6.841 Advanced Complexity Theory Mar 04, 2009

Lecture 09

Lecturer: Madhu Sudan *Scribe: Jeremy Hurwitz*

In this lecture, we introduce a new model of computation and a set of corresponding complexity classes which sit between NP and $PSPACE$. This model is based on considering alternation as an interesting phenomenon in its own right. This will lead to the complexity classes comprising the *Polynomial Hierarchy* (PH) and the *Infinite Hierarchy Assumption* (IHA), which informally says that having more alternations gives you more power. This will then result in the Karp-Lipton Theorem, which states

Theorem 1 (Karp-Lipton Theorem)

$$IHA \Longrightarrow NP \subsetneq P/_{poly}$$

1 Debates

Suppose that we have a statement x ("Universal health care good for the economy.") which party A (Obama) believes to be true and party B (McCain) believes to be false. A verifier V (the voters) must decide which is correct. A and B therefore decide to hold a debate. However, they must agree on a format for the debate. In particular, how many speeches should each candidate be allowed to make? What order should the candidates give their speeches in? Does it matter?

We now formalize this idea of a debate. For a language L, we fix a polynomial-time verifier V and the length of the debate, i. Then, given an input x, the two parties in the debate x's membership in L. A tries to convince V that $x \in L$, while B tries to convince V that $x \notin L$. A and B are both assumed to be infinitely powerful.

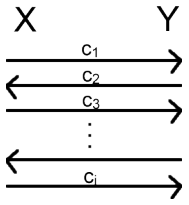

Figure 1: The basic structure of a debate.

Initially, A broadcasts a message c_1. B then responds with a message c_2. A then sends c_3, B sends c_4, and so on until i messages have been broadcast. V now takes the input x and the messages $c_1 \dots c_i$, and decides its final answer.

If $x \in L$, A should be able to win the debate, regardless of what B says. Equivalently,

$$x \in L \Longleftrightarrow \exists c_1 \forall c_2 \dots Q_i c_i V(x, c_1, c_2, \dots, c_i) = 1,$$

where $Q_i \in \{\exists, \forall\}$ is the i-th quantifier. We denote the class of languages recognizable an i-round debate in which A goes first by Σ_i^P.

If we wish to have B go first, then this becomes

$$x \in L \Longleftrightarrow \forall c_1 \exists c_2 \dots Q_i c_i V(x, c_1, c_2, \dots, c_i) = 1.$$

We denote the set of languages recognizable by such a debate by Π_P^i.

Note that we can also think of a debate as an alternating Turing Machine which uses exactly i alternations. If the machine starts with an existential quantifier, it corresponds to Σ_P^i. If it starts with a universal

quantifier, it corresponds to Π_P^i. At each quantifier in the alternation TM, we instead ask A or B which branch to take. In a debate, though, all messages are sent before any computation is performed, while in alternation, the computation is interleaved with the messages. However, since A and B are infinitely powerful, they can predict what queries would be made during the computation and simply answer ahead of time.

2 Basic Facts About Debates

We now list some of the basic facts about debates.

Observation 2 *$P = \Sigma_P^0 = \Sigma_P^0$, $NP = \Sigma_P^1$, and $coNP = \Pi_P^1$.*

Observation 3 *For all $i > 0$, $L \in \Sigma_P^i \iff \overline{L} \in \Pi_P^i$.*

Observation 4 *For all $i > 0$, $\Sigma_P^i \subseteq \Pi_P^{i+1}$ and $\Pi_P^i \subseteq \Sigma_P^{i+1}$.*

These follow directly from the definitions. For observation 3, have the verifier ignore the initial message.

We believe that each of these containments is strict. However, we can consider what would happen if two of these classes turned out to be equivalent. It that case, the entire hierarchy of classes would collapse to that level.

Theorem 5 *If $\Sigma_P^i = \Sigma_P^{i+1}$ if and only if $\Sigma_P^i = \Pi_P^i$. The same holds with Π and Σ reversed.*

Proof We first show that $\Sigma_P^i = \Sigma_P^{i+1}$ implies $\Sigma_P^i = \Pi_P^i$. By Observation 3, $\Pi_P^i \subseteq \Sigma_P^{i+1} = \Sigma_P^i$. For the containment in the other direction, by observation 4 that $L \in \Sigma_P^i$ implies $\overline{L} \in \Pi_P^i \subseteq \Sigma_P^{i+1} = \Sigma_P^{i+1}$. But then $\overline{\overline{L}} = L \in \Pi_P^i$.

For the other direction, we show that if $\Sigma_P^i = \Pi_P^i$, we must show that we can remove one round from the debate. Let $L' = \{(x, c_1) | \forall c_2 \exists c_3 \ldots Q_{i+1} c_{i+1}\} V(x, c_1, c_2, \ldots c_{i+1})\}$. This language is in Π_P^i, and so by assumption is also in Σ_P^i. Therefore, there is another debate for L' in which A goes first.

We can use the debate for L' to generate a debate for L by having A provide c_1 to the verifier in the first round of the debate. But then the debate has A sending two messages in a row, which means that we can simply merge those two messages into one. Therefore, the final debate for L only contains i rounds, as desired.

The proof in the case that Σ and Π are reversed is equivalent. ■

3 The Polynomial Hierarchy, the Infinite Hierarchy Assumption, and the Karp-Lipton Theorem

The polynomial hierarchy is the union over all debatable languages. Formally, we have

$$PH = \bigcup_{i>0} \Sigma_P^i = \bigcup_{i>0} \Pi_P^i.$$

We believe that each of these complexity classes is different. This belief is formalized by the IHA.

Assumption 6 (Infinite Hierarchy Assumption) *For all $i \geq 0$,*

$$\Sigma_P^i \neq \Sigma_P^{i+1}.$$

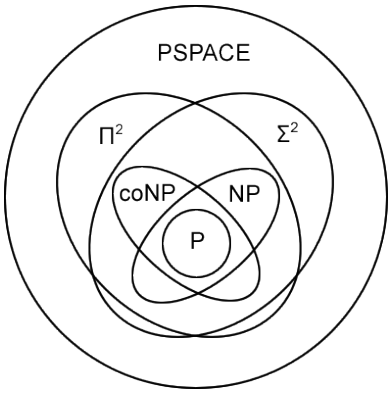

Figure 2: The relationships between classes in the polynomial hierarchy.

The view of the complexity world implied by the IHA is shown in Figure 2.

By Theorem 5, this corresponds to saying that $PH \neq \Sigma_P^i$, for any i. Note that $P \stackrel{?}{=} NP$ corresponds to the IHA for $i = 0$ and $NP \stackrel{?}{=} coNP$ corresponds to the case $i = 1$. The IHA, in other words, is very strong.

We now use the IHA to show that $NP \not\subseteq P/_{poly}$. Specifically, we show that if $NP \subseteq P/_{poly}$, then the polynomial hierarchy collapses to the third level. This result has been improved to the second level, but it remains open whether $NP \subseteq P/_{poly} \Rightarrow NP = coNP$.

We begin by showing that a short debate can determine if SAT has a small circuit. The debate goes as follows:

A: Send a small circuit C which purportedly computes SAT.

B: Send Φ such that either (i) $C(\Phi) =$ TRUE and $\forall x : \Phi(x) = 0$ or (ii) $C(\Phi) =$ FALSE and $\exists x : \Phi(x) = 1$. In case (ii), we also send x.

A: If B used case (i), A sends y such that $\Phi(y) = 1$.

V: The verifier now checks $C(\Phi)$, $\Phi(x)$, and $\Phi(y)$, and accepts or rejects accordingly.

If such a circuit for SAT exists, A sends it in step 1, and B cannot break it in step 2. Any such attempt will be corrected in step 3. However, if the circuit is wrong, B can highlight the error in step 2, and A cannot fix it in step 3.

We are now ready to prove Theorem 1.

Proof [Karp-Lipton Theorem] We assume that $NP \subseteq P/_{poly}$.

Consider a Σ_P^i debate for a language L, and let V be the verifier. We wish to remove the final round from the debate. Without loss of generality, we assume that the final message is sent by A (the proof is symmetric otherwise).

Define L' to be

$$L' = \{(x, c_1, c_2, \ldots c_{i-1}) | \exists c_i : V(x, c_1, \ldots, c_{i-1}, c_i) = 1\}$$

L' is in NP, and so by assumption L' has a small circuit. Therefore, if V knew the circuit for L', it could generate the final line of the debate without A. By the protocol given above, we can use a three-round debate to learn such a circuit. We therefore run the first $i - 1$ rounds from the protocol for L in parallel with the protocol for finding small circuits in parallel. At the end, the verifier checks the circuit-generating routine. If it is correct, it generates the final line of the original debate and then runs the original verifier from the i-round debate.

This entire routine takes $\max\{i - 1, 3\}$ rounds. We have therefore shown that $\Sigma_P^3 = \Sigma_P^4$, which collapses PH to the 3rd level in contradiction of the IHA. ■