Computational Complexity

Homework Sheet 3

Hand in before February 27, 17:00
Preferably by email to `J.Czajkowski@uva.nl`

Exercise 1 (3pt)**.** Is there an oracle such that, relative to this oracle, ...? If so, then give such an oracle and prove that it works. If not, prove why not.

(a) $\mathrm{P} = \mathrm{EXP}$

(b) $\mathrm{coNP} \subseteq \mathrm{P}$ and $\mathrm{NP} \not\subseteq \mathrm{P}$

(c) $\mathrm{DTIME}(n) = \mathrm{DTIME}(n^2)$

(d) $\mathrm{NP} = \mathrm{coNP} \neq \mathrm{EXP}$

For example, in **(a)** you have to either (i) show that there exists an oracle A such that $\mathrm{P}^A = \mathrm{EXP}^A$ or (ii) show that such an oracle does not exist. In **(b)**, you have to either (i) show that there there exists an oracle A such that $\mathrm{coNP}^A \subseteq \mathrm{P}^A$ and $\mathrm{NP}^A \not\subseteq \mathrm{P}^A$ or (ii) show that such an oracle does not exist.

Exercise 2 (3pt)**.** Prove that $\mathrm{NTIME}(n) \neq \mathrm{P}$.

- $\mathrm{NTIME}(n)$ can be characterized as the set of all decision problems that can be verified in linear time with a linear-size certificate. That is, $A \in \mathrm{NTIME}(n)$ if and only if there is a linear-time Turing machine $\mathbb{M}$ and a constant c such that for all $x \in \{0,1\}^*$ it holds that $x \in A$ if and only if there exists some $u \in \{0,1\}^{c \cdot |x|}$ such that $\mathbb{M}(x, u) = 1$. You are allowed to use this characterization of $\mathrm{NTIME}(n)$.
- *Hint:* Use the Nondeterministic Time Hierarchy Theorem.

Exercise 3 (4pt)**.** In this exercise, we will construct a decision problem $A \subseteq \{0\}^*$ that is not auto-reducible, using diagonalization. (For a definition of auto-reducibility, see the previous homework sheet.)

(a) Consider the function $b : \mathbb{N} \to \mathbb{N}$ such that $b(0) = 1$ and for each $n > 0$ it holds that $b(n) = 2^{b(n-1)}$. Show that there exists some i_0 such that for all $i \geq i_0$ it holds that $b(i) > b(i-1)^{i-1}$.

(b) Let $\mathbb{M}$ be a polynomial-time oracle Turing machine that—when given input $x \in \{0\}^*$—does not query x to the oracle. Show that there exists some i such that $\mathbb{M} = \mathbb{M}_i$, and $\mathbb{M}_i^O$ runs in time at most n^i for all oracles O.

- *Hint:* Remember that we can choose our representation scheme $i \mapsto \mathbb{M}_i$ in such a way that every Turing machine has infinitely many representations.

(c) Suppose that $\mathbb{M}_i^O$—from **(b)**—is given the string $0^{b(i)}$ as input. What can you say about the size of the queries that $\mathbb{M}_i^O$ makes to O?

(d) Construct a set $A \subseteq \{0\}^*$ that is not auto-reducible. Construct A in stages A_i such that $A = \bigcup_{i \geq 1} A_i$. Recursively define $A_i \subseteq \{0\}^{b(i)}$ in such a way that A is not auto-reducible by construction. Make sure that you do not forget to prove that the set is not auto-reducible.

- *Hint:* suppose you have constructed $A_1, \ldots, A_{i-1}$. Let $A_{\leq i-1} = \bigcup_{1 \leq j \leq i-1} A_j$. Consider the behavior of machine $\mathbb{M}_i^{A_{\leq i-1}}$ with oracle access to $A_{\leq i-1}$ when given input $0^{b(i)}$—that does not query $0^{b(i)}$. Based on the output of $\mathbb{M}_i^{A_{\leq i-1}}$ on $0^{b(i)}$, choose whether $0^{b(i)}$ is in A_i or not.