February 2

Tuesday, February 2, 2021 1:27 PM

Boolean Functions

1. Summary
   - Restrictions
   - Goldreich-Levin
2. Q+A
3. Problems

Announcements

- Week 2 solutions up

Restriction

$f_{J|z} : \{-1,1\}^J \to \mathbb{R}, \quad f_{J|z}(x) = f(x, z)$

(J: domain; z: fixed bits; (x, z): concatenation)

$$\hat{f}_{J|z}(S) = \sum_{T \subseteq \bar{J}} \hat{f}(S \cup T) z^T$$

$$\mathop{\mathbb{E}}_{z \sim \{-1,1\}^{\bar{J}}}[\hat{f}_{J|z}(S)] = \hat{f}(S)$$

$$\mathop{\mathbb{E}}_{z \sim \{-1,1\}^{\bar{J}}}[\hat{f}_{J|z}(S)^2] = \sum_{T \subseteq \bar{J}} \hat{f}(S \cup T)^2$$

Goldreich-Levin

Given query access to $f: \{-1,1\}^n \to \{-1,1\}$, and $\tau \in (0,1]$ in $\mathrm{poly}(n, \frac{1}{\tau})$ time, output a collection $\mathcal{L}$ of subsets $U \subseteq [n]$ s.t.

- $|\hat{f}(U)| \geq \tau \to U \in \mathcal{L}$
- $U \in \mathcal{L} \to |\hat{f}(U)| \geq \frac{\tau}{2}$

- If f is ϵ-concentrated on M coefficients, can learn f in time $\mathrm{poly}(n, M, \frac{1}{\epsilon})$

GL w/ $\tau = \sqrt{\frac{\epsilon}{4M}}$

Corollary - can learn size s decision trees in time $\mathrm{poly}(n, s, \frac{1}{\epsilon})$

↳ (truncate after depth $\log(\frac{s}{\epsilon})$)

$\geq$ degree

Goldreich-Levin

$\mathcal{S} = \{\phi\}$

For $i=1$ to n

for each $S \in \mathcal{S}$, add $S \cup \{i\} \in \mathcal{S}$

for each $S \in \mathcal{S}$, estimate $\sum_{T : T \cap [i] = S} \hat{f}(T)^2$, remove if $< \frac{\tau^2}{2}$

$$\sum_{T : T \cap [i] = S} \hat{f}(T)^2 = \mathop{\mathbb{E}}_{z \sim \{-1,1\}^{[n] \setminus [i]}}[\hat{f}_{[i]|z}(S)^2]$$

estimate.

$$\hat{f}(S) = \mathop{\mathbb{E}}_{x \sim \{0,1\}^n}[f(x) \chi_S(x)]$$

Problem 1 - Restrictions

Problem 2 - $\hat{\|} f \hat{\|}_1 = \sum |\hat{f}(S)|$

Problem 3 - Simpler than Goldreich-Levin

Problem 4 - Goldreich-Levin used for - (b) - $\widehat{A \quad |f(S)|^{(S)}}$

cryptography

Rooms	Problem
1, 5	1
2, 6	2
3, 7	3
4, 8	4