Problem Set 3
More Exercises on the Polynomial Hierarchy PH
CSCI 6114 Fall 2023

Joshua A. Grochow

Released: September 19, 2023
Due: Monday September 25, 2023

Reading by Thursday Sep 21

Du & Ko Sections 3.1 and 3.2

In-class exercises

1. (a) Show that a language L is in NP iff there exists a poly-time verifier V such that for all x,

$$x \in L \iff (\exists^p y_1)(\exists^p y_2) V(x, y_1, y_2) = 1.$$

   (b) Show that it is only the number of quantifier *alternations* that matter, and not the total number of quantifiers in the definition of $\mathsf{\Sigma_k P}$. More specifically, if in the definition of $\mathsf{\Sigma_k P}$ we allow a block of $\exists^p$ quantifier or a block of $\forall^p$ quantifiers in place of any one of the $\exists^p/\forall^p$ quantifiers in the definition above, we get back the same class.

Definition 1. If $\mathsf{PH} = \mathsf{\Sigma_k P}$ for some fixed k, we say that PH *collapses* (to the k-th level), and otherwise that PH is *infinite*. (Note the latter is a slight abuse of terminology since PH always contains infinitely many langauges.)

2. Show that if there exists $k \geq 0$ such that $\mathsf{\Sigma_k P} = \mathsf{\Pi_k P}$ then $\mathsf{PH} = \mathsf{\Sigma_k P}$. *Hint:* Use the previous problem.

3. (Oracle characterization of PH)

   (a) Show that $\mathsf{P}^{\mathsf{NP}} \subseteq \Sigma_2\mathsf{P}$. Use the fact that P^{NP} is closed under complement to conclude that $\mathsf{P}^{\mathsf{NP}} \subseteq \Sigma_2\mathsf{P} \cap \Pi_2\mathsf{P}$.

   (b) Show that $\Sigma_2\mathsf{P} = \mathsf{NP}^{\mathsf{NP}}$. *Hint:* the idea from part (a) may be useful.

   (c) (Read this one, take on faith in class, do outside of class.) More generally, show that $\Sigma_k\mathsf{P} = \mathsf{NP}^{\Sigma_{k-1}\mathsf{P}} = \Sigma_{k-1}\mathsf{P}^{\mathsf{NP}}$ and $\Pi_k\mathsf{P} = \mathsf{coNP}^{\Pi_{k-1}\mathsf{P}}$. This is called the *oracle characterization* of PH (since it can be used to give an alternative, equivalent, oracle-based definition of $\Sigma_k\mathsf{P}$).

4. Use the oracle characterization of PH to give an alternative (arguably simpler) proof that if $\Sigma_k\mathsf{P} = \Sigma_{k+1}\mathsf{P}$, then $\mathsf{PH} = \Sigma_k\mathsf{P}$.

5. (In which we'll prove the Karp–Lipton Theorem)

   (a) Recall the search-to-decision reduction for SAT from PS1 Q7(a). Show that if $\mathsf{NP} \subseteq \mathsf{P/poly}$, then there is a circuit family (C_n) such that, for all satisfiable Boolean formulas $\varphi(x)$, $\varphi(C_n(\varphi)) = 1$, that is, $C_n(\varphi)$ outputs a satisfying assignment to φ (when one exists). (When one does not exist, we may assume C_n outputs the all-0 string.)

   (b) Show that if $\mathsf{NP} \subseteq \mathsf{P/poly}$ then $\Sigma_2\mathsf{P} = \Pi_2\mathsf{P}$ (and therefore PH collapses to the second level). *Hint:* use part (a). What do you notice about the order of quantifiers?

Outside of class exercises

- Remember to do Exercise 3c above

6. (a) Show that if there exists a $k \geq 0$ such that $\Sigma_k\mathsf{P} = \Sigma_{k+1}\mathsf{P}$, then $\mathsf{PH} = \Sigma_k\mathsf{P}$.

   (b) Show that if PH has a complete problem, then PH collapses.

7. Recall that previously in class we showed that $\mathsf{NP} \cup \mathsf{coNP} \subseteq \mathsf{P}^{\mathsf{NP}}$. Observe that that proof and the proof of Exercise 3a above both relativize, to give a simple proof that $\Sigma_k\mathsf{P} \cup \Pi_k\mathsf{P} \subseteq \mathsf{P}^{\Sigma_k\mathsf{P}} \subseteq \Sigma_{k+1}\mathsf{P} \cap \Pi_{k+1}\mathsf{P}$ for all $k \geq 0$.

Open question: (If you know or look up what the arithmetic hierarchy is from computability theory) Is there an oracle relative to which "PH looks like AH", in the following sense? In the arithmetic hierarchy, we have $\mathsf{\Sigma^0_k} \cup \mathsf{\Pi^0_k} \subsetneq \mathsf{COMP}^{\mathsf{\Sigma^0_k}} = \mathsf{\Sigma^0_{k+1}} \cap \mathsf{\Pi^0_{k+1}}$ for all $k \geq 0$ (note the *strict* containment!). Is there an oracle X such that

$$\mathsf{\Sigma_k P}^X \cup \mathsf{\Pi_k P}^X \subsetneq \mathsf{P}^{\mathsf{\Sigma_k P}^X} = \mathsf{\Sigma_{k+1} P}^X \cap \mathsf{\Pi_{k+1} P}^X$$

for all $k \geq 0$?

8. We define the decision problem $\Sigma_k CIRCUIT\text{-}SAT$ as follows:

    Σ_k **CIRCUIT-SAT**
    Input: A Boolean circuit $\varphi(x_1, \ldots, x_m)$, together with a partition of $\{1, \ldots, m\}$ into k subsets $S_1, \ldots, S_k$.
    Decide: It is the case that $\exists \vec{y} \forall \vec{z} \cdots (\exists/\forall \vec{w}) \varphi(\vec{y}, \vec{z}, \ldots, \vec{w}) = 1$, where $\vec{y} = \vec{x}|_{S_1}, \vec{z} = \vec{x}|_{S_2}, \ldots, \vec{w} = \vec{x}|_{S_k}$, and the final quantifier is $\exists$ if k is odd and $\forall$ if k is even.

    Note 1: these are *not* "$\exists^p$"-style quantifiers, and that each vector $\vec{y}, \vec{z}, \ldots, \vec{w}$ is a vector of Boolean variables. The decision problem is to decide whether the quantified mathematical statement is true or false (note: the question is *not* satisfiable vs unsatisfiable, since all variables are quantified, but literally a true statement or a false statement).

    Note 2: CIRCUIT-SAT is the same as $\Sigma_1 CIRCUIT\text{-}SAT$. (That is, satisfiable unquantified circuits are in essence the same as true statements that are $\exists$-quantified circuits.)

    Question. Show that for any $k \geq 1$, $\Sigma_k CIRCUIT\text{-}SAT$ is $\mathsf{\Sigma_k P}$-complete. (It's also true for $k = 0$, but for somewhat trivial reasons.) *Hint:* Use the idea of the proof that $\mathsf{P} \subseteq \mathsf{P/poly}$ from the first set of exercises.

    (Foreshadowing: when we get to PSPACE, we will see that a related problem, Totally Quantified Boolean Formulas, or TQBF, is PSPACE-complete. TQBF is just like $\Sigma_k CIRCUIT\text{-}SAT$ except that there is no limit placed on how many quantifier alternations there can be.)

Resources

- Schöning & Pruim, *Gems of TCS*, Ch. 16. This is a nice, brief overview of what we've done in class, plus introduces the Boolean Hierarchy (what you get by taking Boolean combinations—AND, OR, NOT—of languages in NP) and shows that if BH collapses to any level, then PH collapses to its second level. And has additional nice references.

- Schaefer and Umans gave a list of many problems that are complete for the second (and a few higher) level of PH in a series of two papers.
- Du & Ko Ch. 3
- Arora & Barak Ch. 5
- Hemaspaandra & Ogihara, *Complexity Theory Companion*, Appendix A.4.1. Quick "cheat sheet"-style definitions.
- Homer & Selman §7.4