Indistinguishability
OUTLINE

hw - p5 deferred.
COMPUTATIONAL INDISTINGUISHABILITY & PSEUDO-RANDOMNESS
NEXT SLIDE HAS 2 PICS

are they the same or different?
same or different?
same or different?

TWICE THE TIME.
same or different?

TWICE THE TIME.
same or different?

TWICE THE TIME.
LESSON:

Ability to answer correctly... depends on your computational resources.
NEW PROBLEM:
consider all drawings consisting of boxes.

**evens**

- # of boxes that overlap another box is even

**odds**

- # of ... is odd
GAME:

I will pick a sample from either evens or odds, and you will have to guess which one.
READY?
READY?
THIS GAME IS PARAMETERIZED BY ITS SIZE: I.E, # OF BOXES.
THIS GAME IS PARAMETERIZED BY ITS SIZE: I.E, # OF BOXES.
AS THE GAME SIZE INCREASES, IT BECOMES INTRACTABLE TO DISTINGUISH B/W EVENS AND ODD
\[ \{ X_n \} \text{ ensemble} \]

sequence of probability distributions \( X_1 X_2 X_3 \ldots \)

where \( X_i \) is a distribution over strings of length \( \ell(i) \) for some polynomial \( \ell \).
PARAMETERIZED EXPERIMENT

\[ \{ X_n \} \quad n \in \mathbb{N} \]

a sequence of probability distributions
where \( X_n \) is a distribution over strings of length \( \ell(n) \)
"let there be two parameterized experiments, $X$ and $Y$. as the experiment size increases, no p.p.t. algorithm $D$ succeeds in distinguishing $X$ from $Y$."

WHAT DOES IT MEAN FOR AN ALGORITHM $D$ TO DISTINGUISH A SAMPLE?
D(\text{even}) = "evens"

D(\text{odd}) = "odds"
Two ensembles are comp. indistinguishable

\[ \xi \{ X_n \}_n \text{ and } \xi \{ Y_n \}_n \text{ written as } \xi \{ X_n \}_n \approx \xi \{ Y_n \}_n \]

if a nuppt "distinguish" D \in \text{ neigh e sit.}

\[ \left| \Pr[t \in X_n : D(t) = 1] - \Pr[t \in Y_n : D(t) = 1] \right| < \epsilon \text{(n)} \]
\forall \delta \\
\left| \Pr[X \in t : D(t) = 1] - \Pr[t \in X : D(t) = 0] \right| < \epsilon
Two ensembles are comp. indistinguishable

\[ \{X_n\}_{n \in N} \approx \{Y_n\}_{n \in N} \]
Two ensembles are comp. indistinguishable

\[ \{ X_n \}_{n \in N} \approx \{ Y_n \}_{n \in N} \]

if for all non-uniform p.p.t. alg \( D \),
there exists a negl function \( \epsilon(n) \)
such that for all \( n \)
Two ensembles are computationally indistinguishable

\[ \{X_n\}_{n \in N} \approx \{Y_n\}_{n \in N} \]

if for all non-uniform p.p.t. alg D, there exists a negl function \( \epsilon(n) \)
such that for all \( n \)

\[ |\Pr [t \leftarrow X_n, D(t) = 1] - \Pr [t \leftarrow Y_n, D(t) = 1]| \leq \epsilon(n). \]
Two ensembles are comp. indistinguishable

\[ \{ X_n \}_{n \in N} \cong \{ Y_n \}_{n \in N} \]
Two ensembles are comp. indistinguishable

\[ \{ X_n \}_{n \in N} \approx \{ Y_n \}_{n \in N} \]

if for all non-uniform p.p.t. alg \( D \),
there exists a negl function \( \epsilon(n) \)
such that for all \( n \)
Two ensembles are comp. indistinguishable

\[ \{X_n\}_{n \in N} \approx \{Y_n\}_{n \in N} \]

if for all non-uniform p.p.t. alg \(D\),
there exists a negl function \(\epsilon(n)\)
such that for all \(n\)

\[ |\Pr[t \leftarrow X_n, D(t) = 1] - \Pr[t \leftarrow Y_n, D(t) = 1]| \leq \epsilon(n). \]
CLOSURE PROPERTIES

\[
\text{IF} \quad \{X_n\}_{n\in\mathbb{N}} \approx \{Y_n\}_{n\in\mathbb{N}}
\]

\[
\text{THEN} \quad \forall \text{ ppt } M, \quad \exists \ M(X_n)_{3n} \approx \{M(Y_n)_{3n}.
\]

\text{Proof:} \quad \text{Suppose that } \exists \text{ a ppt } M \text{ s.t. for infinitely many } n,

(\text{Sketch}) \quad \Pr[t \in M(X_n): D(t) = 1] - \Pr[t \in M(Y_n): D(t)] > \frac{1}{\text{poly}(n)}

Therefore construct } D_1,

\[D_1(t) : \text{ Runs } \overline{D(M(X_n))}.\]

\[\Rightarrow D_1 \text{ violates the indistinguishability of } \{X_n\}_{n\in\mathbb{N}} \approx \{Y_n\}_{n\in\mathbb{N}}.\]
Consider sequence \( \{X^1\}, \{X^2\}, \ldots, \{X^m\} \) and suppose \( \{X^1\} \) could be distinguished from \( \{X^m\} \) w/ prob \( \epsilon \).

\[ \Rightarrow \exists i \text{ s.t. } \{X^i\} \text{ and } \{X^{i+1}\} \text{ are distinguishable w/ pr.} \geq \frac{\epsilon}{m} \]
\[ \Pr(D(x) = 1) \]

The diagram shows a series of intervals \{X^1\}, \{X^2\}, \{X^3\}, ..., \{X^{m-1}\}, \{X^m\} with increasing probability up to \( \frac{\xi}{m} \).
**PROOF:**

Let \( q_i = \Pr [ t \in X^i : D(t) = 1 ] \).

\[
|g_1 - g_2| + |g_2 - g_3| + \cdots + |g_{m-1} - g_m| \geq |g_1 - g_2 + g_2 - g_3 + \cdots - g_m| = |g_1 - g_m| > \varepsilon
\]

\( \Rightarrow \) exist some \( i \) s.t. \( |g_i - g_{i+1}| > \frac{\varepsilon}{m} \)

**TRANSITIVITY:**

\( A \sim B \quad B \sim C \implies A \sim C \), by this hybrid argument.
PROOF: Suppose $\{X^1\}$ can be dist. from $\{X^m\}$
TRANSITIVITY ONLY HOLDS FOR A POLY NUMBER OF STEPS
EXAMPLE OF A SEQUENCE OF DISTRIBUTIONS

\{X^1\}, \ldots , \{X^k\}

where \( \{X^i\} \approx \{X^{i+1}\} \)

but \( \{X^1\} \not\approx \{X^k\} \)
statistically close...

\[ X_1 = \sum \frac{1}{1000}, \frac{1}{999}, \frac{1}{998}, \ldots, \frac{1}{2}, \frac{1}{1}, \ldots \]

\[ X_2 = \exists \]
\[ \{X^1\}_{n \in \mathbb{N}} = \{1, 2, \ldots, 1 + 2^{n/2} \mod 2^n \} \]

\[ \{X_2, 3^n + m \}_{n \in \mathbb{N}} = \{2, 3, 4, \ldots, 2^{n/2} + 2 \} \]

\[ \{X_{ni} \} = \{ n, k+1, \ldots, k+2^{n/2} \} \]

\[ \{X_i \} \sim \{X_{i+1} \} \]

\[ \{X_{i} \} \cap \{X_{2n+2} \} \] disjoint.
UNIFORM DISTRIBUTION ON STRINGS OF LEN $n$

$$U_n = \{ t \leftarrow \{0, 1\}^n \}$$

$2^n$, $\frac{1}{2^n}$
WHAT DOES IT MEAN FOR A PROCESS \{X\} TO BE PSEUDO-RANDOM?
\{X_n\}_{n \in \mathbb{N}}

pseudo-random.

x \leftarrow X_n
\{X_n\}_{n \in \mathbb{N}}

x \leftarrow X_n

\rightarrow \text{roughly same # of 0s and 1s}
\( \{ X_n \} \_{n \in \mathbb{N}} \)

\( x \leftarrow X_n \)

roughly same # of 0s and 1s

roughly same # of 00s and 11s
\( \{ X_n \} \quad n \in \mathbb{N} \)

\[ x \leftarrow X_n \]

- roughly same # of 0s and 1s
- roughly same # of 00s and 11s
- roughly same # of any pattern

any computational test...
\[ \{ X_n \}_{n \in \mathbb{N}} \]

\[ x \leftarrow X_n \]

roughly same # of 0s and 1s
roughly same # of 00s and 11s
roughly same # of any pattern
given any prefix, hard to guess next bit
INDISTINGUISHABILITY PROVIDES A PRECISE WAY OF FORMULATING PSEUDO-RANDOMNESS
PSEUDO-RANDOM

if

\( \{ x_n \} \approx \{ u_n \} \)
An ensemble \( \{X\} \) is said to be 

**PSEUDO-RANDOM**

if


\textbf{PSEUDO-RANDOM} \\

\text{if} \\

\{X\}_{n \in \mathbb{N}} \approx \{U_n\}_{n \in \mathbb{N}}
An ensemble \( \{X\} \) is said to be **PSEUDO-RANDOM** if

\[
\{ X \}_{n \in \mathbb{N}} \approx \{ U_n \}_{n \in \mathbb{N}}
\]
\[ \{X\}_{n \in \mathbb{N}} \approx \{U_n\}_{n \in \mathbb{N}} \]

implies that \(\{X\}\) passes every p.p.t. statistical test

1. NEXT-BN TEST.

2. How to build PRG

\[ \Rightarrow \text{Enc Scheme. (almost)} \]
An ensemble \( \{X\} \) passes this test if for all non-uniform ppt \( A \)

\[
\Pr[t \leftarrow X_n : A(1^n, t_1 t_2 \ldots t_i) = t_{i+1}] \leq \frac{1}{2} + \epsilon(n).
\]