CISC 462 — Computability and Complexity
Problem Set 5
Solutions

Queen's University, Winter 2017

1. (a) $\mathbf{TIME}(4^n) = \mathbf{TIME}(4^{n+4})$, since $4^{n+4} = 4^4 \cdot 4^n = O(4^n)$.

   (b) $\mathbf{SPACE}(2^n) \subsetneq \mathbf{SPACE}(2^{2n})$, since $2^n \leq 2^{2n}$ for all n.

   (c) The relationship between $\mathbf{NSPACE}(n \log n)$ and $\mathbf{SPACE}(n \log^2 n)$ is not known. By Savitch's theorem we have $\mathbf{NSPACE}(n \log n) \subseteq \mathbf{SPACE}(n^2 \log^2 n)$ and by the space hierarchy theorem, we have $\mathbf{SPACE}(n \log^2 n) \subsetneq \mathbf{SPACE}(n^2 \log^2 n)$. However, we cannot conclude anything about the relationship between the two classes from this.

   (d) $\mathbf{NTIME}(n^2) \subsetneq \mathbf{SPACE}(n^{\log n})$. We have $\mathbf{NTIME}(n^2) \subseteq \mathbf{NSPACE}(n^2)$, since every branch of computation for an $f(n)$-time machine can use at most $f(n)$ space. Then by Savitch's theorem we have $\mathbf{NSPACE}(n^2) \subseteq \mathbf{SPACE}(n^4)$. Finally, by the space hierarchy theorem, we have $\mathbf{SPACE}(n^4) \subsetneq \mathbf{SPACE}(n^{\log n})$ since $n^4 = o(n^{\log n})$.

   (e) $\mathbf{TIME}(n^3) \supsetneq \mathbf{TIME}(f(n))$, where

   $$f(n) = \begin{cases} n2^n & \text{when } n \leq 10^9, \\ n^2 \log n & \text{otherwise,} \end{cases}$$

   since $f(n) = o\left(\frac{n^3}{\log n^3}\right)$. To see this, we note that for all $n > 10^9$, we have $f(n) = n^2 \log n < \frac{n^3}{\log n^3}$.

2. Let M be a machine that decides L in time n^6. Now, consider the machine M' for $p(L, n^2)$ that on input w, checks if w has the form $p(u, |u|^2)$ for some string $u \in \Sigma^*$. If not, *reject*. Otherwise, simulate M on u. Then M' runs in time $O(|w|^3) + O(|u|^6) = O(|w|^3)$.

3. Suppose $\mathbf{NP} = \mathbf{P}^{\text{SAT}}$ and let $L \in \mathbf{NP}$. Consider $\overline{L} \in \mathbf{coNP}$. Then we can reduce $\overline{L}$ to $\overline{\text{SAT}}$. Note that $\overline{\text{SAT}} \in \mathbf{P}^{\text{SAT}}$, since for a given boolean formula φ, we simply query the oracle O for SAT to determine whether φ is satisfiable or not. Then this means $\overline{L} \in \mathbf{P}^{\text{SAT}}$ and $\mathbf{coNP} \subseteq \mathbf{NP}$. But by $\mathbf{NP}$-completeness, we have SAT $\leq_P \overline{\text{SAT}}$ and therefore $\overline{\text{SAT}} \leq_P$ SAT. Therefore, $\mathbf{NP} = \mathbf{coNP}$.

4. We can describe a polynomial time algorithm assuming we have access to an oracle O for SAT. Given a boolean formula φ, we query O to determine whether φ is satisfiable. If it isn't, *reject*. Otherwise, we continue onto the next step. Let $x_1, \ldots, x_n$ be the variables in φ and let $\varphi[x_i = X]$ be the formula φ with x_i set to X where X is either 0 or 1. For each variable x_i, query O to determine whether $\varphi[x_i = 0]$ and $\varphi[x_i = 1]$

are satisfiable. If both are satisfiable, we have found two satisfying assignments, so *reject*. If we have queried all variables and not rejected, then φ has a unique satisfying assignment. This runs in polynomial time since all we do is query the oracle twice for each variable of φ.

5. We'll show by induction on i that $\Sigma_i^P, \Pi_i^P \subseteq \mathbf{P}$. Since $\mathbf{P} = \mathbf{NP} = \mathbf{coNP}$, this is true for $i = 1$. Now, suppose it is true for $i-1$ and consider i.

   Let $L \in \Sigma_i^P$. By definition, there is a polynomial time TM M and polynoimal n^c such that

   $$w \in L \quad \Longleftrightarrow \quad \exists u_1 \in \Sigma^{n^c} \forall u_2 \in \Sigma^{n^c} \cdots Q_i u_i \in \Sigma^{n^c} M \text{ accepts } \langle w, u_1, u_2, \ldots, u_i \rangle,$$

   where Q_i is $\exists$ or $\forall$ depending on i. Now, define L' by

   $$\langle w, u_1 \rangle \in L' \quad \Longleftrightarrow \quad \forall u_2 \in \Sigma^{n^c} \cdots Q_i u_i \in \Sigma^{n^c} M \text{ accepts } \langle w, u_1, u_2, \ldots, u_i \rangle.$$

   Then $L' \in \Pi_{i-1}^P$ which means that $L \in \mathbf{P}$ by our assumption. Thus, there is a Turing machine M' and polynomial n^c such that

   $$w \in L \quad \Longleftrightarrow \quad \exists u_1 \in \Sigma^{n^c} M' \text{ accepts } \langle w, u_1 \rangle.$$

   Then by definition, we have $L \in \mathbf{NP}$ and $L \in P$ by our assumption. This proof works symmetrically for Π_i^P.

6. First, suppose $\varepsilon_1 < \frac{1}{2}$ and $\varepsilon > \frac{1}{2}$. Then let $\varepsilon = \max\{1 - \varepsilon_1, \varepsilon_2\} > \frac{1}{2}$. Then we have

   $$\begin{aligned} w \in C \Longrightarrow &\quad Pr(M \text{ accepts } w) \geq \varepsilon, \\ w \notin C \Longrightarrow &\quad Pr(M \text{ accepts } w) \leq 1 - \varepsilon. \end{aligned}$$

   Since $\varepsilon > \frac{1}{2}$, by the error amplification lemma, there exists a polynomial time probabilistic TM M' such that

   $$\begin{aligned} w \in C \Longrightarrow &\quad Pr(M' \text{ accepts } w) \geq \frac{2}{3}, \\ w \notin C \Longrightarrow &\quad Pr(M' \text{ accepts } w) \leq \frac{1}{3}. \end{aligned}$$

   Next, suppose that $\frac{1}{2} \leq \varepsilon_1 < \varepsilon_2 < 1$. Let $\delta = \frac{1}{\varepsilon_1 + \varepsilon_2}$. We construct a probabilistic TM P that on any input word w will either simulate M on w with probability δ or reject with probability $1 - \delta$. Then we have

   $$\begin{aligned} w \notin C \Longrightarrow &\quad Pr(P \text{ accepts } w) \leq \delta\varepsilon_1 \\ w \in C \Longrightarrow &\quad Pr(P \text{ accepts } w) \geq \delta\varepsilon_2. \end{aligned}$$

   Now, since $\delta\varepsilon_1 < \frac{1}{2}$ and $\delta\varepsilon_2 > \frac{1}{2}$, we can perform the same error amplification above to get the desired bound.

Finally, suppose that $\varepsilon_1 < \varepsilon_2 < \frac{1}{2}$. Let M' be a polynomial time probabilistic TM obtained from M that decides $\overline{C}$ with the same error bound as M. That is, we have

$$\begin{aligned} w \in \overline{C} \Longrightarrow \quad & Pr(M' \text{ accepts } w) \geq \gamma_1 = 1 - \varepsilon_1, \\ w \notin \overline{C} \Longrightarrow \quad & Pr(M' \text{ accepts } w) \leq \gamma_2 = 1 - \varepsilon_2. \end{aligned}$$

Observe that we now have $\frac{1}{2} \leq \gamma_2 < \gamma_1 < 1$ as above and we can use the error amplification lemma again to get the desired bound (while noting that in this case, we must remember that we are working with the complement of C and obtain the correct bound accordingly).

Thus, in each case, we have shown that the desired error bounds are attainable and so, $C \in \mathbf{BPP}$.