CS6840: Advanced Complexity Theory Jan 30, 2012

Lecture 14 : Karp-Lipton-Sipser Collapse Theorem

Lecturer: Jayalal Sarma M.N. *Scribe: Anup Joshi*

We showed that $\mathsf{BPP} \subseteq \mathsf{P/poly}$, and as we argued $\mathsf{P/poly}$ seems to be a huge class containing P and BPP, and even some undecidable languages. A natural question is whether NP is also contained in $\mathsf{P/poly}$. We show that both answers to this question has interesting consequences.

Suppose we are able to prove that $\mathsf{NP} \not\subseteq \mathsf{P/poly}$, then we are indeed are proving that $\mathsf{NP} \not\subseteq \mathsf{P}$. That is big !.

Suppose we are able to prove that $\mathsf{NP} \subseteq \mathsf{P/poly}$. Does it have any consequences? In this lecture, we will prove the Karp-Lipton-Sipser theorem, which says that if NP is contained in $\mathsf{P}/poly$, then the polynomial hierarchy collapses to Σ_2. It is believed that the polynomial hierarchy does not collapse, since the flavour of the question about each level of the hierarchy is about elimination of a quantifier, and is of a similar difficulty to to P vs NP question.

Summarising this discussion; we believe that $\mathsf{NP} \not\subseteq \mathsf{P}$, but we do not know how to prove it. But then, since $\mathsf{P} \subseteq \mathsf{P/poly}$ is this not a harder problem to solve that $\mathsf{P}vs\mathsf{NP}$? Yes, but why do we even bother to address it when we do not know how to attack the easier question? As we will see later in the course (when we do circuit complexity) this class $\mathsf{P/poly}$ provides this nice escape from the "combinatorics of a Turing machine" and helps us to prove theorems which we do not know how to prove otherwise. It was for precisely this reason that, in the definition of $\mathsf{P/poly}$ we did not make the advice function even computable (to avoid references to Turing machines).

We state the theorem.

Theorem 1 (Karp-Lipton-Sipser, 1980). *If* $\mathsf{NP} \subseteq \mathsf{P/poly}$*, then* PH *collapses to* Σ_2*.*

We prove the theorem by proving two lemmas. We first show that our assumption implies something much stronger. That is if $\mathsf{NP} \subseteq \mathsf{P/poly}$ then not only NP, but the entire PH will be in $\mathsf{P/poly}$.

Lemma 2. *If* $\mathsf{NP} \subseteq \mathsf{P/poly}$*, then* $\mathsf{PH} \subseteq \mathsf{P/poly}$*.*

Proof. It suffices to show that $\Sigma_k \subseteq \mathsf{P}/poly$ for any k. We prove this by induction on k. For $k = 1$, it is trivially true, since $\Sigma_1 = \mathsf{NP}$. Hence, the base case is true. Consider an $L \in \Sigma_2$, then $L \in \mathsf{NP}^B$ for some $B \in \mathsf{NP}$. But $\mathsf{NP} \subseteq \mathsf{P}/poly$ (by the induction hypothesis), hence, $\exists h : \mathbb{N} \to \{0,1\}^*$ and $C \in P$, such that, $y \in B \leftrightarrow (y, h(y)) \in C$. Now, membership in B is decidable in polynomial time with the help of the advice function. Hence, we do not need to make oracle query to B to resolve membership questions in L, we can embed the polynomial time computation of the oracle with advice function in the NTM for L itself. So we can say that, $L \in \mathsf{NP}$ with the advice function $h : \mathbb{N} \to \{0,1\}^*$. We can rewrite it as $\exists h : \mathbb{N} \to \{0,1\}^* \wedge C' \in \mathsf{NP}$ such that $x \in L \leftrightarrow (x, h(|x|)) \in C'$.

Now, what can we say about C'? We know that $C' \in \mathsf{NP}$, hence $C' \in \mathsf{P}/poly$. Hence there is an advice function for C' also, so that membership in C' is computable in polynomial time with the help of that advice function. That is, $\exists g : \mathbb{N} \to \{0,1\}^* \wedge D \in \mathsf{P}$ such that $y \in C' \leftrightarrow (y, g(|y|)) \in D$. Rewriting it we get:

$$(x, h(|x|)) \in C' \leftrightarrow (x, h(|x|), g(p(x))) \in D$$

Hence from the above argument we see that $L \in \mathsf{P/poly}$. □

Now we show that if any level of PH is in $\mathsf{P}poly$, then it essentially gives a way to express the acceptance condition using only two quantifiers. This is done in the following lemma.

Lemma 3. *For any $k > 2$, if $\Sigma_k \subseteq P/poly$, then $\Sigma_k \subseteq \Sigma_2$.*

Proof. It suffices to show that $L \in \Sigma_k \Rightarrow L \in \Sigma_2$. For this, we take the language SAT_k which is a quantified boolean formula with at most k alternating quantifiers. Since SAT_k is Σ_k-complete for any k, the lemma follows.

Let us assume that for any $k > 2$, $\Sigma_k \subseteq \mathsf{P/poly}$. Let $L \in \Sigma_k$, and since SAT_k is Σ_k-complete, then by our assumption, $\mathsf{SAT}_k \subseteq P/poly$. By the definition of $\mathsf{P/poly}$, $\exists h : \mathbb{N} \to \{0,1\}^* \wedge B \in \mathsf{P}$ such that $\phi \in \mathsf{SAT}_k \leftrightarrow (\phi, h(|\phi|)) \in B$. If $|\phi| = n$, then $h(n) \in \{0,1\}^{p(n)}$. Let us define a new function w in the following way:

$$w = g(n) = (h(0), h(1), ..., h(n))$$

For any $\phi \in \Sigma_k$, such that $|\phi| \le n$, the string w has the following properties:

1. $(0, w) \notin B \wedge (1, w) \in B$
2. If $\phi = \exists y, \psi \wedge \phi \in \mathsf{SAT}_k$, then $(\psi|_{y=0}, w) \in B \vee (\psi|_{y=1}, w) \in B$.
3. If $\phi = \forall y, \psi \wedge \phi \in \mathsf{SAT}_k$, then $(\psi|_{y=0}, w) \in B \wedge (\psi|_{y=1}, w) \in B$.

Hence, $(\phi, w) \in B \Rightarrow 1, 2$, and 3 are satisfied.

It is also true in the other direction. That is, if $1, 2$, and 3 are satisfied, then in order to check if ϕ is true, it suffices to check if $(\phi, w) \in B$. We can show this inductively. When

ϕ is either 0 or 1, then by 1, the above claim is true. Suppose, $\phi = (\exists x)\psi$, then we can apply 2 on ψ to evaluate it. Otherwise, if $\phi = (\forall x)\psi$, then we can apply 3 on ψ to evaluate it. Thus, by recursively evaluating, we can reach upto the leaf where we apply 1. Hence by a consistency check we can make sure that the advice does not give us a wrong answer, and indeed, if it gives a wrong answer to us, we can detect it at some point in the recursive evaluation. Note that we are using the self-reducibility property of SAT_k here. Thus we have proved that,

$$\phi \in \mathsf{SAT}_k \leftrightarrow (\exists w, |w| \leq p(n))(\forall \psi, |\psi| \leq n)(1 \wedge 2 \wedge 3 \wedge (\phi, w) \in B).$$

□