# Worst Case vs. Average Case Hardness

Goal: "Amplify hardness" by taking worst case hard fctn & turn it into (new) average case hard fctn.

how? by showing that if not average case hard, can solve in worst case

## Yao's XOR lemma:

- works for any hard fctn
- Intuition from predicting random coins:
  - given $\delta$-biased coin $(Pr(heads) = \delta)$
  - predict correctly with prob $1-\delta$
  - predict parity of $k$ tosses correctly with prob $\approx \frac{1}{2} + (1-2\delta)^k$

    $\rightarrow \frac{1}{2}$ as $k \rightarrow \infty$

why parity? need to guess each answer correctly

- Is solving $k$ independent copies of $f$ $k$ times harder than solving 1 problem?

maybe not:

matrix vector mult is $\Theta(n^2)$ time

matrix matrix mult is $o(n^3)$

Plan

$\delta$-hard $\Downarrow$ f wrong on some fraction $\delta$ of inputs $\Downarrow$

$\delta'(\varepsilon,\delta)$ - hardcore measure   f wrong on almost ½ in this measure

$\Downarrow$ $\Downarrow$

$2\delta'$ hard core set   f wrong on almost ½ in this special set

$\Downarrow$ $\Downarrow$

$2\delta' + (1-\delta)^k$ hardcore on all domain   $f^*$ wrong on almost ½ of all inputs

More details

nonuniform model

[will show hardness for ckts of size g   uniform model
as opposed to Turing machines with running time t ]

def $f : \{\pm1\}^n \to \{\pm1\}$ is $\delta$-hard on distribution D
for size g if for any Boolean ckt C
with $\le g$ gates   $\Pr_{x \in_D \{\pm1\}^n} [C(x) = f(x)] \le 1-\delta$

i.e. always err on $\ge \delta$ fraction

e.g. if $\delta = 2^{-n}$ then $\ge 1$ input wrong
$\delta = ½$ then no ckt does better than random guessing. (can always get $\delta = ½$ with $C \equiv 1$ or $C \equiv -1$ )

<u>Our goal</u> find (fctn, D) pair that is hard on $\approx \frac{1}{2}$ inputs according to D

Recall: $Adv_c(M) = \sum_x R_c(x) M(x)$ where $R_c(x) = +1$ if $c(x) = f(x)$, $-1$ if $c(x) \neq f(x)$

$|M| = \sum_x M(x)$
$\mu(M) = |M|/2^m$

<u>def</u>. M measure
if $Adv_c(M) < \varepsilon |M|$ (ie. $\Pr_{x \in D_M}[C(x) = f(x)] \leq \frac{1}{2} + \frac{\varepsilon}{2}$)
$\forall$ ckts c of size $\leq g$
then f is $\varepsilon$-hard core on M for size g } Hardcore measure

If M is characteristic fctn of a set: $\Leftarrow$ special case when M is uniform on a set S

<u>def'</u> S set
f is $\varepsilon$-hard core on S for size g if
$\forall$ ckts c of size $\leq g$ $\Pr_{x \in_u S}[C(x) = f(x)] \leq \frac{1}{2} + \frac{\varepsilon}{2}$

$D_M = U_S$

Will show:
$\forall$ worst case hard f, $\exists$ h.c. set on $S = \{\pm 1\}^n$

"Hard fctns have hard core measures"

Thm let f be $\delta$-hard $\leftarrow$ wrong some of the time for size g on uniform dist } weakly ave case hard
let $1 > \varepsilon > 0$
then $\exists$ M st. $\mu(M) \geq \delta$ st.
f is $\varepsilon$-h.c. on M for size $g' = \underbrace{\frac{1}{4}}_{\text{a bit smaller than } g} \varepsilon^2 \delta^2 g$ } ave case hard

wrong almost $\frac{1}{2}$ the time!

Pf.

follow boosting outline:

if not $\Rightarrow \forall M$ s.t. $\mu(M) \geq \delta$, $f$ not $\varepsilon$-h.c. for $g'$

$\Rightarrow \exists$ "weak learner" i.e. ckt with $\underbrace{\text{advantage}}_{\text{predicts } \geq \frac{1}{2} + \frac{\varepsilon}{2}}$ $\varepsilon|M|$

+ size $\leq g'$ on all $M$ s.t. $\mu(M) \geq \delta$

$\Rightarrow \underbrace{\text{Maj of } \frac{1}{\varepsilon^2\delta^2} \text{ ckts of size } g'}_{\text{total size } \leq \frac{1}{\varepsilon^2\delta^2} \cdot g' < g}$ predicts with error $\geq 1-\delta$

$\Rightarrow f$ not $\delta$-hard for size $g$ ∎

Can also get "hard fctns have hard core sets"

Thm $M$ is $\varepsilon$-h.c. measure for size $2n < g' < \frac{\varepsilon^2\delta^2}{8} \frac{2^n}{n}$

then $\exists$ $2\varepsilon$-h.c. set $S$ for $f$ (lose factor of 2)

for size $\underbrace{g'}_{\text{lose nothing}}$ with $|S| \geq \delta 2^n$

Pf # ckts of size $g' \ll \frac{1}{4} e^{2^n \cdot \varepsilon^2\delta^2}$

Pick $S$ randomly according to $D_M$

Show $\Pr[$any $C$ of size $g'$ has $2\varepsilon|M|$ advantage$]$ small via Chernoff + union bnd ∎

twice expectation, but it's sum of lots of independent r.v.'s with expectation near $1/2 + \varepsilon/2$

lots $\approx \delta 2^n$

## Yao's XOR Lemma

(hard core set $\Rightarrow$ hard to predict on all domain but we change the fctn)

given $f$

$f^{\oplus k}(x_1 \ldots x_k) = f(x_1) \oplus f(x_2) \oplus \ldots \oplus f(x_k)$

$f$ is $\varepsilon$-h.c. for some set $H$ of size $\geq \delta 2^n$ for size $g+1$

$\Rightarrow$ $f^{\oplus k}$ is $\underbrace{\varepsilon + 2(1-\delta)^k}_{\text{lose a bit here}}$ -h.c. for size $g$

### Proof

assume ckt $C$ s.t. $\leq g$ gates

$+$ $\Pr_{x_1 \ldots x_k}[C(x_1 \ldots x_k) = f^{\oplus k}(x_1 \ldots x_k)] \geq \frac{1}{2} + \frac{\varepsilon}{2} + (1-\delta)^k$

Plan: $\forall H$ s.t. $|H| \geq \delta 2^n$ will get ckt $C'$ s.t. $|C'| \leq g+1$ which guesses $f$ with prob $\geq \frac{1}{2} + \underbrace{\frac{\varepsilon}{2}}_{\text{so not } \varepsilon\text{-h.c.}}$ on $H$

Realizing the plan:

Construction of $C'$:

get assumption in nicer form

$A_m \equiv$ event that exactly $m$ of $x_1 \ldots x_k$ in $H$

$\Pr_{x_1 \ldots x_k}[A_0] \leq (1-\delta)^k$ (all easy - can't be too likely)

so $\Pr_{x_1 \ldots x_k}[C(x_1 \ldots x_k) = f^{\oplus k}(x_1 \ldots x_k) \mid \cup A_m \text{ for } m > 0] \geq \frac{1}{2} + \frac{\varepsilon}{2}$

+ by averaging

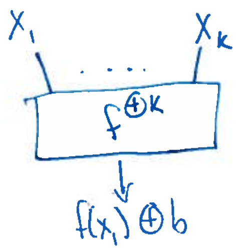
$\exists$ $1 \leq i \leq k$ s.t. $\Pr_{x_1 \ldots x_k}[C(x_1 \ldots x_k) = f^{\oplus k}(x_1 \ldots x_k) \mid A_i] \geq \frac{1}{2} + \frac{\varepsilon}{2}$ $*$

A plan that doesn't work:

Assume $f^{\oplus k}$ not $\varepsilon + 2(1-\delta)^k - hc$ for size $g$

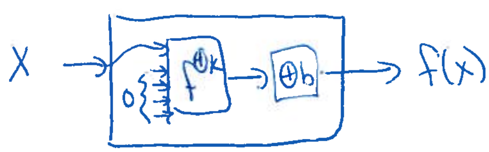
give ckt for $f$ with size $g+1$

idea



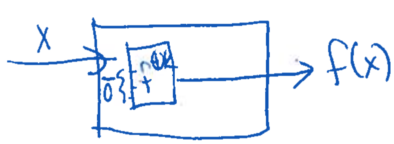

hardwire $x_2 = \dots = x_k = \bar{0}$ — or any arbitrary input

answer to $\bigoplus_{i=2}^{k} f(x_i) = b \in \{0,1\}$ — 2 options

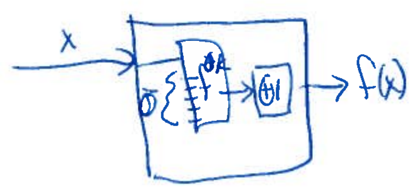



ckt for $f$.

we don't know $b$, but one of these should work:




or




What is the problem?

- $f^{\oplus k}$ might be really bad when $x_2 = x_3 = \dots = x_k = \bar{0}$, or when all $x_i$'s $\notin H$, or other crazy fctns.
- to get contradiction, need to show new ckt does well for $f$ on $H$

Think of this as constructing many many ckts, but we prove that at least one will work

Idealized ckt: (for $x$ drawn from uniform dist on $H$)

given $x \in H$ compute $f(x)$ as:

1. pick $x_1 \cdots x_{m-1} \in_R H$
2. pick $y_{m+1} \cdots y_k \in_R \bar{H}$
3. randomly permute $(x_1, \cdots, x_{m-1}, x, y_{m+1}, \cdots, y_k)$ via random permutation $\pi$

but

$$\Pr_{x_1 \cdots x_{m-1} x\, y_{m+1} \cdots y_k, \pi} \left[ C(\pi(x_i\text{'s}, x\, y_i\text{'s})) = f^{\oplus k}(\pi(x_i\text{'s}, x, y_i\text{'s})) \right]$$

$$\geq \frac{1}{2} + \frac{\varepsilon}{2}$$

(exact same probability stmt as in $*$)

by averaging,

$\exists$ choice of $x_1 \cdots x_{m-1}, y_{m+1}, \cdots y_k, \pi$

s.t. $\Pr_x \left[ C(\pi(x_i\text{'s}, x, y_i\text{'s})) = f^{\oplus k}(\pi(x_i\text{'s}, x, y_i\text{'s})) \right] \geq \frac{1}{2} + \frac{\varepsilon}{2}$

$= f(x) \oplus \underbrace{\bigoplus_i f(x_i) \oplus \bigoplus_i f(y_i)}$

Known bit, same $\forall x$ so can hardcode the bit $b$ and $x_i$'s, $y_i$'s, $\pi$ into ckt + compute $f(x)$ from $C(\pi(x_i\text{'s}, x, y_i\text{'s})) \oplus b$ (correct for same #'s)

each choice of $i$, $x_j$'s, $y_j$'s, $\pi$, bit $b$ gives ckt of size $\leq g$

at least one of them is good

Call it $\tilde{C}$

Real Ckt:

$\tilde{C}$ s.t. $i$, $x_j$'s, $y_j$'s, $\underbrace{\bigoplus_j f(x_j) \oplus \bigoplus_j f(y_j)}_{b}$, $\pi$ encoded into advice

given $x \in H$

use $\tilde{C}$ on $x$ to get $w$ $\Big\}$ size $= |\tilde{C}| + 1$

output $w \oplus b$

$$\Pr_x[\, f(x) = w \oplus b \,] \geq \frac{1}{2} + \frac{\varepsilon}{2}$$

size of ckt $\leq g + 1$

so $f$ is not $\varepsilon$-h.c. for $g+1$

$\rightarrow\leftarrow$ ∎