Exercises on the Polynomial Hierarchy PH and circuits
CSCI 6114 Fall 2026

Joshua A. Grochow

September 3, 2026

Resources

- PH was defined in Stockmeyer, *Theoret. Comp. Sci.*, 1976
- Arora & Barak Ch. 5
- Du & Ko Ch. 3
- Schöning & Pruim, *Gems of TCS*, Ch. 16
- Hemaspaandra & Ogihara, *Complexity Theory Companion*, Appendix A.4.1
- Homer & Selman §7.4 do PH in terms of oracles; we'll see that characterization later, so I'm including it here for future reference, but we haven't gotten to it yet.

Problems

1. (Completing the proof of the Karp–Lipton Theorem)

   (a) For any polynomial-time verifier V we get a language $L_V \in \mathsf{NP}$ defined by $(\forall x)[x \in L \iff \exists^p y V(x,y) = 1]$. Given such a verifier V, let us define

   $$L_{V,left} := \{(x,y) : \exists^p z V(x,yz) = 1\},$$

   that is, the second part of the input, y, is a *prefix* of a V-witness that x is in L_V. Show that for any such language, $L_{V,left}$ is self-reducible, in the sense that the search problem for $L_{V,left}$ (given

(x, y) find a z such that $V(x, yz) = 1$) reduces (by oracle) to the decision problem for $L_{V,left}$ (similar to the problem about SAT from PS1).

(b) Given a polynomial-size circuit (family) C for $L_{V,left}$, show that there exists a polynomial-size circuit (family) D such that $D(x, y)$ outputs $1z$ such that $V(x, yz) = 1$, if any such z exists, and otherwise D outputs 0. (This is basically the "circuit version" of the search-to-decision reduction.)

2. (Kannan's Theorem)

(a) Let $\mathsf{CktSize}(n^k)$ denote the class of language L that are computable by circuit families of size $O(n^k)$ (so, in particular, $\mathsf{CktP} = \bigcup_k \mathsf{CktSize}(n^k)$). Assume Shannon's Theorem, that there exist languages that require circuits of size $\Omega(2^n/n)$. Use this to prove that $\mathsf{CktSize}(N^k) \subsetneq \mathsf{CktSize}(N^{k+1})$. *Hint:* Consider an n-bit function from Shannon's Theorem, but applied to the first n bits of an input of length $N > n$. What size does n need to be to get the resulting function to be in $\mathsf{CktSize}(N^{k+1})$?

(b) Prove that for all k, there exists a language $L_k \in \mathsf{PH} \cap \mathsf{CktSize}(n^{k+1})$ such that L_k is not computed by circuit families of size $O(n^k)$. *Hint:* write down the definition of "circuit family of size $O(n^{k+1})$ not computed by circuit families of size $O(n^k)$" and see how many quantifiers you need. You can do it with only 3 or 4, but if you need more that's okay.

(c) Prove that for every k there exists a language $L_k \in \Sigma_2\mathsf{P}$ that is not in $\mathsf{CktSize}(n^k)$. *Hint:* Split into two cases, depending on whether $\mathsf{NP} \subseteq \mathsf{CktP}$ or not. In one case, use Karp–Lipton.

3. The *complement* of a language $L \subseteq \Sigma^*$ is $\overline{L} := \{x \in \Sigma^* : x \notin L\}$. If $\mathcal{C}$ is a collection of languages, then we define $\mathsf{co}\mathcal{C} := \{\overline{L} : L \in \mathcal{C}\}$.

(a) Show that for any complexity class $\mathcal{C}$, $\mathcal{C} \subseteq \mathsf{co}\mathcal{C}$ iff $\mathcal{C} = \mathsf{co}\mathcal{C}$.

(b) Show that $\mathsf{P} = \mathsf{coP}$. (We say that P "is closed under complement.")

(c) Show that for any $\mathcal{C}$, $\mathsf{co}\mathcal{C} \cup \mathcal{C}$ and $\mathsf{co}\mathcal{C} \cap \mathcal{C}$ are closed under complement.

4. Is $\mathsf{NP} = \mathsf{coNP}$? This is a hard problem. Try to convince each other one way or the other.

5. Show that $\Sigma_k\mathsf{P} = \mathsf{co}\Pi_k\mathsf{P}$. That is, $L \in \Sigma_k\mathsf{P}$ iff $\overline{L} \in \Pi_k\mathsf{P}$ ($\overline{L}$ is our notation for the complement language, $\overline{L} := \Sigma^* \backslash L = \{x \in \Sigma^* | x \notin L\}$). If this feels too abstract, start with $k = 1$.

6. Show that $\mathsf{P} = \Sigma_0\mathsf{P} = \Pi_0\mathsf{P}$, $\mathsf{NP} = \Sigma_1\mathsf{P}$, and $\mathsf{coNP} = \Pi_1\mathsf{P}$.

7. Show that $\Sigma_k\mathsf{P} \subseteq \Sigma_{k+1}\mathsf{P} \cap \Pi_{k+1}\mathsf{P}$. Conclude that (a) $\Sigma_k\mathsf{P} \cup \Pi_k\mathsf{P} \subseteq \Sigma_{k+1}\mathsf{P} \cap \Pi_{k+1}\mathsf{P}$, (b) $\mathsf{PH} = \bigcup_{k \geq 0} \Pi_k\mathsf{P}$.

8. Show that $\Sigma_k\mathsf{P} = \Pi_k\mathsf{P}$ if and only if $\mathsf{PH} = \Sigma_k\mathsf{P}$. (Stated but not proved in class.)