Hardness Amplification within NP

Aaron Councilman and Aman Singh

CS 579 Presentation

December 6, 2023

Hardness Amplification within NP

Ryan O'Donnell

Journal of Computer and System Sciences (2004)

Hardness vs Randomness

- Result from Impagliazzo and Wigderson 1997
  1. If there is a language in E that requires $2^{\Omega(n)}$ size circuits, then BPP $=$ P
  2. If there is a language in EXP that requires $2^{n^{\epsilon}}$ size circuits, then BPP $\subseteq$ TIME$(n^{poly(\log n)})$ (for any $\epsilon > 0$)
  3. If there is a language in EXP that requires $n^{\omega(1)}$ size circuits, then BPP $\subseteq$ TIME$(2^{n^{\epsilon}})$ (for any $\epsilon > 0$)

Circuit Hardness

Definition (Function Hardness)

For $f : \{0,1\}^n \to \{0,1\}$ is $(1-\delta)$-hard for circuits of size s if there is no circuit of size s which can compute f on a $1-\delta$ fraction of the inputs $\{0,1\}^n$.

Definition (Language Hardness)

A language $L \subseteq \{0,1\}^*$ is *infinitely often* $(1-\delta)$-hard for circuits of size s if there are infinitely many n such that $f_n : \{0,1\}^n \to \{0,1\}$ where $f_n(x) = 1$ iff $x \in L$, is $(1-\delta)$-hard for circuits of size $s(n)$.

Hardness amplification within EXP

- If there is a language in EXP which is $(1/2 + 2^{-\Omega(n)})$-hard for sub-exponential size circuits, then there exist sub-exponential time deterministic simulations of BPP (Nisan and Wigderson 1994)
- If there is a language in EXP which is even $(1 - 2^{-n})$-hard for polynomial circuits, then there is a problem in EXP which is $(1/2 + 1/poly(n))$-hard for polynomial circuits
- The objective of this paper is to produce a result of this nature for the class NP

XOR Lemma

- The main ingredient in hardness amplification results is Yao's XOR Lemma (Yao 1982): $f \oplus f \oplus \cdots \oplus f$ much harder than f

Lemma (Yao's XOR Lemma)

If f is a balanced boolean function which is $(1-\delta)$-hard for circuits of size s, then $f \oplus \cdots \oplus f$ (k times) is $(1/2 + (1-1.99\delta)^k/2 + \varepsilon)$ -hard for circuits of size $\Omega(s\varepsilon^2/\log(1/\delta)k)$

- However, XOR may not preserve NP:
  SAT $\oplus$ SAT : $\{\langle \varphi, \psi \rangle \mid$ exactly one of φ and ψ are satisfiable$\}$
  - NP-Hard and coNP-Hard
- For $f \in$ NP, we want $g(f(x_1), \cdots, f(x_k)) \in$ NP so $g \otimes f$ is much harder than f

Monotone Functions preserve NP

- Issue with XOR is negation: $x \oplus y \equiv (x \wedge \neg y) \vee (\neg x \wedge y)$
- *Monotone Binary Functions:* have circuits of only AND and OR gates (Arora and Barak 2009).

Lemma

If $f, g \in \mathrm{NP}$ and g is monotone, then $g \otimes f$ is still in NP

Proof: The NTM for $g \otimes f$ guesses a string $z \in \{0, 1\}^k$ and runs the NTM for g. If it accepts, then it checks if for all i where $z_i = 1$, whether $f(x_i) = 1$ by running the NTM for f. The NTM does not need to check if $f(x_j) = 0$ where $z_j = 0$ as g is monotonic and z_j being 0 or 1 does not matter at j.

Hardness Amplification within NP

Theorem

If there is a function in NP *that is infinitely often balanced and* $(1 - 1/poly(n))$*-hard for circuits of polynomial size, then there is a function in* NP *which is infinitely often* $(1/2 + n^{-1/2+\varepsilon})$*-hard for circuits of polynomial size*

Theorem

If there is a function in NP *that is infinitely often* $(1 - 1/poly(n))$*-hard for circuits of polynomial size, then there is a function in* NP *which is infinitely often* $(1/2 + n^{-1/3+\varepsilon})$*-hard for circuits of polynomial size*

Expected Bias

Theorem (informally)

For $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^k \to \{0,1\}$, if f is $(1-\delta)$-hard for circuits of size s, $g \otimes f$ is $(\mathit{ExpBias}_{2\delta}(g) + \varepsilon)$-hard for circuits of size $s' = \Omega(\frac{\varepsilon^2/\log(1/\delta)}{k} s)$.

Definition (Expected Bias)

$$\mathrm{ExpBias}_\delta(f) = \mathop{\mathbb{E}}_{\rho \in P^n_\delta}[\mathrm{bias}(f_\rho)]$$

$$\mathrm{bias}(f) = \max\{\Pr_x[f(x)=0], \Pr_x[f(x)=1]\}$$

P^n_δ is the probability space over restrictions on n coordinates choosing each independently and $*$ with probability δ, and 0 and 1 each with probability $(1-\delta)/2$

Intuition

- f is $(1-\delta)$-hard for circuits of size s and balanced
- *Hard-Core Scenario*: over all inputs, $1-2\delta$ fraction *we know* $f(x_i)$ is correct, remaining 2δ fraction $f(x_i)$ is a random guess
- For $g \otimes f$ over random inputs x_i, for each i there is $1-2\delta$ probability we know $f(x_i)$ computed correctly and otherwise $f(x_i)$ is random
- Best we can do is guess whichever of 0 and 1 is more likely for g_ρ (ρ based on correct bits)
  - Probability we're correct is $\text{bias}(g_\rho)$
  - Over all inputs, ρ is sampled from $P^n_{2\delta}$
  - So the hardness of $g \otimes f$ is $\text{ExpBias}_{2\delta}(g)$

Proof prerequisites

Theorem (Impagliazzo's Hard-Core set Theorem)

Let f be $(1-\delta)$-hard for size s, and $r > 0$ be any constant. Then f has a "hard-core" of size between $(2-r)\delta 2^n$ and $(2-r/2)\delta 2^n$ where f is $(1/2+\varepsilon)$-hard for size $s' = \Omega(s\varepsilon^2/\log(1/\delta))$

Corollary

Additionally, f has a hard-core of size between $(2-r)\delta 2^n$ and $2\delta 2^n$ which is $(1/2+\varepsilon)$-hard for size s' and on which f is balanced

Proof prerequisites (2)

- Use Impagliazzo's theorem with $\varepsilon/2$ to get a hard-core set S'
- Even if f is biased towards 1 on S', the total number of 1 $\leq (1/2+\varepsilon/2)|S'| \leq (1/2+\varepsilon/2)(2-r/2)\delta 2^n \leq \delta 2^n$
- f takes on value 0 for at least $\delta 2^n$ values in $\{0,1\}^n$ as f is $(1-\delta)$-hard
- It's possible to construct $S' \subseteq S$ such that f is balanced on S
- f is $(1/2+\varepsilon)$-hard on S for size s' circuits

$$
\begin{aligned}
(1/2+\varepsilon/2)\frac{|S'|}{|S|} + \frac{|S \backslash S'|}{|S|} &= 1/2+\varepsilon/2+(1/2-\varepsilon/2)\frac{|S \backslash S'|}{|S|} \\
&\leq 1/2+\varepsilon/2+(1/2-\varepsilon/2)\varepsilon \\
&\leq 1/2+\varepsilon
\end{aligned}
$$

Proof

Theorem

If f is balanced and $(1-\delta)$-hard for circuits of size s and $g : \{0,1\}^k \to \{0,1\}$, then for every $r > 0$, $g \otimes f$ is $(ExpBias_{(2-r)\delta}(g) + \varepsilon)$-hard for circuits of size $s' = \Omega(\frac{\varepsilon^2 / \log(1/\delta)}{k^2} s)$.

- Use δ, r and $\varepsilon' = \varepsilon/8k$ to get balanced hard-core S for f
- Assume C is a circuit of size s' computing $g \otimes f$ on fraction of size $\text{ExpBias}_{(2-r)\delta}(g) + \varepsilon \geq E + \varepsilon$ where $E = \text{ExpBias}_{|S|/2^n}(g)$
- Let $\rho \in P_\eta^k$ be a random restriction and c_ρ be the probability that C computes $(g \otimes f)(x_1, \ldots, x_k)$ correctly, given $(x_1, \ldots, x_k)$ "matches" ρ

Proof (2)

– $\Pr[(x_1, .., x_k) \text{ matches } \rho] = \Pr[\rho] = \eta^{|*|}(1/2 - \eta/2)^{k-|*|}$

$$\begin{aligned} \Pr[C \text{ correct}] &\geq E + \varepsilon \\ \sum_\rho \Pr[(x_1, \dots, x_k) \text{ matches } \rho] c_\rho &\geq \sum_\rho \Pr[\rho] \text{ bias}(g_\rho) + \varepsilon \\ \sum_\rho \Pr[\rho] c_\rho &\geq \sum_\rho \Pr[\rho] \text{ bias}(g_\rho) + \varepsilon \\ \sum_\rho \Pr[\rho](c_\rho - \text{ bias}(g_\rho)) &\geq \varepsilon \end{aligned}$$

Proof (3)

- Through an averaging argument, we get that there is a random restriction ρ such that $c_\rho \geq \text{bias}(g_\rho) + \varepsilon/4$
- Using the same argument, we can fix inputs x_j where $\rho(j) \neq *$
- This gives a circuit C' of size s' which computes $g \otimes f$ correctly on inputs $x_1, \ldots, x_{k'}$ drawn from S with probability at least c_ρ
- Let $p(y)$ be the probability that $C'(x_1, \ldots, x_{k'}) = 0$ given $y_i = f(x_i)$. As we draw x_i from S where f is balanced, all the y_is are equiprobable. The correctness probability of C' is

$$\Big[\sum_{y \in g_\rho^{-1}(0)} p(y) + \sum_{y \in g_\rho^{-1}(1)} (1 - p(y)) \Big] / 2^{k'}$$

Proof prerequisites (3)

Lemma

Let $h : \{0,1\}^k \to \{0,1\}$ *and* $p : \{0,1\}^k \to [0,1]$*. If*

$$\Big[\sum_{y \in h^{-1}(0)} p(y) + \sum_{y \in h^{-1}(1)} (1 - p(y)) \Big] / 2^k \qquad (1)$$

is at least bias$(h) + \varepsilon$*, then there are inputs hamming distance 1 apart such that* $|p(z) - p(z')| \geq \varepsilon / k$

- Let M be the maximum value of $p(y)$ and m the minimum.
- Assuming $|p(z) - p(z')| < \varepsilon / k$, it follows that $M - m < \varepsilon$. Let h be biased towards 0 and $b = \text{ bias}(h) = \text{ Pr}[h = 0]$, then

$$\begin{aligned} (1) &\leq bM + (1-b)(1-m) \\ &< b(m+\varepsilon) + (1-b)(1-m) = m(2b-1) + 1 + b\varepsilon - b \\ &\leq b + \varepsilon \end{aligned}$$

Proof (4)

- Using the lemma, there are inputs (z, z') that differ in one bit such that $|p(z) - p(z')| \geq (\varepsilon/4)/k' \geq (\varepsilon/4)/k = 2\varepsilon'$
- Using an averaging argument, we can fix x_j according to the equal bits in z, z' to get a new circuit C'' still of size s', such that

$$\left| \Pr_{x \in (f|_S)^{-1}(0)}[C''(x) = 0] - \Pr_{x \in (f|_S)^{-1}(1)}[C''(x) = 0] \right| \geq 2\varepsilon'$$

$$\left| \Pr_{x \in (f|_S)^{-1}(0)}[C''(x) = 0] + \Pr_{x \in (f|_S)^{-1}(1)}[C''(x) = 1] - 1 \right| \geq 2\varepsilon'$$

$$\left| \Pr_{x \in S}[C''(x) = f(x)] - 1/2 \right| \geq \varepsilon'$$

- So we get a size s' circuit C'' that computes f correctly on $(1/2 + \varepsilon')$ fraction of inputs drawn from the hard-core S

More generally...

Theorem

Let $g : \{0,1\}^k \to \{0,1\}$. Given f is $(1-\delta)$-hard for circuits of size s and nearly balanced, i.e, bias$(f) \leq 1/2 + (1-2\delta)\varepsilon/4k$. Then for every $r > 0$, $g \otimes f$ is $(ExpBias_{(2-r)\delta}(g) + \varepsilon)$-hard for circuits of size $s' = \Omega(\frac{\varepsilon^2/\log(1/\delta)}{k} s)$.

Approximating Expected Bias

- The expected bias used earlier is hard to compute even for simple functions
- Noise Stability has been studied elsewhere in the literature and is easier to compute
- Intuitively, highly *noise unstable* functions seem like good hardness amplifiers

Noise Stability

Definition (Noise Stability)

$$\mathrm{NoiseStab}_\delta(h) = \Pr_{\substack{x \in \{0,1\}^n \\ y \in N_\delta(x)}}[h(x) = h(y)]$$

Definition (Random Perturbation)

For $x \in \{0,1\}^n$, $N_\delta(x)$ is a random variable given by independently flipping each bit of x with probability δ.

Noise Stability and Expected Bias

Theorem

$$\mathit{NoiseStab}_{\delta}(h)^{*} \leq \mathit{ExpBias}_{2\delta}(h)^{*} \leq \sqrt{\mathit{NoiseStab}_{\delta}(h)^{*}}$$

Where for $z \in \left[\frac{1}{2}, 1\right]$, $z^{*} = 2\left(z - \frac{1}{2}\right)$

- Advantage: $\mathrm{adv}(h) = \mathrm{bias}(h)^{*}$
- For restriction ρ, let stars(ρ) be the coordinates ρ has $*$ in

Noise Stability and Expected Bias (Proof)

$$\mathrm{ExpBias}_{2\delta}(h)^* = \mathbb{E}_{\rho \in P^n_{2\delta}}[\mathrm{adv}(h_\rho)] \text{ by linearity}$$

$$\begin{aligned}\mathrm{NoiseStab}_\delta(h) &= \Pr_{\substack{x \in \{0,1\}^n \\ y \in N_\delta(x)}}[h(x) = h(y)] \\ &= \Pr_{\substack{\rho \in P^n_{2\delta} \\ w,z \in \{0,1\}^{|\mathrm{stars}(\rho)|}}}[h_\rho(w) = h_\rho(z)]\end{aligned}$$

Consider a particular bit in $\rho(w)$ and $\rho(z)$; need this to have flipped with probability δ

- ρ must have a $*$ (probability 2δ)
- w and z differ (probability $1/2$)

Noise Stability and Expected Bias (2)

$$\begin{aligned}
\mathrm{NoiseStab}_\delta(h) &= \Pr_{\substack{\rho \in P^n_{2\delta} \\ w,z \in \{0,1\}^{|\mathrm{stars}(\rho)|}}} [h_\rho(w) = h_\rho(z)] \\
&= \mathop{\mathbb{E}}_{\rho}\left[\Pr_{w,z}[h_\rho(w) = h_\rho(z)]\right] \\
&= \mathop{\mathbb{E}}_{\rho}\left[\frac{1}{2} + \frac{1}{2}\mathrm{adv}(h_\rho)^2\right]
\end{aligned}$$

If x and y are independently and uniformly selected from $\{0,1\}^n$, then $\Pr_{x,y}[h(x) = h(y)] = \frac{1}{2} + \frac{1}{2}\mathrm{adv}(h)^2$

$$\mathrm{NoiseStab}_\delta(h)^* = \mathop{\mathbb{E}}_{\rho}[\mathrm{adv}(h_\rho)^2]$$

$$\mathrm{ExpBias}_{2\delta}(h)^* = \mathop{\mathbb{E}}_{\rho}[\mathrm{adv}(h_\rho)]$$

Noise Stability and Expected Bias (3)

$$\text{NoiseStab}_\delta(h)^* = \mathop{\mathbb{E}}_\rho[\text{adv}(h_\rho)^2]$$
$$\text{ExpBias}_{2\delta}(h)^* = \mathop{\mathbb{E}}_\rho[\text{adv}(h_\rho)]$$

$\text{adv}(h_\rho)^2 \leq \text{adv}(h_\rho)$ so $\text{NoiseStab}_\delta(h)^* \leq \text{ExpBias}_{2\delta}(h)^*$
$\text{ExpBias}_{2\delta}(h)^* \leq \sqrt{\text{NoiseStab}_\delta(h)^*}$ by Cauchy-Schwarz inequality

If $\text{NoiseStab}_\delta(h)$ is $1 - o(1)$, $1 - \Omega(1)$, or $1/2 + o(1)$ then so is $\text{ExpBias}_{2\delta}(h)$

Tools for Noise Stability

- If h is balanced:
  $\mathrm{NoiseStab}_\delta(g \otimes h) = \mathrm{NoiseStab}_{1-\mathrm{NoiseStab}_\delta(h)}(g)$
- Noise Stability can also be computed using the Fourier coefficients, in particular converting h to a multilinear polynomial $\{+1,-1\}^n \to \{+1,-1\}$

First Amplification Result for NP

Definition

For $\ell \geq 1$, REC-MAJ-$3^\ell : \{0,1\}^{3^\ell} \to \{0,1\}$ is defined as a depth-ℓ ternary tree of majority-of-3 gates.

REC-MAJ-3^ℓ is in P and is monotone

First Amplification Result for NP

Definition

For $\ell \geq 1$, REC-MAJ-$3^\ell : \{0,1\}^{3^\ell} \to \{0,1\}$ is defined as a depth-ℓ ternary tree of majority-of-3 gates.

REC-MAJ-3^ℓ is in P and is monotone

For $\ell \geq \log_{1.1}(1/\delta)$, $\mathrm{NoiseStab}_\delta(\text{REC-MAJ-}3^\ell)^* \leq \delta^{-1.1}(3^\ell)^{-0.15}$, and so $\mathrm{ExpBias}_{2\delta}(\text{REC-MAJ-}3^\ell) \leq \delta^{-0.55}(3^\ell)^{-0.075}$.

First Amplification Result for NP

Definition

For $\ell \geq 1$, REC-MAJ-$3^\ell : \{0,1\}^{3^\ell} \to \{0,1\}$ is defined as a depth-ℓ ternary tree of majority-of-3 gates.

REC-MAJ-3^ℓ is in P and is monotone

For $\ell \geq \log_{1.1}(1/\delta)$, $\mathrm{NoiseStab}_\delta(\text{REC-MAJ-}3^\ell)^* \leq \delta^{-1.1}(3^\ell)^{-0.15}$, and so $\mathrm{ExpBias}_{2\delta}(\text{REC-MAJ-}3^\ell) \leq \delta^{-0.55}(3^\ell)^{-0.075}$.

Theorem

If (f_n) is NP *and infinitely often balanced and $(1 - 1/n^c)$-hard for poly-size circuits, then (h_m) where $h_m = \text{REC-MAJ-}3^\ell \otimes f_n$ is $(1/2 + m^{-0.07})$-hard for poly-size circuits.*

Recursive Majority Amplification Proof

- Let $k = n^C$ for some sufficiently large C, let $\ell = \lfloor \log_3 k \rfloor$, and treat REC-MAJ-$3^\ell$ be a function on k inputs (ignoring bits in excess of 3^ℓ)
- $h_m = \text{REC-MAJ-}3^\ell \otimes f_n$ has $m = kn = n^{C+1}$ and is in NP
- Use amplification theorem with $r = 1$, $\varepsilon = 1/n^C$ and $\delta = 1/n^c$.
  h_m is $(\text{ExpBias}_{1/n^c}(\text{REC-MAJ-}3^\ell) + 1/n^C)$-hard for polynomial circuits (for sufficiently large C).

$$\begin{aligned}\text{ExpBias}_{1/n^c}(\text{REC-MAJ-}3^\ell) &\leq 1/2 + (1/2)(1/2n^c)^{-0.55}(3^\ell)^{-0.075} \\ &\leq 1/2 + n^{-0.074C} \leq 1/2 + m^{-0.07}\end{aligned}$$

by taking sufficiently large C.

Second Amplification Result for NP

Definition

For input length k, set a parameter b little less than $\log_2 k$.
$T_k : \{0,1\}^k \to \{0,1\}$ is defined as $T_k(x_1, \ldots, x_k) =$
$(x_1 \wedge \cdots \wedge x_b) \vee (x_{b+1} \wedge \cdots \wedge x_{2b}) \vee \cdots \vee (x_{k-b+1} \wedge \cdots \wedge x_k)$.

T_k is in P and is monotone

By Fourier analysis, $\mathrm{NoiseStab}_\delta(T_k)^* \leq e^{(1-\delta)^b} - 1 + O(\log^2 k / k^2)$
So, for every $\eta > 0$, there is $r > 0$ such that for some large k,

$$\mathrm{ExpBias}_{1-r}(T_k) \leq 1/2 + k^{-1/2+\eta}$$

Putting it all together...

Theorem

If there is a family of functions (f_n) in NP *which is infinitely often balanced and $(1 - 1/poly(n))$-hard for poly-size circuits, then there is a family of functions (h_n) still in* NP *which is $(1/2 + n^{-1/2+\eta})$-hard for poly-size circuits, for any small $\eta > 0$*

- From the hardness amplification using recursive majority, we get a family g_n that is $(1/2 + o(1))$-hard for polynomial circuits
- Consider the function $h = T_k \otimes g$
- Using $\varepsilon = 1/k$, $\delta = 1/2 - o(1)$ and r sufficiently small, we get that the family h_m is infinitely often $(1/2 + k^{-1/2+\eta})$-hard

Limitations

- Using Fourier analysis, we have that for monotone functions g on k size inputs, $\mathrm{NoiseStab}_\delta(g)^* \geq (1-2\delta)\Omega(\log^2 k/k)$
- Applying monotone functions to $(1/2 + \Omega(\log^2 n/n))$-hard functions still gives a $(1/2 + \Omega(\log^2 m/m))$-hard function
- If we use the $\mathrm{ExpBias}_{2\delta}$ approximation, we observe that we can't do any better than $(1/2 + \tilde{\Omega}(n^{-1/2}))$

Theorem

If there is a family of functions (f_n) in NP *which is infinitely often $(1 - 1/poly(n))$-hard for poly-size circuits, then there is a family of functions (h_n) still in* NP *which is $(1/2 + n^{-1/3+\eta})$-hard for poly-size circuits, for any small $\eta > 0$*

  - Proof involves similar techniques and a trick with input lengths

References I

Arora, Sanjeev and Boaz Barak (2009). "Circuit lower bounds: Complexity theory's Waterloo". In: *Computational Complexity: A Modern Approach*. Cambridge University Press, pp. 286–306. DOI: 10.1017/CBO9780511804090.017.

Impagliazzo, Russell and Avi Wigderson (1997). "P = BPP If E Requires Exponential Circuits: Derandomizing the XOR Lemma". In: *Proceedings of the Twenty-Ninth Annual ACM Symposium on Theory of Computing*. STOC '97, pp. 220–229. DOI: 10.1145/258533.258590.

Nisan, Noam and Avi Wigderson (1994). "Hardness vs randomness". In: *Journal of Computer and System Sciences* 49.2, pp. 149–167. DOI: 10.1016/S0022-0000(05)80043-1.

Yao, Andrew C. (1982). "Theory and Application of Trapdoor Functions". In: *23rd Annual Symposium of Computer Science (sfcs 1982)*, pp. 80–91. DOI: 10.1109/SFCS.1982.45.