

# COMPLEXITY CLASSES

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

①  $M(x)$  runs in TIME  $\text{poly}(|x|)$

②  $\Pr_{x,w} \left[ M_w(x) = \text{YES} \mid x \in L \right] > \frac{2}{3}$   
 $\eta$  cases of  
M

③  $\Pr_{x,w} \left[ M_w(x) = \text{YES} \mid x \notin L \right] = 0$

To AMPLIFY  $\frac{2}{3} \rightarrow 1 - \varepsilon(n)$ :  
NEGIGIBLE

Run  $M$   $k$  times w/ FRESH RANDOMNESS.

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

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

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

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

$\text{co-RP}$ :  $L \in \text{co-RP}$  if  $\exists M$  (randomized) s.t.

①  $M(x)$  runs in time  $\text{poly}(|\bar{x}|)$

②  $\Pr_{\substack{w \\ \eta \text{ coin} \\ \text{tosses of } M}}[M_w(\bar{x}) = \text{YES} \mid \bar{x} \in L] = 1$

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

To AMPLIFY  $\frac{2}{3} \rightarrow 1 - \varepsilon(n)$ :

Run  $M$   $k$  times w/ fresh randomness.

If  $M$  outputs YES on ALL instances,  $\therefore \bar{x} \in L$

If  $M$  outputs NO on ANY instance  $\therefore \bar{x} \notin L$

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

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

$\text{BPP} : L \in \text{BPP}$  if  $\exists M$  (randomized) s.t.

①  $M(x)$  runs in time  $\text{poly}(|\bar{x}|)$

②  $\Pr_{\substack{x, w \\ \text{1 coin} \\ \text{races of} \\ M}} [M_w(x) = \text{YES} \mid x \in L] > \frac{2}{3}$

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

To AMPLIFY  $\frac{2}{3} \rightarrow 1 - \varepsilon$ :

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

$X_1, X_2, \dots, X_n$  WITH IDENTICAL PROBABILITY DISTRIBUTIONS, IF  $X = \sum_{i=1}^n X_i$ , THEN

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

~~~~~  
IN ENGLISH: PROBABILITY OF  $X$  BEING

FAR AWAY FROM ITS EXPECTED VALUE DECREASES EXPONENTIALLY AS A FUNCTION OF  $\beta$ , THE DISTANCE FROM  $\mathbb{E}(X)$ . ALSO, DECREASES EXPONENTIALLY AS  $\mathbb{E}(X)$  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  $i^{\text{TH}}$  EXECUTION OF  $M$

$X_i = 0$  OTHERWISE

EACH EXECUTION IS INDEPENDENT, SO  $\Pr[X_i = 1] < \frac{1}{3}$ .

FOR EASE OF NOTATION, SUPPOSE  $\Pr[X_i = 1] = \frac{1}{3}$ .

$$\begin{aligned} \mathbb{E}(X) &= \sum_{i=1}^k 0 \cdot \Pr[X_i = 0] + 1 \cdot \Pr[X_i = 1] \\ &= \sum_{i=1}^k \Pr[X_i = 1] \\ &= k/3 \end{aligned}$$

$M'$  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

$$\Pr_R [X \geq k/2] = \Pr_R [X \geq \frac{3}{2} \cdot \frac{k}{3}] \quad \nwarrow E(X)$$

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

CHERNOFF

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

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

$\therefore \Pr [M' \text{ MAKES MISTAKE}]$  IS NEGIGIBLE 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

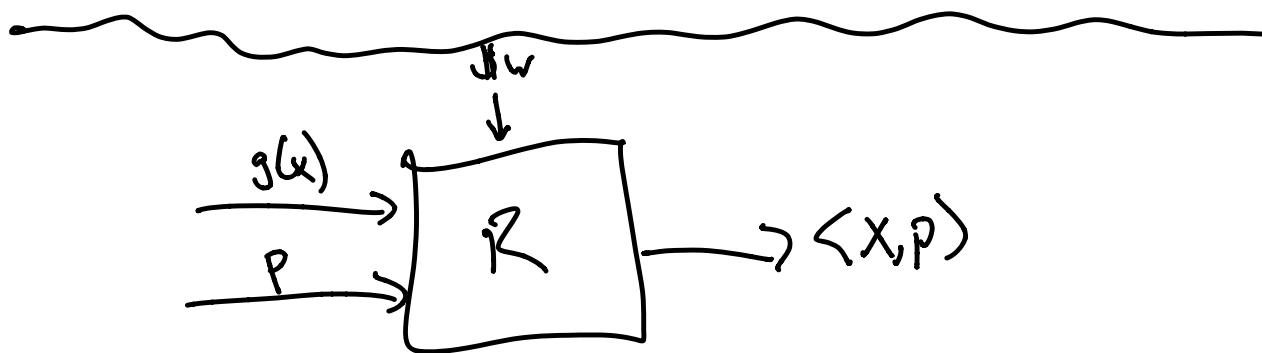
XOR'ed TOGETHER IS A HARDCORE BIT

FOR 1WP  $g(x) = y$

$B(x) = \langle x, p \rangle$  IS HCB

PROOF:

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



$$p_1 = 1000 \dots 0 \rightarrow \boxed{R} \rightarrow x_1$$

$$p_2 = 0100 \dots 0 \rightarrow \boxed{R} \rightarrow x_2$$

⋮

$$p_n = 000 \dots 1 \rightarrow \boxed{R} \rightarrow x_n$$

CAN DETERMINE  $x$  USING  $n$

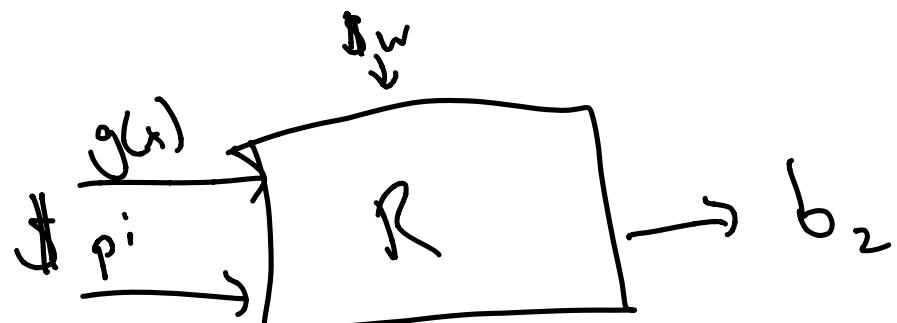
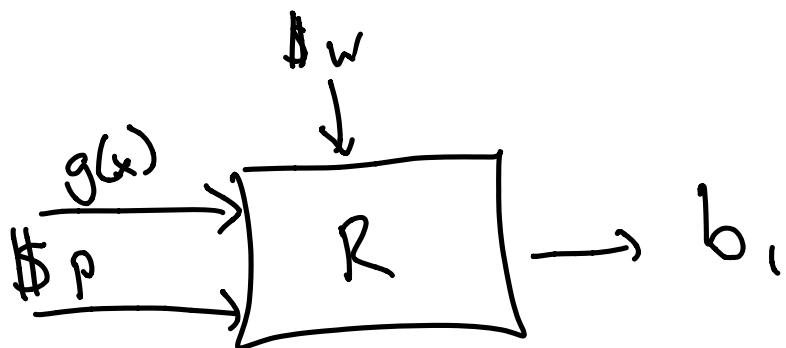
CALLS TO  $R$  AS SUBROUTINE

STEP 2: R PREDICTS  $\langle x, p \rangle$  w/  
PROBABILITY  $\frac{3}{4} + \epsilon$

---

$$\Pr[R \text{ makes mistake}] = \frac{1}{4} - \epsilon$$

$p^i := p$  w/  $i^{\text{th}}$  bit FLIPPED



IF BOTH ARE CORRECT, ONLY

i<sup>th</sup> BIT DOESN'T GET CANCELLED OUT

IN  $b_1 \oplus b_2$ . So  $b_1 \oplus b_2 = x_1$

IF BOTH ARE CORRECT, WHICH

Occurs with PROBABILITY AT LEAST

$$1 - \Pr[b_1 \text{ is wrong}] - \Pr[b_2 \text{ is wrong}]$$

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

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

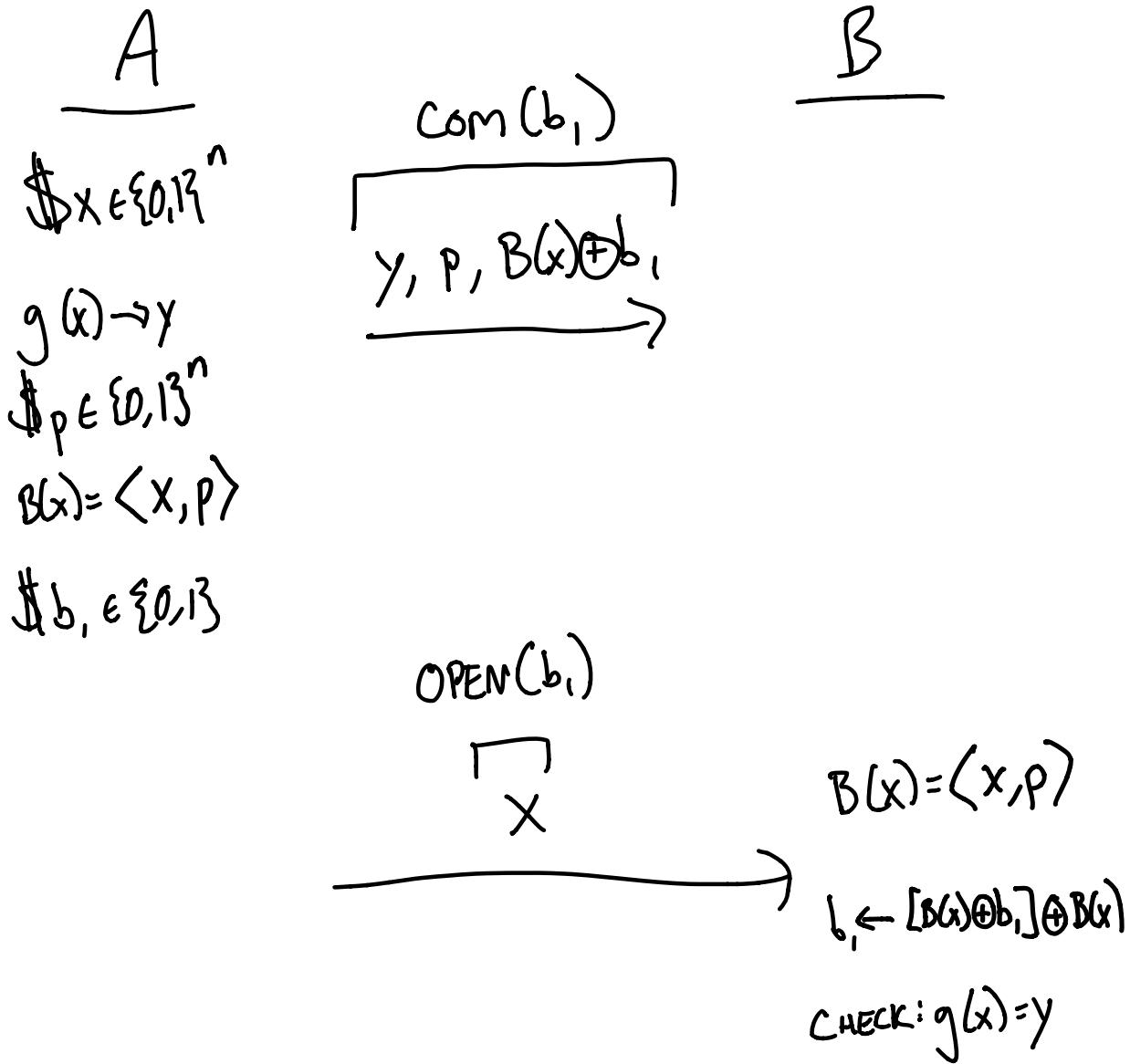
SO WE CAN PREDICT EACH  
BIT OF  $X$  WI PROBABILITY  $\frac{1}{2} + 2\epsilon$   
USING 2 CALLS TO  $R$ .

### 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  $\text{1WF}$ .

\* 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 ALL  $x$ .

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

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

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

TOOL FOR PROOF: BAYESIAN CONDITIONING

---

$$\begin{aligned} \Pr[A] &= \Pr[A|B] \cdot \Pr[B] \\ &\quad + \Pr[A|\neg B] \cdot \Pr[\neg B] \end{aligned}$$

Proof: Suppose  $< \frac{\epsilon}{2}$  inputs are "good"

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

$$= Pr_{x,p,w} [R(g(x), p) = B(x, p) | x \text{ is "good"}] \cdot Pr[x \text{ is "good"}]$$

$$+ Pr_{x,p,w} [R(g(x), p) = B(x, p) | x \text{ not "good"}] \cdot Pr[x \text{ not "good"}]$$

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

$\uparrow$        $\uparrow$        $\uparrow$   
 $Pr[\dots] \leq 1$       ASSUMPTION      DEF.  
 OF "GOOD"       $Pr[\dots] \leq 1$

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

THIS CONTRADICTS THE FACT THAT  $R$  IS SUCCESSFUL W/ PROBABILITY  $\frac{1}{2} + \epsilon$ .  $\therefore$   $\epsilon > 0$

AT LEAST  $\frac{\epsilon}{2}$  FRACTION OF  $x$  ARE "GOOD".  $\square$

## NEW TOPIC: PSEUDO-RANDOM GENERATORS

MOTIVATING EXAMPLE: ONE-TIME PAD Encryption

A

$$m \in \{0,1\}^n$$

$$k \in \{0,1\}^n$$

$$CT = m \oplus k$$

B  
—  
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  $\text{PRG}(s) \rightarrow k$  WHICH TAKES A SHORT, TRULY RANDOM SEED  $s$  + OUTPUTS A LONG "RANDOM-LOOKING" STRING  $k$ ?

THEN, COULD DISTRIBUTE SHORT SEED  $s$  + EACH PARTY USES  $\text{PRG}(s)$  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 NEGIGIBLE  
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:

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

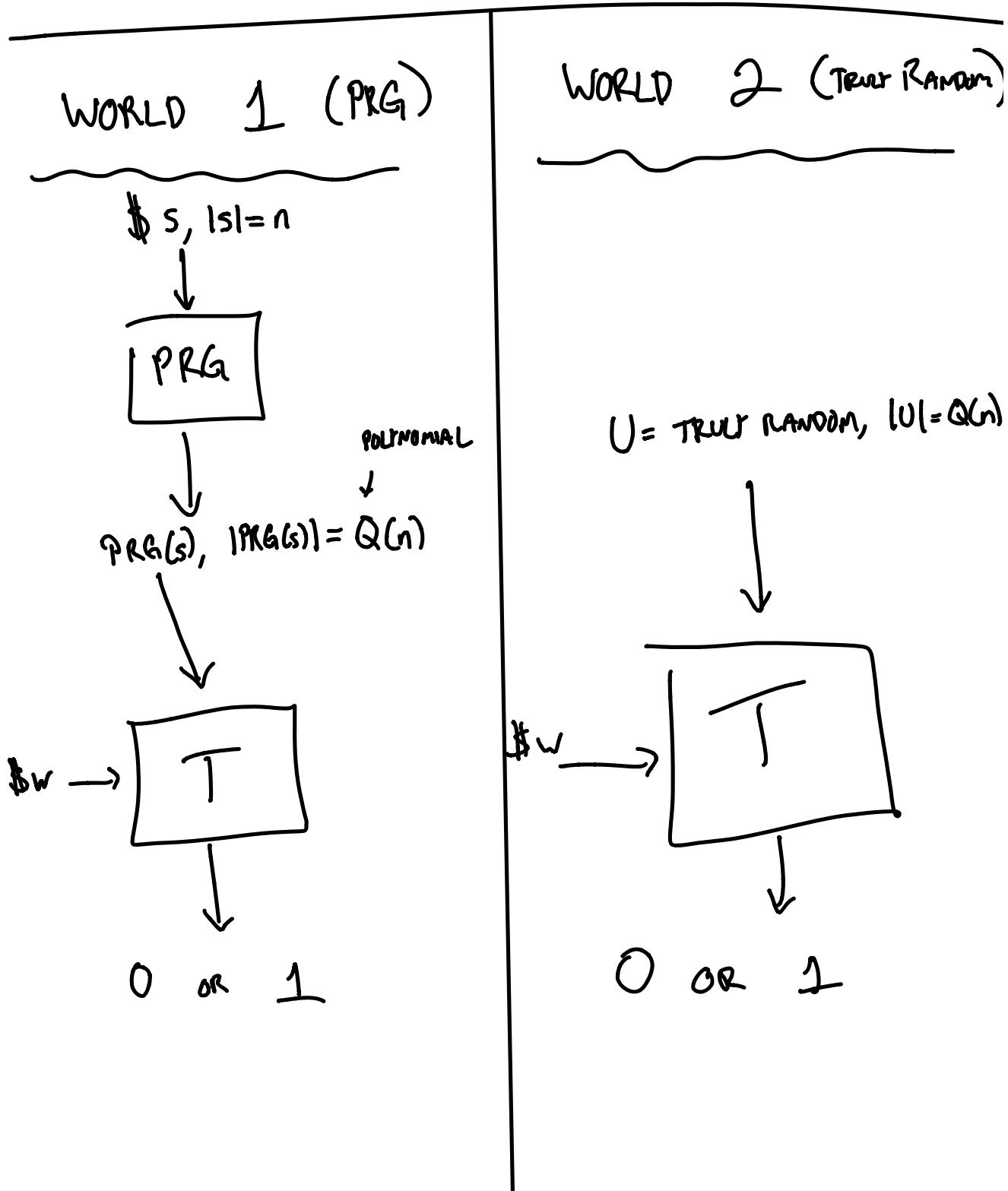
WE CALL THE TESTING ALGORITHM  $\overline{T}$ ,  
 USED TO DETERMINE IF 2 DISTRIBUTIONS  
 ARE THE SAME OR NOT, A STATISTICAL TEST.

THE FOLLOWING DEF SAYS THAT  $X_n, Y_n$   
 ARE INDISTINGUISHABLE WITH RESPECT TO  
 THE TEST  $\overline{T}$  IF  $\overline{T}$  CANNOT DETERMINE  
 WHETHER A SAMPLE COMES FROM  $X_n$  OR  $Y_n$ .

DEF  $X_n, Y_n$  ARE INDISTINGUISHABLE UNDER  
 TEST  $\overline{T}$  IF  $\forall c, \exists N_c$  s.t.  $\forall n > N_c:$

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

# VISUALIZATION OF (INDISTINGUISHABILITY) TESTING:



$X_n$  +  $Y_n$  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

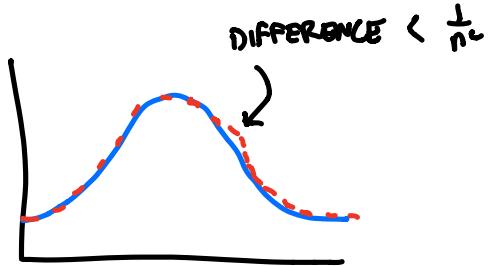
$\forall c, \forall A \in PPT, \exists N_c \text{ s.t. } \forall n > N_c :$

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

## SLIGHTLY STRONGER NOTION: STATISTICAL CLOSENESS

INTUITION: DIFFERENCE BETWEEN ACTUAL DISTRIBUTIONS IS NEGIGIBLE.

VISUALLY:



FORMALLY:  $X_n, Y_n$  ARE STATISTICALLY CLOSE

IF  $\forall c, \exists N_c$  s.t.  $\forall n > N_c$ :

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

# EXTENDED STATISTICAL TEST

WHY DOES  $T$  ONLY GET A SINGLE SAMPLE?

IN REALITY, YOU 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.  
 $\forall n > N_{c_1, c_2}$ :

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

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

ASSUME  $\exists T'$  WHICH DISTINGUISHES  $X_n$  FROM  $Y_n$  USING  $k$  SAMPLES, WITH PROBABILITY GREATER THAN  $\varepsilon(n)$ . THAT IS,

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

← COULD BE FLIPPED, BUT THEN WE CAN REVERSE ENTIRE PROOF

CONSIDER "HYBRIDS"  $P_0, \dots, P_k$  WHERE IN  $P_j$ ,

THE FIRST  $j$  SAMPLES COME FROM  $Y_n$  AND THE REMAINING SAMPLES COME FROM  $X_n$ :

$$P_0 = \left( \Pr_{\substack{X_n, Y_n}} [T'(X_1, X_2, \dots, X_k)] = 1 \right)$$

$$P_1 = \left( \Pr_{\substack{X_n, Y_n}} [T'(Y_1, X_2, \dots, X_k)] = 1 \right)$$

$\vdots$

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

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

REWRITING  $\textcircled{*}$  IN TERMS OF  $P_j$ , WE KNOW

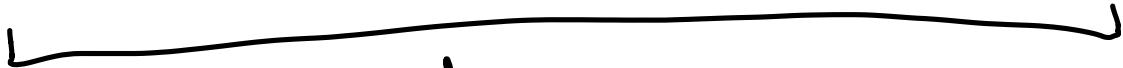
$$P_0 - P_k > \epsilon(n)$$

WE CAN REWRITE THIS AS A "TELESCOPING" SUM:

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

REGROUPING GIVES US:

$$(P_0 - P_1) + (P_1 - P_2) + \dots + (P_{k-2} - P_{k-1}) + (P_{k-1} - P_k) > \epsilon(n)$$

  
k TOTAL TERMS

By PIGEONHOLE PRINCIPLE,  $\exists j$  s.t.

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

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

CONSIDER A DISTRIBUTION  $P(z)$  DEFINED:

$$P(z) = y_1, y_2, \dots, y_j, z, x_{j+1}, \dots, x_k$$

NOTICE: IF  $z$  IS A SAMPLE FROM  $Y_n$ , THEN  $P(z) = P_j$   
IF  $z$  IS A SAMPLE FROM  $X_n$ , 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  $y_1, \dots, y_j \leftarrow Y_n$  AND  
 $x_{j+1}, \dots, x_k \leftarrow X_n$

③ COMPUTE  $T'(y_1, \dots, y_j, z, x_{j+1}, \dots, x_k)$

WHAT IS THE PROBABILITY THAT  $T$  DISTINGUISHES  $Z$ ?

$$\begin{aligned} & \Pr_{X_n} [T(X_n) = 1] - \Pr_{Y_n} [T(Y_n) = 1] \\ &= \Pr[\text{GUESS } j \text{ CORRECT}] \cdot (P_j - P_{j+1}) \\ &= \frac{1}{k} \cdot (P_j - P_{j+1}) \\ &> \frac{1}{k} \cdot \frac{\varepsilon(n)}{k} \\ &= \frac{\varepsilon(n)}{k^2} \\ &= \frac{1}{k^3} \\ &= \frac{1}{(\text{poly}(n))^3} \end{aligned}$$

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.  $\blacksquare$

# CONSTRUCTING A PRG

## FORMAL PRG DEFINITION:

A DETERMINISTIC ALGORITHM  $G$  IS A PRG IF:

①  $G(x, Q)$  RUNS IN TIME  $\text{POLY}(l_x l, Q(l_x))$

WHERE  $Q$  IS A POLYNOMIAL

②  $G(x, Q)$  OUTPUTS STRINGS OF LENGTH  
 $Q(l_x l)$  FOR ALL  $x$

③ FOR EVERY POLYNOMIAL  $Q$ , THE  
DISTRIBUTION  $\{G(x, Q)\}$  IS COMPUTATIONALLY  
INDISTINGUISHABLE FROM  $\{U_{Q(l_x l)}\}$ , WHERE

$U_{Q(l_x l)}$  IS A UNIFORM DISTRIBUTION ON  
STRINGS OF LENGTH  $Q(l_x l)$

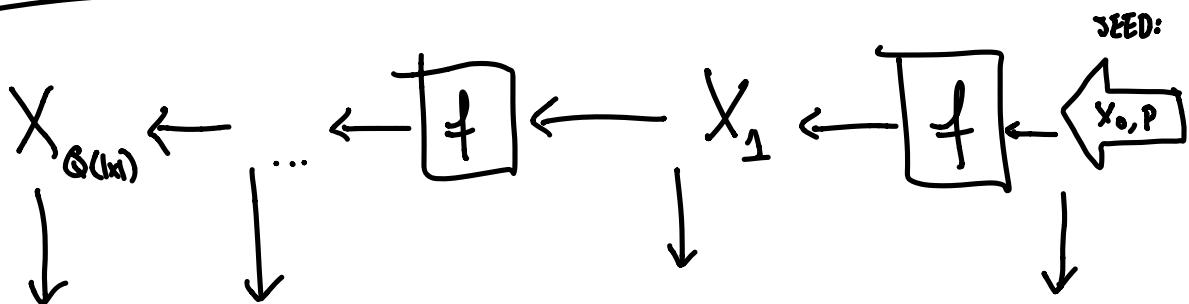
# CONSTRUCTING PRG FROM 1WP

LET  $f$  BE 1-WAY PERMUTATION

CHOOSE RANDOM SEED  $X_0$ , RANDOM STRING  $P$ ,

$$|X_0| = |P| = n$$

## VISUALIZATION



$P \quad X_{Q(x_1)} \quad \langle P, X_{Q(x_1)-1} \rangle \quad \dots \quad \langle P, X_1 \rangle \quad \langle P, X_0 \rangle$

OUTPUT

## ALGORITHM FOR G

① Pick 1wl 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 REVERSE ORDER

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  $\frac{1}{2}$ .

(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  $\forall i \in [0, n]$ :

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

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,  $\exists A \in \text{PPT}$  S.T.

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

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  
 $X_{n-i}$  ; TIMES AS DESCRIBED BY  $G_i$ , AND  
COMPUTE THE FIRST  $i$  BITS OF THE OUTPUT  
 $G_1, \dots, G_i$ . THEN, COMPUTE

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

NOTE THIS IS PRECISELY  $G_{i+1} = \langle X_{n-i}, P \rangle$   
WITH PROBABILITY  $\frac{1}{2} + \epsilon(n)$ . Thus we  
PREDICTED THE HCB OF  $f(X_{n-i})$ , WHICH  
IMPLIES WE CAN INVERT  $f(X_{n-i})$  WITH  
SIGNIFICANT PROBABILITY.  $\blacksquare$

CLAIM ② :

$X_n$  IS PSEUDORANDOM



$X_n$  IS UNPREDICTABLE

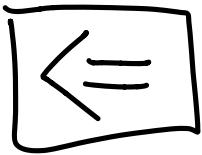
PROOF:



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 MBT



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  $\epsilon(n)$ . BY PREVIOUS HYBRID ARGUMENT

APPLIED TO  $X_n, U_n, \exists i$  SUCH THAT

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

WHERE  $l$  IS TOTAL # OF SAMPLES.

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



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

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

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

CALCULATION:

$$\begin{aligned}
 & \Pr[A(x_1, \dots, x_i) = x_{i+1}] \\
 &= \Pr[x_{i+1} = b] \cdot \Pr[D(x_1, \dots, x_i, x_{i+1}, u_{i+2}, \dots, u_e) = 1] \\
 &\quad + \Pr[x_{i+1} = \bar{b}] \cdot \underbrace{\Pr[D(x_1, \dots, x_i, \bar{x}_{i+1}, u_{i+2}, \dots, u_e) = 0]}_{\text{CALL THIS } q} \\
 &= \frac{1}{2} \cdot P_{i+1} + \frac{1}{2} \cdot q
 \end{aligned}$$

WHAT IS  $q$ ? LET'S EXPAND  $P_i$

$$\begin{aligned}
 P_i &= \Pr[D(x_1, \dots, x_i, u_{i+1}, \dots, u_e) = 1] \\
 &= \Pr[D(x_1, \dots, x_i, x_{i+1}, u_{i+2}, \dots, u_e) = 1] \cdot \Pr[u_{i+1} = x_{i+1}] \\
 &\quad + \Pr[D(x_1, \dots, x_i, \bar{x}_{i+1}, u_{i+2}, \dots, u_e) = 1] \cdot \Pr[u_{i+1} = \bar{x}_{i+1}] \\
 &= P_{i+1} \cdot \frac{1}{2} + (1-q) \cdot \frac{1}{2}
 \end{aligned}$$

THUS,

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

FINALLY, SUBSTITUTING THIS  $q$  VALUE YIELDS:

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

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

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

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

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

THUS, A PREDICTS THE  $i+1^{\text{st}}$  BIT OF  $X_n$  WITH SIGNIFICANT ADVANTAGE, WHICH COMPLETES THE PROOF.  $\blacksquare$