CS 229r: IT ∈ CS — 4/18/2019

LECTURE 22

TODAY: "ENTROPY IN COMPUTATIONAL COMPLEXITY"

- Statistical Difference Problem (SD)
- $SD \equiv \overline{SD}$

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 $D(P \| Q)$
- CS: $H_\infty(X)$; Statistical distance $\delta(P,Q)$.

Definitions:

- $$H_\infty(X) = \min_{\omega \in \Omega} \log_2 \frac{1}{\Pr[X=\omega]} \quad \text{vs.} \quad H(X) = \mathbb{E}_{\omega \in \Omega}\left[\log \frac{1}{\Pr[X=\omega]}\right]$$

Very popular in "randomness extraction"...

(Not today's focus).

TOPS FORM 33041
LITHO IN U. S. A.

$$- \delta(P,Q) = \frac{1}{2}\sum_{\omega\in\Omega} \left|P(\omega)-Q(\omega)\right| = \max_{T:\Omega\to\{0,1\}} \left\{ \Pr_{X\sim P}[T(X)=1] - \Pr_{X\sim Q}[T(X)=1] \right\}$$

↑ max. distinguishing prob.

- Stress in CS: Distributions that are not very distinguishable

$$\delta(P,Q)\to 0 \quad \left(\frac{1}{n^{100}}, \frac{1}{2^{\sqrt{n}}}, \dots\right)$$

- Useful features: - Δ-inequality $\underbrace{\Delta(P,Q)+\Delta(Q,R)}_{}\geq \Delta(P,R)$

"indistinguishability" is "transitive".

- Computational Indist.

$$\delta^c(P,Q) = \max_{\substack{T:\Omega\to\{0,1\} \\ T \text{ efficiently computable}}} \left\{ \mathbb{E}_{X\sim P}[T(X)] - \mathbb{E}_{Y\sim Q}[T(Y)] \right\}$$

$$\delta^c(P,Q) \leq \delta(P,Q)$$

$$\delta^c(P,Q) \leq \delta^c(P,R) + \delta(R,Q) \quad \text{(as an example).}$$

Comparisons: (1) Pinsker: $\delta(\,,\,)$ vs. $D(\,\|\,)$

(2) $\cancel{H_\infty(X^n)} \geq \varepsilon$ for X^n, $\exists\, \bar{X} \approx_{o(1)} X^n$ with

$$H_\infty(\bar{X}) = n\cdot H(X).$$

Historically: 1. Prob. Encryption [Goldwasser-Micali] "Comp. Indist"

$\Downarrow$ (in a few steps)

2. [GMW]: Graph-Non-Isomorphism $\in$ "(Statistical) Zero Knowledge"

$\Downarrow$ (many years later)

3. Statistical Difference is SZK-complete

$\Downarrow$

4. $SD \approx \overline{SD}$ $\leftarrow$ This is what we'll define & prove.

- Give some idea of steps above (including idea of definitions).

- [GMW] $GNI \in SZK$ (TLA-galore).

Question: How can I prove to you that two n-vertex graphs are not isomorphic

Defn: $G = (V, E)$ $H = (W, F)$ are isomorphic

if $\exists$ $\pi : V \to W$ 1-1

s.t. $(u, v) \in E \iff (\pi(u), \pi(v)) \in F$

- Proving isomorphism easy: I can send π to you.

- Non-isomorphism? Can send all $n!$ π's to you?

No good!

~~What else can be~~

Proof (Interactive, Zero Knowledge):

Verifier (you) — Prover (me)

$G = G_0 = ([n], E)$

$H = G_1 = ([n], F)$

- Pick $b \in_R \{0,1\}$
- $\pi : [n] \to [n]$ unif.

send $\pi(G_b) = K \xrightarrow{\quad K \quad}$

(Challenge: Guess b)

$\xleftarrow{\quad \hat{b} \quad}$

Accept if $b = \hat{b}$.

Assertions: ① if $G \not\cong H$ I can (with exp(n) time) guess b from K (K isomorphic to G_b only)

$\Rightarrow \Pr[\text{accept}] = 1$

② if $G \not\cong H$ I can't do better than random guessing. formally

$$\{K \mid b=0, G, H\} \cong \{K \mid b=1, G, H\}.$$

or equiv. $I(K; b \mid G, H) = 0$.

③ Verifier learns nothing except $G \not\cong H$ (if so.).

"Zero Knowledge" - No formalism here!

Question: What other statements can be proved like this.

<u>Theorem</u> [SV]: SD is SZK-Complete.

<u>Definition</u>: Given boolean circuit $C : \{0,1\}^m \to \{0,1\}^n$ bits

with $m, |C| = \text{poly}(n)$,

we say C "represents" a <u>sampleable distribution</u>

(also called) C supported on $\{0,1\}^n$ given by $\{C(Y) \mid Y \sim \text{Unif}(\{0,1\}^m)\}$

("circuits" are "sampleable distributions")

$SD^{c,f}$:

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

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

<u>Problem</u>: Given $(C_1, C_2) \in CLOSE \cup FAR$ decide if $(C_1, C_2) \in CLOSE^c$

or $(C_1, C_2) \in FAR^f$

<u>Claims</u> (1) $SD^{1/3, 2/3}$ is SZK-Complete [won't define or prove]

(2) $SD^{1/3, 2/3} \equiv SD^{2^{-n^c}, 1-2^{-n^c}}$

Hint of $\overline{SD}^{2^{-n^\epsilon}, 1-2^{-n^\epsilon}} \in SZK$

Verifier Prover

C_0, C_1

Pick $b \in \{0,1\}$ at random

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

$$\xrightarrow{\quad Y = C_b(x) \quad}$$

$$\xleftarrow{\quad \hat{b} \quad}$$

Completeness: $\delta(C_0, C_1) \geq 1 - 2^{-n^\epsilon}$ $\Rightarrow$ Prover accepted w.p. $1 - 2^{-n^\epsilon}$

Soundness: $\delta(C_0, C_1) \leq 2^{-n^\epsilon}$ $\Rightarrow$ Prover accepted w.p. $\leq \frac{1}{2} + 2^{-n^\epsilon}$

"Z"K: $\cancel{\Pr(b, \hat{b})}$ $\Pr[b = \hat{b} \mid \underset{\text{FAR}}{\cancel{\text{CLOSE}}}] \geq 1 - 2^{-n^\epsilon} \approx 1$

So ~~verifier~~ (~~who~~ ~~at~~) gets ~~an~~ the expected answer;

No knowledge gained.

{ Note: if FAR = 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:

$\cancel{SD^{1/3,\,2/3} \leq SD^{\ldots,\,1}}$

(1) $SD^{c,f} \leq SD^{c^t,\,f^t}$ "XOR REDUCTION"

$$(C_0, C_1) \longmapsto (D_0, D_1)$$

$$D_i(b_1 .. b_{t-1}, X_1 .. X_t) = (C_{b_1}(X_1), \ldots C_{b_{t-1}}(X_{t-1}), C_{b_t}(X_t))$$

where $b_t = i \oplus \left(\bigoplus_{j=1}^{t-1} b_j \right)$

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

– makes it very hard to distinguish

Exercise: $\delta(D_0, D_1) = \delta(C_0, C_1)^t$.

(2) $SD^{c,f} \leq SD^{t\cdot c,\, \underbrace{1-2e^{-tf^2/2}}}$

$\Downarrow$ Δ-inequality

$\Downarrow$ "BPP amplification"

Putting (1) + (2) + (1) together

$\Rightarrow SD^{1/3,\,2/3} \leq SD^{2^{-n^c},\, 1-2^{-n^c}}$.

Main Result for next lecture:

$SD \leq \overline{SD}$: [Notice surprising switch]

Main tool:

- ED^{Δ}: ~~(C_0, C_1)~~ (LOW, HIGH)

  HIGH $= (C_0, C_1)$ s.t. $H(C_0) \leq H(C_1) - \Delta$

  LOW $= (C_0, C_1)$ s.t. $H(C_0) \geq H(C_1)$

  Task: Given $(C_0, C_1) \in$ HIGH $\cup$ LOW
  decide which.

- Main Results

  1. $SD \leq ED \longrightarrow$ [mostly simple]
  2. $ED \leq \overline{ED} \longrightarrow$ [trivial]
  3. $ED \leq SD \longrightarrow$ [next time]

$SD \leq ED$

$$(C_0, C_1) \longrightarrow (P, Q)$$

$$\cancel{P = (}\quad P(x,b,s) = (C_s(x), \cancel{b}\, s)$$
$$Q(x,b,s) = (C_s(x), b)$$

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

$$\text{so} \quad H(P) = v + o(1) \qquad v \triangleq \frac{H(C_0) + H(C_1)}{2}$$
$$H(Q) = v + 1$$

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

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