| | |
|---|---|
| **CS 388T: Advanced Complexity Theory** | Spring 2020 |
| Natural Proofs | |
| *Prof. Dana Moshkovitz* | *Scribe: Maruth Goyal* |

# 1 Overview

Complexity theorists have long been working on proving relations between various complexity classes. Their proofs would often treat Turing Machines as black boxes. However, they seemed to be unable to prove equality or separation for $\mathsf{NP} \not\subset \mathsf{P}$. A reason for this was found with Baker, Gill, and Solovay's Relativization barrier [BGS75], which should any proof for such a separation must be non-relativizing. i.e., it must not hold with respect to arbitrary oracles. Hence, researchers turned to circuits as a way of analyzing various classes by considering more explicit constructions. This begs the question, is their a similar barrier for separating $\mathsf{NP}$ from $\mathsf{P}$/poly?

To separate a function $f$ from some circuit complexity class $\mathcal{C}$, mathematicians often consider some larger property of $f$, and then separate that property from $\mathcal{C}$. For instance, in the case of PARITY [FSS84], we observed it cannot be simplified even under arbitrary random restrictions, while $\mathsf{AC}^0$ functions can be. While this seemed like a powerful proof technique, in 1997 Razborov and Rudich [RR] showed that to separate $\mathsf{NP}$ from $\mathsf{P}$/poly, there is a large classification of properties which cannot be the basis for such a proof. They called these properties "natural properties".

# 2 Natural Properties

**Definition 1.** *A property $\mathcal{P}$ is said to be* natural *if:*

1. Useful*: $\forall g \in \mathcal{C}. g \notin \mathcal{P}$ but $f \in \mathcal{P}$*
2. Constructivity*: Given $g : \{0,1\}^n \to \{0,1\}$ can check if $g \in \mathcal{P}$ in time $2^{O(n)}$.*
3. Largeness*: At least $\dfrac{1}{n}$ fraction of $g : \{0,1\}^n \to \{0,1\}$ have the property.*

For instance consider the property $\mathcal{P}(f) = f$ simplifies under random restrictions. Observe $\mathcal{P}$ is useful, since this hold for circuits in $\mathsf{AC}^0$, but our proof showed PARITY $\notin \mathcal{P}$. It is constructive, since we can simplify check every single random restriction and see if $f$ simplifies in $2^{O(n)}$ time. Finally it satisfies largeness, since an arbitrary boolean function does not simplify, with high probability (consider functions that are sensitive to $s(n)$ bits on $n$-length inputs).

Razborov and Rudich then proved the following theorem:

**Theorem 1.** ([RR], Sipser 1980s)*: If one-way functions exist, no natural property can be used to show $\mathsf{NP} \not\subseteq \mathsf{P}$/poly.*

## 3 One Way Functions

**Definition 2.** *A function $f : \{0,1\}^n \to \{0,1\}$ is said to be a one-way function (OWF) if it satisfies the following:*

1. *Given input $x$, $f(x)$ can be computed in $\text{poly}(|x|)$ time.*
2. *For any randomized algorithm $A$,*

$$\underset{x\in\{0,1\}^n}{\mathbb{P}}[f(A(f(x))) = f(x)] = \frac{1}{n^{\omega(1)}}$$

**Definition 3.** *A psuedorandom function family (PRFF) is a set $\{f_s : \{0,1\}^m \to \{0,1\}\}_{s\in\{0,1\}^m}$ such that:*

1. *Given $s, x$ we can compute $f_s(x)$ in $\text{poly}(m)$ time.*
2. *For a fixed constant $\varepsilon$, and any probabilistic algorithm $A$ running in $2^{m^\varepsilon}$ time,*

$$\left| \underset{s\in\{0,1\}^m}{\mathbb{P}}[A^{f_s}(1^m) = 1] - \underset{s\in\{0,1\}^m}{\mathbb{P}}[A^{f}(1^m) = 1] \right| \leq \frac{1}{n^{\omega(1)}}$$

That is, $f_s$ is indistinguishable from a random oracle.

## 4 Razborov Rudich

We utilize the following theorem in our proof:

**Theorem 2.** [GGM19, HILL99] *If one way functions exist, then psuedorandom function families exist.*

The proof will proceed by contradiction. We will assume a natural property $\mathcal{P}$ exists separating $\mathsf{NP}$ from $\mathsf{P}$/poly. We will then construct a psuedorandom function $f{*}_s$ which is in $\mathcal{P}$. This will let us distinguish random functions from functions in our psuedorandom function family efficiently, which contradicts the definition of PRFFs.

*Proof of Theorem 1.* Suppose there exists a natural property $\mathcal{P}$ separating $\mathsf{NP}$ from $\mathsf{SIZE}(n^k)$. Furthermore, suppose that one-way functions exist. Then from theorem 2, we are guaranteed a psuedorandom function family $\{f_s : \{0,1\}^m \to \{0,1\}\}_{s\in\{0,1\}^m}$. Suppose $\varepsilon$ is the fixed constant from the definition of PRFFs, such that for any probabilistic algorithm $A$ running in $2^{m^\varepsilon}$ time, $A$ cannot distinguish between a random oracle and $f_s$. Then, define $n = m^{\varepsilon/2}$. Finally, for any random function $g : \{0,1\}^m \to \{0,1\}$ define, $h : \{0,1\}^n \to \{0,1\}$:

$$h(x) = g(x \circ 0^{m-n})$$

Now consider the following cases:

1. $g$ is some random boolean function. Then, by the largeness attribute of $\mathcal{P}$, we have

$$\mathbb{P}[g \text{ has property } \mathcal{P}] \leq 1 - \frac{1}{n}$$

2. $g = f_s$ for some $s$. Then, by definition of a PRFF, $f_s$ can be computed in polynomial time and hence has a poly-size circuit. Hence, since $\mathcal{P}$ is useful, we just consider the probability that $g \in \mathsf{SIZE}(n^k)$. Thus

$$\mathbb{P}[g \text{ has property } \mathcal{P}] \geq \mathbb{P}[g \in \mathsf{SIZE}(n^k)] = 1$$

Notice that this gives us the ability to distinguish between a random function $g$, and $f_s$ with probability $\geq 1/n$. More importantly, however, we distinguish efficiently since $\mathcal{P}(g)$ can be computed in time $2^{O(n)}$. But, $n = m^{\varepsilon/2}$ by assumption. Thus, we are able to distinguish in time $2^{O(m^{\varepsilon/2})}$. This contradicts the definition of PRFFs, that no algorithm running in time $2^{m^{\varepsilon}}$ can distinguish them from random functions with high probability. Thus, no such $\mathcal{P}$ can exist. $\square$

# References


[BGS75] Theodore Baker, John Gill, and Robert Solovay. Relativizations of the p=?np question. *SIAM Journal on computing*, 4(4):431–442, 1975.

[FSS84] Merrick Furst, James B Saxe, and Michael Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical systems theory*, 17(1):13–27, 1984.

[GGM19] Oded Goldreich, Shafi Goldwasser, and Silvio Micali. How to construct random functions. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 241–264. 2019.

[HILL99] Johan Håstad, Russell Impagliazzo, Leonid A Levin, and Michael Luby. A pseudorandom generator from any one-way function. *SIAM Journal on Computing*, 28(4):1364–1396, 1999.

[RR] Alexander A Razborov and Steven Rudich. Natural proofs.