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

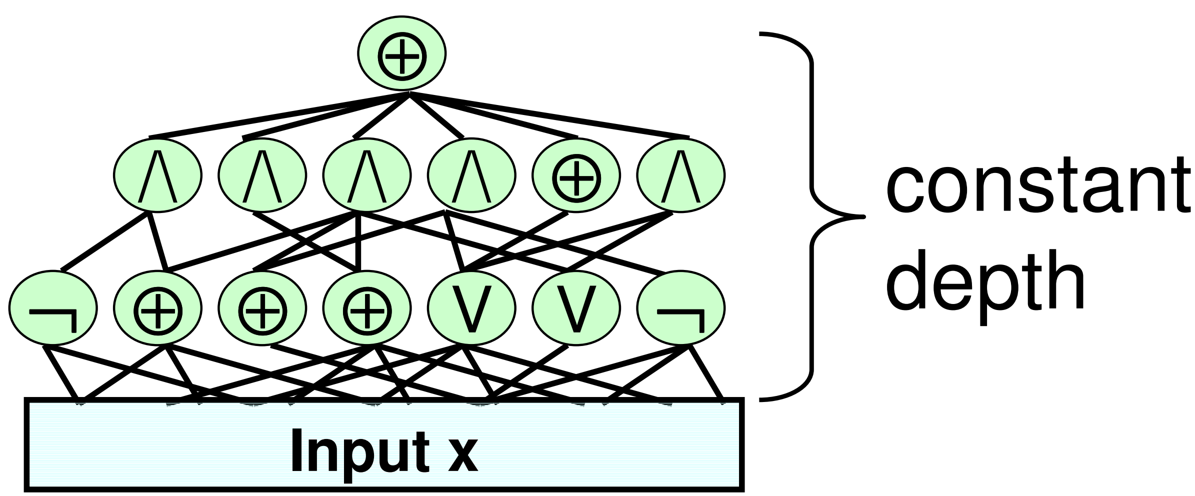
Circuit lower bounds

- Success with restricted circuits
  [Furst Saxe Sipser, Ajtai, Yao, Hastad, Razborov, Smolensky,…]

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

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

  $AC^0[\oplus]$ =



$\oplus$ = parity
$\vee$ = or
$\wedge$ = and
$\neg$ = not

Natural proofs barrier

- Little progress for general circuit models
- Natural Proofs [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 $\notin$ **C** → Hardness amplification against **C** → Enc(f) (1/2 – ε)-hard for **C**

  (lower bound) (average-case hardness)

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

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

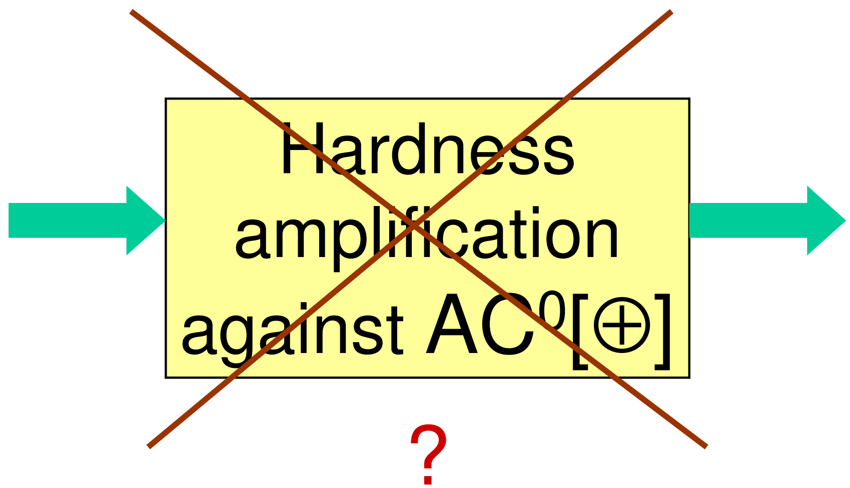
  Proof of correctness = decoding algorithm in **C**

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

The problem we study

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

- Have
  $f \notin AC^0[\oplus]$



Open
f :(1/2 – 1/n)-hard for $AC^0[\oplus]$?

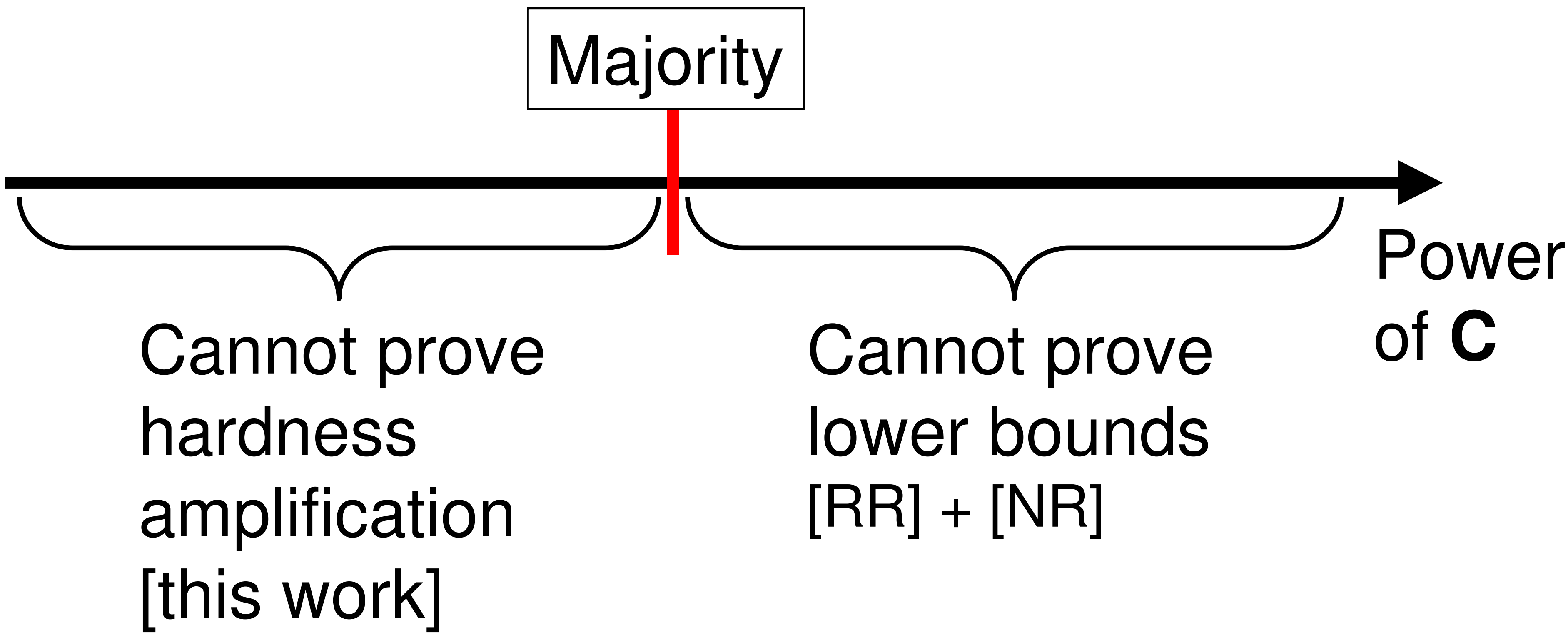
- Conjecture[V. '04]: Black-box hardness amplification against class **C** $\Rightarrow$ Majority $\in$ **C**

Our results

- Theorem[This work] Black-box (non-adaptive) $(1/2 - \varepsilon)$-hardness amplification against class **C** $\Rightarrow$
  - (i) $C \in$ **C** computes majority on $1/\varepsilon$ bits
  - (ii) $C \in$ **C** makes $\geq n/\varepsilon^2$ queries
- Generalizes to $\delta \to (1/2 - \varepsilon)$-hardness amplification
- Both tight
  - (i) [Impagliazzo, Goldwasser Gutfreund Healy Kaufman Rothblum]
  - (ii) [Impagliazzo, Klivans Servedio]

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
  Enc(f)(x) $\in$ {0,1} requires majority
  Enc(f)(x) $\in$ $\{0,1\}^t$ does not [Impagliazzo Jaiswal Kabanets Wigderson]

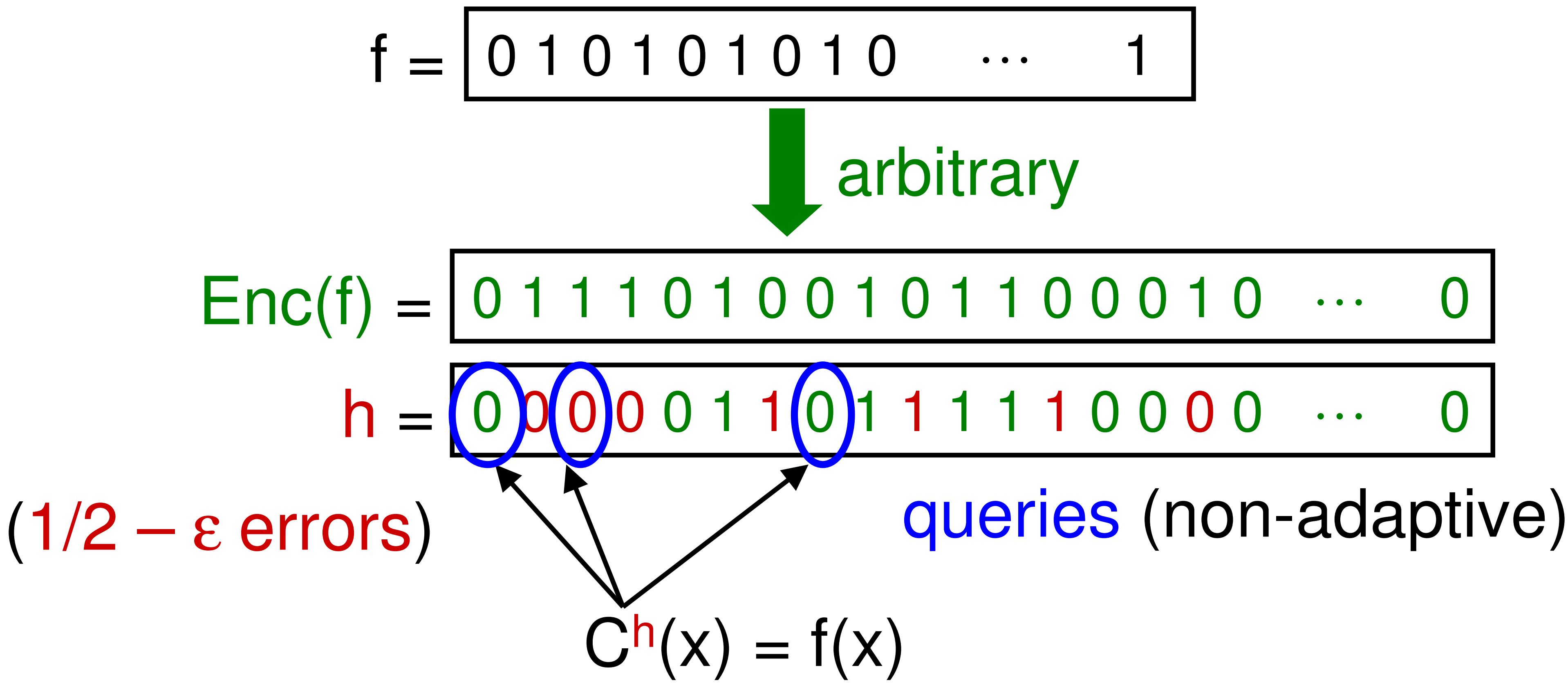
- Loss in circuit size: Lower bound for size s
  $\Rightarrow$ $(1/2 - \varepsilon)$-hard for size $s \cdot \varepsilon^2/n$

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

Outline

- Overview and our results
- Formal statement of our results
- Proof

Black-box hardness amplification



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

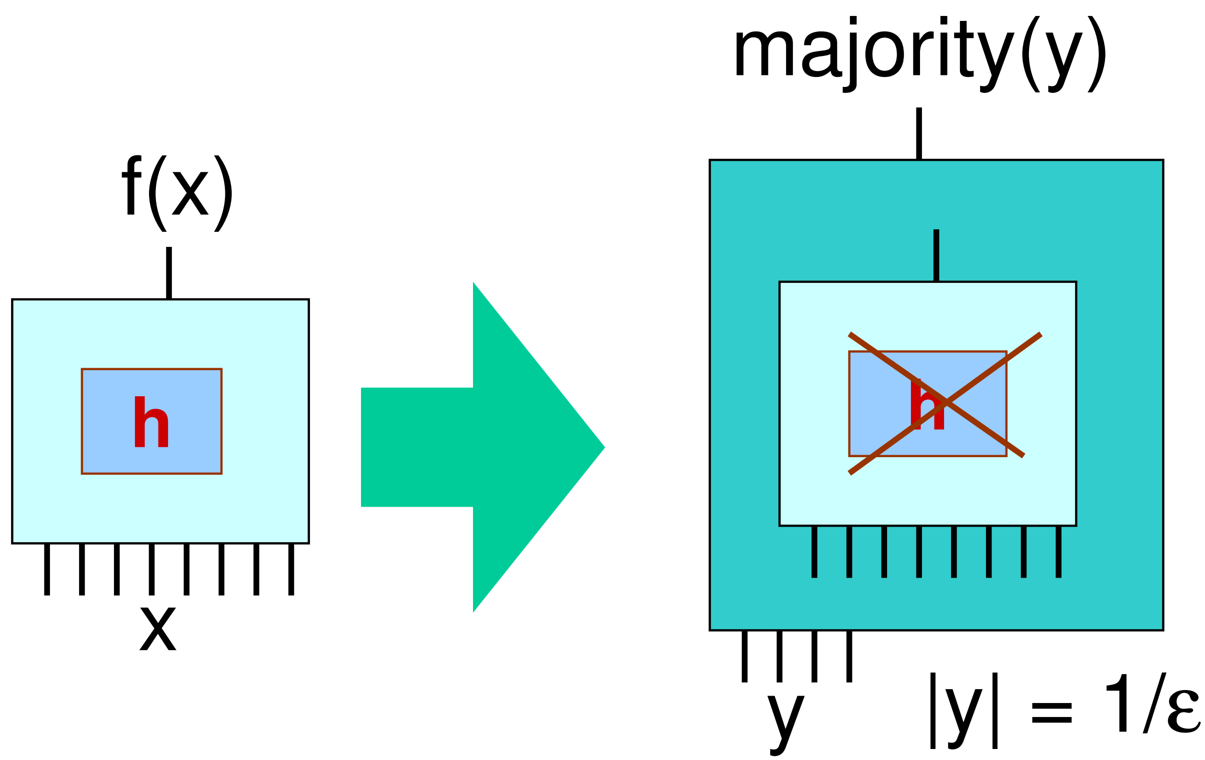
Our results

- Theorem

  Black-box non-adaptive $(1/2 - \varepsilon)$-hardness amplification against **C** ⟹ $\exists$ M $\in$ **C** computes majority on $1/\varepsilon$ bits

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

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



Outline

- Overview and our results
- Formal statement of our results
- Proof

Proof

- Recall Theorem: Black-box (non-adaptive) $(1/2 - \varepsilon)$-hardness amplification against class **C** $\Rightarrow$
  - (i) $C \in$ **C** computes majority on $1/\varepsilon$ bits
  - (ii) $C \in$ **C** makes $q \geq n/\varepsilon^2$ queries

- We show hypot. $\Rightarrow$ $C \in$ **C** : tells Noise 1/2 from $1/2 - \varepsilon$

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

- (i) $\Leftarrow$ (D) + manipulations

  Ack: Madhu Sudan

  (ii) $\Leftarrow$ (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 $C \in \mathbf{C}$: $C^h(x) = f(x) \quad \forall x$

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

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

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

  $C^h(x) = f(x) \quad \forall x$

Proof in uniform case

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

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

  $H(y) \sim N_{1/2-\varepsilon} \Rightarrow C^{\mathrm{Enc}(F) \oplus H}(X) = F(X)$ always
  $\mathrm{Enc}(F) \oplus H$ is $(1/2-\varepsilon)$-close to $\mathrm{Enc}(F)$

- 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 $\mathrm{Enc}(F)(y_i) \oplus z_i$

Q.e.d.

Proof outline in non-uniform case

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

1) Fix C to C' that works for many f,h
   Condition F' := F | C', H' := H | C'

2) Information-theoretic lemma
   There is good set $G \subseteq \{0,1\}^n$ s.t. if all $y_i \in G$:

   $$\mathrm{Enc}(F') \oplus H' (y_1,\ldots,y_q) \approx \mathrm{Enc}(F) \oplus H (y_1,\ldots,y_q)$$

   Can argue as for uniform case if all $y_i \in G$

3) Deal with queries y_i not in G

Fixing C

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

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

  With probability 1 over F,H there is $C \in \mathbf{C}$:

$$C^{Enc(F) \oplus H}(x) = F(x) \quad \forall x$$

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

$$C'^{Enc(F) \oplus H}(x) = F(x) \quad \forall x$$

- 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.

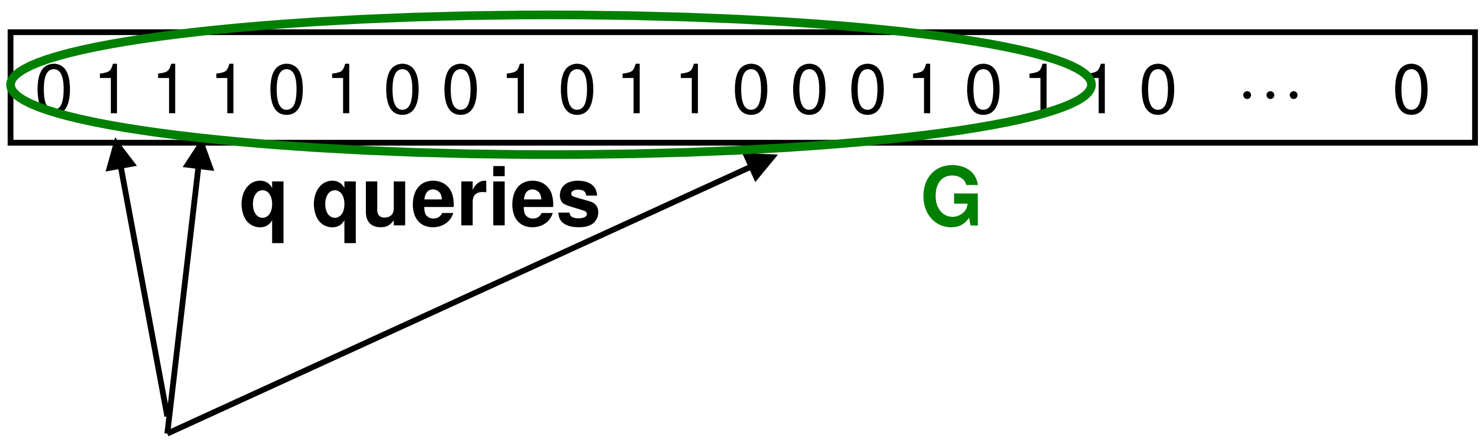
- Also in [Edmonds Rudich Impagliazzo Sgall, Raz]

Applying the lemma

- $V_x = H(x)$ ~ Noise $1/2\text{-}\varepsilon$

- $E := \{ H : C'^{\,Enc(F) \oplus H}(x) = F(x) \ \ \forall x \}$, $\Pr[E] \geq 1/|\mathbf{C}|$

$H' = H \mid E =$



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

- 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

- 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? (OK in special cases [V., Gutfreund Rothblum])
  1/3-pseudorandom construction $\Rightarrow$ majority?