CS221: Computational Complexity Prof. Salil Vadhan

Lecture 13: Does the PH collapse? and an application of alternation, $\mathbf{DTIME}(n) \neq \mathbf{DTIME}(n)$

10/21 *Scribe: Grant Schoenebeck*

Contents

1 Recap on Polynomial Hierarchy

$\Sigma_k\mathbf{P}$: can have up to k alternations and starts with an exist alternation.

$\Pi_k\mathbf{P}$: can have up to k alternations and starts with a for all alternation.

$PH = \bigcup_k \Sigma_k\mathbf{P}$

$QBF_k = \{\varphi(x_1, \ldots, x_k) : \exists x_1, \forall x_2, \ldots Qx_k \text{ such that } \varphi(x_1, \ldots, x_k) = 1\}$

Theorem 1 *QBF_k is complete for $\Sigma_k\mathbf{P}$*

Theorem 2 $\Sigma_k\mathbf{P} = \mathbf{NP}^{\Sigma_{k-1}\mathbf{P}} (= \mathbf{NP}^{\Pi_{k-1}\mathbf{P}})$

$\Pi_k\mathbf{P} = \mathbf{co\text{-}NP}^{\Sigma_{k-1}\mathbf{P}}$

Definition 3 $\Delta_k\mathbf{P} = \mathbf{P}^{\Sigma_{k-1}\mathbf{P}}$

2 Does PH Collapse?

Theorem 4 $\Sigma_k\mathbf{P} = \Pi_k\mathbf{P} \Rightarrow \forall j \geq k\ \Sigma_j\mathbf{P} = \Pi_j\mathbf{P} = \Sigma_k\mathbf{P}$. *That is to say that the the PH would collapse to the kth level.*

Remark 5 *This is part of the general trend that equality translates upward and inequality translates downward.*

Intuitively the classes are not closed under complement, and if they were the hierarchy would fall.

Proof:

It suffices to show that $\Sigma_k\mathbf{P} = \Pi_k\mathbf{P} \Rightarrow QBF_k \in \Sigma_k\mathbf{P}$. This would then imply that $\Sigma_{k+1}\mathbf{P} = \Sigma_k\mathbf{P}$ and it follows that that $\Sigma_{k+1}\mathbf{P} = \Pi_{k+1}\mathbf{P}$. Then we can proceed by induction.

So we examine the problem $\exists x_1, \forall x_2, \ldots, Qx_k$ such that $\varphi(x_1, \ldots, x_k) = 1$. If we fix x_1 we get an instance of $\overline{QBF_k} \in \Pi_k\mathbf{P}$. Call the formula with a fixed x_1 ψ_{x_1}. (It begins with a for all clause.) But by assumption $\Pi_k\mathbf{P} = \Sigma_k\mathbf{P}$ so $\overline{QBF_k} \in \Sigma_k\mathbf{P}$. So now we can guess x_1 and run the $\Sigma_k\mathbf{P}$ algorithm on ψ_{x_1}, but this is also a $\Sigma_k\mathbf{P}$ algorithm.

■

Corollary 6 $\mathbf{P} = \mathbf{NP} \Rightarrow \mathbf{PH}$ *collapses.* $\mathbf{PH} = \mathbf{P} = \mathbf{NP}$.

Corollary 7 $\mathbf{NP} = \mathbf{co\text{-}NP} \Rightarrow \mathbf{PH}$ *collapses to* $\mathbf{NP}$.

Remark 8 *Normally when we show such results we show them with a complete language and a reduction. For instance, we can reduce any language in* $\mathbf{NP}$ *to SAT so if* $SAT \in \mathbf{P} \Rightarrow \mathbf{NP} \subseteq \mathbf{P}$*, but here we have shown that* $SAT \in \mathbf{P} \Rightarrow \mathbf{PH} = \mathbf{P}$ *without ever giving a reduction.*

If $\mathbf{NP} \subseteq \mathbf{TIME}(t(n)) \Rightarrow \mathbf{PH} \subset$?? or $\Sigma_k\mathbf{P} \subset$??. What if $\mathbf{NTIME}(n^2) = \mathbf{TIME}(n^2)$?

Conjecture 9 $\mathbf{PH}$ *does not collapse.*

Evidence for it:

- Analogy with Arithmetic Hierarchy in Recursion Theory (known to work). But not everything seems analogous, for instance in recursion theory the recursive languages = RE languages ∩ coRE languages, but it seems unlikely that $\mathbf{P} = \mathbf{NP} \cap \mathbf{co\text{-}NP}$.

Reasons to be skeptical:

- Would mean that any constant number of quantifiers can be replaced by a fixed number of qualifiers.
- Humans have trouble with more than a few qualifiers.
- There are very few natural problems in the higher levels of **PH**.

Remark 10 *There are many results of the form, if X is true the the* **PH** *collapses.*

3 An application of Alternation(Paul, Pippenser, Szemeredi, Trotter)

Theorem 11 $\mathbf{TIME}(f(n)) \subseteq \Sigma_4\mathbf{TIME}(o(f(n)))$ *if f is a proper complexity function.* $(o(f(n)) = O\left(\frac{f(n)}{\log^*(n)}\right))$.

Corollary 12 $\mathbf{NTIME}(n) \neq \mathbf{TIME}(n)$

Proof Corollary: Proof is in 4 easy steps:

1) Suppose that are equal.

2) $\Rightarrow \Sigma_4\mathbf{TIME}(n) = \mathbf{TIME}(n)$ (analogous to $\mathbf{P} = \mathbf{NP} \Rightarrow \mathbf{PH} = \mathbf{P}$.) must prove the previous results with out passing through QBF otherwise it blows up more than a linear amount (can just use certificates to do this).

3) By padding $\Sigma_4\mathbf{TIME}(f(n)) \leq \mathbf{TIME}(f(n) \leq \Sigma_4\mathbf{TIME}(o(f(n)))$ (by Thm).

4) This contradicts a hierarchy theorem for Σ_4 time. (Such theorems are more refined for the **PH** than they are in general.)

■

Proof Sketch: In five not so easy steps.

Given a TM $M \in \mathbf{TIME}(f(n))$

1) Simulate M by a "block-respecting" TM M_b. Divide the tapes of M to blocks of size $b(n) = \sqrt{f(n)}$. Then the heads of M_b only cross boundaries of these blocks at time increments which are integer multiples of $b(n)$. What

this means is that we divide the computations that M performs into $a(n) = \frac{f(n)}{b(n)} = \sqrt{f(n)}$ segments of length $\sqrt{f(n)}$.

How do we make such a TM? In some way we copy the information from the adjacent blocks to the current block. The specifics are messy.

2) Define a computational graph G [Valient]. The vertices of such a graph $V = \{1, \ldots, a(n)\}$ correspond to the time segments. The edges are $(i, i+1) \forall i$ and (i, j) if for some tape of M_b the block of cells used in time j was last used in time i (this graph represents information flow through time in the computation).

3) Observe structural properties of graph. In degree $\leq k + 1$ (k = number of tapes). Can decompose it into the union of 2k + 1 graphs of degree ≤ 1 (no crossing).

4) (Hard) Graph-theoretic lemma. Every such graph has $o(a(n))$ segregators of size $o(a(n))$. Can remove o(a(n)) "predecessors" not necessarily immediate.

5) Σ_4 simulation. $\exists$ Guess computations in removed time steps. $\forall$ Check that the computations link together well. (they have very few predecessors so there is relatively little to guess and to check).

□