Lecture 13 - Natural Proofs

Rafael Oliveira
rafael.oliveira.teaching@gmail.com
University of Waterloo

CS 860 - Graduate Complexity Theory
Fall 2022

Overview

- Current (Non-Uniform) Circuit Lower Bounds

- Natural Proofs

Example: $AC^0_{/\text{poly}}$ lower bounds

- Random restriction with parameter $q \in [0,1]$:

$$\rho(x_i) = \begin{cases} x_i, & \text{with probability } q \\ 0, & \text{with probability } (1-q)/2 \\ 1, & \text{with probability } (1-q)/2 \end{cases}$$

Example: $AC^0_{/\text{poly}}$ lower bounds

- Random restriction with parameter $q \in [0, 1]$:

$$\rho(x_i) = \begin{cases} x_i, & \text{with probability } q \\ 0, & \text{with probability } (1-q)/2 \\ 1, & \text{with probability } (1-q)/2 \end{cases}$$

- Switching lemma (Furst-Saxe-Sipser 1981): if $q = n^{2/3}$, then for any DNF of polynomial size $p(n)$, and $\delta = 1/\text{poly}(n)$, after random restriction we get a CNF of size C with probability $(1 - \delta)$ where C is constant.

Example: $AC^0_{/\text{poly}}$ lower bounds

- Random restriction with parameter $q \in [0,1]$:

$$\rho(x_i) = \begin{cases} x_i, & \text{with probability } q \\ 0, & \text{with probability } (1-q)/2 \\ 1, & \text{with probability } (1-q)/2 \end{cases}$$

- Switching lemma (Furst-Saxe-Sipser 1981): if $q = n^{2/3}$, then for any DNF of polynomial size $p(n)$, and $\delta = 1/\text{poly}(n)$, after random restriction we get a CNF of size C with probability $(1-\delta)$ where C is constant.
- $\bigoplus$ does not have poly-sized $AC^0_{/\text{poly}}$ circuits

Example: $AC^0_{/\text{poly}}$ lower bounds

- Random restriction with parameter $q \in [0, 1]$:

$$\rho(x_i) = \begin{cases} x_i, & \text{with probability } q \\ 0, & \text{with probability } (1-q)/2 \\ 1, & \text{with probability } (1-q)/2 \end{cases}$$

- Switching lemma (Furst-Saxe-Sipser 1981): if $q = n^{2/3}$, then for any DNF of polynomial size $p(n)$, and $\delta = 1/\text{poly}(n)$, after random restriction we get a CNF of size C with probability $(1 - \delta)$ where C is constant.
- $\bigoplus$ does not have poly-sized $AC^0_{/\text{poly}}$ circuits
- Proof by induction on depth. Reduce d to $d - 1$ by switching bottom layer. Base case $d = 2$ easy.

- Current (Non-Uniform) Circuit Lower Bounds
- Natural Proofs

Natural Properties

- Denote the set of all boolean functions on n bits as

$$\mathcal{F}_n := \{f : \{0,1\}^n \to \{0,1\}\} \simeq \{0,1\}^{2^n}$$

Natural Properties

- Denote the set of all boolean functions on n bits as

$$\mathcal{F}_n := \{f : \{0,1\}^n \to \{0,1\}\} \simeq \{0,1\}^{2^n}$$

- A combinatorial property of boolean functions is a family of subsets $\mathcal{P} := \{\mathcal{P}_n \subseteq \mathcal{F}_n\}_n$.

Can think of $\mathcal{P}_n$ as function from $\mathcal{F}_n$ to $\{0,1\}$.

$$\mathcal{P}_n(f) = 1 \Leftrightarrow f \in \mathcal{P}_n.$$

$$\mathcal{P}_n : \{0,1\}^{2^n} \to \{0,1\}$$

Natural Properties

- Denote the set of all boolean functions on n bits as

$$\mathcal{F}_n := \{f : \{0,1\}^n \to \{0,1\}\} \simeq \{0,1\}^{2^n}$$

- A combinatorial property of boolean functions is a family of subsets $\mathcal{P} := \{\mathcal{P}_n \subseteq \mathcal{F}_n\}_n$.

Definition 1 (Natural Property **[RR 1997]**)

Let Γ be a complexity class. A combinatorial property $\mathcal{P}$ is Γ-natural if there is a combinatorial property $\mathcal{P}^* \subset \mathcal{P}$ such that

1. Constructive: function $\mathcal{P}_n^*(f)$ computable in Γ
2. Large: $\dfrac{|\mathcal{P}_n^*|}{|\mathcal{F}_n|} \geq \dfrac{1}{2^{O(n)}}$.

Natural Properties

- Denote the set of all boolean functions on n bits as

$$\mathcal{F}_n := \{f : \{0,1\}^n \to \{0,1\}\} \simeq \{0,1\}^{2^n}$$

- A combinatorial property of boolean functions is a family of subsets $\mathcal{P} := \{\mathcal{P}_n \subseteq \mathcal{F}_n\}_n$.

Definition 1 (Natural Property [RR 1997])

Let Γ be a complexity class. A combinatorial property $\mathcal{P}$ is Γ-natural if there is a combinatorial property $\mathcal{P}^* \subset \mathcal{P}$ such that

1. Constructive: function $\mathcal{P}_n^*(f)$ computable in Γ
2. Large: $\dfrac{|\mathcal{P}_n^*|}{|\mathcal{F}_n|} \geq \dfrac{1}{2^{O(n)}}$.

- If $\Gamma = \mathrm{P}$ then we simply say that $\mathcal{P}$ is natural.

Natural Properties

- Denote the set of all boolean functions on n bits as

$$\mathcal{F}_n := \{f : \{0,1\}^n \to \{0,1\}\} \simeq \{0,1\}^{2^n}$$

- A combinatorial property of boolean functions is a family of subsets $\mathcal{P} := \{\mathcal{P}_n \subseteq \mathcal{F}_n\}_n$.

Definition 1 (Natural Property [RR 1997])

Let Γ be a complexity class. A combinatorial property $\mathcal{P}$ is Γ-natural if there is a combinatorial property $\mathcal{P}^* \subset \mathcal{P}$ such that

1. Constructive: function $\mathcal{P}_n^*(f)$ computable in Γ
2. Large: $\dfrac{|\mathcal{P}_n^*|}{|\mathcal{F}_n|} \geq \dfrac{1}{2^{O(n)}}$.

- If $\Gamma = \mathrm{P}$ then we simply say that $\mathcal{P}$ is natural.
- $\mathcal{P}^*$ is called core combinatorial property of $\mathcal{P}$

Natural Proofs

Definition 2 (Natural Proofs [RR 1997])

Let Γ and Λ be complexity classes (Λ non-uniform). A combinatorial property $\mathcal{P}$ is a Γ-natural proof for Λ if

1. $\mathcal{P}$ is Γ-natural
2. Useful: for any sequence of functions $f \in \mathcal{P}$, we have $f \notin \Lambda$

Natural Proofs

Definition 2 (Natural Proofs **[RR 1997]**)

Let Γ and Λ be complexity classes (Λ non-uniform). A combinatorial property $\mathcal{P}$ is a Γ-natural proof for Λ if

1. $\mathcal{P}$ is Γ-natural
2. Useful: for any sequence of functions $f \in \mathcal{P}$, we have $f \notin \Lambda$

- combinatorial property useful against Λ if any function having property is not in Λ

Natural Proofs

Definition 2 (Natural Proofs **[RR 1997]**)

Let Γ and Λ be complexity classes (Λ non-uniform). A combinatorial property $\mathcal{P}$ is a Γ-natural proof for Λ if

1. $\mathcal{P}$ is Γ-natural
2. Useful: for any sequence of functions $f \in \mathcal{P}$, we have $f \notin \Lambda$

- Standard lower bound argument for Λ:
    1. Define combinatorial property $\mathcal{P}$
    2. Prove $\mathcal{P}$ useful against Λ
    3. Construct family of functions $f = \{f_n\}$ and prove $f \in \mathcal{P}$

Natural Proofs

Definition 2 (Natural Proofs **[RR 1997]**)

Let Γ and Λ be complexity classes (Λ non-uniform). A combinatorial property $\mathcal{P}$ is a Γ-natural proof for Λ if

1. $\mathcal{P}$ is Γ-natural
2. Useful: for any sequence of functions $f \in \mathcal{P}$, we have $f \notin \Lambda$

- Standard lower bound argument for Λ:
  1. Define combinatorial property $\mathcal{P}$
  2. Prove $\mathcal{P}$ useful against Λ
  3. Construct family of functions $f = \{f_n\}$ and prove $f \in \mathcal{P}$
- A natural lower bound for Λ is a standard lower bound argument which uses a natural property $\mathcal{P}$

Example

OWFs against circuits

Definition 3

A string function $f : \{0,1\}^* \to \{0,1\}^*$ is a one-way function against SIZE(s) if:

1. Easy to compute: f is poly-time computable
2. Hard to invert: for every circuit family $C \in$ SIZE(s)

$$\Pr_{x \in \{0,1\}^n}[C_n(f_n(x)) \in f_n^{-1}(x)] < 1/s(n)$$

OWFs against circuits

Definition 3

A string function $f : \{0,1\}^* \to \{0,1\}^*$ is a one-way function against SIZE(s) if:

1. Easy to compute: f is poly-time computable
2. Hard to invert: for every circuit family $C \in$ SIZE(s)

$$\Pr_{x \in \{0,1\}^n}[C_n(f_n(x)) \in f_n^{-1}(x)] < 1/s(n)$$

Theorem 4 (HILL 1999)

If there is a OWF against SIZE(s), then there is a PRG G of stretch $\ell(n) = 2n$ against SIZE(s). That is, $G_n : \{0,1\}^n \to \{0,1\}^{2n}$ such that for all $C \in$ SIZE(s)

$$|\Pr[C_n(G(U_n)) = 1] - \Pr[C_n(U_{2n}) = 1]| < 1/s(n)$$

Natural Proof Theorem

Theorem 5 (Natural Proofs [RR 1997])

If there is $\varepsilon > 0$ and a OWF against SIZE(2^{n^ε}), then there is no natural proof for P$_{/poly}$.

Natural Proof Theorem

Theorem 5 (Natural Proofs **[RR 1997]**)

If there is $\varepsilon > 0$ and a OWF against SIZE$(2^{n^{\varepsilon}})$, then there is no natural proof for $P_{/poly}$.

- General theorem deals with Γ and Λ.

Natural Proof Theorem

Theorem 5 (Natural Proofs **[RR 1997]**)

If there is $\varepsilon > 0$ and a OWF against SIZE(2^{n^ε}), then there is no natural proof for $P_{/poly}$.

- **Idea:** natural property $\mathcal{P}$ can efficiently distinguish between pseudorandom functions from truly random functions
- But crypto assumption implies existence of PRGs

Proof of Natural Proof Theorem

- From Theorem 9, let G be our PRG with stretch $\ell(k) = 2k$. Think of $G_k : \{0,1\}^k \to \{0,1\}^k \times \{0,1\}^k$

$$G_k(x) = (y_0, y_1) =: (G_{k0}(x), G_{k1}(x))$$

Proof of Natural Proof Theorem

- From Theorem 9, let G be our PRG with stretch $\ell(k) = 2k$. Think of $G_k : \{0,1\}^k \to \{0,1\}^k \times \{0,1\}^k$
- From G, construct a pseudorandom set of functions in $\mathcal{F}_n$
- Construction (board): let $n = k^\alpha$ for some $\alpha > 0$ (TBD later).

$$F : \{0,1\}^k \to \{0,1\}^{2^n} \simeq \mathcal{F}_n$$

such that $f_z := F(z)$ yields function in $\mathcal{F}_n$

Proof of Natural Proof Theorem

- From Theorem 9, let G be our PRG with stretch $\ell(k) = 2k$. Think of $G_k : \{0,1\}^k \to \{0,1\}^k \times \{0,1\}^k$
- From G, construct a pseudorandom set of functions in $\mathcal{F}_n$
- Construction (board): let $n = k^\alpha$ for some $\alpha > 0$ (TBD later).

$$F : \{0,1\}^k \to \{0,1\}^{2^n} \simeq \mathcal{F}_n$$

  such that $f_z := F(z)$ yields function in $\mathcal{F}_n$
- Given $z \in \{0,1\}^k$ and $x \in \{0,1\}^n$, can compute $f_z(x)$ in $n \cdot \text{poly}(k)$ time

$$\{f_{z(k)}\} \in \mathsf{P}_{/poly}$$

Proof of Natural Proof Theorem

- If $\mathcal{P}$ is a natural proof for $\mathsf{P}_{/poly}$, then:
  1. Useful: for family $z := \{z^{(k)}\}_k$, family of functions $f := \{f_z\} \notin \mathsf{P}_{/poly}$
  2. Constructive: $f_{z^{(k)}} \in \mathcal{P}_n$ can be computed in poly-time
  3. Large: $\frac{|\mathcal{P}_n|}{|\mathcal{F}_n|} \geq 1/2^{O(n)}$

Proof of Natural Proof Theorem

- If $\mathcal{P}$ is a natural proof for $\mathsf{P}_{/poly}$, then:
  1. Useful: for family $z := \{z^{(k)}\}_k$, family of functions $f := \{f_z\} \notin \mathsf{P}_{/poly}$
  2. Constructive: $f_{z^{(k)}} \in \mathcal{P}_n$ can be computed in poly-time
  3. Large: $\frac{|\mathcal{P}_n|}{|\mathcal{F}_n|} \geq 1/2^{O(n)}$

  - Above and Proposition 2 from Lecture 6 imply that there is circuit $C \in \mathsf{SIZE}(N^c) = \mathsf{SIZE}(2^{ck^\alpha})$ such that

$$|\Pr[C(F(U_k)) = 1] - \Pr[C(U_N) = 1]| \geq 1/2^{O(n)}$$

Conclusion

- To prove circuit lower bounds (bypassing issue of OWFs) we must either
  - violate largeness: find property specific to few hard functions (not by random functions)
  - violate constructivity: identify feature of hard functions that cannot be computed efficiently

Conclusion

- To prove circuit lower bounds (bypassing issue of OWFs) we must either
  - violate largeness: find property specific to few hard functions (not by random functions)
  - violate constructivity: identify feature of hard functions that cannot be computed efficiently
- Are there examples of non-natural proofs?
  - Geometric Complexity Theory [Mulmuley Sohoni 2001]

    Symmetries of Determinant and Permanent characterize them!

    Violates largeness, approach is highly sophisticated.

References I

Arora, Sanjeev and Barak, Boaz (2009)
Computational Complexity, A Modern Approach — Chapters 9, 23
Cambridge University Press

Razborov, A. and Rudich, S. (1997)
Natural Proofs
Journal of Computer and System Sciences