Hardness amplification proofs require majority

Emanuele Viola
Columbia University
Work done at Harvard, IAS, and Columbia

Joint work with

Ronen Shaltiel
University of Haifa

January 2008
Circuit lower bounds

• Major goal of computational complexity theory

• Success with constant-depth circuits (1980’s)
  [Furst Saxe Sipser, Ajtai, Yao, Hastad, Razborov, Smolensky,…]

• Theorem [Razborov ’87] Majority not in $\text{AC}^0[\oplus]$
  Majority($x_1,…,x_n$) := 1 ⇔ $\sum x_i > n/2$

$\text{AC}^0[\oplus] = \begin{array}{c}
\oplus \\
\land \land \land \land \oplus \land \\
\lor \lor \lor \lor \lor \lor \\
\text{input}
\end{array}$

$\oplus = \text{parity}$
$\lor = \text{or}$
$\land = \text{and}$
Natural proofs barrier

• Lack of progress for general circuit models

• Theorem [Razborov Rudich] + [Naor Reingold]: Standard techniques cannot prove lower bounds for circuits that can compute Majority

• We have lower bounds for $\text{AC}^0[\oplus]$ because Majority not in $\text{AC}^0[\oplus]$
Average-case hardness

- Particularly important kind of lower bound

- Def.: \( f : \{0,1\}^n \rightarrow \{0,1\} \) is \( \delta \)-hard for class \( \mathcal{C} \) if every \( C \in \mathcal{C} \) : \( \Pr_x[f(x) \neq C(x)] \geq \delta \) \((\delta \in [0,1/2])\)

- E.g. \( \mathcal{C} = \) general circuits of size \( n^{\log n} \), \( AC^0[\oplus] \), …

- Strong average-case hardness: \( \delta = 1/2 - 1/n^{\omega(1)} \)
  Need for cryptography, pseudorandom generators

[∗Nisan Wigderson,…∗]
Hardness amplification

- \( \delta \)-hard \( f \) for \( C \)
- Hardness amplification against \( C \)
- \( \delta \)-hard \( \Rightarrow (1/2 - 1/n^{\omega(1)}) \)-hard (\( t = \text{poly}(n/\delta) \))

Major line of research (1982 – present)
[Y, GL, L, BF, BFL, BFNW, I, GNW, FL, IW, IW, CPS, STV, TV, SU, T, O, V, T, HVV, SU, GK, IJK, IJKW, …]

Yao XOR lemma: \( \text{Enc}(f)(x_1, \ldots, x_t) := f(x_1) \oplus \cdots \oplus f(x_t) \) 
\( \delta \)-hard \( \Rightarrow (1/2 - 1/n^{\omega(1)}) \)-hard against \( C = \text{general circuits} \)
The problem we study

• Known hardness amplifications fail against any class $\mathcal{C}$ for which have lower bounds

• Have $f \not\in \text{AC}^0[\oplus]$. Open $f : (1/2-1/n)$-hard for $\text{AC}^0[\oplus]$?

• Motivation: pseudorandom generators [Nisan Wigderson, …] lower bounds [Hajnal Maass Pudlak Szegedy Turan, …], per se

• Conj. [V ‘04]: Black-box hardness amplification against class $\mathcal{C}$ requires Majority $\in \mathcal{C}$
Our results

• Theorem[This work] Black-box hardness amplification against class $\mathcal{C}$ requires Majority $\in \mathcal{C}$

• No black-box hardness amplification against $\text{AC}^0[\oplus]$ because Majority not in $\text{AC}^0[\oplus]$

• Black-box amplification to $(1/2-\varepsilon)$-hard requires $\mathcal{C}$ to compute majority on $1/\varepsilon$ bits – tight
Our results + [Razborov Rudich] + [Naor Reingold]

“Lose-lose” reach of standard techniques:

Majority

Cannot prove hardness amplification [this work]

Cannot prove lower bounds [RR] + [NR]

“You can only amplify the hardness you don’t know”
Outline

• Overview

• Formal statement of our results

• Significance of our results

• Proof
Black-box hardness amplification

- **Def.** Black-box $\delta \rightarrow (1/2-\epsilon)$ hardness amplification against $C$

  \[ f : \{0,1\}^k \rightarrow \{0,1\} \xrightarrow{Enc} \text{Enc}(f) : \{0,1\}^n \rightarrow \{0,1\} \]

  For every $f$, $h : \Pr_y[\text{Enc}(f)(y) \neq h(y)] < 1/2-\epsilon$
  
  there is oracle circuit $C \in C : \Pr_x[f(x) \neq C^h(x)] < \delta$

- **Rationale:** $f$ $\delta$-hard $\Rightarrow$ $\text{Enc}(f)$ $(1/2-\epsilon)$-hard
  
  ($f$ $\delta$-hard for $C$ if $\forall C \in C : \Pr_x[f(x) \neq C(x)] \geq \delta$)

- **Captures most techniques.**
  
  Note: $\text{Enc}$ is arbitrary. Caveat: $C$ non-adaptive
The local list-decoding view

[Sudan Trevisan Vadhan ’99]

\[
f = \begin{array}{cccccccccccc}
0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & \ldots & 1
\end{array}
\]

\[
\text{Enc}(f) = \begin{array}{cccccccccccccccccccc}
0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & \ldots & 0
\end{array}
\]

\[
h = \begin{array}{cccccccccccccccccccc}
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & \ldots & 0
\end{array}
\]

(1/2–ε errors)

\[
C^h(x) = f(x) \quad \text{(for 1-δ x’s)}
\]

q queries
Our results

• **Theorem** [this work]: Black-box
  \( \delta \rightarrow (1/2-\varepsilon) \) hardness amplification against \( C \Rightarrow \)
  
  (1) \( C \in C \) computes majority on \( 1/\varepsilon \) bits
  
  (2) \( C \in C \) makes \( q \geq \log(1/\delta)/\varepsilon^2 \) oracle queries

• Both tight
  
  (1) [Impagliazzo, Goldwasser Gutfreund Healy Kaufman Rothblum]
  
  (2) [Impagliazzo, Klivans Servedio]
Outline

• Overview

• Formal statement of our results

• Significance of our results

• Proof
Our results somewhat explain

- Lack of hardness vs. randomness tradeoffs [Nisan Wigderson] for constant-depth circuits

- Lack of strongly average-case lower bound for $\text{AC}^0[\oplus]$, perceptrons ($\text{Maj-AC}^0$),…

despite known lower bounds

- Loss in circuit size: $\delta$-hard for size $s$
  $\Rightarrow (1/2-\varepsilon)$-hard for size $s \cdot \varepsilon^2 / \log(1/\delta)$
Direct product vs. Yao’s XOR

- Yao XOR lemma:
  \[ \text{Enc}(f)(x_1, \ldots, x_t) := f(x_1) \oplus \cdots \oplus f(x_t) \in \{0,1\} \]

- Direct product lemma (non-Boolean)
  \[ \text{Enc}(f)(x_1, \ldots, x_t) := f(x_1) \circ \cdots \circ f(x_t) \in \{0,1\}^t \]

- Direct product \(\Leftrightarrow\) Yao XOR [Goldreich Levin]

- Yao XOR requires majority [this work]
  direct product does not [folklore, Impagliazzo Jaiswal Kabanets Wigderson]
Outline

• Overview

• Formal statement of our results

• Significance of our results

• Proof
Proof

• Recall Theorem: Black-box
  \( \delta \rightarrow (1/2-\varepsilon) \) hardness amplification against \( C \Rightarrow \)

(1) \( C \in C \) computes majority on \( 1/\varepsilon \) bits
(2) \( C \in C \) makes \( q \geq \log(1/\delta)/\varepsilon^2 \) oracle queries

• We show hypot. \( \Rightarrow C \in C : \) tells Noise \( 1/2 \) from \( 1/2 - \varepsilon \)

\[ \text{(D)} \mid \Pr[C(N_{1/2}, \ldots, N_{1/2})=1] - \Pr[C(N_{1/2-\varepsilon}, \ldots, N_{1/2-\varepsilon})=1] \mid > 0.1 \]

• (1) \( \Leftarrow \text{(D)} \) [Sudan]
  (2) \( \Leftarrow \text{(D)} + \text{tightness of Chernoff bound} \)
Warm-up: uniform reduction

• Want: non-uniform reductions (∀ f, h ∃ C)

For every f, h : Pr_y[Enc(f)(y) ≠ h(y)] < 1/2-ε
there is circuit C ∈ C : Pr_x[f(x) ≠ C^h(x)] < δ

• Warm-up: uniform reductions (∃ C ∀ f, h)

There is circuit C ∈ C :

For every f, h : Pr_y[Enc(f)(y) ≠ h(y)] < 1/2-ε
Pr_x[f(x) ≠ C^h(x)] < δ
Proof in uniform case

• Let $F : \{0,1\}^k \rightarrow \{0,1\}$, $X \in \{0,1\}^k$ be random
  Consider $C(X)$ with oracle access to $\text{Enc}(F)(y) \oplus H(y)$

  $H(y) \sim N_{1/2} \Rightarrow C^{\text{Enc}(F)} \oplus H(X) = C^H(X) \neq F(X)$ w.h.p.
  C has no information about $F$

  $H(y) \sim N_{1/2-\varepsilon} \Rightarrow C^{\text{Enc}(F)} \oplus H(X) = F(X)$ w.h.p.
  $\text{Enc}(F) \oplus H$ is $(1/2-\varepsilon)$-close to $\text{Enc}(F)$

• To tell $z \sim \text{Noise } 1/2$ from $z \sim \text{Noise } 1/2 - \varepsilon$, $|z| = q$
  Run $C(X)$; answer i-th query $y_i$ with $\text{Enc}(F)(y_i) \oplus z_i$

Q.e.d.
Proof outline in non-uniform case

- **Non-uniform**: \( C \) depends on \( F \) and \( H \) (\( \forall f,h \exists C \))

- New proof technique
  1) Fix \( C \) to \( C' \) that works for many \( f,h \)
     
     Condition \( F' := F | C' \), \( H' := H | C' \)

  2) **Information-theoretic lemma**
     \[ \text{Enc}(F') \oplus H' (y_1, \ldots, y_q) \approx \text{Enc}(F) \oplus H (y_1, \ldots, y_q) \]
     If all \( y_i \in \text{good set } G \subseteq \{0,1\}^n \)
     Can argue as for uniform case if all \( y_i \in G \)

  3) Deal with queries \( y_i \) not in \( G \)
Fixing $C$

- Choose $F : \{0,1\}^k \rightarrow \{0,1\}$ uniform, $H(x) \sim N_{1/2-\varepsilon}$

- $Enc(F) \oplus H$ is $(1/2-\varepsilon)$-close to $Enc(F)$. We have $(\forall f, h \exists C)$
  With probability 1 over $F, H$ there is $C \in C$ :

  $$\Pr_x[C^{Enc(F) \oplus H}(X) \neq F(X)] < \delta$$

- $\Rightarrow$ there is $C' \in C$ : with probability $1/|C|$ over $F, H$
  $$\Pr_x[C'^{Enc(F) \oplus H}(X) \neq F(X)] < \delta$$

- Note: $C =$ all circuits of size $\text{poly}(k)$, $1/|C| = 2^{-\text{poly}(k)}$
The information-theoretic lemma

**Lemma**
Let $V_1, ..., V_t$ i.i.d., $V_1', ..., V_t' := V_1, ..., V_t$ | E

$E$ noticeable $\Rightarrow$ there is large good set $G \subseteq [t]$:
for every $i_1, ..., i_q \in G$ : $(V'_{i_1}, ..., V'_{i_q}) \approx (V_{i_1}, ..., V_{i_q})$

**Proof:** $E$ noticeable $\Rightarrow H(V_1', ..., V_t')$ large
$\Rightarrow H(V'_{i} | V'_{1}, ..., V'_{i-1})$ large for many $i \in G$

$\text{Closeness}[(V_{i_1}, ..., V_{i_q}),(V'_{i_1}, ..., V'_{i_q})] \geq H(V'_{i_1}, ..., V'_{i_q})$
$\geq H(V'_{i_q} | V'_{1}, ..., V'_{i_q-1}) + ... + H(V'_{i_1} | V'_{1}, ..., V'_{i_1-1})$ large

Q.e.d.

**Similar to** [Edmonds Rudich Impagliazzo Sgall, Raz]
Applying the lemma

• $V_x = H(x) \sim \text{Noise } 1/2-\epsilon$

• $E := \{ H : \Pr_X[C' \operatorname{Enc}(F) \oplus H(X) \neq F(X)] < \delta \}, \quad \Pr[E] \geq 1/|C|$

\[
H' = H | E = \begin{array}{l}
0 \ 1 \ 1 \ 1 \ 0 \ 1 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 0 \ 0 \ 1 \ 0 \ 1 \ 1 \ 0 \ 
\end{array}
\]

• All queries in $G \Rightarrow$ proof for uniform case goes thru
Handling bad queries

- Problem: \( C(x) \) may query bad \( y \in \{0,1\}^n \) not in \( G \)

- Idea: Fix bad query. Queries either in \( G \) or fixed \( \Rightarrow \) proof for uniform case goes thru

- Delicate argument:

  Fixing bad query \( H(y) \) creates new bad queries  

  Instead fix heavy queries: asked by \( C(x) \) for many \( x \)'s

  OK because new bad queries are light, affect few \( x \)'s
Conclusion

- **Theorem** [This work] Black-box hardness amplification against class $\mathbb{C}$ requires Majority $\in \mathbb{C}$

- Reach of standard techniques in circuit complexity
  [This work] + [Razborov Rudich], [Naor Reingold]
  “Can amplify hardness $\iff$ cannot prove lower bound”

- **New proof technique** to handle non-uniform reductions

- **Open problems**
  
  Adaptivity? (Cover [Sudan Trevisan Vadhan], [Goldreich Levin])
  1/3-pseudorandom from 1/3-hard requires majority?