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

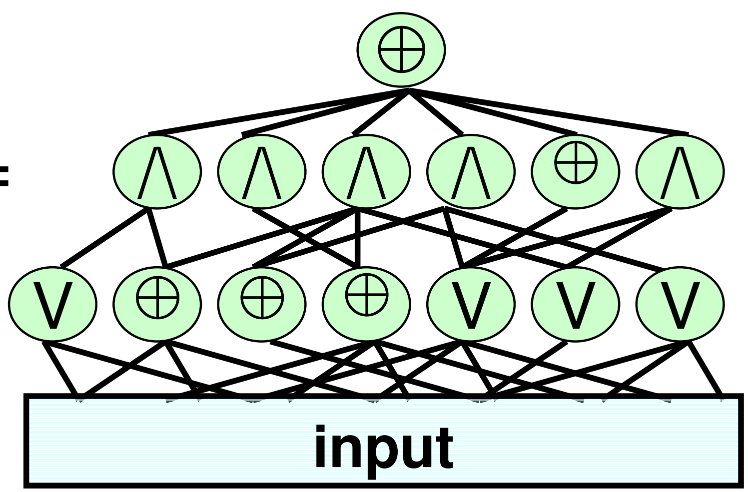
Circuit lower bounds

- 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 $AC^0[\oplus]$

  $\text{Majority}(x_1,\ldots,x_n) := 1 \Leftrightarrow \sum x_i > n/2$

$AC^0[\oplus] =$



$\oplus$ = parity

$\vee$ = or

$\wedge$ = 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 $AC^0[\oplus]$ because Majority not in $AC^0[\oplus]$

Average-case hardness

- Particularly important kind of lower bound

- Def.: $f : \{0,1\}^n \to \{0,1\}$ δ-hard for class **C** if
  every $C \in$ **C** : $\Pr_x[f(x) \neq C(x)] \geq \delta$ $\quad (\delta \in [0,1/2])$

- E.g. **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

- δ-hard f for **C** → Hardness amplification against **C** → Enc(f) $(1/2-\varepsilon)$-hard for **C**

- 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: $\mathrm{Enc}(f)(x_1,\ldots,x_t) := f(x_1) \oplus \cdots \oplus f(x_t)$
δ-hard $\Rightarrow (1/2 - 1/n^{\omega(1)})$-hard $\quad (t = \mathrm{poly}(n/\delta))$
against **C** = general circuits

The problem we study

- Known hardness amplifications fail
  against any class **C** for which have lower bounds

- Have f $\not\in$ AC$^0[\oplus]$. Open f : (1/2-1/n)-hard for 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 **C** requires Majority $\in$ **C**

Our results

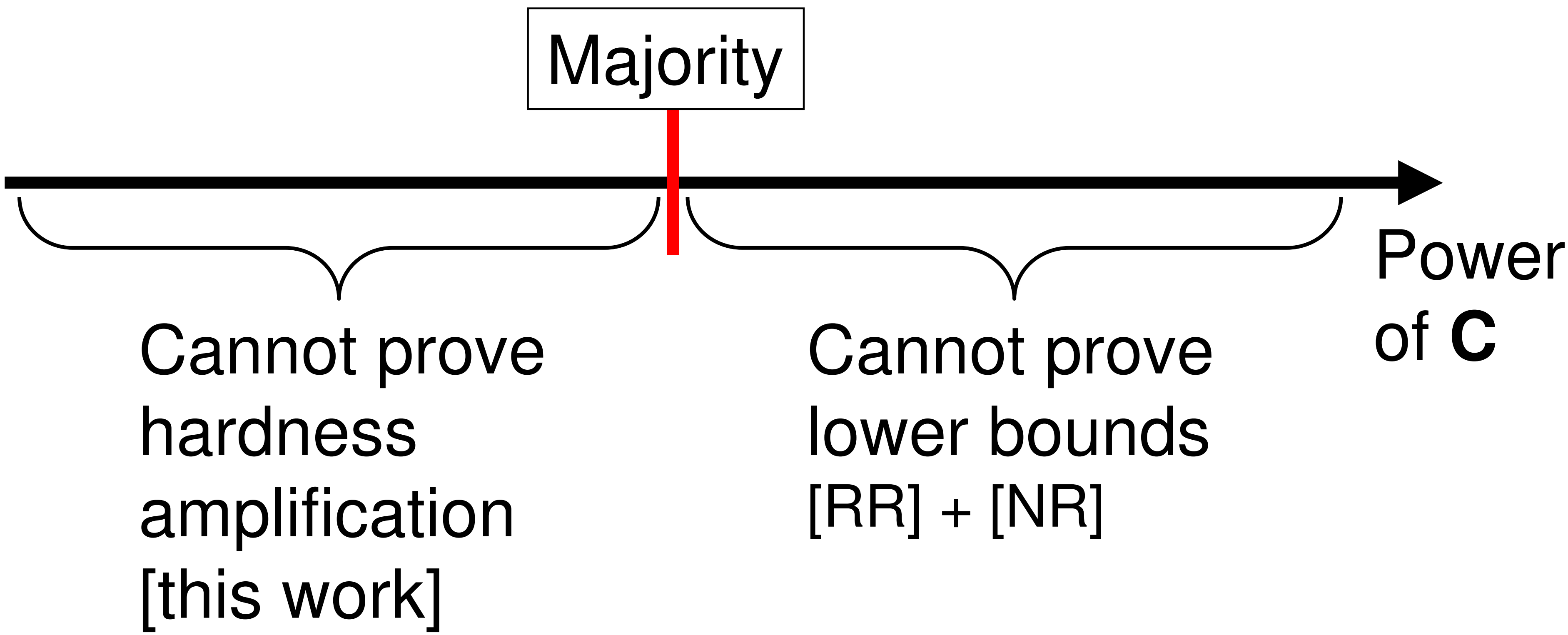
- Theorem[This work] Black-box hardness amplification against class **C** requires Majority $\in$ **C**

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

- Black-box amplification to (1/2-ε)-hard requires **C** to compute majority on 1/ε bits – tight

Our results + [Razborov Rudich] + [Naor Reingold]

"Lose-lose" reach of standard techniques:



"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 $\delta \to (1/2-\varepsilon)$ hardness amplific. against **C**

$f : \{0,1\}^k \to \{0,1\}$ $\longrightarrow$ $\boxed{\textbf{Enc}}$ $\longrightarrow$ $\mathrm{Enc}(f) : \{0,1\}^n \to \{0,1\}$

$$\boxed{\begin{array}{l}\text{For every } f,\ h : \Pr_y[\mathrm{Enc}(f)(y) \neq h(y)] < 1/2-\varepsilon \\ \text{there is oracle circuit } C \in \mathbf{C} : \Pr_x[f(x) \neq C^h(x)] < \delta\end{array}}$$

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

- Captures most techniques.
Note: Enc is arbitrary. Caveat: C non-adaptive

The local list-decoding view

[Sudan Trevisan Vadhan ’99]

f = | 0 1 0 1 0 1 0 1 0 1 0 ⋯ 1 |

Enc(f) = | 0 1 1 1 0 1 0 0 1 0 1 1 0 0 0 1 0 1 1 0 ⋯ 0 |

h = | 0 0 0 0 0 1 1 0 1 1 1 1 1 0 0 0 1 0 1 0 ⋯ 0 |

(1/2–ε errors)

q queries

$C^h(x) = f(x)$ (for 1-δ x’s)

Our results

- Theorem[this work]: Black-box
  $\delta \to (1/2-\varepsilon)$ 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 $AC^0[\oplus]$, perceptrons (Maj-AC^0),…

  despite known lower bounds

- Loss in circuit size: δ-hard for size s

  $\Rightarrow$ (1/2-ε)-hard for size $s \cdot \varepsilon^2 / \log(1/\delta)$

Direct product vs. Yao's XOR

- Yao XOR lemma:

  $\mathrm{Enc}(f)(x_1,\ldots,x_t) := f(x_1) \oplus \cdots \oplus f(x_t) \in \{0,1\}$

- Direct product lemma (non-Boolean)

  $\mathrm{Enc}(f)(x_1,\ldots,x_t) := f(x_1) \circ \cdots \circ f(x_t) \in \{0,1\}^t$

- 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
  $\delta \to (1/2\text{-}\varepsilon)$ 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 $1/2 - \varepsilon$

$$\text{(D)} \; \left| \Pr[C(\underbrace{N_{1/2},\ldots,N_{1/2}}_{q})=1] - \Pr[C(\underbrace{N_{1/2\text{-}\varepsilon},\ldots,N_{1/2\text{-}\varepsilon}}_{q})=1] \right| > 0.1$$

- (1) $\Leftarrow$ (D) [Sudan]

  (2) $\Leftarrow$ (D) + tigthness of Chernoff bound

Warm-up: uniform reduction

- Want: non-uniform reductions ($\forall$ f,h $\exists$ C)

For every f ,h : $Pr_y[Enc(f)(y) \neq h(y)] < 1/2-\varepsilon$

there is circuit $C \in \mathbf{C}$: $Pr_x[f(x) \neq C^h(x)] < \delta$

- Warm-up: uniform reductions ($\exists$ C $\forall$ f,h)

There is circuit $C \in \mathbf{C}$:

For every f, h : $Pr_y[Enc(f)(y) \neq h(y)] < 1/2-\varepsilon$

$Pr_x[f(x) \neq C^h(x)] < \delta$

Proof in uniform case

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

  $H(y) \sim N_{1/2} \Rightarrow C^{Enc(F) \oplus H}(X) = C^H(X) \neq F(X)$ w.h.p.

  C has no information about F

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

  $Enc(F) \oplus H$ is $(1/2-\varepsilon)$-close to $Enc(F)$

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

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
   $\mathrm{Enc}(F')\oplus H'\ (y_1,\ldots,y_q) \approx \mathrm{Enc}(F)\oplus H\ (y_1,\ldots,y_q)$
   If all $y_i \in$ 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 $F : \{0,1\}^k \to \{0,1\}$ 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 $C \in \mathbf{C}$:

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

- $\Rightarrow$ there is $C' \in \mathbf{C}$: with probability $1/|\mathbf{C}|$ over F,H

$$\Pr_X\left[C'^{\,Enc(F)\oplus H}(X) \neq F(X)\right] < \delta$$

- Note: $\mathbf{C}$ = all circuits of size poly(k), $1/|\mathbf{C}| = 2^{-poly(k)}$

The information-theoretic lemma

- **Lemma**
  Let $V_1,\ldots,V_t$ i.i.d., $V_1',\ldots,V_t' := V_1,\ldots,V_t \mid E$
  E noticeable $\Rightarrow$ there is large good set $G \subseteq [t]$:
  for every $i_1,\ldots,i_q \in G$: $(V'_{i_1},\ldots,V'_{i_q}) \approx (V_{i_1},\ldots,V_{i_q})$

- Proof: E noticeable $\Rightarrow H(V_1',\ldots,V_t')$ large
  $\Rightarrow H(V'_i \mid V'_1,\ldots,V'_{i-1})$ large for many i ($\in G$)

  Closeness$[(V_{i_1},\ldots,V_{i_q}),(V'_{i_1},\ldots,V'_{i_q})] \geq H(V'_{i_1},\ldots,V'_{i_q})$
  $\geq H(V'_{i_q} \mid V'_1,\ldots,V'_{i_q-1}) + \ldots + H(V'_{i_1} \mid V'_1,\ldots,V'_{i_1-1})$ large

  Q.e.d.

- Similar to [Edmonds Rudich Impagliazzo Sgall, Raz]

Applying the lemma

- $V_x = H(x) \sim$ Noise $1/2-\varepsilon$

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

$H' = H \mid E =$ 0 1 1 1 0 1 0 0 1 0 1 1 0 0 0 1 0 1 1 0 $\cdots$ 0

q queries **G**

$C'^{\,Enc(F')\oplus H'}(x) \approx C'^{\,Enc(F)\oplus H}(x)$

- 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 **C** requires Majority $\in$ **C**

- Reach of standard techniques in circuit complexity
  [This work] + [Razborov Rudich], [Naor Reingold]
  "Can amplify hardness $\Leftrightarrow$ 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?