CS388T Project: Karp-Lipton Style Theorems

Maruth Goyal

UT Austin

Spring 2020

Table of Contents

1 Introduction

2 Interactive Proofs

3 PP and more

4 Lower bounds for P^{NP}

5 Algebraization

Introduction

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

Introduction

1. Until about 70s, primary way to show lower bounds was by considering Turing Machines as black boxes .
2. Baker, Gill, and Solovay [Baker et al., 1975] introduced the relativization barrier

Introduction

1. Until about 70s, primary way to show lower bounds was by considering Turing Machines as black boxes .
2. Baker, Gill, and Solovay [Baker et al., 1975] introduced the relativization barrier
3. This created the need for a computation model which is more "explicit"

Introduction

1. Until about 70s, primary way to show lower bounds was by considering Turing Machines as black boxes .
2. Baker, Gill, and Solovay [Baker et al., 1975] introduced the relativization barrier
3. This created the need for a computation model which is more "explicit"
4. Enter: circuits

Circuits

1. 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.

Circuits

1. Many big results over the years, PARITY $\notin$ AC^0, NEXP $\not\subset$ ACC^0, ...

Circuits

1. Many big results over the years, PARITY $\notin$ AC^0, NEXP $\not\subset$ ACC^0, ...
2. We focus on circuit lower bounds for complexity classes

Circuits

1. Many big results over the years, PARITY $\notin$ AC^0, NEXP $\not\subset$ ACC^0, ...
2. We focus on circuit lower bounds for complexity classes
3. In particular, the role of Karp-Lipton style theorems in proving these bounds

Karp-Lipton Theorem I

Recall:

Theorem

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

Proof.

Simulate $\forall y \exists z \varphi(x, y, z)$ in Σ_2 by guessing the poly-size circuit to generate witnesses for SAT, i.e $\exists C \forall y \varphi(x, y, C(\varphi, x, y))$. $\square$

Karp-Lipton Theorem II

From this, we derived Kannan's theorem:

Theorem

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

Proof.

If NP $\not\subset$ P/poly, we are done. Otherwise PH $= \Sigma_2$, thus the Σ_3 language $L \notin \mathsf{SIZE}(n^k)$ is in Σ_2. □

Karp-Lipton Theorems

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

Karp-Lipton Theorems

1. General framework: If $\mathcal{C} \in \mathsf{P}/\mathrm{poly}$, the a "big" class collapses down to $\mathcal{C}$, but PH doesn't have poly-size circuits
2. Turns out, very useful framework. Used to prove
   1. PP $\not\subset$ SIZE(n^k) [Vinodchandran, 2005]
   2. PP does not have poly-size quantum circuits, even with quantum advice [Aaronson, 2006]
   3. $\mathrm{Promise}-\mathsf{MA} \not\subset \mathsf{SIZE}(n^k)$ [Santhanam, 2009]
   4. $\mathsf{MA}_{\mathsf{EXP}} \not\subset \mathsf{P}/\mathrm{poly}$
   5. ...

Karp-Lipton Theorems

1. General framework: If $\mathcal{C} \in \mathsf{P}/\mathrm{poly}$, the a "big" class collapses down to $\mathcal{C}$, but PH doesn't have poly-size circuits
2. Turns out, very useful framework. Used to prove
    1. $\mathsf{PP} \not\subset \mathsf{SIZE}(n^k)$ [Vinodchandran, 2005]
    2. PP does not have poly-size quantum circuits, even with quantum advice [Aaronson, 2006]
    3. $\mathrm{Promise} - \mathsf{MA} \not\subset \mathsf{SIZE}(n^k)$ [Santhanam, 2009]
    4. $\mathsf{MA}_{\mathsf{EXP}} \not\subset \mathsf{P}/\mathrm{poly}$
    5. ...
3. Even "unavoidable" in a sense

Theorem

$\mathsf{P}^{\mathsf{NP}} \not\subset \mathsf{SIZE}(n^k)$ *iff* $\mathsf{NP} \subset \mathsf{P}/\mathrm{poly} \implies \mathsf{PH} = \mathrm{i.o.} - \mathsf{P}^{\mathsf{NP}}_{/n}$
[Chen et al., 2019]

Table of Contents

1. Introduction
2. Interactive Proofs
3. PP and more
4. Lower bounds for P^{NP}
5. Algebraization

Results about MA

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

Theorem

If $\mathsf{NP} \subseteq \mathsf{P}/\mathrm{poly}$ *then* $\mathsf{AM} = \mathsf{MA}$ *[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

$\text{Promise} - \mathsf{MA} \not\subset \mathsf{SIZE}(n^k)$ *[Santhanam, 2009]*

Lemma

$\mathsf{MA}/O(n) \not\subset \mathsf{SIZE}(n^k) \implies \text{Promise} - \mathsf{MA} \not\subset \mathsf{SIZE}(n^k)$

Results about MA

Theorem

$\text{Promise} - \mathsf{MA} \not\subset \mathsf{SIZE}(n^k)$ *[Santhanam, 2009]*

Lemma

$\mathsf{MA}/O(n) \not\subset \mathsf{SIZE}(n^k) \implies \text{Promise} - \mathsf{MA} \not\subset \mathsf{SIZE}(n^k)$

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.

Table of Contents

1 Introduction

2 Interactive Proofs

3 PP and more

4 Lower bounds for P^{NP}

5 Algebraization

Results about PP

Theorem

PP $\not\subset$ SIZE(n^k) *[Vinodchandran, 2005]*

Proof.

If PP $\not\subset \mathrm{P/poly}$, done. Otherwise PP $\subset \mathrm{P/poly} \implies$ PP $\subseteq$ MA. From Toda's theorem, PH $\subseteq$ BP $\cdot$ PP, thus PH $\subseteq$ BP $\cdot$ $MA = AM$. But AM $=$ MA under assumption. So PH $=$ MA, but PH $\not\subset$ SIZE(n^k). Thus, MA $\not\subset$ SIZE(n^k). But MA $\subset$ PP, so PP $\not\subset$ SIZE(n^k). $\square$

Aaronson's Proof

1. Vinodachandran's proof kind of unsatisfactory.

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.

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 $\mathsf{PP} \subset \mathsf{BQP}/\mathrm{poly}$ *then* $\mathsf{QCMA} = \mathsf{PP}$. *Likewise, if* $\mathsf{PP} \subset \mathsf{BQP}/\mathrm{qpoly}$ *then* $\mathsf{CH} = \mathsf{MA}$[*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 $\mathsf{PP} \subset \mathsf{BQP}/\mathrm{poly}$ *then* $\mathsf{QCMA} = \mathsf{PP}$*. Likewise, if* $\mathsf{PP} \subset \mathsf{BQP}/\mathrm{qpoly}$ *then* $\mathsf{CH} = \mathsf{MA}$*[Aaronson, 2006].*

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

Table of Contents

1 Introduction

2 Interactive Proofs

3 PP and more

4 Lower bounds for P^{NP}

5 Algebraization

Lower bounds for P^{NP}

1. This must all be a big co-incidence

Lower bounds for P^{NP}

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?

Lower bounds for P^{NP}

WRONG

Lower bounds for P^{NP}

Theorem

$\mathsf{P}^{\mathsf{NP}} \not\subset \mathsf{SIZE}(n^k)$ *iff* $\mathsf{NP} \subset \mathsf{P}/\mathrm{poly} \implies \mathsf{PH} = \mathrm{i.o.} - \mathsf{P}^{\mathsf{NP}}_{/n}$
[Chen et al., 2019]

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

Lower bounds for P^{NP}

Theorem

$\mathsf{P}^{\mathsf{NP}} \not\subset \mathsf{SIZE}(n^k)$ *iff* $\mathsf{NP} \subset \mathsf{P}/\mathrm{poly} \implies \mathsf{PH} = \mathrm{i.o.} - \mathsf{P}^{\mathsf{NP}}_{/n}$
[Chen et al., 2019]

1. $L \in \mathrm{i.o.}{-}\mathcal{C}$ means there's some language $L' \in \mathcal{C}$ for which there are infinitely many n such that $L_n = L'_n$
2. $\mathrm{i.o.} - \mathsf{P}^{\mathsf{NP}}_{/n}$: Set of languages decidable in P with oracle access to NP, given n bits of advice, infinitely often.

Lower bounds for P^{NP}

Theorem

$\mathsf{P}^{\mathsf{NP}} \not\subset \mathsf{SIZE}(n^k)$ *iff* $\mathsf{NP} \subset \mathsf{P}/\mathrm{poly} \implies \mathsf{PH} = \mathrm{i.o.} - \mathsf{P}^{\mathsf{NP}}_{/n}$
[Chen et al., 2019]

Lower bounds for P^{NP}

Theorem

$\mathsf{P}^{\mathsf{NP}} \not\subset \mathsf{SIZE}(n^k)$ *iff* $\mathsf{NP} \subset \mathsf{P}/\mathrm{poly} \implies \mathsf{PH} = \mathrm{i.o.} - \mathsf{P}^{\mathsf{NP}}_{/n}$
[Chen et al., 2019]

Lemma

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

Lower bounds for P^{NP}

Theorem

$\mathsf{P}^{\mathsf{NP}} \not\subset \mathsf{SIZE}(n^k)$ *iff* $\mathsf{NP} \subset \mathsf{P}/\mathrm{poly} \implies \mathsf{PH} = \mathrm{i.o.} - \mathsf{P}^{\mathsf{NP}}_{/n}$
[Chen et al., 2019]

Lemma

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

Proof of Theorem

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

Lower bounds for P^{NP}

Theorem

$\mathsf{P}^{\mathsf{NP}} \not\subset \mathsf{SIZE}(n^k)$ *iff* $\mathsf{NP} \subset \mathsf{P}/\mathrm{poly} \implies \mathsf{PH} = \mathrm{i.o.} - \mathsf{P}^{\mathsf{NP}}_{/n}$
[Chen et al., 2019]

Lemma

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

Proof of Theorem

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

Lower bounds for P^{NP}

Theorem

$\mathsf{P}^{\mathsf{NP}} \not\subset \mathsf{SIZE}(n^k)$ *iff* $\mathsf{NP} \subset \mathsf{P}/\mathrm{poly} \implies \mathsf{PH} = \mathrm{i.o.} - \mathsf{P}^{\mathsf{NP}}_{/n}$
[Chen et al., 2019]

Proof of Theorem cont'd

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

Table of Contents

1. Introduction
2. Interactive Proofs
3. PP and more
4. Lower bounds for P^{NP}
5. Algebraization

Meta time

1. KL-theorems seem to be pretty useful

Meta time

1. KL-theorems seem to be pretty useful
2. Moreover, a lot of the proofs don't relativize, or naturalize

Meta time

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?

Meta time

WRONG

Meta Time

1. Aaronson and Wigderson [Aaronson and Wigderson, 2009] introduced the Algebraization proof Barrier.

Meta Time

1. 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" $\tilde{A}$, $\mathcal{C}^{\tilde{A}} \not\subset \mathcal{D}^{A}$.

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

Meta Time

1. 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" $\tilde{A}$, $\mathcal{C}^{\tilde{A}} \not\subset \mathcal{D}^{A}$.

2. They showed that any proof for NP $\not\subset$ P must be non-algebraizing, as well as for NP $\not\subset$ SIZE(n^k).
3. Unfortunately, a lot of the proofs mentioned today, do algebraize

Meta Time

The following results algebraize: (non-exhaustive)

1. $\text{Promise} - \mathsf{MA} \not\subset \mathsf{SIZE}(n^k)$
2. $\mathsf{MA}_{\mathsf{EXP}} \not\subset \mathsf{P}/\text{poly}$
3. $\mathsf{PP} \not\subset \mathsf{SIZE}(n^k)$
4. ...

Meta Time

1. Still, given all the results seen today seems like KL-theorems are still a powerful framework for circuit lower bounds.

Meta Time

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.

Meta Time

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

Meta Time

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.
3. For the future, interesting if we can get even tighter collapses of PH (for instance, getting rid of the advice, or infinitely-often parts).
4. P^{NP} seems "barely" above NP, can we get a similar equivalence for something just below P^{NP}?

Questions?

Thank You!

Aaronson, S. (2006).
Oracles are subtle but not malicious.
In *21st Annual IEEE Conference on Computational Complexity (CCC'06)*, pages 15–pp. IEEE.

Aaronson, S. and Wigderson, A. (2009).
Algebrization: A new barrier in complexity theory.
ACM Transactions on Computation Theory (TOCT), 1(1):1–54.

Arvind, V., Köbler, J., Schöning, U., and Schuler, R. (1995).
If np has polynomial-size circuits, then ma= am.
Theoretical Computer Science, 137(2):279–282.

Baker, T., Gill, J., and Solovay, R. (1975).
Relativizations of the p=?np question.
SIAM Journal on computing, 4(4):431–442.

Chen, L., McKay, D. M., Murray, C. D., and Williams, R. R. (2019).
Relations and equivalences between circuit lower bounds and karp-lipton theorems.

In *34th Computational Complexity Conference (CCC 2019)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

Kannan, R. (1982).
Circuit-size lower bounds and non-reducibility to sparse sets.
Information and control, 55(1-3):40–56.

Karp, R. M. and Lipton, R. J. (1980).
Some connections between nonuniform and uniform complexity classes.
In *Proceedings of the Twelfth Annual ACM Symposium on Theory of Computing*, STOC '80, page 302–309, New York, NY, USA. Association for Computing Machinery.

Köbler, J. and Watanabe, O. (1998).
New collapse consequences of np having small circuits.
SIAM Journal on Computing, 28(1):311–324.

Santhanam, R. (2009).
Circuit lower bounds for merlin–arthur classes.
SIAM Journal on Computing, 39(3):1038–1061.

Vinodchandran, N. (2005).
A note on the circuit complexity of pp.
Theoretical Computer Science, 347(1-2):415–418.