Complexity Theory Exercies

Ray Tsai

Diagonolization

Problem 3.1

Prove that $\mathbf{SPACE}(n) \neq \mathbf{NP}$.

Proof. We prove that $\mathbf{NP}$ is closed under log-space reduction but $\mathbf{SPACE}(n)$ is not.

Given a log-space reduction from L_1 to L_2, there is a log-space turing machine R which performs the reduction. Since $\mathbf{SPACE}(\log n) \subset P$, both the runtime and the output length of R is bounded by a polynomial. If $L_2 \in \mathbf{NP}$, then there exists a polynomial-time non-deterministic turning machine M which decides L_2. Hence, a non-deterministic turning machine which runs R then M decides L_1 in polynomial-time, and so $L_1 \in \mathbf{NP}$.

We now show that $\mathbf{SPACE}(n)$ is not closed under log-space reduction. Let R be a reduction which pads $n^2 - n$ 1's after an input of length n. Note that R uses $O(\log n)$ space. Pick $L_1 \in \mathbf{SPACE}(n^2) \backslash \mathbf{SPACE}(n)$, and let L_2 be the padded version of L_1. Consider a turing machine M which checks the (1) input is of a square number length, say $|x| = n^2$, (2) checks the first n symbols are in L_1, and (3) checks the remaining $n^2 - n$ symbols are all 1's. M decides L_2. Since step (1) and (3) takes $O(\log n)$ space, and (2) takes $O(|x|) = O(n^2)$ space, M only uses linear space. But then $L_2 \in \mathbf{SPACE}(n)$ and $L_1 \notin \mathbf{SPACE}(n)$. □

Polynomial Hierarchy

Problem 5.3

Show that if `3SAT` is polynomial-time reducible to $\overline{\texttt{3SAT}}$, then $\mathbf{PH} = \mathbf{NP}$.

Proof. We show that $\Sigma_i^p, \Pi_i^p \subseteq NP$ for all $i \geq 1$, by induction on i. Since `3SAT` is $\mathbf{NP}$-complete, $\mathbf{NP} \subseteq \mathbf{coNP}$ by assumption. Let $L \in \mathbf{coNP}$. Since $\texttt{3SAT} \in \mathbf{coNP}$, $\overline{\texttt{3SAT}} \in \mathbf{NP}$. But then $\overline{\texttt{3SAT}}$ is $\mathbf{coNP}$-complete, and thus $\mathbf{coNP} \subseteq \mathbf{NP}$. Hence, $\Pi_1^p = \mathbf{NP}$. Suppose $i \geq 2$. Let $L \in \Sigma_i^p$. There exists a polynomial-time turing maching M and a polynomial q such that $x \in L$ if and only if

$$\exists u_1 \in \{0,1\}^{q(|x|)} \forall u_2 \in \{0,1\}^{q(|x|)} \cdots Q_i u_i \in \{0,1\}^{q(|x|)}, M(x, u_1, u_2, \ldots, u_i) = 1.$$

Define language L' such that $\langle x, u_1 \rangle \in L'$ if and only if

$$\forall u_2 \in \{0,1\}^{q(|x|)} \cdots Q_i u_i \in \{0,1\}^{q(|x|)}, M(x, u_1, u_2, \ldots, u_i) = 1.$$

By induction, $L' \in \Pi_{i-1}^p \subseteq \mathbf{NP}$, so there exists a polynomial-time turing machine M' which verifies L'. Combining it into L, we get $x \in L$ if and only if

$$\exists (u_1, u_2) \in \{0,1\}^{2q(|x|)}, M'(x, u_1, u_2) = 1.$$

Hence, $L \in \mathbf{NP}$. By the same argument, we may also show that $\Pi_i^p \subseteq \mathbf{coNP}$. But then by the base case, $\mathbf{coNP} = \mathbf{NP}$, and this completes the induction. $\square$

Problem 5.11

Show that $\texttt{SUCCINCT SET-COVER} \in \Sigma_2^p$.

Proof. Let $S = \{\varphi_1, \ldots, \varphi_m\}$ be a set of 3-DNF formulae on n variables $V = \{v_1, \ldots, v_n\}$. $\langle S, k\rangle \in \texttt{SUCCINCT SET-COVER}$ if and only if there exists $I \subseteq [m]$ such that $|I| \leq k$ and for all assignments to $\bigvee_{i \in I} \varphi_i$ results in 1. Hence, there exists a turing machine M such that $\langle S, k\rangle \in \texttt{SUCCINCT SET-COVER}$ if and only if

$$\exists I \subseteq [m]\ \forall f : V \to \{0,1\}, M(S, k, I, f) = 1.$$

Since calculating each φ_i with assignment f takes polynomial time and there are at most m of them, M runs in polynomial time. Hence, $\texttt{SUCCINCT SET-COVER} \in \Sigma_2^p$. $\square$

Problem 5.13

This problem studies the Vapnik-Chervonenkis (VC) dimensions, an important concept in machine learning. If $\mathcal{S} = \{S_1, S_2, \ldots, S_m\}$ is a collection of subsets of a finite set U, the *VC dimension* of $\mathcal{S}$, denoted $VC(\mathcal{S})$, is the size of the largest set $X \subseteq U$ such that for every $X' \subseteq X$, there is an i for which $S_i \cap X = X'$. (We say that X is shattered by S.)

A Boolean circuit C succinctly represents collection $\mathcal{S}$ if S_i consists of exactly those elements $x \in U$ for which $C(i, x) = 1$. Finally, the

$$\text{VC-DIMENSION} = \{\langle C, k\rangle : C \text{ represents a collection } \mathcal{S} \text{ s.t. } VC(\mathcal{S}) \geq k\}$$

(a) Show that VC-DIMENSION $\in \Sigma_3^p$.

Proof. Let U be a set. $\langle C, k\rangle \in$ VC-DIMENSION if and only if

$$\exists X \subseteq U\ \forall X' \subseteq X\ \exists i \in [m], X \geq k \text{ and } \forall x \in X, x \in X' \Leftrightarrow C(i, x) = 1. \quad (1)$$

Note that a collection $\mathcal{S}$ of 2^m subsets of U can shatter a subset $X \subseteq U$ of size at most m, as each subset X' of X corresponds an $S_i \in S$ such that $S_i \cap X = X'$. Hence, the VC dimension of $\mathcal{S}$ is at most m. Suppose circuit C represents $\mathcal{S}$. Since $m \leq |C|$, $|X|$, $|X'|$, and $|i|$ are bounded by $|C|$, and thus (1) can be computed in polynomial time with respect to $|C|$. Therefore, VC-DIMENSION $\in \Sigma_3^p$. $\square$

(b) Show that VC-DIMENSION is Σ_3^p-complete.

Proof. It suffices to show an polynomial-time reduction Σ_3SAT to VC-DIMENSION. idk how tho :($\square$