[\text{CORRECT}] = 1$

BPP: $L \in BPP$ IF $\exists M$ (RANDOMIZED) S.T.

① $M(x)$ RUNS IN TIME $POLY(|x|)$

② $Pr_{x,w}[M_w(x) = YES \mid x \in L] > \frac{2}{3}$

(w: COIN TOSSES OF M)

③ $Pr_{x,w}[M_w(x) = YES \mid x \notin L] < \frac{1}{3}$

TO AMPLIFY $2/3 \to 1-\varepsilon$:

RUN M MANY TIMES W/ FRESH RANDOMNESS.

IF M OUTPUTS YES ON MOST INSTANCES, $\therefore x \in L$

IF M OUTPUTS NO ON MOST INSTANCES, $\therefore x \notin L$

★ HOW DO WE KNOW PROBABILITY THAT THIS ↖ WORKS?

CHERNOFF BOUND!

Chernoff Bound:

Given n independent random variables $X_1, X_2, \ldots, X_n$ with identical probability distributions, if $X = \sum_{i=1}^{n} X_i$, then

$$P_R[X \geq (1+\beta)E(X)] < e^{\frac{-\beta^2 E(X)}{2}}$$

In English: Probability of X being far away from its expected value decreases exponentially as a function of β, the distance from $E(X)$. Also, decreases exponentially as $E(X)$ increases, which happens as we increase the # of trials n.

Using Chernoff for BPP

Let M' execute M k times + output "Yes" if majority of executions output "Yes", "No" otherwise.

$X_i = 1$ if M' makes a mistake on i^{TH} execution of M

$X_i = 0$ otherwise

Each execution is independent, so $Pr[X_i = 1] < \frac{1}{3}$.

For ease of notation, suppose $Pr[X_i = 1] = \frac{1}{3}$.

$$E(X) = \sum_{i=1}^{k} 0 \cdot Pr[X_i = 0] + 1 \cdot Pr[X_i = 1]$$

$$= \sum_{i=1}^{k} Pr[X_i = 1]$$

$$= k/3$$

M' WILL BE WRONG IF MORE THAN HALF OF M OUTCOMES ARE WRONG. THAT IS, IF

$$\sum_{i=1}^{k} X_i \geq k/2$$

THUS, WE WANT TO BOUND

$$\Pr[X \geq k/2]$$

$$= \Pr\left[X \geq \frac{3}{2} \cdot \frac{k}{3}\right] \quad \leftarrow E(X)$$

$$= \Pr\left[X \geq \left(1 + \frac{1}{2}\right) \cdot \frac{k}{3}\right]$$

CHERNOFF ↓

$$= e^{\frac{-(\frac{1}{2})^2 \cdot \frac{k}{3}}{2}}$$

$$= e^{\frac{-k}{24}}$$

$\therefore \Pr[M' \text{ MAKES MISTAKE}]$ IS NEGLIGIBLE IN k.

SIDE NOTE: $P \subseteq RP \subseteq NP$

$P \subseteq RP$: IGNORE RANDOMNESS

$RP \subseteq NP$: WITNESS w IS THE RANDOMNESS WHICH GIVES

$M_w(x) = 1$.

Review of Hardcore Bits

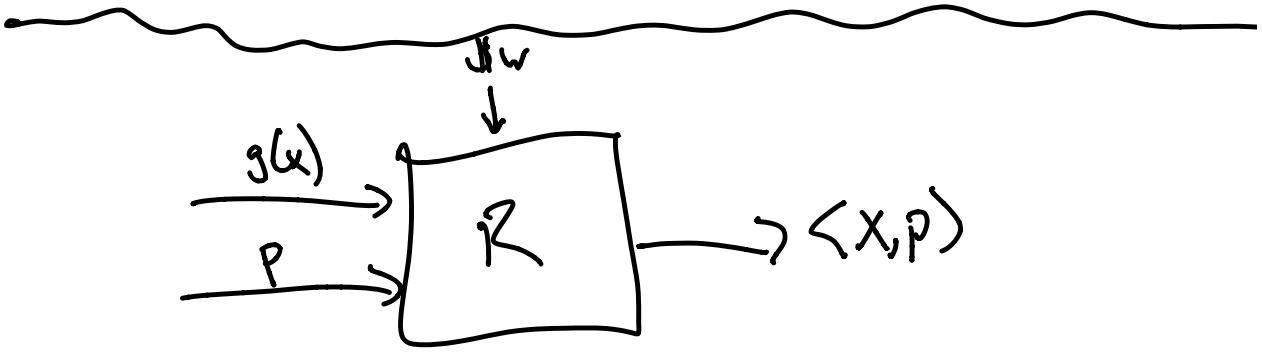
Thm: (Goldreich, Levin)

A "random" subset of bits of input x XOR'd together is a hardcore bit for 1WP $g(x) = y$

$$B(x) = \langle x, p \rangle \text{ is HCB}$$

PROOF:

STEP 1: SUPPOSE R PREDICTS $\langle x, p \rangle$ W/ PROBABILITY 1.



$p_1 = 1000\ldots0 \rightarrow [R] \rightarrow x_1$

$p_2 = 0100\ldots0 \rightarrow [R] \rightarrow x_2$

$\vdots$

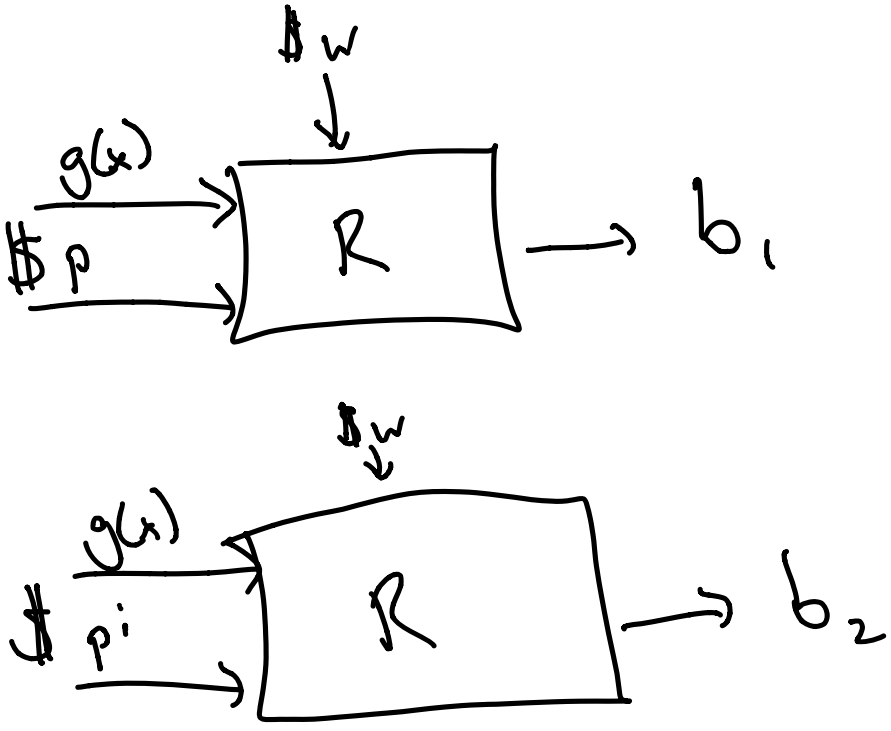
$p_n = 000\ldots1 \rightarrow [R] \rightarrow x_n$

CAN DETERMINE X USING n CALLS TO R AS SUBROUTINE

STEP 2: R PREDICTS $\langle x, p \rangle$ W/ PROBABILITY $3/4 + \varepsilon$

$$\Pr_R[R \text{ MAKES MISTAKE}] = \frac{1}{4} - \varepsilon$$

$p^i := p$ W/ i^{TH} BIT FLIPPED



IF BOTH ARE CORRECT, ONLY

i^{TH} BIT DOESN'T GET CANCELLED OUT

IN $b_1 \oplus b_2$. SO $b_1 \oplus b_2 = x_i$

IF BOTH ARE CORRECT, WHICH

OCCURS WITH PROBABILITY AT LEAST

$$1 - \Pr[b_1 \text{ IS WRONG}] - \Pr[b_2 \text{ IS WRONG}]$$

$$= 1 - \left(\frac{1}{4} - \varepsilon\right) - \left(\frac{1}{4} - \varepsilon\right)$$

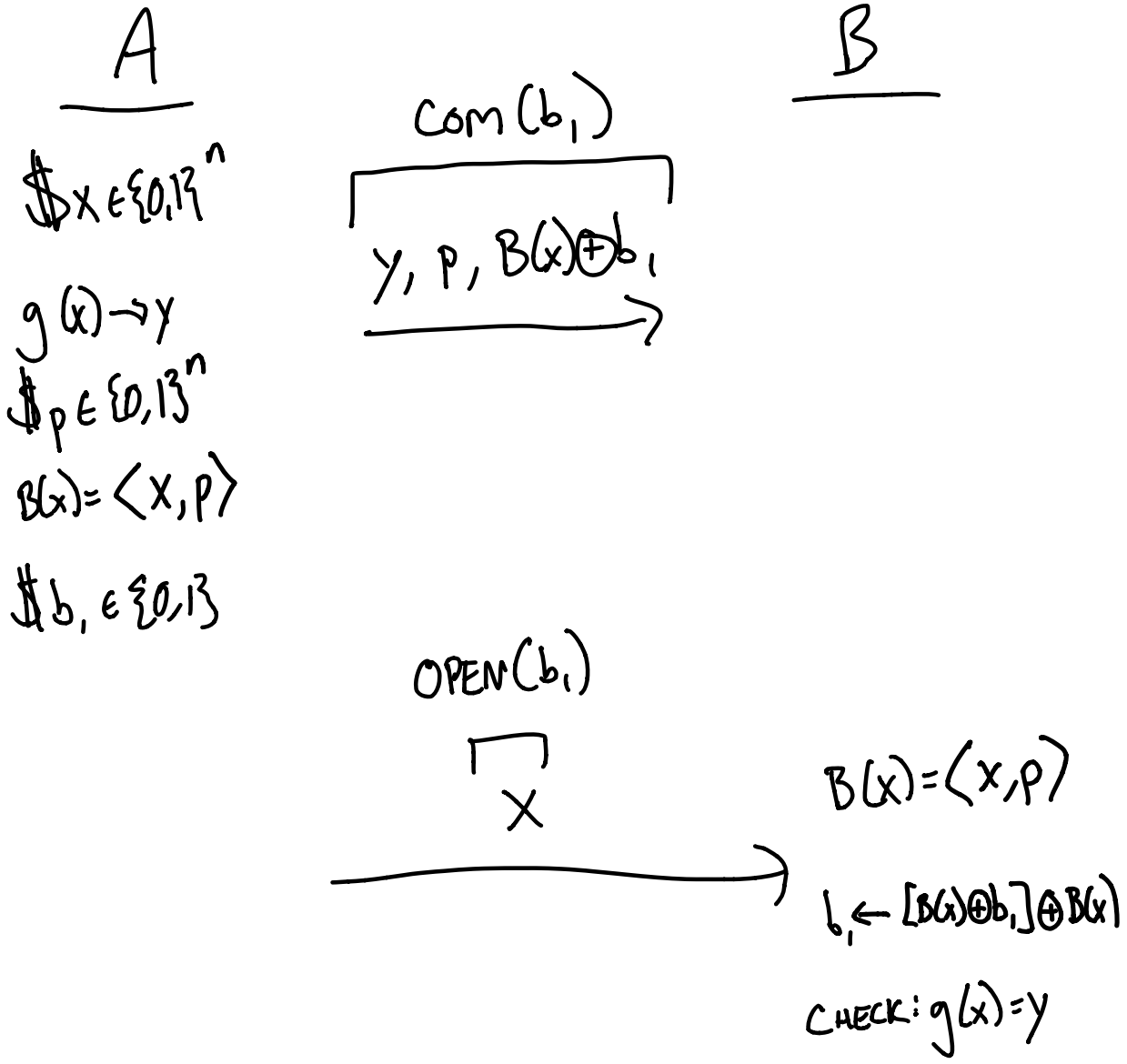
$$= \frac{1}{2} + 2\varepsilon$$

So we can predict each bit of X w/ probability $\frac{1}{2}+2\varepsilon$ using 2 calls to R.

Amplification

We can amplify this probability as close to 1 as we want by repeating k times + taking the majority (BPP amplification)

Application: Bit commitment via HCB



ALICE CAN'T CHANGE MIND ABOUT b, BECAUSE SHE CAN'T CHANGE MIND ABOUT x, BECAUSE f IS A PERMUTATION, AND SHE ALREADY SENT p WHICH DETERMINES $B(x)$.

BOB CAN'T DETERMINE b, FROM THE COMMITMENT BECAUSE IT IS MASKED BY $B(x)$, AND PREDICTING $B(x)$ WITHOUT KNOWING x IS AS HARD AS INVERTING f, WHICH IS A 1WF.

* IF ALICE HANGS UP W/O OPENING, BOB WINS. TO PREVENT "ABORT" ATTACKS.

Eliminating x from Probability of A inverting g

In our "proof", we assumed R is successful w/ probability $\frac{3}{4} + \varepsilon$ for <u>all</u> x.

In reality, R has success probability $\frac{1}{2} + \varepsilon$ over x, p, & w.

Can we select a set of "good" x values for which $\Pr[\text{success}] > \frac{1}{2} + \frac{\varepsilon}{2}$?

Then, try to invert g only on good values x.

DEF: INPUT x IS "GOOD" IF

$$Pr_{p,w}\left[R(g(x), p) = B(x,p)\right] > \frac{1}{2} + \frac{\varepsilon}{2}$$

CLAIM: AT LEAST $\frac{\varepsilon}{2}$ FRACTION OF INPUTS x ARE "GOOD"

TOOL FOR PROOF: BAYESIAN CONDITIONING

$$Pr_R[A] = Pr_R[A|B] \cdot Pr_R[B] + Pr_R[A|\neg B] \cdot Pr_R[\neg B]$$

PROOF: SUPPOSE $< \frac{\varepsilon}{2}$ INPUTS ARE "GOOD"

$$\Pr_{x,p,w}\left[R(g(x), p) = B(x,p)\right]$$

$$= \Pr_{x,p,w}\left[R(g(x), p) = B(x,p) \,\middle|\, x \text{ IS "GOOD"}\right] \cdot \Pr\left[x \text{ IS "GOOD"}\right]$$

$$+ \Pr_{x,p,w}\left[R(g(x), p) = B(x,p) \,\middle|\, x \text{ NOT "GOOD"}\right] \cdot \Pr\left[x \text{ NOT "GOOD"}\right]$$

$$< 1 \cdot \frac{\varepsilon}{2} + \left(\frac{1}{2} + \frac{\varepsilon}{2}\right) \cdot 1$$

- $1 \cdot$: $\Pr[\ldots] \le 1$
- $\frac{\varepsilon}{2}$: ASSUMPTION
- $\left(\frac{1}{2} + \frac{\varepsilon}{2}\right)$: DEF. OF "GOOD"
- $\cdot\, 1$: $\Pr[\ldots] \le 1$

$$= \frac{1}{2} + \varepsilon.$$

THIS CONTRADICTS THE FACT THAT R IS SUCCESSFUL W/ PROBABILITY $\frac{1}{2} + \varepsilon$. THUS, AT LEAST $\frac{\varepsilon}{2}$ FRACTION OF x ARE "GOOD". ∎

New Topic: Pseudo-Random Generators

Motivating Example: One-Time Pad Encryption

A		B
$m \in \{0,1\}^n$		
$\$ k \in \{0,1\}^n$		
$CT = m \oplus k$	$\xrightarrow{CT}$	$m = CT \oplus k$

Information-Theoretic Security:

Even infinitely powerful Adv cannot learn m without k, because many message/key pairs yield the same CT.

ISSUE: KEY k MUST BE AS LONG AS MESSAGE m. DIFFICULT TO GENERATE + DISTRIBUTE.

IDEA: WHAT IF WE HAD A FUNCTION $PRG(s) \longrightarrow k$ WHICH TAKES

A SHORT, TRULY RANDOM SEED s

+ OUTPUTS A LONG "RANDOM-LOOKING" STRING k?

THEN, COULD DISTRIBUTE SHORT SEED s + EACH PARTY USES $PRG(s)$ TO GENERATE KEY k.

Crucial Concept:

What does "random-looking" mean?

Intuition: No PPT algorithm can distinguish "random-looking" string from truly random string, except with negligible probability.

Analogy: Turing Test for artificial intelligence.

NOTE: BOTH RANDOM & PSEUDO-RANDOM STRINGS MUST COME FROM "SAMPLEABLE" DISTRIBUTIONS.

INTUITION: DISTRIBUTION X_n IS SAMPLEABLE IF THERE IS A PPT ALGORITHM S WHICH RANDOMLY OUTPUTS VALUES OF X_n ACCORDING TO THE DISTRIBUTION.

FORMALLY:

$$P_{R_r}[S(1^n, r) = \alpha] = P_{R_{X_n}}[X_n = \alpha]$$

We call the testing algorithm T, used to determine if 2 distributions are the same or not, a statistical test.

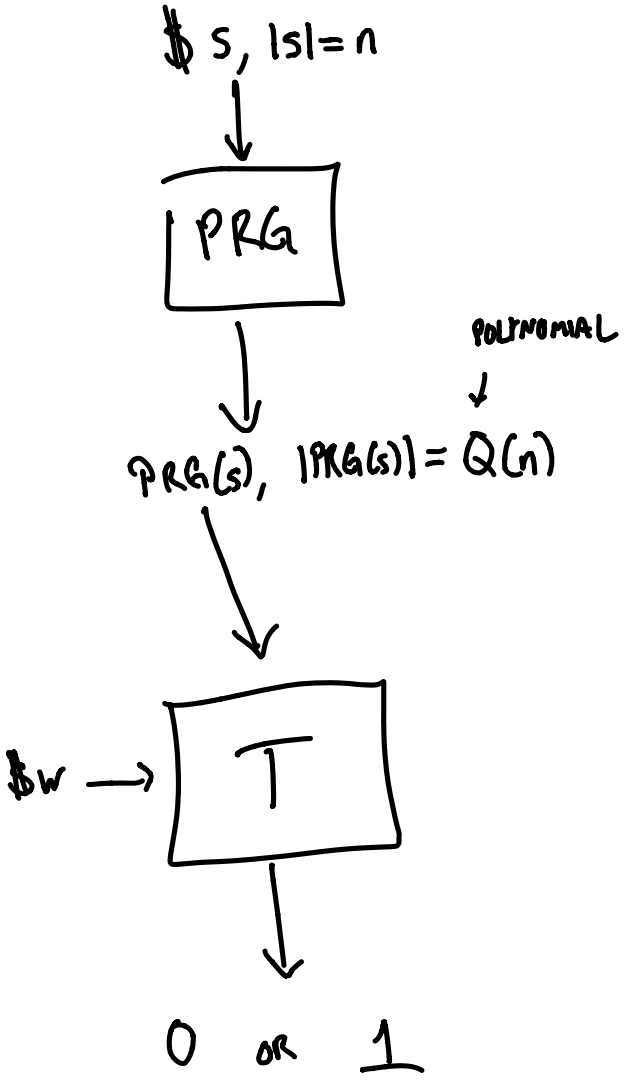
The following def says that sampleable X_n, Y_n are indistinguishable with respect to the test T if T cannot determine whether a sample comes from X_n or Y_n.

Def X_n, Y_n are indistinguishable under test T if $\forall c, \exists N_c$ s.t. $\forall n > N_c$:

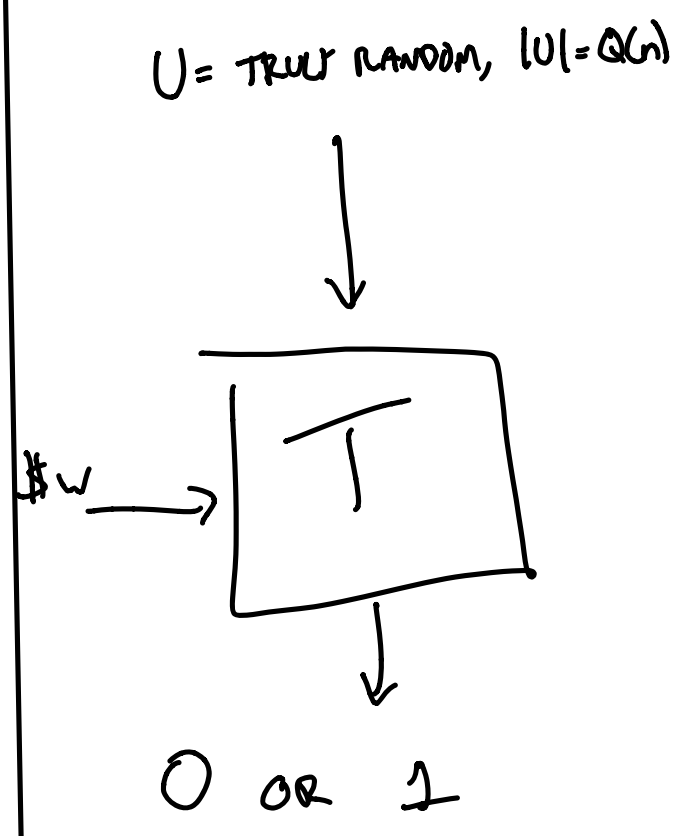
$$\left| Pr_{w,X_n}[T_w(X_n)=1] - Pr_{w,Y_n}[T_w(Y_n)=1] \right| < \frac{1}{n^c}$$

VISUALIZATION OF INDISTINGUISHABILITY TESTING:

WORLD 1 (PRG)



WORLD 2 (TRULY RANDOM)



X_n & Y_n ARE COMPUTATIONALLY INDISTINGUISHABLE IF $\forall T \in PPT$, X_n & Y_n ARE INDISTINGUISHABLE UNDER T.

FORMAL DEFINITION:

X_n, Y_n ARE COMPUTATIONALLY INDISTINGUISHABLE (EQUIVALENTLY, POLY-TIME INDISTINGUISHABLE) IFF

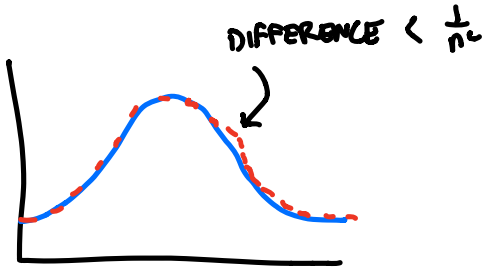
$\forall c, \forall A \in PPT, \exists N_c$ S.T. $\forall n > N_c$:

$$\left| P_R[A(X_n)=1] - P_R[A(Y_n)=1] \right| < \frac{1}{n^c}$$

Slightly stronger notion: Statistical Closeness

Intuition: Difference between actual distributions is negligible.

Visually:



Formally: X_n, Y_n are **statistically close** if $\forall c, \exists N_c$ s.t. $\forall n > N_c$:

$$\sum_{\alpha \in \{0,1\}^n} \left| Pr[X_n = \alpha] - Pr[Y_n = \alpha] \right| < \frac{1}{n^c}$$

Extended Statistical Test

Why does T only get a single sample?

In reality, Adv might see many PRG outputs.

Want to show: If X_n, Y_n computationally indistinguishable for just one sample, then they are also indistinguishable given a polynomial # of samples.

New Proof Strategy: Hybrid Argument!

Def (Extended Statistical Test):

Sampleable distributions X_n, Y_n pass extended statistical test T' if $\forall c_1, c_2, \exists N_{c_1,c_2}$ s.t. $\forall n > N_{c_1,c_2}$:

$$\left| Pr\left(T'\left(X_n^1, \ldots, X_n^{c_2}\right) = 1\right) - Pr\left(T'\left(Y_n^1, \ldots, Y_n^{c_2}\right) = 1\right) \right| < \frac{1}{n^{c_1}}$$

Note: Either ALL samples from X_n,

or ALL samples from Y_n.

No mix & match.

CLAIM: IF X_n, Y_n ARE SAMPLEABLE DISTRIBUTIONS WHICH CAN BE DISTINGUISHED BY EXTENDED STATISTICAL TEST T', THEN THERE EXISTS A SINGLE SAMPLE STATISTICAL TEST T WHICH DISTINGUISHES X_n FROM Y_n.

CONSEQUENCE: PROVING INDISTINGUISHABILITY WITH A SINGLE SAMPLE IS ENOUGH!

Proof of Claim:

Let $k = \text{poly}(n)$, $\varepsilon(n) = 1/k$.

Assume $\exists T'$ which distinguishes X_n from Y_n using k samples, with probability greater than $\varepsilon(n)$. That is,

(*) $$\Pr_{X_n}\left[T'(X_1, \ldots, X_k) = 1\right] - \Pr_{Y_n}\left[T'(Y_1, \ldots, Y_k) = 1\right] > \varepsilon(n)$$

could be flipped, but then we can reverse entire proof

Consider "Hybrids" $P_0, \ldots, P_k$ where in P_j, the first j samples come from Y_n and the remaining samples come from X_n:

$$P_0 = \left(\Pr_{(X_n, Y_n)}\left[T'(X_1, X_2, \ldots, X_{k-1}, X_k)\right] = 1\right)$$

$$P_1 = \left(\Pr_{(X_n, Y_n)}\left[T'(Y_1, X_2, \ldots, X_{k-1}, X_k)\right] = 1\right)$$

$$\vdots$$

$$P_{k-1} = \left(\Pr_{(X_n, Y_n)}\left[T'(Y_1, Y_2, \ldots, Y_{k-1}, X_k)\right] = 1\right)$$

$$P_k = \left(\Pr_{(X_n, Y_n)}\left[T'(Y_1, Y_2, \ldots, Y_{k-1}, Y_k)\right] = 1\right)$$

REWRITING (*) IN TERMS OF P_j, WE KNOW

$$P_0 - P_k > \varepsilon(n)$$

WE CAN REWRITE THIS AS A "TELESCOPING" SUM:

$$\left[P_0 + (-P_1 + P_1) + (-P_2 + P_2) + \dots + (-P_{k-1} + P_{k-1}) - P_k \right] > \varepsilon(n)$$

REGROUPING GIVES US:

$$\underbrace{(P_0 - P_1) + (P_1 - P_2) + \dots + (P_{k-2} - P_{k-1}) + (P_{k-1} - P_k)}_{k \text{ TOTAL TERMS}} > \varepsilon(n)$$

BY PIGEONHOLE PRINCIPLE, $\exists j$ S.T.

$$P_j - P_{j+1} > \frac{\varepsilon(n)}{k} = \frac{1}{(\text{poly}(n))^2}$$

WHICH IS STILL $\frac{1}{\text{poly}(n)}$ FOR A NEW POLYNOMIAL.

Consider a distribution $P(z)$ defined:

$$P(z) = y_1, y_2, \ldots, y_j, z, x_{j+2}, \ldots, x_k$$

Notice: If z is a sample from X_n, then $P(z) = P_j$

If z is a sample from Y_n, then $P(z) = P_{j+1}$

Thus, we can define our single sample distinguisher T as follows:

Given z from either X_n or Y_n,

① Guess value of location $j \in [1, k]$

② Sample $y_1, \ldots, y_j \leftarrow Y_n$ and
$x_{j+2}, \ldots, x_k \leftarrow X_n$

③ Compute $T'(y_1, \ldots, y_j, z, x_{j+2}, \ldots, x_k)$

WHAT IS THE PROBABILITY THAT T DISTINGUISHES Z?

$$\Pr_{X_n}[T(X_n)=1] - \Pr_{Y_n}[T(Y_n)=1]$$

$$= \Pr[\text{GUESS } j \text{ CORRECTLY}] \cdot (P_j - P_{j+1})$$

$$= \frac{1}{k} \cdot (P_j - P_{j+1})$$

$$> \frac{1}{k} \cdot \frac{\varepsilon(n)}{k}$$

$$= \frac{\varepsilon(n)}{k^2}$$

$$= \frac{1}{k^3}$$

$$= \frac{1}{(\text{poly}(n))^3}$$

WHICH IS STILL $\frac{1}{\text{poly}(n)}$, FOR A NEW POLYNOMIAL.

THUS, T DISTINGUISHES X_n FROM Y_n USING A SINGLE SAMPLE WITH SIGNIFICANT PROBABILITY. ∎

Constructing a PRG

Formal PRG definition:

A deterministic algorithm G is a PRG if:

1. $G(x, Q)$ runs in time $\text{poly}(|x|, Q(|x|))$ where Q is a polynomial
2. $G(x, Q)$ outputs strings of length $Q(|x|)$ for all x
3. For every polynomial Q, the distribution $\{G(x,Q)\}$ is computationally indistinguishable from $\{U_{Q(|x|)}\}$, where $U_{Q(|x|)}$ is a uniform distribution on strings of length $Q(|x|)$

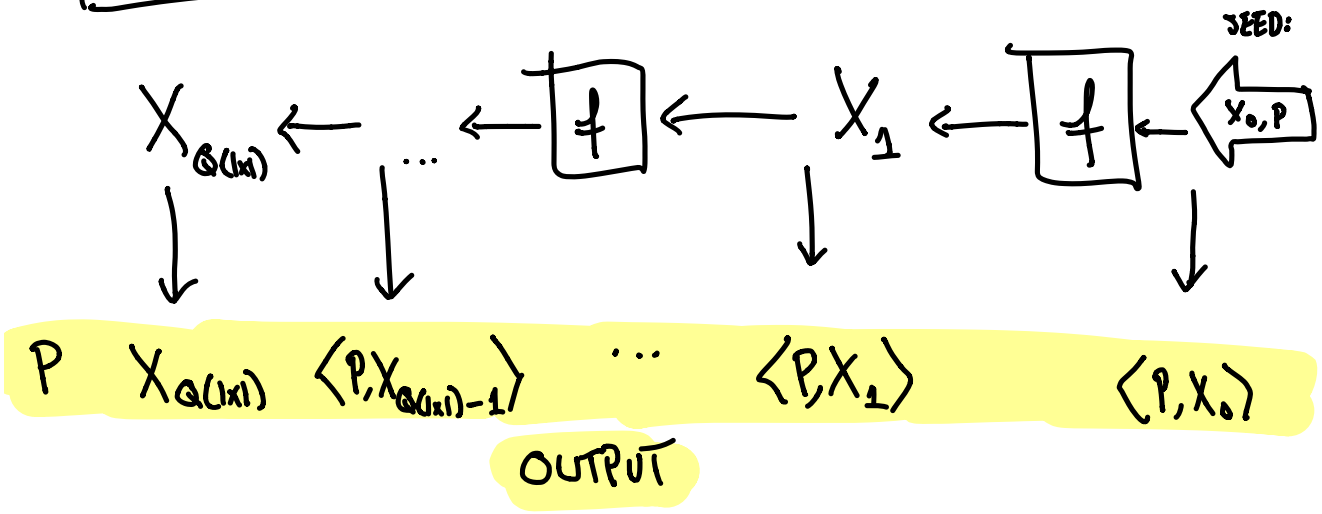
Constructing PRG from 1WP

Let f be 1-way permutation

Choose random seed X_0, random string P,

$|X_0| = |P| = n$

Visualization



Algorithm for G

(1) Pick 1WP f, random seed X_0, & random string P, $|X_0| = |P| = n$

(2) For $i = 1$ to $Q(|x|)$, do:

$X_i \leftarrow f(X_{i-1})$

Add $\langle P, X_{i-1} \rangle$ to output sequence

(3) Output $X_{Q(|x|)}$ and P

(4) Return output sequence in <u>reverse order</u>

How do we prove G is pseudorandom?

(1) Prove G is unpredictable. That is, given first k bits of $G()$, hard to predict next bit G_k with probability better than $1/2$.

(2) Prove that if G is unpredictable, then G is pseudorandom.

Def X_n passes the next bit test (is unpredictable) if $\forall c$ and $\forall A \in PPT$, $\exists N_c$ s.t. $\forall n > N_c$ and $\forall i \in [0, n]$:

$$Pr_{X_n, w}\left[A_w(x_1, \ldots, x_i \mid x \leftarrow X_n) = x_{i+1}\right] < \frac{1}{2} + \frac{1}{n^c}$$

Claim 1:

If f is a 1WP, then G as defined previously is unpredictable.

Proof:

We will show: If G fails next bit test, then we can invert f on a random input.

By assumption, $\exists A \in PPT$ s.t.

$$Pr_{G(1),w}\left[A_w(G_1, \ldots, G_i) = G_{i+1}\right] < \frac{1}{2} + \varepsilon(n)$$

We will invert f on input X_{n-i} by using A to predict the HCB $\langle X_{n-i}, P \rangle$. Since A which predicts HCB can be used to invert f (previous proof), we will be done.

To predict $\langle X_{n-i}, P \rangle$, apply f to X_{n-i} i times as described by G, and compute the first i bits of the output $G_1, \ldots, G_i$. Then, compute

$$A(G_1, \ldots, G_i)$$

Note this is precisely $G_{i+1} = \langle X_{n-i}, P \rangle$ with probability $\frac{1}{2} + \varepsilon(n)$. Thus we predicted the HCB of $f(X_{n-i})$, which implies we can invert $f(X_{n-i})$ with significant probability. ∎

CLAIM ②:

X_n IS PSEUDORANDOM

$\Updownarrow$

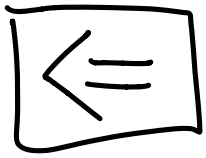
X_n IS UNPREDICTABLE

PROOF:

$\Rightarrow$ SINCE NEXT-BIT TEST IS A STATISTICAL TEST, THIS IS TRIVIAL.

X_n PSEUDORANDOM $\Rightarrow$ X_n PASSES ALL STATISTICAL TESTS

$\Rightarrow$ X_n PASSES NBT



PROOF BY CONTRADICTION: WANT TO SHOW,

IF X_n NOT PSEUDORANDOM,

THEN X_n FAILS NEXT-BIT TEST.

THAT IS,

IF $\exists D$ WHICH DISTINGUISHES X_n FROM U_n,

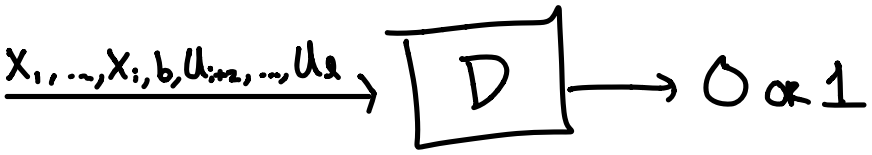
THEN $\exists A$ WHICH PREDICTS NEXT BIT OF X_n

ASSUME D DISTINGUISHES X_n FROM U_n WITH PROBABILITY $\varepsilon(n)$. BY PREVIOUS HYBRID ARGUMENT APPLIED TO X_n, U_n, $\exists i$ SUCH THAT

$$P_{i+1} - P_i > \frac{\varepsilon}{l}$$

WHERE l IS TOTAL # OF SAMPLES.

IDEA: $x_1, \ldots, x_i \leftarrow x_n$, $\$ b \in \{0,1\}$,
$u_{i+2}, \ldots, u_2 \leftarrow u_n$



IF $D(\cdots) = 1$, A PREDICTS $x_{i+1} = b$

IF $D(\cdots) = 0$, A PREDICTS $x_{i+1} = \bar{b}$

INTUITION: D OUTPUTS 1 MORE OFTEN WHEN $b = x_{i+1}$

CALCULATION:

$$\Pr\left[A(x_1,\dots,x_i) = x_{i+1}\right]$$

$$= \Pr[x_{i+1}=b] \cdot \Pr\left[D(x_1,\dots,x_i,x_{i+1},u_{i+2},\dots,u_\ell)=1\right]$$

$$+ \Pr[x_{i+1}=\bar{b}] \cdot \underbrace{\Pr\left[D(x_1,\dots,x_i,\overline{x_{i+1}},u_{i+2},\dots,u_\ell)=0\right]}_{\text{CALL THIS } q}$$

$$= \frac{1}{2}\cdot P_{i+1} + \frac{1}{2}\cdot q$$

WHAT IS q? LET'S EXPAND P_i

$$P_i = \Pr\left[D(x_1,\dots,x_i,u_{i+1},\dots,u_\ell)=1\right]$$

$$= \Pr\left[D(x_1,\dots,x_i,x_{i+1},u_{i+2},\dots,u_\ell)=1\right]\cdot \Pr[u_{i+1}=x_{i+1}]$$

$$+ \Pr\left[D(x_1,\dots,x_i,\overline{x_{i+1}},u_{i+2},\dots,u_\ell)=1\right]\cdot \Pr[u_{i+1}=\overline{x_{i+1}}]$$

$$= P_{i+1}\cdot\frac{1}{2} + (1-q)\cdot\frac{1}{2}$$

THUS,

$$q = 1 + P_{i+1} - 2 \cdot P_i$$

FINALLY, SUBSTITUTING THIS q VALUE YIELDS:

$$\Pr[A(x_1, \ldots, x_i) = x_{i+1}]$$

$$= \frac{1}{2} \cdot P_{i+1} + \frac{1}{2} \cdot q$$

$$= \frac{1}{2} \cdot P_{i+1} + \frac{1}{2} \cdot (1 + P_{i+1} - 2 \cdot P_i)$$

$$= \frac{1}{2} + [P_{i+1} - P_i]$$

$$> \frac{1}{2} + \frac{\varepsilon}{l}.$$

THUS, A PREDICTS THE $i+1^{ST}$ BIT OF X_n WITH SIGNIFICANT ADVANTAGE, WHICH COMPLETES THE PROOF. ■