# Hardness amplification proofs require majority


Emanuele Viola

Columbia University

Work also done at Harvard and IAS

Joint work with

Ronen Shaltiel

University of Haifa


May 2008

# Circuit lower bounds

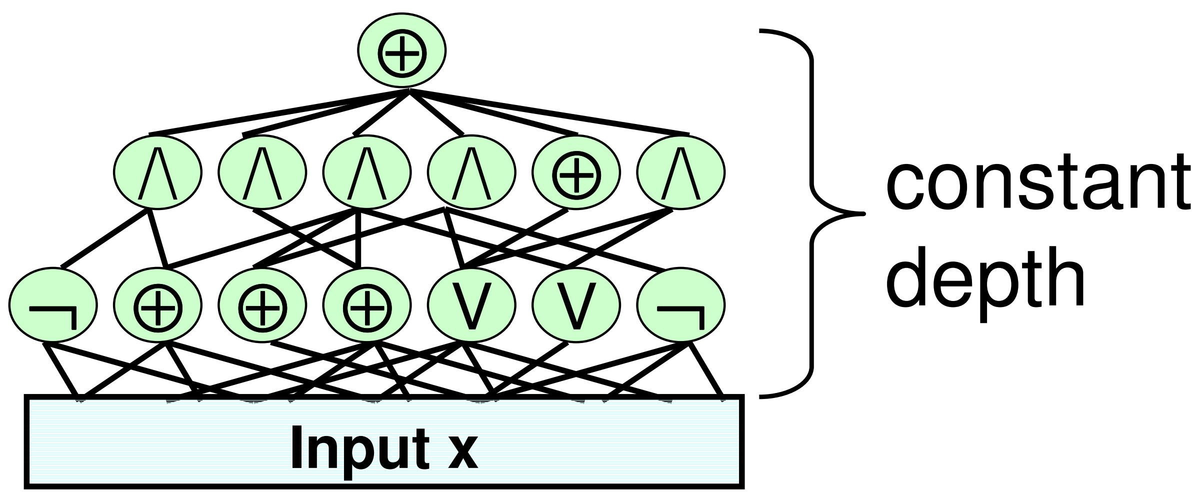
- Success with restricted circuits

  [Furst Saxe Sipser, Ajtai, Yao, Hastad, Razborov, Smolensky,…]

- Theorem[Razborov '87] Majority $\notin$ $AC^0[\oplus]$

  Majority(x) = 1 $\Leftrightarrow \sum x_i > |x|/2$

$AC^0[\oplus]$ =




$\oplus$ = parity

$\vee$ = or

$\wedge$ = and

$\neg$ = not

# Natural proofs barrier

- Little progress for general circuit models

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

- " We have lower bounds for $AC^0[\oplus]$
  because Majority $\notin AC^0[\oplus]$ "

# Average-case hardness

- Definition: $f : \{0,1\}^n \to \{0,1\}$ $(1/2 - \varepsilon)$-hard for class **C** :
  for every $M \in$ **C** : $\Pr_x[f(x) \neq M(x)] \geq 1/2 - \varepsilon$

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

- Strong average-case hardness: $1/2 - \varepsilon = 1/2 - 1/n^{\omega(1)}$
  Need for cryptography
  pseudorandom generators [Nisan Wigderson,…]
  lower bounds [Hajnal Maass Pudlak Szegedy Turan,…]

# Hardness amplification

[Y,GL,L,BF,BFL,BFNW,I,GNW,FL,IW,CPS,STV,TV,SU,T,O,V,HVV,GK,IJK,…]

- $f \notin \mathbf{C}$ (lower bound) → Hardness amplification against **C** → Enc(f) $(1/2 - \varepsilon)$-hard for **C** (average-case hardness)

- Usually black-box, i.e. code-theoretic

  Enc(f) = Encoding of (truth-table of) f

  Proof of correctness = decoding algorithm in **C**

- Results hold when **C** = general circuits

# The problem we study

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

- Have
  $f \notin AC^0[\oplus]$ $\Rightarrow$ ~~Hardness amplification against $AC^0[\oplus]$~~ ? $\Rightarrow$ Open
  $f$ :$(1/2 - 1/n)$-hard for $AC^0[\oplus]$ ?

- Conjecture[V. '04]: Black-box hardness amplification against class **C** $\Rightarrow$ Majority $\in$ **C**

# Our results

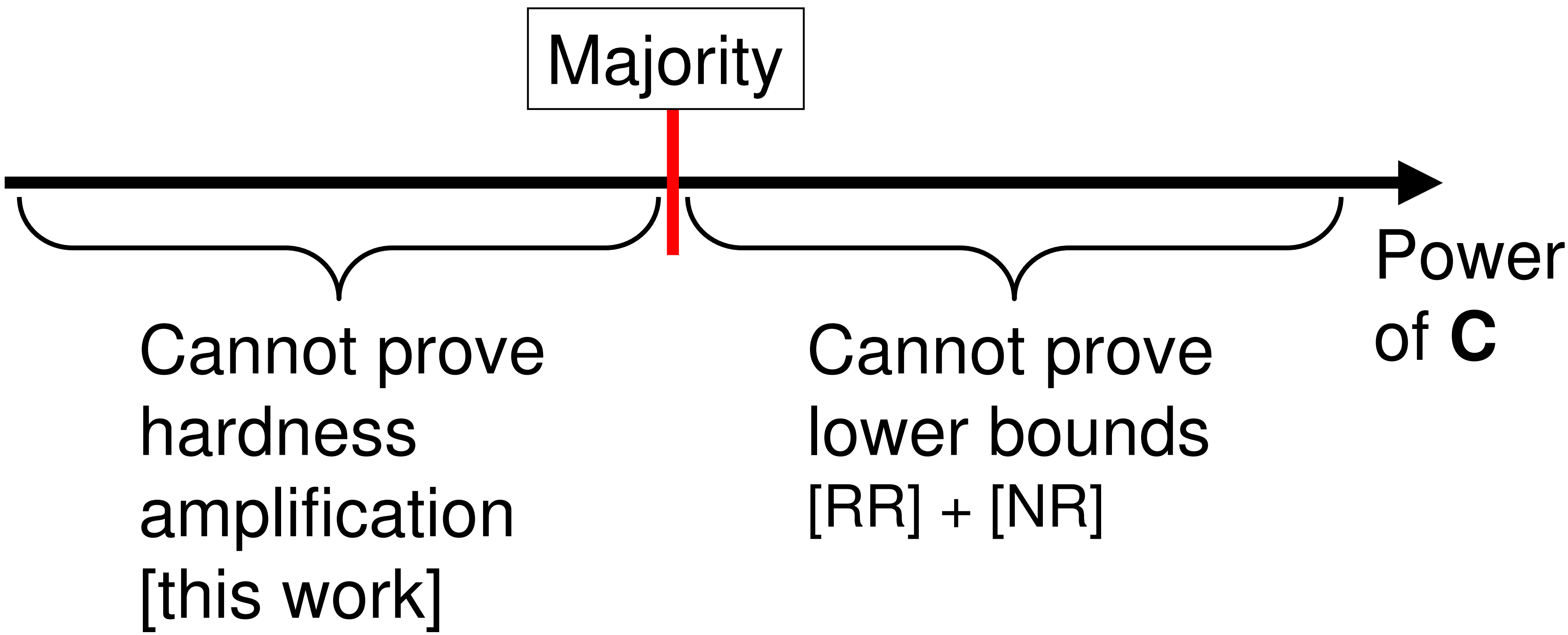
- Theorem[This work] Black-box (non-adaptive) $(1/2 - \varepsilon)$-hardness amplification against class **C** $\Rightarrow$ **C** computes majority on $1/\varepsilon$ bits.

- Tight

  [Impagliazzo, Goldwasser Gutfreund Healy Kaufman Rothblum]

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

"Lose-lose" reach of standard techniques:




"You can only amplify the hardness you don't know"

# Other consequences of our results

- Boolean vs. non-Boolean hardness amplification
  $\mathrm{Enc}(f)(x) \in \{0,1\}$ requires majority
  $\mathrm{Enc}(f)(x) \in \{0,1\}^t$ does not [Impagliazzo Jaiswal Kabanets Wigderson]

- Loss in circuit size: Lower bound for size s
  $\Rightarrow (1/2 - \varepsilon)$-hard for size $s \cdot \varepsilon^2/n$
  Tight [Impagliazzo, Klivans Servedio]

- Decoding is more difficult than encoding
  Encoding: Parity ($\oplus$)
  Decoding: Majority

# Outline

- Overview and our results
- Formal statement of our results

# Black-box hardness amplification

f = 0 1 0 1 0 1 0 1 0 … 1

arbitrary

Enc(f) = 0 1 1 1 0 1 0 0 1 0 1 1 0 0 0 1 0 … 0

h = 0 0 0 0 0 1 1 0 1 1 1 1 1 0 0 0 0 … 0

(1/2 – ε errors)

queries (non-adaptive)

$D^h(x) = f(x)$

- In short: $\forall$ f $\forall$ h $\approx$ Enc(f) $\Rightarrow$ $\exists$ D $\in$ **C** : $D^h$ = f
- Rationale: f $\notin$ **C** $\Rightarrow$ Enc(f) (1/2 – ε)-hard for **C**

# Our results

- Theorem

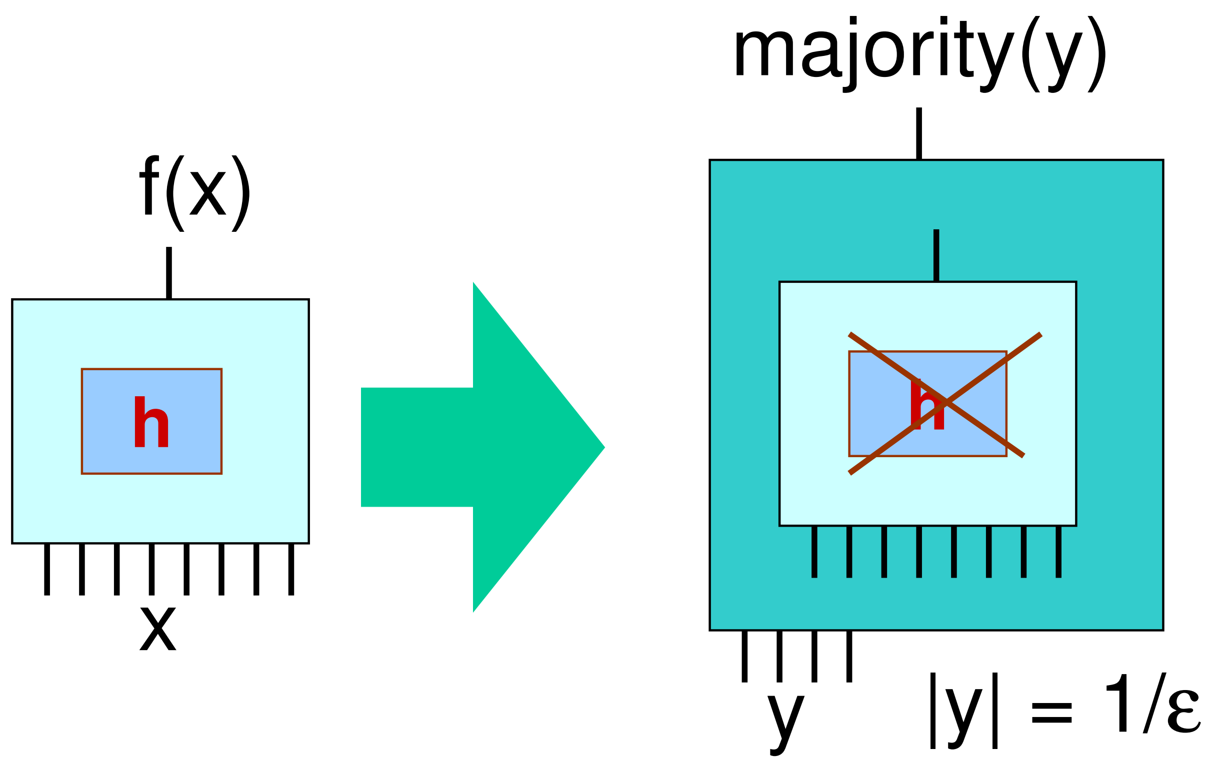
  Black-box non-adaptive $(1/2 - \varepsilon)$-hardness amplification against **C**

  $\Rightarrow$

  $\exists$ M $\in$ **C** computes majority on $1/\varepsilon$ bits

$\forall$ f, h $\approx$ Enc(f)

$\exists$ D $\in$ **C** : $D^h = f$



# Proof idea

- $(1/2 - \varepsilon)$ hardness amplification against **C**

  $\Rightarrow \exists\, D \in$ **C** : tells Noise rate 1/2 from $1/2 - \varepsilon$

  $h$ = noise 1/2 $\Rightarrow D^h \neq f$

  $h = \mathrm{Enc}(f) \oplus$ noise $1/2 - \varepsilon$ $\Rightarrow D^h = f$

  $\Rightarrow$ compute majority

  Ack: Madhu Sudan

- Problem: D depends on h
- This work: Technique to fix D independent of h

# Conclusion

- This work: Black-box (non-adaptive) hardness amplification against **C** $\Rightarrow$ Majority $\in$ **C**

- Reach of standard techniques
  [This work] + [Razborov Rudich] + [Naor Reingold]
  "Can amplify hardness $\Leftrightarrow$ cannot prove lower bound"

- Open problems
  Adaptivity? (Already can handle special cases)
  1/3-pseudorandom construction $\Rightarrow$ majority?