6.841: Advanced Complexity Theory Fall 2012

Lecture 6 — 25th September, 2012

Prof. Dana Moshkovitz *Scribe: Cheung Wang Chi*

1 Overview

In the last two lectures we proved two results on circuit lower bounds, namely $PARITY \notin AC^0$, and that computing $CLIQUE_{k,n}$ requires superpolynomial size monotonic circuit. Recalling that relativizing proof technique is not sufficient for proving $P \neq NP$, one might wonder if there is also a limitation for proving circuit lower bound by those combinatorial techniques. Indeed, in this lecture, we are going to show that if a proof technique follows the "natural proof" paradigm [2], then such technique could not separate NP from $SIZE(n^k)$.

2 The Natural Proof Paradigm

Suppose we have a proof for $f \notin C$ (e.g. $SAT \notin SIZE(n^k)$), where C is a class of circuits. Often, the proof goes by showing that f does not satisfy some property $\mathcal{P}$ while every language in C does. Now, we say that a proof is a *natural proof* if it has the following three attributes:

1. Usefulness: It shows that $f \notin P$, but $C \subset \mathcal{P}$, where $\mathcal{P}$ is a property/predicate
2. Constructivity: Given $g : \{0,1\}^n \to \{0,1\}$, we can decide whether g has property $\mathcal{P}$ in $2^{O(n)}$ time, i.e. in time polynomial of size of the truth table of g.
3. Largeness: At least $1/n$ of all possible functions $g : \{0,1\}^n \to \{0,1\}$ (there are 2^{2^n} of them) are outside $\mathcal{P}$

Here are two examples to illustrate the definition of a natural proof:

Example 1: $PARITY \notin AC^0$ Recall that we proved this result by using the property

$$\mathcal{P}' = \text{If we randomly restrict all but } n^\epsilon \text{ variables, then the function can be computed by a polysize CNF/DNF with high probability}$$

It could be shown that $\mathcal{P}'$ has the three attributes of a natural proof.

On the other hand, the result could also be proved by the following property

$$\mathcal{P}'' = \text{If we randomly restrict all but } n^\epsilon \text{ variables, then the function is constant with high probability}$$

This proof goes by showing that $AC^0 \subset \mathcal{P}''$, but $PARITY \notin \mathcal{P}''$. Thus, $\mathcal{P}''$ has the Usefulness Attribute. $\mathcal{P}''$ also has the Constructivity Attribute, since for a function g, we can enumerate all

possible restrictions and all possible ways of setting the remaining variables in $2^{O(n)}$ time. Lastly, it has the Largeness Attribute, as a random boolean function does not have property $\mathcal{P}''$ with high property.

Example 2: Monotone Circuit Lower Bound for $CLIQUE_{k,n}$ Although its proof has the Usefulness and Constructivity Attributes, it does not have the Largeness Attribute, since the proof only concerns monotone circuits.

3 A Theorem of Razborov and Rudich

Before stating the theorem, we would like to first define one-way function (OWF) and pseudorandom function family (PRFF), which originate from cryptography, but we are utilizing these concepts to prove the result in complexity. Intuitively, an OWF is a function that is easy to compute, but computationally hard to invert, i.e. hard to find the preimage given the image. Moreover, it is even computationally hard to guess the inverse correctly with reasonable probability.

Definition A function f is a *one-way function* if

- Given x, $f(x)$ can be computed in poly($|x|$) time.
- For all probabilistic polynomial time algorithms A, we have

$$\Pr_{x \in_U \{0,1\}^n}[f(A(f(x))) = f(x)] = \frac{1}{n^{\omega(1)}}.$$

Next, we define a pseudorandom function family (PRFF). Intuitively, a PRFF is a family of Boolean functions that is computationally indistinguishable from a random Boolean function.

Definition A *pseudorandom function family* is a set of functions $\{f_s : \{0,1\}^m \to \{0,1\}\}_{s \in \{0,1\}^m}$ such that

- Given $s, x \in \{0,1\}^m$, we can compute $f_s(x)$ in poly(m) time.
- For any probabilistic 2^{m^ϵ} time algorithm A, where ϵ is an absolute constant, we have

$$\left| \Pr_{s \in_U \{0,1\}^m}[A^{f_s}(1^m) = 1] - \Pr_{f \text{u.a.r.}}[A^f(1^m) = 1] \right| < \frac{1}{m^{\omega(1)}}.$$

  where A^f denotes the algorithm A with oracle access to f.

Note that a PRFF has 2^m functions, which is a very small number compared to the total number of 2^{2^m} possible Boolean functions.

Now we are ready to state the theorem of Razborov and Rudich:

Theorem 1 (Razborov - Rudich, 1994)**.** *Assuming that one way function exists, no natural proof (i.e. a proof that satisfies the three attributes) can show $NP \subsetneq SIZE(n^k)$.*

Before proving this theorem, we remark that the premise is strong, since the existence of OWF implies $P \neq NP$. However, the existence of OWF is widely believed by the complexity and cryptography community. We also note that the existence of OWF implies the existence of problems in NP that are hard on average. Lastly, to prove the theorem, we recall the following result:

Theorem 2 (GGM, HILL)**.** *If one way function exists, then pseudorandom function family exists.*

Proof. (of Razborov-Rudich Theorem) Assume for contradiction that there existed such a property $\mathcal{P}$ that is natural. Let $\{f_s\}_{s\in\{0,1\}^m}$ be a PRFF, which exists by [4], assuming the existence of OWF. Define $n = m^{\epsilon/2}$, where ϵ is the absolute constant in the definition of PRFF. Also define, for all $s \in \{0,1\}^m$ and $x \in \{0,1\}^n$, the padded function

$$f_s^*(x) = f_s(x0^{m-n}).$$

Now, by the Largeness Attribute, for a random $f : \{0,1\}^n \to \{0,1\}$, we have

$$\Pr_{f u.a.r}[f \text{ has property } \mathcal{P}] \leq 1 - \frac{1}{n}.$$

On the other hand, we have

$$\Pr_{s\in_U\{0,1\}^m}[f_s^* \text{ has property } \mathcal{P}] \geq \Pr_{s\in_U\{0,1\}^m}[f_s^* \in SIZE(n^k)] = 1$$

where the first inequality is by the Usefulness Attribute. The second equality is by the definition of PRFF that f_s, and hence f_s^*, can be computed in $m^{O(1)} = n^{O(1)}$ time. This implies that there exists a size $n^{O(1)}$ circuit that computes f_s^*; we could construct a polynomial size circuit that imitates the computation of f_s^*.

However, it contradicts the definition of a PRFF, since testing if a function has property $\mathcal{P}$ is a probabilistic 2^{m^ϵ} time algorithms that distinguishes f_s from a random boolean function f with probability $\geq 1/n$. Indeed, testing $\mathcal{P}$ can be done in 2^{m^ϵ} time, since by the Constructivity Attribute, for all $g : \{0,1\}^n \to \{0,1\}$, we can determine whether g has property $\mathcal{P}$ in time $2^{O(n)} \leq 2^{m^\epsilon}$. □

4 Concluding Thoughts

We have shown that no natural proof can prove that $NP \subsetneq SIZE(n^k)$, which shows us yet another barrier to separating P vs NP or NP vs $P/poly$, in addition to the barrier on the relativization technique. Nevertheless, it does not mean that the development of complexity theory is in vain. In fact, there are proofs that are non-natural. An example would be the proof of $\Sigma_3 \subsetneq SIZE(n^k)$ in previous lecture.

Moreover, there are proofs that are both non-natural and non-relativizing. The a proof of from Santhanam [5] is one such. (This can be found in Theorem 23.8 (Page 504 – 505) in the text book). Apart from the relativization and natural proof barriers, there is also a barrier on algebraization [1]. Nevertheless, the recent proof of $NEXP \subsetneq ACC^0$ by Ryan Williams [6] is non-relativizing, non-natural and non-algebraizing.

References

[1] S. Aaronson, A. Wigderson, *Algebrization: A New Barrier in Complexity Theory*, Proc. ACM STOC, 731–740, 2008.

[2] A. A. Razborov, S. Rudich, *Natural proofs*, Proc. ACM STOC, 204-213, 1994.

[3] O. Goldreich, S. Goldwasser, S. Micali, *H*ow to construct random functions, Journal of the ACM (JACM), 33(4): 792-807, 1986.

[4] J. Hastad, R. Impagliazzo, L. A. Levin, M. Luby, *A Pseudorandom Generator from any One-way Function*, SIAM Journal on Computing, 28(4): 1364–1396, 1999.

[5] R. Santhanam, *Circuit lower bounds for Merlin-Arthur classes*, Proc. ACM STOC, 275–283, 2007.

[6] R. Williams, *Non-uniform ACC Circuit Lower Bounds*, IEEE Conference on Computational Complexity, 115–125, 2011