CSE 531: Computational Complexity I	Winter 2016

Lecture 10: Circuit Complexity and the Polytime Hierarchy

Feb 8, 2016

Lecturer: Paul Beame | *Scribe: Paul Beame*

1 Circuit Complexity and the Polynomial-Time Hierarchy

We now show that although P/poly contains undecidable problems, it is unlikely to contain even all of NP. This implies that circuits, despite having the advantage of being non-uniform, may not be all that powerful.

Theorem 1.1 (Karp-Lipton). *If* $\mathsf{NP} \subseteq \mathsf{P}/\mathsf{poly}$*, then* $\mathsf{PH} = \Sigma_2^{\mathsf{P}} \cap \Pi_2^{\mathsf{P}}$.

The original paper by Karp and Lipton credits Sipser with sharpening the result.

Proof. Suppose to the contrary that $\mathsf{NP} \subseteq \mathsf{P}/\mathsf{poly}$. We'll show that this implies $\Sigma_2^{\mathsf{P}} = \Pi_2^{\mathsf{P}}$. From the collapsing Lemma from Lecture 9 this will prove the Theorem.

(For convenience we use the dual form vs. what we did in class. It avoids a negation at the inner level.) Let $A \in \Pi_2^{\mathsf{P}}$. Therefore there exists a polynomial-time TM M and a polynomial p such that

$$x \in A \Leftrightarrow \forall y_1 \in \{0,1\}^{p(|x|)}\ \exists y_2 \in \{0,1\}^{p(|x|)}.\ (M(x, y_1, y_2) = 1).$$

The idea behind the proof is as follows. The inner predicate in this definition,

$$\varphi(x, y_1) = 1 \Leftrightarrow \exists y_2 \in \{0,1\}^{p(|x|)}.\ (M(x, y_1, y_2) = 1),$$

is an NP predicate. $\mathsf{NP} \subseteq \mathsf{P}/\mathsf{poly}$ implies that there exists a circuit family $\{C_\varphi\}$ of size at most $q(|x| + |y_1|)$ for some polynomial q computing this inner predicate. Given that $|y_1|$ is $p(|x|)$, this is $q_1(|x|) = q(|x| + |y_1|)$ for some polynomial q_1. We would like to simplify the definition of A using this circuit family. by

$$x \in A \Leftrightarrow \exists \text{circuit } [C_\varphi]\ \forall y_1 \in \{0,1\}^{p(|x|)}.\ C_\varphi \text{ correctly computes } f(x, y_1) \text{ and } C_\varphi(x, y) = 1.$$

This would put A in Σ_2^{P}, except that it is unclear how to efficiently verify that C_φ actually computes the correct inner relation corresponding to φ.

To handle this we modify the construction using the search-to-decision reduction for NP to say that there is a polynomial-size multi-output circuit C'_φ that on input (x, y_1) finds an assignment y_2

that makes $M(x, y_1, y_2) = 1$ if one exists. Let q' be the polynomial bound on the encoding of the circuit as a function of $|x|$.

(Technically, we need to create a modified version of φ suitable for this reduction where

$$\varphi'(x, y_1, y_2',) = 1 \Leftrightarrow \exists y_2'' \in \{0,1\}^{p(|x|)-|y_2'|}. \ (M(x, y_1, y_2', y_2'') = 1).$$

Here y_2' acts as a prefix of the assignment y_2 in the earlier definition of φ. Note that we also have $\varphi' \in \mathsf{NP}$. Therefore, using the assumption $\mathsf{NP} \subseteq \mathsf{P/poly}$, φ' is computed by a polynomial size circuit family $C_{\varphi'}$ as before. The circuit to produce y_2, if it exists, runs the circuit family $C_{\varphi'}$ on increasing lengths of y_2' beginning with $|y_2'| = 0$ and ending with $|y_2'| = p(|x|)$. Since the input size varies, we need to include circuits for all of the input sizes in our guessed circuit.)

Now observe that since $\varphi(x, y_1) = 1$ iff there is a $y_2 \in \{0,1\}^{p(|x|)}$ such that $M(x, y_1, y_2) = 1$ we have

$$x \in A \Leftrightarrow \exists [C_{\varphi'}'] \{0,1\}^{q'(|x|)} \forall y_1 \in \{0,1\}^{p(|x|)}. \ (M(x, y_1, C_{\varphi}'(x, y_1)) = 1).$$

Since M is polynomial-time computable and $C_{\varphi}'(x, y_1)$ is polynomial-time computable given $[C_{\varphi}']$, x, and y_1 as inputs, this shows that $A \in \Sigma_2^{\mathsf{P}}$.

This proves that $\Pi_2^{\mathsf{P}} \subseteq \Sigma_2^{\mathsf{P}}$. This also implies that $\Sigma_2^{\mathsf{P}} = \Sigma_2^{\mathsf{P}} \cap \Pi_2^{\mathsf{P}}$ and that PH collapses to the $\Sigma_2^{\mathsf{P}} \cap \Pi_2^{\mathsf{P}}$ level, finishing the proof. □

We now prove that even very low levels of the polynomial time hierarchy cannot be computed by circuits of size n^k for any fixed k. This result, unlike our previous Theorem, is *unconditional*; it does not depend upon our belief that the polynomial hierarchy is unlikely to collapse.

Theorem 1.2 (Kannan)**.** *For all k,* $\Sigma_2^{\mathsf{P}} \cap \Pi_2^{\mathsf{P}} \not\subseteq \mathsf{SIZE}(\mathsf{n^k})$.

Proof. We know that $\mathsf{SIZE}(\mathsf{n^k}) \subsetneq \mathsf{SIZE}(\mathsf{n^{k+1}})$ by the circuit hierarchy theorem. To prove this Theorem, we will give a problem in $\mathsf{SIZE}(\mathsf{n^{k+1}})$ and $\Sigma_2^{\mathsf{P}} \cap \Pi_2^{\mathsf{P}}$ that is not in $\mathsf{SIZE}(\mathsf{n^k})$.

We first show that such a problem can be found in Σ_4^{P} and then use Karp-Lipton Theorem above to say that it must be found at lower levels. The general idea of the argument is that we can use quantifiers to say that a circuit C of a certain size is not equivalent to any circuit of at most some smaller size:

$$\forall \text{circuits } C'. \ (size(C') \leq n^k) \ \exists \text{input } y. \ C(y) \neq C'(y).$$

We know that such circuits of relatively small size exist but we need to settle on a fixed circuit C and define a function based on it. To do this we use quantifiers to fix the lexicographically first such circuit.

For each n, let C_n be the lexicographically first circuit on n inputs such that $size(C_n) \geq n^{k+1}$ and C_n is not equivalent to any circuit of size at most n^k. (For lexicographic ordering on circuit encodings, we'll use the notation $\prec$.) Let $\{C_n\}_{n=0}^{\infty}$ be the corresponding circuit family and let A

be the language decided by this family. By our choice of C_n, $A \notin \mathsf{SIZE(n^k)}$. Also, $size(A)$ is at most kn^{k+1}.

<u>Claim</u>: $A \in \Sigma_4^{\mathsf{P}}$.
The proof of this claim involves characterizing the set A using a small number of quantifiers. By definition, $x \in A$ if and only if

$$\begin{aligned}\exists[C] \in \{0,1\}^{p(|x|)} \quad & (size(C) \geq |x|^{k+1} \wedge C(x) = 1 \\ & \bigwedge \forall[C'] \in \{0,1\}^{p(|x|)}\, [size(C') \leq |x|^k \rightarrow \exists y \in \{0,1\}^{|x|}.\, C'(y) \neq C(y)] \\ & \bigwedge \forall[D] \in \{0,1\}^{p(|x|)}.\, (\, ([D] \prec [C]) \wedge (size(D) \geq |x|^{k+1})) \rightarrow \\ & \quad \exists[C''] \in \{0,1\}^{p(|x|)}([size(C'') \leq |x|^k) \wedge (\forall y' \in \{0,1\}^{|x|}.\, C''(y') = D(y')))\end{aligned}$$

The second condition states that the circuit C is not equivalent to any circuit C' of size at most n^k. The third condition enforces the lexicographically-first requirement; *i.e.*, if there is a lexicographically-earlier circuit D of size at least $|x|^{k+1}$, then D is equivalent to a circuit C'' of size at most $|x|^k$. These conditions uniquely identify C and x is in A iff $C(x) = 1$. When we convert this formula into prenex form, all quantifiers, being in positive form, do not flip. This gives us that $x \in A$ iff $\underbrace{\exists[C]}\ \underbrace{\forall[C']\forall[D]}\ \underbrace{\exists y\ \exists[C'']}\ \underbrace{\forall y'}\ .\ \phi$ for a certain quantifier free polynomially decidable formula ϕ. Hence $A \in \Sigma_4^{\mathsf{P}}$.

This proves the claim and imples that $\Sigma_4^{\mathsf{P}} \not\subseteq \mathsf{SIZE(n^k)}$. We finish the proof of the Theorem by analyzing two possible scenarios:

a. $\mathsf{NP} \not\subseteq \mathsf{P/poly}$. In this simpler case, for some $B \in \mathsf{NP} \subseteq \Sigma_2^{\mathsf{P}} \cap \Pi_2^{\mathsf{P}}$, $B \notin \mathsf{P/poly}$. This implies that $B \notin \mathsf{SIZE(n^k)}$ and proves, in particular, that $\Sigma_2^{\mathsf{P}} \cap \Pi_2^{\mathsf{P}} \not\subseteq \mathsf{SIZE(n^k)}$.

b. $\mathsf{NP} \subseteq \mathsf{P/poly}$. In this case, by the Karp-Lipton Theorem, $A \in \Sigma_4^{\mathsf{P}} \subseteq \mathsf{PH} = \Sigma_2^{\mathsf{P}} \cap \Pi_2^{\mathsf{P}}$ because the polynomial time hierarchy collapses, and we are done.

This finishes the proof of the Theorem. $\square$