

09/11

Class may move to CS 1211.

Goal: build function  $G: \{0, 1\}^l \rightarrow \{0, 1\}^L$   
that "looks random"

Distinguishability

defn. Distributions  $D$  and  $D'$  are  $\epsilon$ -statistically indistinguishable if for all algorithms  $A$

$$\text{Adv } A = |P[A(x)=1; x \leftarrow D] - P[A(x)=1; x \leftarrow D']| \leq \epsilon$$

- always outputs 1,  $\text{Adv } A = 1$
- is a random bit,  $\text{Adv } A = 0$

Ex:  $D_1 = \begin{cases} 0: 100\% \\ 1: 0\% \end{cases}$       $D_2 = \begin{cases} 0: 50\% \\ 1: 50\% \end{cases}$

$$A(0) = 0$$

$$A(1) = 1$$

$$\text{Adv } A = |0 - .5| = 0.5$$

Lemma: If  $D$  and  $D'$  are  $\epsilon$ -statistically indistinguishable, then  $\sum_x |D(x) - D'(x)| \leq 2\epsilon$

Proof: consider adversary  $A(x) = \begin{cases} 0 & \text{if } D(x) > D'(x) \\ 1 & \text{if } \text{c.w.} \end{cases}$

$$\text{Adv } A = |\Pr[A(x)=1; x \leftarrow D] - \Pr[A(x)=1; x \leftarrow D']|$$

$$= \left| \sum_{x: D(x) \geq D'(x)} D(x) - \sum_{x: D(x) \geq D'(x)} D'(x) \right|$$

$$= \left| \sum_{x: D'(x) \geq D(x)} D(x) - D'(x) \right|$$

$$= \sum_{x: D'(x) \geq D(x)} D'(x) - D(x)$$

$$= \sum_{x: D'(x) \geq D(x)} |D'(x) - D(x)| \leq \epsilon$$

By symmetry

$$\sum_{x: D'(x) \geq D(x)} |D'(x) - D(x)| \leq \epsilon$$

$$\sum_{x: D'(x) \geq D(x)} |D'(x) - D(x)| \leq 2\epsilon$$

Defn: Distributions  $D$  and  $D'$  are  $(t, \epsilon)$ -computationally indistinguishable iff for all algorithms  $A$  executing in less than time  $t$ ,

$$\text{Adv } A \leq \epsilon$$

Ex.: Suppose  $D$  = uniform distribution on graphs with 1,000 nodes and containing a Hamiltonian cycle.

$D'$  = uniform distribution on graphs with 1,000 nodes without a Hamiltonian cycle

Conj.  $D$  and  $D'$  are  $(t, \epsilon)$ -comp. ind.  $\iff$   $[A]$  is computationally indistinguishable  $[A]$ .

Notation:  $D \stackrel{t}{\approx} D' \iff \exists A \text{ s.t. } A \text{ runs in time } t \text{ and } \text{Adv}_A > \epsilon$

Lemma: (Data Processing Inequality)

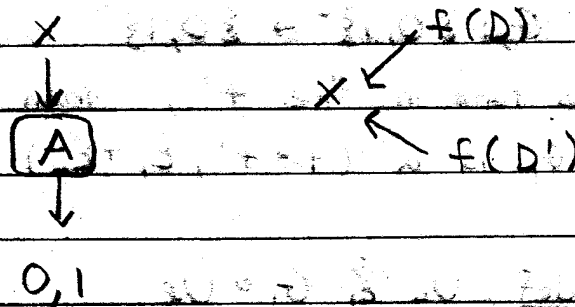
If  $D, D'$  are  $(t, \epsilon)$ -comp. ind. and  $f$  is any function executing in time  $t'$ , then

$$f(D) \stackrel{t+t'}{\approx} f(D')$$

Proof: (by contrapositive)

Assume  $A$  has  $\text{Adv}_A > \epsilon$  and  $A$  runs in time  $\leq t+t'$

Then  $B = A \circ f$  can distinguish  $D$  and  $D'$  with probability  $\epsilon$ .  $B$ 's time is  $t$ .



Lemma: If  $D \stackrel{t}{\approx} D'$  and  $D' \stackrel{t'}{\approx} D''$ , then  $D \stackrel{t+t'}{\approx} D''$

Proof: For any  $A$  running in time  $t+t'$

$$\text{Adv}_A = |\Pr[A(D)=1] - \Pr[A(D'')=1]|$$

$$= |\Pr[A(D)=1] - \Pr[A(D')=1]|$$

$$+ |\Pr[A(D')=1] - \Pr[A(D'')=1]|$$

$$\leq |P_r[A(D)=1] - P_r[A(D')=1]| + |P_r[A(D')=1] - P_r[A(D'')=1]|$$

$$= \text{Adv}_{D'}^A + \text{Adv}_{D''}^A \leq \epsilon_1 + \epsilon_2$$

Defn:  $G: \{0,1\}^l \rightarrow \{0,1\}^L$  is a  $(t, \epsilon)$  Pseudo-random generator (PRG) if  $G \circ U_l \stackrel{t}{\approx} U_L$

Give you  $L$ -bit string  $x$

Suppose try to compute  $k$  s.t.  $G(k) = x$

(1) success! Guess  $x$  is from  $G$

(2) failure! Guess  $x$  is uniform

Thm: If  $G_1: \{0,1\}^l \rightarrow \{0,1\}^L$  is  $(t, \epsilon_1)$  PRG and  $G_2: \{0,1\}^L \rightarrow \{0,1\}^m$  is  $(t', \epsilon_2)$  PRG and  $G_2$  runs in-time  $t'$ , then  $G_2 \circ G_1$  is a  $(t+t', \epsilon_1 + \epsilon_2)$  PRG

Running one after another

Proof: ① By def,  $U_l \stackrel{t}{\approx} G_1 \circ U_l$

② By DPI,  $G_2 \circ U_l \stackrel{t+t'}{\approx} G_2 \circ G_1 \circ U_l$

③ By def,  $G_2 \circ U_l \stackrel{t+t'}{\approx} U_m$

④ By obvious,  $G_2 \circ U_l \stackrel{t+t'}{\approx} U_m$

⑤ By trans,  $U_m \stackrel{t+t'}{\approx} G_2 \circ G_1 \circ U_l$

DPI  
= data  
processing  
inequality

running two  
side by

Thm: If  $G_1: \Sigma_1 \rightarrow \Sigma_2$  is  $(t_1, \epsilon_1)$  PRG

and  $G_2: \Sigma_2 \rightarrow \Sigma_3$  is  $(t_2, \epsilon_2)$  PRG

and  $G_2$  runs in time  $t'$ , then:

$G_1 \parallel G_2$  is a  $(\min(t_1 - t', t_2 - t'), \epsilon_1 + \epsilon_2)$  PRG

Proof: By def,  $G_1 \circ U_{\epsilon_1} \xrightarrow{t_1} U_{\epsilon_1}$

$G_2 \circ U_{\epsilon_2} \xrightarrow{t_2} U_{\epsilon_2}$

$G_1 \circ U_{\epsilon_1} \parallel G_2 \circ U_{\epsilon_2} \xrightarrow{t_1 - t' + t_2} U_{\epsilon_1} \parallel U_{\epsilon_2}$

By DPI

w  $f(x) = x \parallel G_2 \circ U$