CS 229r: IT & CS

LECTURE 22

Today:

"Entropy in Computational Complexity"

- Statistical Difference Problem (SD)
- \( SD = \overline{SD} \)

Probability Distributions in (T)CS vs. IT:

- TCS focus: One sample from distribution on large support
- IT focus: Many samples from distribution on small support

Resulting Concepts:

- IT: \( H(X) \), KL Divergence \( D(P \parallel Q) \)
- CS: \( H_\infty(X) \); Statistical distance \( S(P, Q) \).

Definition:

\[
H_\infty(X) = \min_{w \in \Omega} \log \frac{1}{\Pr[X = w]} \quad \text{vs.} \quad H(X) = \mathbb{E}_{w \in \Omega} \left[ \log \frac{1}{\Pr[X = w]} \right]
\]

Very popular in "randomness extraction" ...

(Not today’s focus).
- \[ S(P, Q) = \frac{1}{2} \sum_{w \in \mathcal{X}} |P(w) - Q(w)| = \max \left\{ \frac{1}{2} \sum_{x \in \mathcal{X}} |P_T(x) - Q_T(x)| \right\} \]

- Since in CS: Distributions that are not very distinguishable,
  \[ S(P, Q) \to 0 \quad (\frac{1}{n^{10}}, \frac{1}{2^{2n}}, \ldots) \]

- Useful feature: \( \Delta \)-Inequality
  \[ \Delta(P, Q) + \Delta(Q, R) \geq \Delta(P, R) \]
  "Indistinguishability" is "transitive."

- Computational Indist.
  \[ S^c(P, Q) = \max_{T: \mathcal{X} \to \{0, 1\}} \sum_{x \in \mathcal{X}} \mathbb{E}_{P \times Q}[T(x) - T(y)] \]

Comparisons:
1. Pinsker: \( S(.) \) vs. \( D(\|) \)
2. \( H_{\infty}(X^n) = \infty \) for \( X^n \), \( \exists \bar{x} \approx_{o(1)} X^n \) with
   \[ H_{\infty}(\bar{x}) = n \cdot H(X) \]
Historically:

1. Prob. Encryption \( \text{[Goldwasser-Micali]} \) \( \text{Comp. Int.} \)
2. \( \text{(GMW)} \): Graph-Non-Isomorphism \( \subseteq \) \( \text{(Statistical) Zero Knowledge} \)
   \( \downarrow \) (many years later)
3. Statistical Difference is \( \text{SZK-complete} \)
4. \( \text{SD} \approx \text{SD} \) \( \leftarrow \) This is what we'll define & prove.

- Given some ideas & steps above: (include idea of definitions).

- \( \text{[GMW]} \) \( \text{GIN1} \subseteq \text{SZK} \) (TLA-galore).

Question: How can I prove to you that two \( n \)-vertex graph are not isomorphic?

**Defn:** \( G_1 = (V_1, E_1) \) \( H = (W, F) \) are isomorphic if \( \exists \text{ \Pi: } V \rightarrow W \) 1-1

\[ \forall (u,v) \in E \leftrightarrow (\Pi(u), \Pi(v)) \in F \]

- Proving isomorphism easy: I can send \( \Pi \) to you.
- Non-isomorphism? Can send all \( n! \) \( \Pi \)'s to you?
  - No good!
What else can be

Proof (Interactive, Zero Knowledge):

Verifiers (You)

Prover (me)

\( G_0 \overset{H}{=} G = G_0 = (\mathbb{G}, \mathcal{E}) \)

\( 1_t = G_{1_t} = (\mathbb{G}, \mathcal{F}) \)

\( \vdash \)

Pick \( b \in \mathbb{R}_{0,1}^2 \)

\( \Pi : \mathbb{G} \rightarrow \mathbb{G} \) unit.

Send \( \Pi (G_0) = \overline{K} \rightarrow \Phi \)

(Challenge: Guess \( b \) )

Accept if \( b = \overline{b} \).

Assertions: 0 if \( b \neq H \) I can (with \( \mathcal{O}(m^2) \) time) guess \( b \) from \( \pi K \) (isomorphic to \( G_0 \) only)

\( \Rightarrow Pr[\text{Accept}] = 1 \)

2. If \( b \neq H \) I can't do better than random guessing. Formally

\[ \sum_{K \in \mathbb{K}} b = 0 \] \[ \sum_{K \in \mathbb{K}} b = 0 \]

or equivalent \( I(K; b | G, H) = 0 \).

3. Verifier learns nothing except \( b \neq H \) (if \( 1_t \)).

"Zero Knowledge" - No formalism here!
Question: What other statement can be proved like this.

**Theorem** [SV]: SD is SZK-complete.

**Definition**: Given boolean circuit $C : \{0,1\}^m \rightarrow \{0,1\}^n$ bits with $m, |C| = \text{poly}(n)$, we say $C$ "represents" a sampleable distribution (also called $C$ supported on $\{0,1\}^n$ given by $\{ C(Y) \} Y \leftarrow \text{Unif}(2^n)$ ("circuits" are "sampleable distributions").

$SD_{C,f}^c$:

$\text{CLOSE}^c = \{ (C_1, C_2) \mid S(C_1, C_2) \leq c \}$

$\text{FAR}^f = \{ (C_1, C_2) \mid S(C_1, C_2) > s \}$

**Problem**: Given $(C_1, C_2)$ decide if $(C_1, C_2) \in \text{CLOSE}^c$ or $(C_1, C_2) \in \text{FAR}^f$.

**Claims**

1. $SD^{\frac{1}{3}, \frac{2}{3}}$ is SZK-complete. [Won't define or prove]
2. $SD^{\frac{1}{3}, \frac{2}{3}} = SD^{2^n, 1-2^{-n}}$
Hint of \[ SD^{-n_k} = 1 - 2^{-n_k} \leq \text{SZK} \]

Verifier

\[ C_0, C_1 \]

Pick \( b \in \{0, 1\} \) at random

\( Y \in \{0, 1\}^m \) at random

\[ Y = C_b(x) \]

Prover

\[ \Diamond \]

Completeness: \( S(C_0, C_1) \geq 1 - 2^{-n_k} \) \( \Rightarrow \) Prover accepted w.p. \( 1 - 2^{-n_k} \)

Soundness: \( S(C_0, C_1) \leq 2^{-n_k} \) \( \Rightarrow \) Prover accepted w.p. \( \leq \frac{1}{2} + 2^{-n_k} \)

\[ Z_k : \quad \Pr[b = \hat{b}] \geq 1 - 2^{-n_k} = 1 \]

\[ \text{So, at least one answer; no knowledge gained.} \]

Note: if \( \text{FAR} = \text{FAR}^{2/3} \) then \( \Pr[b = \hat{b} \mid \text{FAR}] \geq \frac{2}{3} \) (some knowledge could be gained)

so amplification essential
Amplifying SD:

1. \( \text{SD}_{C, f} \leq \text{SD}_{C_k, f_k} \quad \text{"XOR REDUCTION"} \)

\((C_0, C_1) \longrightarrow (C_0, C_1) \otimes (D_0, D_1) \)

\(D_i (b_1 \ldots b_{t+1}, x_1 \ldots x_t) = (C_{b_1} (x_1), \ldots, C_{b_{t+1}} (x_{t+1}), C_0 (x_t)) \)

where \( b_{t+1} = t \oplus (\bigoplus_{j=1}^{t} b_j) \)

[so mixes odd/even \# C_0's with rest C_1's]

- makes it very hard to distinguish

Exercise: \( \mathcal{S} (D_0, D_1) = \mathcal{S} (C_0, C_1) \).

2. \( \text{SD}_{C, f} \leq \text{SD}_{C', f, 1 - 2e^{-tf/2}} \)

\( \Downarrow \quad \text{"BPP amplifier"} \)

\( \Delta \)-inequality

Putting \( \odot \) (1) + (2) + (1) together

\( \Rightarrow \quad \text{SD}_{C, f} \leq \text{SD}_{2^{-n \epsilon}, 1 - 2e^{-tf/2}} \).
Main Result for next lecture:

SD ≤ SD: [Notice surprising switch]

Main Tool:

- \( ED \uparrow (C_0, C) \) (LOW, \( H_{16}H \))

\[
\text{HIGH} = (C_0, C_t) \ \text{s.t.} \quad H(C_0) \leq H(C_1) - \Delta
\]

\[
\text{LOW} = (C_0, C_i) \ \text{s.t.} \quad H(C_0) \geq H(C_i)
\]

Task: Given \( (C_0, C_i) \in \text{HIGH} \cup \text{LOW} \)
decide which.

- Main Results
  1. \( SD \leq ED \rightarrow [\text{mostly simple}] \)
  2. \( ED \leq ED \rightarrow [\text{trivial}] \)
  3. \( ED \leq SD \rightarrow [\text{next time}] \)
$SD < ED$

$\begin{align*}
(C_0, C_1) & \rightarrow (P, Q) \\
\mathcal{P} & \equiv \begin{cases} 
\mathcal{P}(x, b, s) = (C_s(x), b_s) \\
\mathcal{Q}(x, b, s) = (C_s(x), b) 
\end{cases}
\end{align*}$

if $(C_0, C_1)$ - far then $C_s(x)$ reveals $s$

so $H(P) = V + o(1) \quad V \leq \frac{H(C_0) + H(C_1)}{2}$

$H(Q) = V + 1$

if $(C_0, C_1)$ - close then $C_s(x)$ does not reveal $s$

$\Rightarrow H(P) \approx H(Q) \approx V + 1.$