CS388T Project:
Karp-Lipton Style Theorems

Maruth Goyal

UT Austin

Spring 2020
Until about 70s, primary way to show lower bounds was by considering Turing Machines as black boxes.
Until about 70s, primary way to show lower bounds was by considering Turing Machines as black boxes.

Until about 70s, primary way to show lower bounds was by considering Turing Machines as black boxes.


This created the need for a computation model which is more "explicit"
Until about 70s, primary way to show lower bounds was by considering Turing Machines as black boxes.


This created the need for a computation model which is more "explicit".

Enter: circuits
Circuits act as a low-level model of computation, everything is at the bit level.
Circuits

1. Circuits act as a low-level model of computation, everything is at the bit level
2. They let us be more explicit about our constructions
Circuits

1. Circuits act as a low-level model of computation, everything is at the bit level
2. They let us be more explicit about our constructions
3. Have proven to be very useful method for analyzing computational complexity.
Many big results over the years, $\text{PARITY} \not\in \text{AC}^0$, $\text{NEXP} \not\subset \text{ACC}^0$, …
Many big results over the years, $\text{PARITY} \notin \text{AC}^0$, $\text{NEXP} \notin \text{ACC}^0$, …

We focus on circuit lower bounds for complexity classes
Many big results over the years, \( \text{PARITY} \notin \text{AC}^0, \text{NEXP} \notin \text{ACC}^0, \ldots \)

We focus on circuit lower bounds for complexity classes

In particular, the role of \textbf{Karp-Lipton} style theorems in proving these bounds
Recall:

**Theorem**

[Karp and Lipton, 1980] If $\text{NP} \subseteq \text{P/poly}$ then $\Pi_2 = \Sigma_2$, and thus $\text{PH} = \Sigma_2$

**Proof.**

Simulate $\forall y \exists z \varphi(x, y, z)$ in $\Sigma_2$ by guessing the poly-size circuit to generate witnesses for SAT, i.e. $\exists C \forall y \varphi(x, y, C(\varphi, x, y))$. 

□
From this, we derived Kannan’s theorem:

**Theorem**

\[ \text{[Kannan, 1982]} \quad \Sigma_2 \not\subset \text{SIZE}(n^k) \text{ for all } k > 0 \]

**Proof.**

If \( \text{NP} \not\subset \text{P/poly} \), we are done. Otherwise \( \text{PH} = \Sigma_2 \), thus the \( \Sigma_3 \) language \( L \not\in \text{SIZE}(n^k) \) is in \( \Sigma_2 \).
General framework: If \( C \in \text{P/poly} \), the a ”big” class collapses down to \( C \), but PH doesn’t have poly-size circuits
Karp-Lipton Theorems

1. General framework: If $C \in \text{P/poly}$, the a "big" class collapses down to $C$, but PH doesn’t have poly-size circuits

2. Turns out, very useful framework. Used to prove
   1. $\text{PP} \not\subset \text{SIZE}(n^k)$ [Vinodchandran, 2005]
   2. $\text{PP}$ does not have poly-size quantum circuits, even with quantum advice [Aaronson, 2006]
   3. Promise $\text{−MA} \not\subset \text{SIZE}(n^k)$ [Santhanam, 2009]
   4. $\text{MA}_{\text{EXP}} \not\subset \text{P/poly}$
   5. . . .
Karp-Lipton Theorems

1. General framework: If $C \in P/poly$, the a ”big” class collapses down to $C$, but PH doesn’t have poly-size circuits

2. Turns out, very useful framework. Used to prove
   1. $PP \not\subset \text{SIZE}(n^k)$ [Vinodchandran, 2005]
   2. PP does not have poly-size quantum circuits, even with quantum advice [Aaronson, 2006]
   3. Promise – $MA \not\subset \text{SIZE}(n^k)$ [Santhanam, 2009]
   4. $MA_{EXP} \not\subset P/poly$
   5. …

3. Even ”unavoidable” in a sense

Theorem

$$P^{NP} \not\subset \text{SIZE}(n^k) \iff NP \subset P/poly \implies PH = i.o. - P^{NP}$$

[Chen et al., 2019]
# Table of Contents

1. Introduction

2. Interactive Proofs

3. PP and more

4. Lower bounds for $P^{NP}$

5. Algebraization
This framework has been used to prove a bunch of results for MA and its friends.

**Theorem**

If \( \text{NP} \subseteq \text{P/poly} \) then \( \text{AM} = \text{MA} \) [Arvind et al., 1995]

**Proof Sketch**

A formulation for AM is \( x \in L \implies \Pr[\exists y \ M(x, y, z) = 1] \geq 2/3 \), and similarly for MA, \( x \in L \implies \exists y \ \Pr[M(x, y, z) = 1] \geq 2/3 \). Expression inside brackets AM is essentially an NP language. Reduce to SAT, replace condition with guessed poly-size circuit. et voila, MA.
Results about MA

**Theorem**

Promise – MA \( \not\subset \text{SIZE}(n^k) \) [Santhanam, 2009]

**Lemma**

MA/O(n) \( \not\subset \text{SIZE}(n^k) \) \( \implies \) Promise – MA \( \not\subset \text{SIZE}(n^k) \)
Results about MA

**Theorem**

Promise – MA $\not\subset$ SIZE($n^k$) [Santhanam, 2009]

**Lemma**

MA/O($n$) $\not\subset$ SIZE($n^k$) $\implies$ Promise – MA $\not\subset$ SIZE($n^k$)

**Proof Sketch**

Pick language $L$ and MA machine $M$ that takes $cn$ advice that solves it. Define promise problem $X$. Promise not satisfied if $|x| \neq (c + 1)n$ for some $n$. $U_{YES}$ if $M$ outputs yes with first $n$ bits as input, and next $cn$ bits as advice, otherwise $U_{NO}$. If poly size circuits $\{C_n\}$ for $X$, then construct poly-size circuit for $L$ by padding $x$ with correct advice and passing to $\{C_n\}$. Contradiction.
Results about PP

Theorem

\[ \text{PP} \nsubseteq \text{SIZE}(n^k) \ [\text{Vinodchandran, 2005}] \]

Proof.

If \( \text{PP} \nsubseteq \text{P/poly} \), done. Otherwise \( \text{PP} \subseteq \text{P/poly} \implies \text{PP} \subseteq \text{MA} \). From Toda’s theorem, \( \text{PH} \subseteq \text{BP} \cdot \text{PP} \), thus \( \text{PH} \subseteq \text{BP} \cdot \text{MA} = \text{AM} \). But \( \text{AM} = \text{MA} \) under assumption. So \( \text{PH} = \text{MA} \), but \( \text{PH} \nsubseteq \text{SIZE}(n^k) \). Thus, \( \text{MA} \nsubseteq \text{SIZE}(n^k) \). But \( \text{MA} \subseteq \text{PP} \), so \( \text{PP} \nsubseteq \text{SIZE}(n^k) \).
Aaronson’s Proof

1 Vinodachandran’s proof kind of unsatisfactory.

Aaronson did demonstrate Vinodachandran’s proof does not relativize, by constructing an oracle $A$ such that $\text{PP}^A \subseteq \text{SIZE}_A(n^k)$. 
Aaronson’s Proof

1. Vinodachandran’s proof kind of unsatisfactory.
2. Aaronson’s proof constructs explicit languages to show $P^{PP}$ doesn’t have poly size [quantum] circuits.

Remarkably, language for classical circuits extends almost directly to quantum equivalent.

Finish proof with "Quantum Karp-Lipton" theorem

Theorem

If $PP \subseteq BQP/\text{poly}$ then $QCMA = PP$. Likewise, if $PP \subseteq BQP/\text{qpoly}$ then $CH = MA[Aaronson, 2006]$.

Aaronson did demonstrate Vinodachandran’s proof does not relativize, by constructing an oracle $A$ such that $PP^A \subseteq \text{SIZE}^A(n^k)$.
Aaronson’s Proof

1. Vinodachandran’s proof kind of unsatisfactory.
2. Aaronson’s proof constructs explicit languages to show $P^{PP}$ doesn’t have poly size [quantum] circuits.
3. Remarkably, language for classical circuits extends almost directly to quantum equivalent.
Aaronson’s Proof

1. Vinodachandran’s proof kind of unsatisfactory.
2. Aaronson’s proof constructs explicit languages to show $P^{PP}$ doesn’t have poly size [quantum] circuits.
3. Remarkably, language for classical circuits extends almost directly to quantum equivalent.
4. Finish proof with ”Quantum Karp-Lipton” theorem

Theorem

If $PP \subset BQP/poly$ then $QCMA = PP$. Likewise, if $PP \subset BQP/qpoly$ then $CH = MA[Aaronson, 2006]$. 
Aaronson’s Proof

1. Vinodachandran’s proof kind of unsatisfactory.
2. Aaronson’s proof constructs explicit languages to show $P^{PP}$ doesn’t have poly size [quantum] circuits.
3. Remarkably, language for classical circuits extends almost directly to quantum equivalent.
4. Finish proof with ”Quantum Karp-Lipton” theorem

Theorem

If $PP \subseteq BQP/poly$ then $QCMA = PP$. Likewise, if $PP \subseteq BQP/qpoly$ then $CH = MA[Aaronson, 2006]$. 

5. Aaronson did demonstrate Vinodachandran’s proof does not relativize, by constructing an oracle $A$ such that $PP^A \subseteq SIZE^A(n^k)$. 
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Introduction</td>
</tr>
<tr>
<td>2</td>
<td>Interactive Proofs</td>
</tr>
<tr>
<td>3</td>
<td>PP and more</td>
</tr>
<tr>
<td>4</td>
<td>Lower bounds for $P^{NP}$</td>
</tr>
<tr>
<td>5</td>
<td>Algebraization</td>
</tr>
</tbody>
</table>
This must all be a big co-incidence
1. This must all be a big co-incidence
2. There is certainly a way to side-step these K-L theorems right? A combinatorial argument, perhaps?
Wrong
Lower bounds for $P^{NP}$

**Theorem**

$$P^{NP} \not\subset SIZE(n^k) \iff NP \subset P/poly \implies PH = \text{i.o.} - P^{NP}$$

[Chen et al., 2019]

1. $L \in \text{i.o.} - C$ means there’s some language $L' \in C$ for which there are infinitely many $n$ such that $L_n = L'_n$
Lower bounds for $P^{NP}$

**Theorem**

$P^{NP} \not\subset \text{SIZE}(n^k)$ iff $NP \subset P/poly \implies PH = \text{i.o. } - P^{NP}/_n$

[Chen et al., 2019]

1. $L \in \text{i.o. } - C$ means there’s some language $L' \in C$ for which there are infinitely many $n$ such that $L_n = L'_n$

2. $\text{i.o. } - P^{NP}/_n$: Set of languages decidable in P with oracle access to NP, given $n$ bits of advice, infinitely often.
Theorem

\[ \text{P}^\text{NP} \not\subset \text{SIZE}(n^k) \iff \text{NP} \subset \text{P}/\text{poly} \implies \text{PH} = \text{i.o.} - \text{P}^\text{NP} \]

[Chen et al., 2019]
Lower bounds for $P^{NP}$

**Theorem**

$P^{NP} \not\subset\text{SIZE}(n^k)$ iff $NP \subset P/\text{poly} \implies PH = i.o. - P^{NP}$

[Chen et al., 2019]

**Lemma**

Suppose there is a $k$ such that for all functions $f$ in $FP^{NP}$, $f(x)$ has circuit complexity at most $|x|^k$ for all but finitely many $x$, then $P^{NP} \subseteq \Sigma_3 \text{TIME}[n^{O(k)}]$. 
Lower bounds for $\text{P}^{\text{NP}}$

**Theorem**

$\text{P}^{\text{NP}} \not\subset \text{SIZE}(n^k)$ iff $\text{NP} \subset \text{P}/\text{poly}$ $\implies \text{PH} = \text{i.o.} - \text{P}^{\text{NP}}$

[Chen et al., 2019]

**Lemma**

Suppose there is a $k$ such that for all functions $f$ in $\text{FP}^{\text{NP}}$, $f(x)$ has circuit complexity at most $|x|^k$ for all but finitely many $x$, then $\text{P}^{\text{NP}} \subseteq \Sigma_3 \text{TIME}[n^{O(k)}]$.

**Proof of Theorem**

Assume $\text{P}^{\text{NP}} \not\subset \text{SIZE}(n^k)$ and $\text{NP} \subset \text{P}/\text{poly}$. Then, $\Sigma_3 \text{TIME}[n^{O(k)}] \subseteq \text{SIZE}(n^k)$. However, by our first assumption we get $\text{P}^{\text{NP}} \not\subset \Sigma_3 \text{TIME}[n^{O(k)}]$.
Lower bounds for $P^{NP}$

**Theorem**

$$P^{NP} \not\subseteq \text{SIZE}(n^k) \iff \text{NP} \subset P/\text{poly} \implies \text{PH} = \text{i.o.} - P^{NP} / n$$

[Chen et al., 2019]

**Lemma**

Suppose there is a $k$ such that for all functions $f$ in $\text{FP}^{NP}$, $f(x)$ has circuit complexity at most $|x|^k$ for all but finitely many $x$, then $P^{NP} \subseteq \Sigma_3 \text{TIME}[n^{O(k)}]$.

**Proof of Theorem**

Assume $P^{NP} \not\subseteq \text{SIZE}(n^k)$ and $\text{NP} \subset P/\text{poly}$. Then, $\Sigma_3 \text{TIME}[n^{O(k)}] \subseteq \text{SIZE}(n^k)$. However, by our first assumption we get $P^{NP} \not\subseteq \Sigma_3 \text{TIME}[n^{O(k)}]$. Thus, by the contrapositive of the lemma, for all $k$ there is a function $B \in \text{FP}^{NP}$ with circuit complexity at least $|x|^k$ for infinitely many $x$. 
Lower bounds for $P^{NP}$

**Theorem**

\[ P^{NP} \not\subset \text{SIZE}(n^k) \iff \text{NP} \subset P/poly \implies PH = i.o. - P^{NP}_{/n} \]

[Chen et al., 2019]

**Proof of Theorem cont’d**

From [Köbler and Watanabe, 1998], PH collapses to $ZPP^{NP}$ under $\text{NP} \subset P/poly$. We derandomize $ZPP^{NP}$ in $i.o. - P^{NP}_{/n}$ by passing in the seed for our PRG (obtained from $B$) as advice, and using the NP oracle to answer the $ZPP^{NP}$ oracle queries.
Table of Contents

1 Introduction

2 Interactive Proofs

3 PP and more

4 Lower bounds for $P^{NP}$

5 Algebraization
KL-theorems seem to be pretty useful
KL-theorems seem to be pretty useful

Moreover, a lot of the proofs don't relativize, or naturalize
1. KL-theorems seem to be pretty useful
2. Moreover, a lot of the proofs don't relativize, or naturalize
3. Life seems pretty great, right?
WRONG
Aaronson and Wigderson [Aaronson and Wigderson, 2009] introduced the Algebraization proof Barrier.
Aaronson and Wigderson [Aaronson and Wigderson, 2009] introduced the Algebraization proof Barrier.

**Definition**

A separation $\mathcal{C} \not\subset \mathcal{D}$ is said to algebraize if for all oracles $A$, and their "low-degree extensions" $\tilde{A}$, $\mathcal{C}^\tilde{A} \not\subset \mathcal{D}^A$.

They showed that any proof for NP $\not\subset$ P must be non-algebraizing, as well as for NP $\not\subset$ SIZE($n^k$).
Aaronson and Wigderson [Aaronson and Wigderson, 2009] introduced the Algebraization proof Barrier.

**Definition**
A separation $C \not\subset D$ is said to algebraize if for all oracles $A$, and their "low-degree extensions" $\tilde{A}$, $C^{\tilde{A}} \not\subset D^A$.

They showed that any proof for $\text{NP} \not\subset \text{P}$ must be non-algebraizing, as well as for $\text{NP} \not\subset \text{SIZE}(n^k)$.

Unfortunately, a lot of the proofs mentioned today, do algebraize
The following results algebraize: (non-exhaustive)

1. Promise $\neg MA \subsetneq SIZE(n^k)$
2. $\text{MA}_{\text{EXP}} \not\subset P/poly$
3. $\text{PP} \not\subset SIZE(n^k)$
4. ...
Still, given all the results seen today seems like KL-theorems are still a powerful framework for circuit lower bounds.
1. Still, given all the results seen today seems like KL-theorems are still a powerful framework for circuit lower bounds.

2. They might be a smaller part of an overall non-algebraizing proof for future results.
Still, given all the results seen today seems like KL-theorems are still a powerful framework for circuit lower bounds.

They might be a smaller part of an overall non-algebraizing proof for future results.

For the future, interesting if we can get even tighter collapses of PH (for instance, getting rid of the advice, or infinitely-often parts).
Still, given all the results seen today seems like KL-theorems are still a powerful framework for circuit lower bounds.

They might be a smaller part of an overall non-algebraizing proof for future results.

For the future, interesting if we can get even tighter collapses of PH (for instance, getting rid of the advice, or infinitely-often parts).

$P^{NP}$ seems "barely" above NP, can we get a similar equivalence for something just below $P^{NP}$?
Questions?
Thank You!
Oracles are subtle but not malicious.
In *21st Annual IEEE Conference on Computational Complexity (CCC'06)*, pages 15–pp. IEEE.

Algebrization: A new barrier in complexity theory.

If NP has polynomial-size circuits, then MA=AM.

Relativizations of the P=?NP question.

Relations and equivalences between circuit lower bounds and karp-lipton theorems.

