Today

Multiplicative Weight Update Method (part V)

- Hardcore set lemma
- XOR Lemma
- Wrapup

CSS.205.1 Toolkit in TCS
- Lecture # 19
(26 Apr '21)
Instructor: Prahladh Harsha

Application: Impagliazzo's Hardcore Set Lemma

Previously, proved using von-Neumann's Minimax Theorem

Today, "Constructive" proof using MWUM.

(Hardcore Set Lemma $\Rightarrow$ XOR Lemma)

Hard-core Sets:

Boolean functions: $f: \underbrace{\{0,1\}^n}_{\text{Boolean hypercube (replaced by any set } X)} \to \underbrace{\{0,1\}}_{\text{Boolean}}$

Model of computation: Circuits.
(DAG w/ internal nodes

corresponding to binary $\wedge$,
binary $\vee$ or unary NOT gates
& leaves - input variables)

Size of such circuit = # gates of the circuit.

How well does a ckt of size atmost S compute $f:\{0,1\}^n \to \{0,1\}$?

$$\delta(C,f) \triangleq \Pr_{x \leftarrow \{0,1\}^n} \left[C(x) = f(x) \right].$$

① Worst case Hardness:
$\delta(C,f) < 1$ for all ckts of size S.

② Average-case Hardness:

(a) Mildly average-case hard.

ε-weakly hard $(\varepsilon \in (0, \tfrac{1}{2}))$
against ckts of size S.

if $\forall$ ckts C of size (at most) S

$\delta(C,f) \leq 1-\varepsilon.$

(b) Strongly average-case hard

γ-strongly hard against ckt of size S $(\gamma \in (0, 1/2))$

if $\forall$ ckts C of size (at most) S

$$\delta(C, f) \le \frac{1}{2} + \gamma$$

Yao's XOR Lemma: Mildly average case hard f

$$\Downarrow$$

Strongly average-case hard f'

$f : \{0,1\}^n \to \{0,1\}$.

$f' = f^{\oplus k} : \{0,1\}^{nk} \to \{0,1\}$

$(x_1 \ldots x_k) \longmapsto f(x_1) \oplus f(x_2) \oplus \ldots \oplus f(x_k)$

Yao's XOR Lemma:

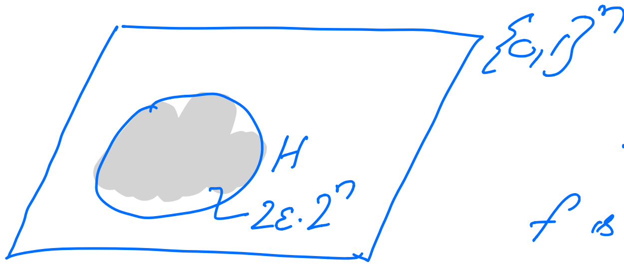
f is ε-weakly hard against ckts of size S

$$\Downarrow$$

$f^{\oplus k}$ is $\gamma + (1-\varepsilon)^k$-strongly hard against ckts of size $S' = O(\varepsilon^2 \gamma^2 S)$

Proof (due to Impagliazzo) via Hardcore Sets

Hardcore Sets



$f: \{0,1\}^n \to \{0,1\}$

f is ε-mildly hard against ckts of size S

$\forall$ ckts C of size S $\Pr_{x \leftarrow \{0,1\}^n}[f(x) = C(x)] \leq 1 - \varepsilon$

$H \subseteq \{0,1\}^n$ is γ-hardcore set for f against ckts of size S.
if $\forall$ ckts C of size S $\Pr_{x \leftarrow H}[C(x) = f(x)] \leq \frac{1}{2} + \gamma$

Obs: $H \subseteq \{0,1\}^n$. $|H| = 2\varepsilon \cdot 2^n$ is a γ-hardcore set for ckts of size S

$\Downarrow$

f is $(\varepsilon - \gamma)$-weakly hard against ckts of size S.

Hardcore set Lemma: Converse to the observation.

H - set of size $\Theta(\varepsilon)$.

H - hardcore distribution

ε-smooth distribution.

For any $\varepsilon \in (0,1)$., $\mathcal{D} \sim \{0,1\}^n$ is said to be ε-smooth

if $\forall x \in \{0,1\}^n$, $\Pr_{X \sim \mathcal{D}}[X = x] \leq \frac{1}{\varepsilon \cdot 2^n}$

eg: ε-smooth distribution.

(1) uniform dist on $\{0,1\}^n$

(2) $\left. \begin{array}{l} H \subseteq \{0,1\}^n. \quad |H| = \varepsilon \cdot 2^n \\ \mathcal{D} \text{- unif dist on } H \end{array} \right\}$ - ε-smooth
ε-flat distributi

(3) ε-smooth dist is a convex combination of ε-flat dist
(we wont use this).

(4) $\mathcal{P} = \{\mathcal{D} \mid \mathcal{D} \text{ is } \varepsilon\text{-smooth}\}$.

$\mathcal{D} : \{0,1\}^n \to [0,1]$

$\mathcal{P}$ - convex set.

Impagliazzo's Hardcore Set Lemma:

$f : \{0,1\}^n \to \{0,1\}$ is ε-weakly hard against ckts of size S then, $\forall \gamma \in (0, 1/2)$ there is a ε-smooth dist H

s.t f is γ-strongly hard against ckts of size $S' = O\left(\frac{\gamma^2 S}{\log(\frac{1}{\varepsilon})}\right)$ on H

$\forall$ (i.e, $\forall$ ckts C of size S'

$$\Pr_{x \sim H}[C(x) = f(x)] \leq \frac{1}{2} + \gamma$$

<u>Pf:</u> By contradiction

Suppose for every ε-smooth distribution H there is a ckt C of size S'

s.t $\Pr_{x \leftarrow H}[f(x) = C(x)] \geq \frac{1}{2} + \gamma$.

(Last time: weak learner against every dist

$\Downarrow$

strong learner)

Now: weak learner against ε-smooth dist

$\Downarrow$

strong learner.

<u>Catch:</u> $p^{(t)}$ - MWUM outputs must be an ε-smooth dist.)

Boosting:

1. Initialize $p^{(1)} \leftarrow$ Unif dist on $\{0,1\}^n$

2. For $t \leftarrow 1$ to T.

   (a). Construct the ckt C of size $\leq S'$ that

   $$\Pr_{x \leftarrow p^{(t)}}\left[C(x) = f(x)\right] \geq \frac{1}{2} + \gamma$$

   (b) Update

   $$\underbrace{\tilde{p}^{(t+1)}_{(x)}}_{\varepsilon\text{-smooth}} \leftarrow p^{(t)}_{(x)}\left(1 - \eta\, m_i^{(t)}(x)\right) / \Phi^{(t)}$$

   $$m_t^{(t)}(x) = 1 - |C(x) - f(x)|$$

   Project $\tilde{p}^{(t+1)}$ to $\mathcal{P}$ to obtain an ε-smooth distribution

   $$p^{(t+1)} = \min_{p \in \mathcal{P}} RE\left(\tilde{p}^{(t+1)} \| p\right).$$

MWUM (rel entropy).

$$\sum_{t=1}^{T} m^{(t)} \cdot p^{(t)} \leq (1+\eta) \sum m_i^{(t)} \cdot p + RE(p \| p^{(1)}).$$

$$\forall p \in \mathcal{P}.$$

MWUM: Majority of T ckts $C_1 \ldots C_T$ is an $(1-\varepsilon)$-approximation to f

If $T = \left\lceil \frac{2}{\varepsilon^2} \log\left(\frac{1}{\mu}\right) \right\rceil$

$$S' = O\left(\frac{\varepsilon^2 S}{\log(\frac{1}{\mu})}\right).$$

$\boxtimes$

Proof of Yao's XOR Lemma.

Suppose

$f: \{0,1\}^n \to \{0,1\}$ is ε-weakly hard against ckts of size S.

i.e., $\Pr_{x \leftarrow \{0,1\}^n} [C(x) = f(x)] \leq 1-\varepsilon$, $\forall C$ of size $\leq S$

$\Downarrow$ Hard-core Set Lemma.

$\forall \gamma \in (0, \frac{1}{2})$

$\exists$ ε-hardcore dist H on $\{0,1\}^n$ s.t.

$$\Pr_{x \leftarrow H} [C(x) = f(x)] \leq \frac{1}{2} + \gamma \quad \forall C \text{ of size } O\left(\frac{\gamma^2 S}{\log(\frac{1}{\varepsilon})}\right)$$

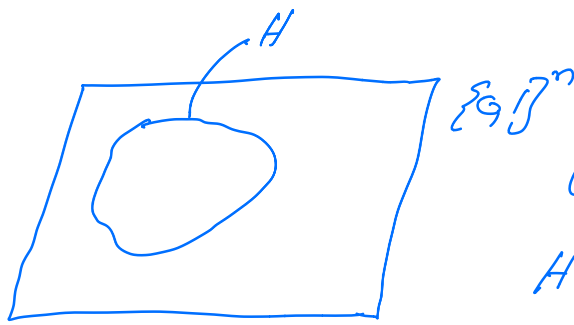
$\Downarrow$ Proof of XOR Lemma.

(Needs to be proved).

$\forall \gamma \in (0, \frac{1}{2})$.

$f^{\oplus k}: \{0,1\}^{nk} \to \{0,1\}$

$(x_1, \ldots, x_k) \mapsto \bigoplus_{i=1}^{k} f(x_i)$ is $\gamma + (1-\varepsilon)^k$-strongly hard against ckts of size $O\left(\frac{r^2 S}{\log(\frac{1}{\varepsilon})}\right)$



U_n – uniform dist on $\{0,1\}^n$

H – ε-smooth distribution

$\forall x,\quad H(x) \leq \frac{1}{\varepsilon \cdot 2^n}$

Define distribution G. on $\{0,1\}^n$

$$G(x) = \frac{\frac{1}{2^n} - \varepsilon H(x)}{1-\varepsilon} = \frac{U_n(x) - \varepsilon H(x)}{1-\varepsilon}$$

ie, $U_n(x) = \varepsilon \cdot H(x) + (1-\varepsilon)\, G(x)$.

Qns (1) $G(x) \geq 0 \quad \forall x$?
(equiv to $H(x) \leq \frac{1}{\varepsilon \cdot 2^n}$)

(2) $\sum_x G(x) = 1$.
(since $\sum H(x) = 1$ & $\sum U_n(x) = 1$)

} – distribution

Hence, G is valid distribution on $\{0,1\}^n$

$U_n(x) = \varepsilon H(x) + (1-\varepsilon)\, G(x)$, $\forall x \in \{0,1\}^n$

U – $(\varepsilon, 1-\varepsilon)$ convex combination of the 2 dist H & G.

U - can be generated as follows:

- first toss a coin $Pr[heads] = \varepsilon$
  $Pr[tails] = 1-\varepsilon$
- If coin = heads, then o/p a sample from H
- otherwise o/p a sample from G.

How well do ckts compare $f(x_1) \oplus f(x_2) \oplus \cdots \oplus f(x_k)$?

<u>$k=2$</u> :

$$\Pr_{x_1, x_2 \leftarrow U_n \times U_n} \left[C(x_1, x_2) = f(x_1) \oplus f(x_2) \right]$$

For any 2 dist D_1, D_2

$$\Pr_{x_1, x_2 \leftarrow D_1 \times D_2} \left[C(x_1, x_2) = f(x_1) \oplus f(x_2) \right] = P_{D_1, D_2}$$

Suppose for contradiction
assume $P_{U_1, U_2} \geq \frac{1}{2} + r + (1-\varepsilon)^2$

$\frac{1}{2} + r + (1-\varepsilon)^2 \leq P_{U_1, U_2}$

$U_1 = \varepsilon H_1 + (1-\varepsilon) G_1$
$U_2 = \varepsilon H_2 + (1-\varepsilon) G_2.$

$$P_{U_1,U_2} = P_{\varepsilon H_1+(1-\varepsilon)G_1,\ \varepsilon H_2+(1-\varepsilon)G_2}.$$

$$= \varepsilon^2 P_{H_1,H_2} + \varepsilon(1-\varepsilon) P_{H_1,G_2} + (1-\varepsilon)\varepsilon P_{G_1,H_2}$$

$$+ (1-\varepsilon)^2 P_{G_1,G_2}$$

$\Big\}$ U can be simulated using H & G

$$P_{G_1,G_2} \le 1$$

$$\frac{1}{2}+\gamma+(1-\varepsilon)^2 \le \varepsilon^2 P_{H_1,H_2} + \varepsilon(1-\varepsilon) P_{H_1,G_2} + P_{G_1,H_2}\varepsilon(1-\varepsilon)$$

$$+(1-\varepsilon)P_{G_1,G_2}^2$$

$$\frac{1}{2}+\gamma \le \varepsilon^2 P_{H_1,H_2} + \varepsilon(1-\varepsilon)P_{H_1,G_2} + \varepsilon(1-\varepsilon)P_{G_1,H_2}$$

At least one P_{H_1,H_2}, P_{H_1,G_2} & P_{G_1,H_2} $\ge \frac{1}{2}+\gamma$

Assume $P_{H_1,G_2} \ge \frac{1}{2}+\gamma$.

$$\frac{1}{2}+\gamma \le \Pr_{\substack{x_1\leftarrow H\\ x_2\leftarrow G}}\left[C(x_1,x_2) = f(x_1)\oplus f(x_2)\right]$$

$\exists\ x_2 \sim G$. st above is true.

Fix that x_2.

$$\frac{1}{2}+\gamma \le \Pr_{x_1 \leftarrow H}\left[C(x_1,x_2) \oplus f(x_2) = f(x_1)\right]$$

That means the ckt $C(x_1, x_2)\underbrace{\oplus f(x_2)}_{\text{constant}}$

compute f correctly on H w/p $\frac{1}{2}+\gamma$

(but this contradicts Hardcore set Lemma).

Our assumption that $C(x_1 .. x_2)$ computes $f(x_1) \oplus f(x_2)$ w/p $\geq \frac{1}{2}+\gamma+(1-\varepsilon)^2$ is false

$\boxtimes$