LECTURE 7

EECS 575 – Fall 2022

Alexandra Veliche

Announcements & Reminders

- Homework 2
  - Due September 30 at 23:59.
- Homework 1 grading half-done
- Office Hours
  - Today: outside 3956 BBB (Theory Annex)

Agenda for this Lecture

- Indistinguishability
  - Statistical & Computational indistinguishability
  - Composition Lemma
  - Hybrid Lemma
- Pseudorandom Generators (PRGs)

Statistical Distance

- Let $\mathcal{X}$ and $\mathcal{Y}$ be two probability distributions over a common finite set Ω.

  The *statistical distance* between $\mathcal{X}$ and $\mathcal{Y}$ is given by

$$\Delta(\mathcal{X}, \mathcal{Y}) \coloneqq \max_{A \subseteq \Omega} \{ |\mathcal{X}(A) - \mathcal{Y}(A)| \},$$

  where $\mathcal{X}(S) \coloneqq \sum_{z \in A} \mathbb{P}[\mathcal{X} = z]$ is the probability that A occurs under $\mathcal{X}$.

Statistical Distance

- Let $\mathcal{X}$ and $\mathcal{Y}$ be two probability distributions over a common finite set Ω.

  The *statistical distance* between $\mathcal{X}$ and $\mathcal{Y}$ is given by

$$\Delta(\mathcal{X},\mathcal{Y}) \coloneqq \max_{A\subseteq\Omega}\{|\mathcal{X}(A)-\mathcal{Y}(A)|\},$$

  where $\mathcal{X}(\overset{A}{\cancel{S}}) \coloneqq \sum_{a\in A}\mathbb{P}[\mathcal{X}=a]$ is the probability that A occurs under $\mathcal{X}$.

$$|\mathcal{X}(\bar{A})-\mathcal{Y}(\bar{A})| = |(1-\mathcal{X}(A))-(1-\mathcal{Y}(A))| = |\mathcal{Y}(A)-\mathcal{X}(A)| = |\mathcal{X}(A)-\mathcal{Y}(A)|$$

$\bar{A} = \Omega \setminus A$

- Note: When Ω is infinite, the maximum is replaced with the *supremum*.

Statistical Distance

- Theorem: $\Delta(\mathcal{X},\mathcal{Y}) = \frac{1}{2}\sum_{\omega\in\Omega}|\mathcal{X}(\omega) - \mathcal{Y}(\omega)|$.

Proof: $A = \{\omega \in \Omega : X(\omega) > Y(\omega)\}$ maximizes $|X(A) - Y(A)|$

$$\Delta(X,Y) = |X(A) - Y(A)| = \sum_{\omega\in A} |X(\omega) - Y(\omega)|$$

$$\Delta(X,Y) = |Y(\bar{A}) - X(\bar{A})| = \sum_{\omega\in \bar{A}} |X(\omega) - Y(\omega)|$$

(+)

$$2\Delta(X,Y) = \sum_{\omega\in \Omega} |X(\omega) - Y(\omega)|$$

$$\Delta(X,Y) = \frac{1}{2}\sum_{\omega\in \Omega} |X(\omega) - Y(\omega)| \checkmark$$

$\square$

Statistical Distance

❖ Theorem: $\Delta(\mathcal{X},\mathcal{Y}) = \frac{1}{2}\underbrace{\sum_{\omega\in\Omega}|\mathcal{X}(\omega) - \mathcal{Y}(\omega)|}_{1}$.

Example:

$\mathcal{X} = \mathcal{U}(\{0,1\}^n)$ uniform

$\mathcal{Y} = \{0\} \times \mathcal{U}(\{0,1\}^{n-1})$

$\Rightarrow \Delta(\mathcal{X},\mathcal{Y}) = \frac{1}{2}(1) = \frac{1}{2}$

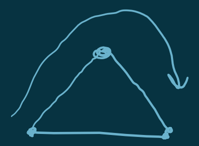
maximizing test: $A = \{1\} \times \mathcal{U}(\{0,1\}^{n-1})$

$\mathcal{X}(A) = \frac{1}{2}$, $\mathcal{Y}(A) = 0$

$\Rightarrow \Delta(\mathcal{X},\mathcal{Y}) = \frac{1}{2}$ ✓

Statistical Distance

- Lemma: Statistical distance is a metric, i.e.
  - (identity of indiscernibles) $\Delta(\mathcal{X}, \mathcal{Y}) = 0 \iff \mathcal{X} = \mathcal{Y}$
  - (symmetry) $\Delta(\mathcal{X}, \mathcal{Y}) = \Delta(\mathcal{Y}, \mathcal{X})$
  - (triangle inequality) $\Delta(\mathcal{X}, \mathcal{Z}) \leq \Delta(\mathcal{X}, \mathcal{Y}) + \Delta(\mathcal{Y}, \mathcal{Z})$.



- Lemma: ("information processing") Let f be any function (or randomized procedure) on Ω. Then $\Delta\big(f(\mathcal{X}), f(\mathcal{Y})\big) \leq \Delta(\mathcal{X}, \mathcal{Y})$.

Statistical Indistinguishability

❖ Definition: Let $\mathcal{X} = \{\mathcal{X}_n\}_{n\in\mathbb{N}}$ and $\mathcal{Y} = \{\mathcal{Y}_n\}_{n\in\mathbb{N}}$ be sequences of probability distributions, called *ensembles*. $\mathcal{X}$ and $\mathcal{Y}$ are *statistically indistinguishable,* denoted by $\mathcal{X} \approx_s \mathcal{Y}$, iff $\Delta(\mathcal{X}_n, \mathcal{Y}_n) = negl(n)$.

Example:

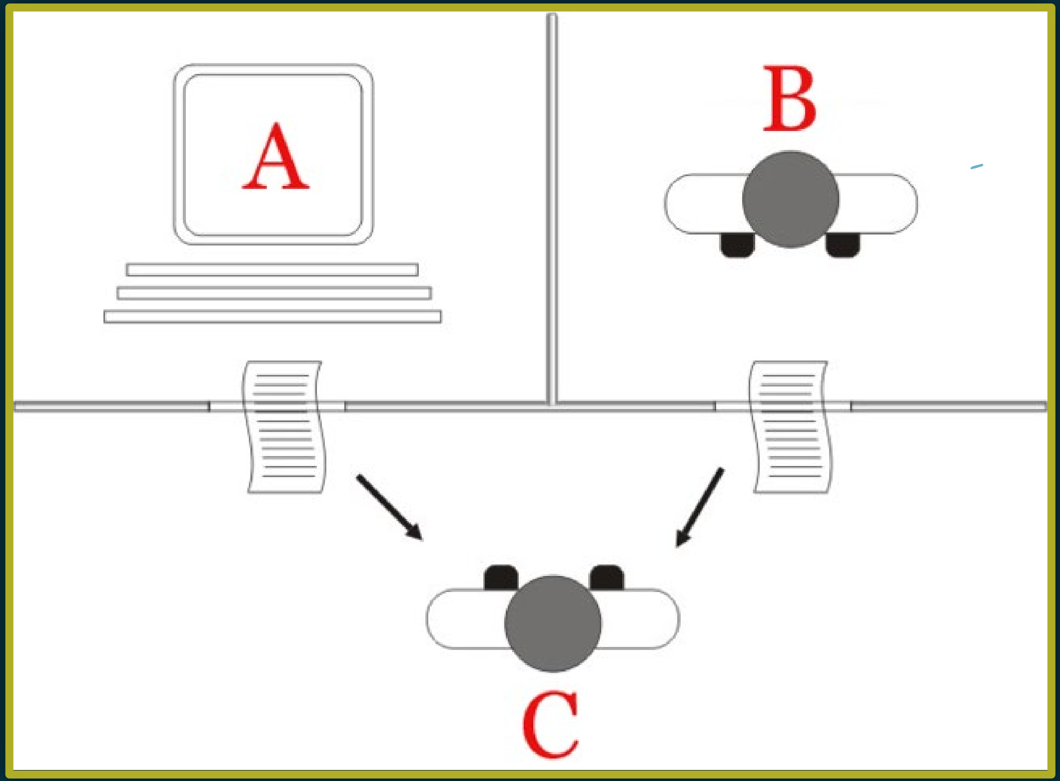
$X_n = \mathcal{U}(\{0,1\}^n)$ uniform $\longrightarrow \mathcal{X}$

$Y_n = \mathcal{U}(\{0,1\}^n \setminus \{0^n\}) \longrightarrow \mathcal{Y}$

$$A = \{0^n\} \Rightarrow \left.\begin{array}{l} X_n(A) = \frac{1}{2^n} \\ Y_n(A) = 0 \end{array}\right\} \Rightarrow \Delta(X_n, Y_n) = \left|\frac{1}{2^n} - 0\right| = \frac{1}{2^n} = negl(n)$$

Computational Indistinguishability

Turing test:



Computational Indistinguishability

- Definition: Let $\mathcal{X}$ and $\mathcal{Y}$ be distributions and $\mathcal{A}$ be a (possibly randomized) algorithm. The *distinguishing advantage* of $\mathcal{A}$ between $\mathcal{X}$ and $\mathcal{Y}$ is given by

$$Adv_{\mathcal{X},\mathcal{Y}}(\mathcal{A}) \coloneqq |\mathbb{P}[\mathcal{A}(\mathcal{X}) = 1] - \mathbb{P}[\mathcal{A}(\mathcal{Y}) = 1]|.$$

$$= \left| \underset{z \leftarrow \mathcal{X}}{\mathbb{P}} [\mathcal{A}(z) = 1] - \underset{z \leftarrow \mathcal{Y}}{\mathbb{P}} [\mathcal{A}(z) = 1] \right|$$

- For ensembles $\mathcal{X} = \{\mathcal{X}_n\}_{n\in\mathbb{N}}, \mathcal{Y} = \{\mathcal{Y}_n\}_{n\in\mathbb{N}}, Adv_{\mathcal{X},\mathcal{Y}}(\mathcal{A})$ is a function on n.

Computational Indistinguishability

- Definition: Let $\mathcal{X} = \{\mathcal{X}_n\}_{n\in\mathbb{N}}$ and $\mathcal{Y} = \{\mathcal{Y}_n\}_{n\in\mathbb{N}}$ be ensembles over $\{0,1\}^{\ell(n)}$ for $\ell(n) = poly(n)$. $\mathcal{X}$ and $\mathcal{Y}$ are *computationally indistinguishable,* denoted by $\mathcal{X} \approx_c \mathcal{Y}$, if for any nuPPT algorithm $\mathcal{A}$, $Adv_{\mathcal{X},\mathcal{Y}}(\mathcal{A}) = negl(n)$.

Computational Indistinguishability

- Definition: Let $\mathcal{X} = \{\mathcal{X}_n\}_{n\in\mathbb{N}}$ and $\mathcal{Y} = \{\mathcal{Y}_n\}_{n\in\mathbb{N}}$ be ensembles over $\{0,1\}^{\ell(n)}$ for $\ell(n) = poly(n)$. $\mathcal{X}$ and $\mathcal{Y}$ are *computationally indistinguishable*, denoted by $\mathcal{X} \approx_c \mathcal{Y}$, if for any nuPPT algorithm $\mathcal{A}$, $Adv_{\mathcal{X},\mathcal{Y}}(\mathcal{A}) = negl(n)$.

- $\mathcal{X}$ is *pseudorandom* if $\mathcal{X} \approx_c \{\mathcal{U}_{\ell(n)}\}_{n\in\mathbb{N}}$ the ensemble of uniform distributions over $\{0,1\}^{\ell(n)}$.

Composition Lemma

- Lemma: ("composition lemma", analogue of information processing)

Let $\mathcal{B}$ be nuPPT algorithm. If $\{\mathcal{X}_n\}_{n\in\mathbb{N}} \approx_c \{\mathcal{Y}_n\}_{n\in\mathbb{N}}$, then $\{\mathcal{B}(\mathcal{X}_n)\}_{n\in\mathbb{N}} \approx_c \{\mathcal{B}(\mathcal{Y}_n)\}_{n\in\mathbb{N}}$.

- Note: $\mathcal{B}(\mathcal{X}_n)$ is the distribution obtained by sampling $x \leftarrow \mathcal{X}_n$ and outputting $\mathcal{B}(x)$.

Composition Lemma

Proof: $\{X_n\} \approx_c \{y_n\} \Leftrightarrow \forall$ nuPPT $\mathcal{A}$, $Adv_{X_n, y_n}(\mathcal{A}) = negl(n)$

To show: $\{\mathcal{B}(X_n)\} \approx_c \{\mathcal{B}(y_n)\} \Leftrightarrow \forall$ nuPPT $\mathcal{D}$, $Adv_{\mathcal{B}(X_n), \mathcal{B}(y_n)}(\mathcal{D}) = negl(n)$.

(reduction) Let $\mathcal{D}$ be any nuPPT algo attempting to distinguish between $\{\mathcal{B}(X_n)\}$ and $\{\mathcal{B}(y_n)\}$.

Construct $\mathcal{A}$: given x, compute $\mathcal{B}(x)$, run $\mathcal{D}(\mathcal{B}(x))$, output what $\mathcal{D}$ outputs.

$\mathcal{D}, \mathcal{B}$ nuPPT $\Rightarrow \mathcal{A}$ nuPPT ✓

$$Adv_{x_n, y_n}(\mathcal{A}) = |\mathbb{P}[\mathcal{A}(x_n) = 1] - \mathbb{P}[\mathcal{A}(y_n) = 1]|$$

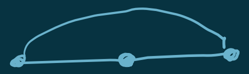
$$= |\mathbb{P}[\mathcal{D}(\mathcal{B}(X_n)) = 1] - \mathbb{P}[\mathcal{D}(\mathcal{B}(y_n)) = 1]|$$ by construction

$$\underbrace{\phantom{Adv_{x_n,y_n}(\mathcal{A})}}_{negl(n)} = Adv_{\mathcal{B}(X_n), \mathcal{B}(y_n)}(\mathcal{D}) = negl(n) \checkmark$$

□

Hybrid Lemma

❖ Lemma: ("hybrid lemma", analogue of triangle inequality)



$\{1, \ldots, m\}$

Let $\mathcal{X}^i = \{\mathcal{X}_n^i\}_{n\in\mathbb{N}}$ for $i \in [m], m = poly(n)$. If $\mathcal{X}^i \approx_c \mathcal{X}^{i+1}$ for any $i \in [m-1]$, then $\mathcal{X}^1 \approx_c \mathcal{X}^m$.

Hybrid Lemma

$\forall a,b,c \in \mathbb{R}$,
$|a-c| \leq |a-b| + |b-c|$

$X_n^1 \approx_c X_n^2 \approx_c X_n^3 \approx_c \dots \approx_c X_n^m$

Proof: Let D be any nuPPT algo. against X_n^1 vs. X_n^m.

Denote $p_i(n) := \mathbb{P}[D(X_n^i)=1] \in \mathbb{R}$

$$Adv_{X^1,X^m}(D) = |p_1(n) - p_m(n)| \leq \sum_{i=1}^{m-1} |p_i(n) - p_{i+1}(n)| = \sum_{i=1}^{m-1} \underbrace{Adv_{X^i,X^{i+1}}(D)}_{negl(n)}$$

$$= (m-1)\, negl(n) = poly(n) \cdot negl(n) = negl(n).$$

$Adv_{X^1,X^m}(D) = negl(n)$. ✓

$\square$

Pseudorandom Generators

- Definition: A *pseudorandom generator (PRG)* is a deterministic, efficiently-computable function $G : \{0,1\}^* \rightarrow \{0,1\}^*$ with expansion $\ell(n) > n$ that satisfies
  - (expansion) $|G(x)| = \ell(|x|) > x$ for any $x \in \{0,1\}^*$
  - (pseudorandomness) the ensemble $\{G(\mathcal{U}_n)\}_{n \in \mathbb{N}}$ is pseudorandom, i.e. for any nuPPT $\mathcal{D}$, $Adv_G^{PRG}(\mathcal{D}) := \left|\mathbb{P}_{x \leftarrow \{0,1\}^n}\left[\mathcal{D}\big(G(x)\big) = 1\right] - \mathbb{P}\left[\mathcal{D}\big(\mathcal{U}_{\ell(n)}\big) = 1\right]\right|$.

Pseudorandom Generators

Examples: Determine if the functions below are PRGs.

- $H(x) \coloneqq \overline{G(x)}$, assuming G is a PRG. $\longrightarrow$ Yes! use composition lemma exercise!

  B

- $H(x) \coloneqq x || \underbrace{(x_1 \oplus \cdots \oplus x_n)}_{\in \{0,1\}}$. $\longrightarrow$ No!

$D(y \in \{0,1\}^{n+1})$: if $y_1 \oplus \ldots \oplus y_n = y_{n+1}$: output 1
else: output 0.

$\longrightarrow \mathrm{Adv}_{H(U_n), U_{n+1}}(D) = \frac{1}{2} \neq \mathrm{negl}(n)$

References

- J. Katz, Y. Lindell. *Introduction to Modern Cryptography.* 2nd ed. CRC Press. 2015. pg.
- C. Peikert. Theory of Cryptography: Lecture 4 & 5. Lecture Notes. »
- R. Pass, A. Shelat. *A Course in Cryptography.* § 3.1. »
- Y. Kalai, N. Stephens-Davidowitz. *Cryptography & Cryptanalysis (6.875).* Lecture notes. Fall 2019.
- C. Peikert. *Advanced Cryptography (EECS 575).* Lecture notes. Fall 2020.