Karp-Lipton Style Theorems

CS388T, Spring 2020 Instructor: Prof. Dana Moshkovitz

Maruth Goyal
maruth@cs.utexas.edu
The Universtiy of Texas at Austin

Abstract

Circuits, and their power with respect to other classical models of computation have long been studied in Complexity Theory. Circuits were studied as non-uniform model of computation, as opposed to Turing Machines which represent a uniform model of computation. There have been several results relating the two models of computation, one of the first being the classic result by Karp and Lipton [KL80] from the 80's that showed $\mathsf{NP} \subseteq \mathsf{P/poly} \implies \mathsf{PH} = \Sigma_2$. That is, if there are poly-size circuits for NP then the polynomial hierarchy collapses to the 2nd level. While the proof of this result is so simple that it has been featured on bags at conferences, and acted as a guide for the duration one should wash their hands, it has had a very big impact. We study some results which are, in a way, descendants of this result, including a recent remarkable result by Chen et al. [CMMW19], demonstrating the power of this style of theorems.

1 Introduction

Circuits have served as an interesting model of computation, especially because of the non-uniformity they offer. While they are ridiculously powerful in some ways (for instance, they can solve otherwise undecidable problems such as the Unary Halting Problem), they have been extensively studied for their applications across fields including Electric Engineering and such, however to theorists, one of their purposes is as a great tool to analyze the hardness of different complexity classes. Earlier, researchers focused mostly on Turing Machines to analyze complexity classes, however when Baker, Gill, and Solovay [BGS75] introduced the relativization barrier, researchers sought alternate, lower level models to escape its teeth. Thus circuits have made it easier to reason about these problems by simplifying problems to the level of bits, and often letting us "look" inside in some cases, by virtue of their simpler structure. Many big techniques and results have been discovered over the years (the switching lemma etc), but we focus particularly on results similar in form to the one posed by Karp and Lipton. Their result, and following results are particularly interesting since they tie together bounds on non-unifrom models of computation (circuits), with uniform models of computation in a very nice way.

The Karp-Lipton theorem showed that if there are poly-sized circuits for NP then the polynomial hierarchy collapses to the second level. This result was then used by Kannan [Kan82] to show $\Sigma_2 \nsubseteq \mathsf{SIZE}(n^k)$ for all k. There have been multiple other results in a similar vein. For instance, Santhanam [San09] showed that $\mathsf{MA}/1 \nsubseteq \mathsf{SIZE}(n^k)$ for all k, and $\mathsf{MA}/O(n) \nsubseteq \mathsf{SIZE}(n^k) \implies \mathrm{Promise}-\mathsf{MA} \nsubseteq \mathsf{SIZE}(O(n^k))$ to conclude for each $k > 0$, $\mathrm{Promise}-\mathsf{MA} \nsubseteq \mathsf{SIZE}(n^k)$. Arvind et

al. [AKSS95] showed that $\mathsf{NP} \subseteq \mathsf{P/poly} \implies \mathsf{AM} = \mathsf{MA}$. This was then used by Vinodachandran [Vin05] along with some other results to show that $\mathsf{PP} \nsubseteq \mathsf{SIZE}(n^k)$ for all k. Aaronson [Aar06] introduced a "Quantum Karp-Lipton theorem", $\mathsf{PP} \subset \mathsf{BQP/poly} \implies \mathsf{QCMA} = \mathsf{PP}$. He used this, in addition to P^{PP} not having quantum circuits of size n^k for any k to show PP does not have quantum circuits, even with quantum advice of size n^k for any k.

Given that there are so many results utilizing this form, one might wonder if there are stronger equivalences between these results and circuit lower bounds for various classes. Indeed, Chen, McKay, Murray, and Williams [CMMW19] show that polynomial lower bounds for P^{NP} are **equivalent** to showing $\mathsf{NP} \subset \mathsf{P/poly} \implies \mathsf{PH} \subset \text{i.o.}-\mathsf{P}^{\mathsf{NP}}_{/n}$, a Karp-Lipton style theorem. Since proofs utilizing theorems of this style are often non-constructive, and employ the law of excluded middle, one might imagine (some, even hope) there are other combinatorial proofs which can sidestep these theorems, but this result showed that intuition is incorrect. In this project, we expand on parts of the relevant results we have mentioned in this section. We begin with the work pertaining to interactive proofs, followed by the results regarding PP, and then the more recent result. We finally present a discussion of potential future directions.

2 Fun with Interactive Proofs

The relation between MA and its sister class AM is an interesting question in complexity theory. We know $\mathsf{MA} \subseteq \mathsf{AM}$ since $\mathsf{MA} \subseteq \mathsf{AM}[3]$. However, the question of $\mathsf{AM} \nsubseteq \mathsf{MA}$ is open. However, in the 90s, Arvind et al. [AKSS95] showed an interesting conclusion assuming polynomial size circuits for NP. In particular, they showed that $\mathsf{AM} = \mathsf{MA}$ under this assumption! Their proof of this result is similar to that of the original theorem of Karp and Lipton.

Definition 1. *A language L is in AM if there is a polynomial-time Turing Machine M such that*

$$x \in L \implies \Pr_{y \in \{0,1\}^{p(|x|)}}[\exists z \in \{0,1\}^{q(|x|)}.\ M(x,y,z) = 1] \geq 2/3$$
$$x \notin L \implies \Pr_{y \in \{0,1\}^{p(|x|)}}[\exists z \in \{0,1\}^{q(|x|)}.\ M(x,y,z) = 1] \leq 1/3$$

Definition 2. *A language L is in MA if there is a polynomial-time Turing Machine M such that*

$$x \in L \implies \exists y.\ \Pr_{z \in \{0,1\}^{p(|x|)}}[M(x,y,z) = 1] \geq 2/3$$
$$x \notin L \implies \forall y.\ \Pr_{z \in \{0,1\}^{p(|x|)}}[M(x,y,z) = 1] \leq 1/3$$

Theorem 2.1. *If $\mathsf{NP} \subseteq \mathsf{P/poly}$ then $\mathsf{AM} = \mathsf{MA}$*

Proof. The proof proceeds by taking a language in AM and transforming its definition to fit the above definition of MA. Consider any $L \in \mathsf{AM}$. Then, there exists a Turing Machine M s.t

$$x \in L \implies \Pr[\exists z\ M(x,y,z) = 1] \geq 2/3 \quad x \notin L \implies \Pr[\exists z\ M(x,y,z) = 1] \leq 1/3$$

Observe that the expression in the brackets is exactly of the form of languages in NP. To complete the proof, we will modify the expression to testing for membership in an NP language. We will then guess a polynomial size circuit to decide the language, bringing us to an MA language.

Define $C = \{(x, y) \mid \exists z. M(x, y, z) = 1\}$. Clearly $C \in \mathsf{NP}$. Thus, we can simply rephrase the above expression as

$$x \in L \implies \Pr[(x, y) \in C] \geq 2/3 \quad x \notin L \implies \Pr[(x, y) \in C] \leq 1/3$$

By our assumption, $\mathsf{NP} \in \mathsf{P/poly}$, so we simply guess a polynomial size circuit to decide the inner expression, giving

$$x \in L \implies \exists c. \Pr[c(x, y) = 1] \geq 2/3 \quad x \notin L \implies \forall c. \Pr[c(x, y) = 1] \leq 1/3$$

Where the domain for c is a string of polynomial length, encoding the circuit. Observe this is exactly the form for MA. Thus, $\mathsf{AM} = \mathsf{MA}$. □

We will see this proof in play in future sections. This result gives a good flavor for what such theorems might look like in the world of interactive proofs. However, Santhanam's work provides an interesting perspective by considering interactive proofs with small advice, but also their promise versions. In particular, they show

Theorem 2.2. $\mathsf{MA}/1$ *is not contained in* $\mathsf{SIZE}(n^k)$ *for any* $k > 0$.

Lemma 2.1. *If* $\mathsf{MA}/O(n) \not\subseteq \mathsf{SIZE}(n^k)$, *then* $\text{Promise} - \mathsf{MA} \not\subseteq \mathsf{SIZE}(O(n^k))$.

And from these two results, it follow that

Theorem 2.3. $\text{Promise} - \mathsf{MA} \not\subseteq \mathsf{SIZE}(n^k)$ *for each* $k > 0$.

While the first theorem has an interesting proof, we omit it to focus on the proof of the Karp-Lipton style lemma. Briefly, for the first theorem the authors consider a specific PSPACE-complete language L, and perform a case split on $L \in \mathsf{SIZE}(n^k)$. If the condition holds, they invoke $\mathsf{PSPACE} \subset \mathsf{P/poly} \implies \mathsf{PSPACE} = \mathsf{MA}$, another Karp-Lipton Style Theorem. Since PSPACE doesn't have poly-size circuits by diagonalization, neither does MA. For the other case, they create a padded version of L such that $L' \in \mathsf{MA}/1$ but $L' \notin \mathsf{SIZE}(n^k)$. As for the lemma, it is a simple proof by contradiction; it is different from the previous proofs since it provides explicit constructions of circuits, with no guessing involved.

Proof of Theorem 2.3. Consider any language $L \in \mathsf{MA}/O(n)$ which takes cn bits of advice on inputs of length n for some $c > 0$. Furthermore, define $\{a_i\}$ to be the advice strings for which an MA machine M gives the current answer, where $|a_i| = ci$. We define a promise problem $X = (U_{YES}, U_{NO})$ where the promise is satisfied iff $|x| = (c + 1)n$ for some n. Then, $x \in U_{YES}$ iff M accepts with the first n bits as input, and the remaining cn bits as advice.

For contradiction, assume on inputs of length l, X has circuits of size $\dfrac{l^k}{2(c+1)^k}$. Observe when $l = (c+1)n$ the expression boils down to $n^k/2$. We will use use these circuits to construct circuits of size $n^k/2$ that decide L, thus giving us our contradiction. Let $\{C_i\}$ be the family of circuits deciding X. Then, we construct a family of circuits $\{D_i\}$ such that on input x of length i, it pads x with the correct advice, a_i and invokes $C_{(c+1)i}$. i.e., it invokes $C_{(c+1)i}(x \circ a_i)$. Observe that $x \circ a_i$ necessarily satisfies the promise, and hence $C_{(c+1)i}$ will correctly decide if $x \circ a_i \in U_{YES}$ which decides if $x \in L$. The size $|D_i|$ is the size of $C_{(c+1)i}$, and as noted above this gives us circuits of size $n^k/2$ to decide L which is a contradiction. □

For completeness, we also present a proof of the Karp-Lipton theorem used in the proof of Theorem 2.2.

Lemma 2.2. $\mathsf{PSPACE} \subset \mathsf{P/poly} \implies \mathsf{PSPACE} = \mathsf{MA}$

Proof. Consider any PSPACE language L. We know $\mathsf{IP} = \mathsf{PSPACE}$ from Shamir [Sha92]. Thus, there is an interactive system for L where the prover can be run in PSPACE. By assumption, there is a polynomial size circuit for PSPACE, and thus for the prover. We thus present the following MA procedure: (1) Merlin guesses this polynomial size circuit and sends it to Arthur, (2) Arthur simulates the IP protocol on his own. Thus $\mathsf{PSPACE} = \mathsf{MA}$. □

3 PP and more

Having explored circuit lower bounds for interactive protocols, we now focus our attention on another complexity class, namely PP.

Definition 3. *A language L is in PP if there exists a non-deterministic poly-time Turing Machine M that for all inputs $x \in L$, M outputs accept on at least half the paths.*

Observe that PP is the decision version of #P. A canonical PP-complete problem is MajSAT, where $\varphi \in$ MajSAT if for at least half the assignments to $x_1 \dots x_n$, φ is true. Vinodachandran [Vin05] showed that $\mathsf{PP} \subsetneq \mathsf{SIZE}(n^k)$ for each $k > 0$. This proof relies heavily on previous results, and chains them together nicely. Aaronson [Aar06], however, gave a mostly self-contained proof of the same fact, but also extended the proof to hold for quantum circuits, even with quantum advice.

Theorem 3.1. (Vinodachandran): $\mathsf{PP} \subsetneq \mathsf{SIZE}(n^k)$ *for all* $k > 0$

Proof. It is the case that either $\mathsf{PP} \subset \mathsf{P/poly}$ or $\mathsf{PP} \subsetneq \mathsf{P/poly}$. In the second case, we are done. We assume the first case holds. From [BFL91] we know that $\mathsf{PP} \subseteq \mathsf{P/poly} \implies \mathsf{PP} \subseteq \mathsf{MA}$. We also know that $\mathsf{PH} \subseteq \mathsf{BP} \cdot \mathsf{PP}$ from an extension of Toda's theorem. Thus, we get $\mathsf{PH} \subseteq \mathsf{BP} \cdot \mathsf{MA} = \mathsf{AM}$. Then from [AKSS95] we have that $\mathsf{AM} = \mathsf{MA}$ under our assumption. Thus, $\mathsf{PH} \subseteq \mathsf{MA} \subseteq \mathsf{PP}$. But, $\mathsf{PH} \subsetneq \mathsf{SIZE}(n^k)$ for any $k > 0$ from Kannan's theorem [Kan82]. Thus, $\mathsf{PP} \subsetneq \mathsf{SIZE}(n^k)$. □

We highlight a lemma used in the above proof, as well as the following one.

Lemma 3.1. $\mathsf{PP} \subset \mathsf{P/poly} \implies \mathsf{PP} \subseteq \mathsf{MA}$

The proof is the same as the collapse of PSPACE.

While the above proof gets the job done, it leaves something to be desired as no explicit insight or understanding about PP is immediately gained from it. Hence, we turn to Aaronson's proof which may provide greater insight into why the result may hold. Their proof proceeds in 2 steps: (1) Show $\mathsf{P}^{\mathsf{PP}} \subsetneq \mathsf{SIZE}(n^k)$, even for quantum circuits with quantum advice (2) Show $\mathsf{PP} \subset \mathsf{BQP/qpoly} \implies \mathsf{CH} = \mathsf{MA}$. We present the proof for the classical version of (1), and briefly sketch the rest of the proof, and (2).

Theorem 3.2. P^{PP} *does not have classical circuits of size n^k for any k.*

Proof. Let $\mathcal{C}$ be the set of all circuits of size n^k. Let $\{x_i\}$ be all the bitstrings of length n in lexicographical order. Let $\mathcal{C}_t \subseteq \mathcal{C}$ be the set of circuits that correctly decide $x_1, \dots, x_t$. We construct the language $L \cap \{0,1\}^n$ as follows:

1. For each $i \in \{0, \ldots, N\}$, if more than half of the circuits in $\mathcal{C}_i$ accept x_{i+1}, then $x_{i+1} \notin L$.

2. Otherwise, $x_{i+1} \in L$.

For each $i > N$, set $x_i \notin L$. Here, $N = \lceil \log_2 |\mathcal{C}| \rceil + 1$. We show that $L \in \mathsf{P}^{\mathsf{PP}}$. If we want to decide if $x_t \in L$, if $t > N$ we reject, otherwise we must first compute $\mathcal{C}_{t-1}$. Thus, we must decide $x_1, \ldots, x_{t-1}$ first. This is done iteratively by querying our PP oracle $t-1$ times. i.e., at step 1 query if majority of the circuits in $\mathcal{C}$ accept x_1, and pick the circuits that answer correctly, giving us $\mathcal{C}_1$, and then repeat till $\mathcal{C}_{t-1}$. Now we may decide x_t by simply doing one more PP query.

However, observe that $|\mathcal{C}_{t+1}| \leq |\mathcal{C}_t|/2$ for all $t < N$. This follows by a simple combinatorial argument on our construction. Thus, $|\mathcal{C}_N| \leq |\mathcal{C}_{N-1}|/2 \leq \cdots \leq |\mathcal{C}|/2^N = 1/2$ by definition of N. Thus, $\mathcal{C}_N$ must be empty. Hence, no circuit in $\mathcal{C}$ decides L correctly. □

Aaronson's proof remarkably almost directly extends this algorithm to a quantum equivalent to derive the full result. For (2), the proof proceeds by first observing that the counting hierarchy, CH which is the union of $\mathsf{PP}, \mathsf{PP}^{\mathsf{PP}}, \mathsf{PP}^{\mathsf{PP}^{\mathsf{PP}}}$ and so on collapses to BQP if you can get quantum polysize circuits for MajSAT. This follows from Fortnow and Rogers' result that $\mathsf{PP}^{\mathsf{BQP}} = \mathsf{PP}$. Next, observe that under $\mathsf{PP} \subset \mathsf{BQP/poly}$, $\mathsf{P}^{\#\mathsf{P}} = \mathsf{P}^{\mathsf{PP}}$. They then present an algorithm in QCMA which can decide Permanent, which is a $\#\mathsf{P}$ complete language, and thus they can also decide MajSAT. Hence, $\mathsf{QCMA} = \mathsf{PP}$ under the assumption. The final result follows by contradiction: if PP had poly-size quantum circuits, then from (2) $\mathsf{QCMA} = \mathsf{PP} = \mathsf{P}^{\mathsf{PP}}$, and so P^{PP} would have quantum poly-size circuits. But from (1), this is not the case. Hence, PP does not have even quantum poly-size circuits.

For a more thorough treatment, we refer the reader to the original paper [Aar06]. However, our goal here is accomplished in showing the applicability of Karp-Lipton style theorems even in the quantum world.

4 Equivalence to Lower bounds for P^{NP}

Insofar we have seen Karp-Lipton style theorems be used to prove circuit lower bounds for various classes, including MA, and PP, extending even to quantum circuits. But what's in a name? That which we call a theorem would by any other proof smell just as sweet. One would imagine that there must be other ways to prove these bounds, while completely escaping these Karp-Lipton results. In a recent work, Chen et al. [CMMW19] show this is in fact, false! In particular, they show that proving polynomial lower bounds for P^{NP} is equivalent to showing $(\mathsf{NP} \subset \mathsf{P/poly} \implies \mathsf{PH} \subset \text{i.o.} - \mathsf{P}^{\mathsf{NP}}_{/n})$.

We can show the $(\mathsf{NP} \subset \mathsf{P/poly} \implies \mathsf{PH} \subset \text{i.o.} - \mathsf{P}^{\mathsf{NP}}_{/n}) \implies \mathsf{P}^{\mathsf{NP}} \not\subset \mathsf{SIZE}(n^k)$ by contradiction. Assume $\mathsf{P}^{\mathsf{NP}} \subset \mathsf{SIZE}(n^k)$ and $\mathsf{NP} \subset \mathsf{P/poly} \implies \mathsf{PH} \subset \text{i.o.} - \mathsf{P}^{\mathsf{NP}}_{/n}$. Then, we derive that $\mathsf{PH} \subset \text{i.o.} - \mathsf{P}^{\mathsf{NP}}_{/n} \subset \text{i.o.} - \mathsf{SIZE}(O(n)^k)$. However, this contradicts the known lower bounds for PH, i.e., it doesn't have polynomial size circuits.

The other direction is more involved. The proof can be broken down into the following lemmas:

Lemma 4.1. $\mathsf{NP} \subset \mathsf{P/poly} \implies \mathsf{\Sigma_3 TIME}[n^{O(k)}] \subset \mathsf{SIZE}(n^{O(k)})$

Lemma 4.2. *If* $\mathsf{P}^{\mathsf{NP}} \subsetneq \mathsf{\Sigma_3 TIME}[n^{O(k)}]$ *then, for all* k*, for all functions* f *in* $\mathsf{FP}^{\mathsf{NP}}$*, there are infinitely many* x *such that* $f(x)$ *has circuit complexity at least* $|x|^k$*.*

Theorem 4.1. [KW98] *If* $\mathsf{NP} \subset \mathsf{P/poly}$ *then* $\mathsf{PH} \subseteq \mathsf{ZPP}^{\mathsf{NP}}$.

Essentially, the proof uses the first and second lemma to get a hard function in order to construct a PRG which can then be used to derandomize $\mathsf{ZPP}^{\mathsf{NP}}$ in i.o.$-\mathsf{P}^{\mathsf{NP}}_{/n}$. Thus, $\mathsf{PH} \subset \mathsf{ZPP}^{\mathsf{NP}} \subset$ i.o.$-\mathsf{P}^{\mathsf{NP}}_{/n}$.

Theorem 4.2. *If* $\mathsf{P}^{\mathsf{NP}} \subsetneq \mathsf{SIZE}(n^k)$*, then* $\mathsf{NP} \subset \mathsf{P/poly} \implies \mathsf{PH} \subseteq$ i.o. $- \mathsf{P}^{\mathsf{NP}}_{/n}$

Proof. From lemma 4.1 we have that $\mathsf{\Sigma_3TIME}[n^{O(k)}] \subset \mathsf{SIZE}(n^{O(k)})$. Moreover, by assumption $\mathsf{P}^{\mathsf{NP}} \subsetneq \mathsf{SIZE}(n^k)$. Thus, $\mathsf{P}^{\mathsf{NP}} \subsetneq \mathsf{\Sigma_3TIME}[n^{O(k)}]$. Hence, from lemma 4.2 there exists a function $B(x)$ such that for infinitely many x, $B(x)$ has circuit complexity at least $|x|^k$ for all k. It is a known result that PRGs can be generated from worst-case, or average-case hard functions [NW94, DMOZ19]. From theorem 4.1 we have that $\mathsf{PH} \subseteq \mathsf{ZPP}^{\mathsf{NP}}$. Consider any $\mathsf{ZPP}^{\mathsf{NP}}$ algorithm A. There is some k such that for all inputs of length n, a PRG generated using a string of complexity at least n^k will fool A.

We noted above that $B(x)$ will output such hard functions for infinitely many x. Thus, we can construct a $\mathsf{P}^{\mathsf{NP}}_{/n}$ algorithm that takes the x of required length to make B output a hard function as advice. It then simulates A using $B(x)$ as the randomness, and using its NP oracle to simulate the NP oracle queries of A. Thus, we derandomize $\mathsf{ZPP}^{\mathsf{NP}}$ in $\mathsf{P}^{\mathsf{NP}}_{/n}$ infinitely often, giving us $\mathsf{PH} \subseteq \mathsf{ZPP}^{\mathsf{NP}} \subseteq$ i.o. $- \mathsf{P}^{\mathsf{NP}}_{/n}$. □

The reader might find it slightly irking that the collapse is to i.o. $- \mathsf{P}^{\mathsf{NP}}_{/n}$ instead of something more "standard" like P^{NP} or even $\mathsf{P}^{\mathsf{NP}}_{/n}$. The burden of removing the infinitely often constraint seems to rely mostly on lemma 4.2. Since the authors prove that lemma by contraposition, the constraint that the circuit complexity of $f(x)$ is at most $|x|^k$ for all but **finitely** many x would have to be relaxed. However, this would mean that for all $f \in \mathsf{FP}^{\mathsf{NP}}$, for all x there is an $O(|x|^k)$ circuit which can output $f(x)$.

While we have omit the proof of lemma 4.2, we briefly describe the sketch here. The authors construct an explicit $\mathsf{\Sigma_3TIME}[n^{O(k)}]$ algorithm for any language $L \in \mathsf{P}^{\mathsf{NP}}$. The algorithm guesses 2 circuits, f_{sol} and f_{history}. The latter circuit is supposed to encode the state of the tape of the oracle machine M that can solve L at each step. The former circuit essentially encodes explicit solutions to the SAT oracle queries made by M. The algorithm then verifies the correctness of the circuits by simply checking consistency between the states of the two. i.e., C_{history} is consistent with the starting state, and all transitions are valid, and the final state accepts, and cross-checks the claimed answer to oracle queries with C_{sol}.

In the same work, the authors also demonstrate better Karp-Lipton collapses under the assumption that $\mathsf{NP} \not\subset \mathsf{P/poly}$. In particular,

Theorem 4.3. *If* $\mathsf{NP} \not\subset \mathsf{P/poly}$ *then for* $\mathcal{C} \in \{\oplus\mathsf{P}, \mathsf{PP}, \mathsf{EXP}, \mathsf{PSPACE}\}$*, for all* $\varepsilon > 0$*,* $\mathcal{C} \subset \mathsf{P/poly} \implies \mathcal{C} \subset$ i.o.$-\mathsf{NP}_{/n^\varepsilon}$.

The proof of this theorem starts with a downward self-reducible, and random self-reducible $\mathcal{C}$-complete language for $\mathcal{C} \in \{\oplus\mathsf{P}, \mathsf{PP}, \mathsf{PSPACE}\}$. They then show that under the assumption, circuits for this language can be guessed and verified in MA. They then invoke their lemma that under the assumption, $\mathsf{MA} \subset$ i.o.$-\mathsf{NP}_{/n^\varepsilon}$ to complete the proof. We present an informal sketch of their proof, referring the reader to the original paper for the full details [CMMW19]

Proof. We focus specifically on $\oplus\mathsf{P}$. Suppose $\mathsf{NP} \not\subset \mathsf{SIZE}(n^k)$ for all k, and $\oplus\mathsf{P} \subset \mathsf{P/poly}$. We will show $\oplus\mathsf{P} \subset \mathsf{MA}$. Let Π be the random self-reducible, and downward self-reducible $\oplus\mathsf{P}$-complete language in [IKV18]. By assumption, Π has poly-size circuits. We guess-and-verify the circuits in MA. First, guess the circuits $C_1, \ldots, C_k$, each for inputs of length $1 \ldots k$ resp. C_1 can be verified trivially. Using downward self reducibility, we can verify a length $m+1$ circuit for Π_{m+1} using a length m circuit for Π_m by testing on random inputs. Using random self-reducibility we can construct an exact circuit for Π_{m+1} using C_{m+1} which approximates Π_{m+1} very well by virute of the previous verification. Thus, we have a circuit for Π_n using a poly-time computation in MA. Hence, $\oplus\mathsf{P} \subset \mathsf{MA} \subset \text{i.o.}-\mathsf{NP}_{/n^\varepsilon}$. □

5 Discussion and Future

So far, it seems that Karp-Lipton style theorems are indeed a powerful proof framework for showing circuit lower bounds. We looked at how these kind of collapses were used to show lower bounds for interactive proof classes, and classes like PP (even when extended to quantum circuits), but also how these collapses are equivalent to lower bounds for P^{NP}. There are certainly more instances of these collapses being useful. For instance, Impagliazzo, Kabanets, and Wigderson [IKW02] utilize $\mathsf{EXP} \subset \mathsf{P/poly} \implies \mathsf{EXP} = \mathsf{MA}$, and $\mathsf{NEXP} \subset \mathsf{P/poly} \implies \mathsf{NEXP} = \mathsf{MA}$. Even the proof of $\mathsf{MA}_{\mathsf{EXP}} \not\subset \mathsf{P/poly}$ utilizes $\mathsf{MA}_{\mathsf{EXP}} \subseteq \mathsf{P/poly} \implies \mathsf{PSPACE} = \mathsf{MA}$.

These proofs also often have the benefit of being non-relativizing, and non-naturalizing. For instance, Aaronson [Aar06] showed that Vinodachandran's [Vin05] proof that $\mathsf{PP} \not\subset \mathsf{SIZE}(n^k)$ does not relativize by giving an oracle A such that $\mathsf{PP}^A \subseteq \mathsf{SIZE}^A(n)$. Similarly, Buhrman et al. gave an oracle A w.r.t which $\mathsf{MA}^A_{\mathsf{EXP}} \subseteq \mathsf{P}^A\text{/poly}$. However, apart from the Relativization [BGS75] and Natural Proofs barrier [RR], Aaronson and Wigderson introduced the Algebraization Barrier [AW09]. They showed that, unfortunately, the proofs of many circuit lower bounds algebraize.

Definition 4. *If an oracle A is a boolean function $A : \{0,1\}^n \to \{0,1\}$, then its low degree extension $\tilde{A} : \mathbb{F}^n \to \mathbb{F}$ is a low degree multilinear polynomial s.t $\tilde{A}(x) \in \{0,1\}$ for all $x \in \{0,1\}^n$, and is in fact equal.*

Definition 5. *An inclusion $\mathcal{C} \subseteq \mathcal{D}$ is said to algebraize, if for all oracles A and their low-degree extensions $\tilde{A}$, $\mathcal{C}^A \subseteq \mathcal{D}^{\tilde{A}}$. Likewise, $\mathcal{C} \subseteq \mathcal{D}$ does not algebraize if there exists an oracle A and extension $\tilde{A}$ such that $\mathcal{C}^A \not\subset \mathcal{D}^{\tilde{A}}$.*

A separation $\mathcal{C} \not\subset \mathcal{D}$ algebraizes if $\mathcal{C}^{\tilde{A}} \not\subset \mathcal{D}^A$ for all $A, \tilde{A}$. Similarly, $\mathcal{C} \not\subset \mathcal{D}$ does not algebraize if there exist $A, \tilde{A}$ such that $\mathcal{C}^{\tilde{A}} \subseteq \mathcal{D}^A$.

They showed that Vinodachandran's proof of $\mathsf{PP} \not\subset \mathsf{SIZE}(n^k)$ does indeed algebraize, as well as Santhanam's [San09] proof that $\text{Promise}-\mathsf{MA} \not\subset \mathsf{SIZE}(n^k)$. To give a flavor of why this is the case, we present their proof for Vinodachandran's proof:

Lemma 5.1. *If $\mathsf{PP}^{\tilde{A}} \subset \mathsf{P}^{\tilde{A}}\text{/poly}$ then $\mathsf{P}^{\#\mathsf{P}^A} \subseteq \mathsf{MA}^{\tilde{A}}$*

Theorem 5.1. *For all $A, \tilde{A}$ and constants k, we have $\mathsf{PP}^{\tilde{A}} \not\subset \mathsf{SIZE}^A(n^k)$.*

Proof. Much like the original proof, if $\mathsf{PP}^{\tilde{A}} \not\subset \mathsf{P}^A\text{/poly}$, we are done. Suppose then that $\mathsf{PP}^{\tilde{A}} \subset \mathsf{P}^A\text{/poly}$. We then get that $\mathsf{PP}^{\tilde{A}} \subset \mathsf{P}^{\tilde{A}}\text{/poly}$. Then, from lemma 5.1, we get that $\mathsf{P}^{\#\mathsf{P}^A} \subseteq \mathsf{MA}^{\tilde{A}}$.

From Toda's theorem (relativizes), we have that $\Sigma_2 \subseteq \mathsf{PH} \subseteq \mathsf{P}^{\#\mathsf{P}}$, and thus $\Sigma_2^A \subseteq \mathsf{P}^{\#\mathsf{P}^A}$. Furthermore, from Kannan's theorem (relativizes), $\Sigma_2 \not\subset \mathsf{SIZE}(n^k)$ and thus $\Sigma_2^A \not\subset \mathsf{SIZE}^A(n^k)$. Thus, $\mathsf{MA}^{\tilde{A}} \not\subset \mathsf{SIZE}^A(n^k)$, and hence since $\mathsf{MA} \subseteq \mathsf{PP}$ relativizes, we get $\mathsf{PP}^{\tilde{A}} \not\subset \mathsf{SIZE}^A(n^k)$. □

This barrier thus suggests that new techniques are certainly in order to prove better circuit lower bounds. However, given the results we have presented we believe that these collapse theorems will nonetheless be an important, yet algebraizing, part of an overall non-algebraizing proof for new results.

There is also the question of exactly how much we can collapse. As we asked above, [CMMW19] also question whether lower bounds for NP is equivalent a Karp-Lipton collapse of PH fully to NP — not infinitely often, and without advice.

6 Acknowledgements

I would like to thank Professor Dana Moshkovitz for pointing me in the direction of Chen et al. 's work for this project, but also for everything over the course of the semester. All the topics covered over the semester, from the polynomial hierarchy and Toda's theorem, Relativization, and Natural Proofs, to derandomization and PRGs came in handy while exploring papers for this project. The class was great fun, and I am glad to have been a part of it.

References

[Aar06] Scott Aaronson. Oracles are subtle but not malicious. In *21st Annual IEEE Conference on Computational Complexity (CCC'06)*, pages 15–pp. IEEE, 2006.

[AKSS95] Vikraman Arvind, Johannes Köbler, Uwe Schöning, and Rainer Schuler. If np has polynomial-size circuits, then ma= am. *Theoretical Computer Science*, 137(2):279–282, 1995.

[AW09] Scott Aaronson and Avi Wigderson. Algebrization: A new barrier in complexity theory. *ACM Transactions on Computation Theory (TOCT)*, 1(1):1–54, 2009.

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. Non-deterministic exponential time has two-prover interactive protocols. *Computational complexity*, 1(1):3–40, 1991.

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

[CMMW19] Lijie Chen, Dylan M McKay, Cody D Murray, and R Ryan Williams. Relations and equivalences between circuit lower bounds and karp-lipton theorems. In *34th Computational Complexity Conference (CCC 2019)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2019.

[DMOZ19] Dean Doron, Dana Moshkovitz, Justin Oh, and David Zuckerman. Nearly optimal pseudorandomness from hardness. *Electronic Colloquium on Computational Complexity (ECCC)*, 26:99, 2019.

[IKV18] Russell Impagliazzo, Valentine Kabanets, and Ilya Volkovich. The power of natural properties as oracles. In *33rd Computational Complexity Conference (CCC 2018)*. Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik, 2018.

[IKW02] Russell Impagliazzo, Valentine Kabanets, and Avi Wigderson. In search of an easy witness: Exponential time vs. probabilistic polynomial time. *Journal of Computer and System Sciences*, 65(4):672–694, 2002.

[Kan82] Ravi Kannan. Circuit-size lower bounds and non-reducibility to sparse sets. *Information and control*, 55(1-3):40–56, 1982.

[KL80] Richard M. Karp and Richard J. Lipton. 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, 1980. Association for Computing Machinery.

[KW98] Johannes Köbler and Osamu Watanabe. New collapse consequences of np having small circuits. *SIAM Journal on Computing*, 28(1):311–324, 1998.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs randomness. *Journal of computer and System Sciences*, 49(2):149–167, 1994.

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

[San09] Rahul Santhanam. Circuit lower bounds for merlin–arthur classes. *SIAM Journal on Computing*, 39(3):1038–1061, 2009.

[Sha92] Adi Shamir. Ip= pspace. *Journal of the ACM (JACM)*, 39(4):869–877, 1992.

[Vin05] NV Vinodchandran. A note on the circuit complexity of pp. *Theoretical Computer Science*, 347(1-2):415–418, 2005.