CS 221: Computational Complexity	**Prof. Salil Vadhan**
Lecture Notes 7	
February 10, 2010	**Scribe: Kyu Bok Lee**

1 Agenda

- **PH** via oracles
- Time-Space Tradeoffs for SAT

2 Oracle TMs

Definition 1 *An* oracle TM M *is a TM with a special (write-only) oracle query tape, a (read-only) oracle answer tape, and an oracle query state.*

When M is run with an oracle $\mathcal{O} : \{0,1\}^* \to \{0,1\}^*$ and goes into an oracle query state with $q \in \{0,1\}^*$ on its query tape, then $\mathcal{O}(q)$ appears on the answer tape in 1 step.

Similarly, we can define oracle NTMs, coNTMs, ATMs,...

We can define new complexity classes given an oracle $\mathcal{O}$: $\mathbf{P}^{\mathcal{O}}, \mathbf{NP}^{\mathcal{O}}, \mathbf{co\text{-}NP}^{\mathcal{O}}$, etc.

Remark 2 *We have $\mathbf{P}^{\mathcal{O}} = \{L \subset \{0,1\}^* : L \leq_C \mathcal{O}\}$ since Cook reductions by definition are performed in deterministic polynomial time.*

Remark 3 *For a class $\mathcal{C}$ of functions or oracles, we note $\mathbf{P}^{\mathcal{C}} = \bigcup_{\mathcal{O}\in\mathcal{C}} \mathbf{P}^{\mathcal{O}} = \mathbf{P}^{\mathcal{O}^*}$ where $\mathcal{O}^*$ is any complete problem for $\mathcal{C}$ (even under $\leq_C$). And we define $\mathbf{\Delta^p_{k+1}} := \mathbf{P}^{\mathbf{\Sigma^p_k}}$.*

Theorem 4 $\mathbf{\Sigma^p_{k+1}} = \mathbf{NP}^{\mathbf{\Sigma^p_k}}$.

Proof: We first show $\mathbf{\Sigma^p_{k+1}} \subseteq \mathbf{NP}^{\mathbf{\Sigma^p_k}}$. Given $L \in \mathbf{\Sigma^p_{k+1}}$, there exists a polynomial time M such that

$$x \in L \iff \exists u_1 \forall u_2 \ldots Q_{k+1} u_{k+1}, M(x, u_1, \ldots, u_{k+1}),$$

where the length of each u_i is bounded by some fixed polynomial. Define a new language L' which is in $\mathbf{\Pi^p_k}$:

$$L' := \{(x, u_1) : \forall u_2 \exists u_3 \ldots Q_{k+1} u_{k+1}, M(x, u_1, \ldots, u_{k+1})\} \in \mathbf{\Pi^p_k}.$$

We can easily give an $\mathbf{NP}^{L'}$ algorithm for L:

- Nondeterministically guess u_1.
- Ask oracle $(x, u_1) \in L'$, and `accept`/`reject` accordingly.

Now we show the inclusion in the other direction: $\mathbf{NP}^{\mathbf{\Sigma_k^p}} \subseteq \mathbf{\Sigma_{k+1}^p}$.
Given $L \in \mathbf{NP}^{\mathbf{\Sigma_k^p}}$, decided by some oracle NTM M (using an oracle $L' \in \mathbf{\Sigma_k^p}$), our first attempt at $\mathbf{\Sigma_{k+1}^p}$ algorithm for L may be the following:

- Simulate M by using the first $\exists$ for M's nondeterminism.
- Use remaining k quantifiers for queries to L'.

The problem with this approach is that we can run out of quantifiers for answering the first query. The correct $\mathbf{\Sigma_{k+1}^p}$ simulation on input x is the following (by observing that M can make at most polynomially many queries to L'):

- We can guess all of M's nondeterministic choices $c_1, \ldots, c_m$, the correct sequence of queries $q_1, \ldots, q_k$, and the answers $a_1, \ldots, a_k \in \{0, 1\}$ using a single $\exists$. (There are polynomially many.)
- Now we can verify that $M(x)$ would make the queries $q_1, \ldots, q_t$ given nondeterministic choices $c_1, \ldots, c_m$ and answers $a_1, \ldots, a_t$.
- Next we can verify that $L'(q_i) = a_i$ for $i = 1, \ldots, t$ using the remaining k alternations (in parallel for all i).

Our claim follows. ■

Corollary 5 $\mathbf{\Sigma_{k+1}^p} = \mathbf{NP}^{\mathbf{\Sigma_k^p}} = \mathbf{NP}^{\Sigma_k \mathrm{SAT}} = \mathbf{NP}^{\mathbf{\Pi_k^p}}$

Proof Sketch: We can just flip the answer of the oracles. □

3 Time-Space Tradeoffs

Definition 6

$$\mathbf{TISP}(T(n), S(n)) := \{L : L \textit{ decided by TMs running in time } O(T(n)) \textit{ and space } O(S(n))\}.$$

Theorem 7 *For all* $\varepsilon > 0$, SAT $\notin \mathbf{TISP}(n^{1+o(1)}, n^{1-\varepsilon})$.

Remark 8 *The above result also holds on a RAM model.*

Lemma 9 *For all* $\varepsilon > 0$, $\mathbf{TISP}(T^{1+o(1)}, T^{1-\varepsilon}) \subseteq \mathbf{\Sigma_2 TIME}(T^{1-\varepsilon'})$ *provided* $\varepsilon' < \varepsilon/2$.
Here $T = T(n)$ *and* $T(n)^{1-\varepsilon'} \geq n$ *(time-constructible).*

Proof of Lemma: The proof is similar to the proof of the result $\mathbf{PSPACE} \subseteq \mathbf{AP}$.
Given M running in $\mathbf{TISP}(T^{1+o(1)}, T^{1-\varepsilon})$, $\mathbf{\Sigma_2 TIME}$ simulation on M will work as follows:

- $\exists$ guesses a sequence of configurations $C_1, \ldots, C_{T^{\varepsilon/2}}$. (takes time $T^{\varepsilon/2} \cdot T^{1-\varepsilon} < T^{1-\varepsilon'}$)
- $\forall_i$ verifies that $C_i \to C_{i+1}$ runs within $T^{1-\varepsilon'}$ steps and that $C_{T^{\varepsilon/2}}$ is accepting. (takes time $T^{1-\varepsilon'}$)

■

Proof of Theorem 7: Suppose SAT $\in \mathbf{TISP}(n^{1+o(1)}, n^{1-\varepsilon})$. This implies $\mathbf{NTIME}(n) \subseteq \mathbf{TISP}(n^{1+o(1)}, n^{1-\varepsilon'})$ since $\mathbf{NTIME}(n)$ reduces to SAT by reduction that runs in time $O(n \log n)$ and space $O(\log n)$. Now by translation, we get the first line of inclusion below

$$\begin{aligned} \mathbf{DTIME}(n^2) \subseteq \mathbf{NTIME}(n^2) &\subseteq \mathbf{TISP}(n^{2+o(1)}, n^{2-\varepsilon''}) \\ &\subseteq \mathbf{\Sigma_2 TIME}(n^{2-\varepsilon'''}) \qquad \text{(by Lemma)} \\ &\subseteq \mathbf{DTIME}(n^{2-\varepsilon''''}) \end{aligned}$$

The second inclusion is established by the lemma above. The third inclusion follows from

$$\mathbf{NTIME}(n) \subseteq \mathbf{DTIME}(f(n)) \implies \mathbf{\Sigma_k TIME}(t(n)) \subseteq \mathbf{DTIME}(f^{(k)}(t(n)))$$

and $f(n) = n^{1+o(1)} \implies f(f(n)) = n^{1+o(1)}$.

This contradicts the time hierarchy theorem! $\blacksquare$