Computational Complexity

Exercise Session 3

Note: these solutions are (often) merely pointers to the right idea that is needed to solve the problems. These are not fully worked-out solutions. So please do not take these solutions as an example for how to write up your solutions for, e.g., the homework assignments. :-)

Exercise 1. 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) $\mathsf{DTIME}(n^2) = \mathsf{DTIME}(n^3)$

(b) $\mathsf{DTIME}(n^2) \neq \mathsf{DTIME}(n^3)$

(c) $\mathsf{P} = \mathsf{coNP}$

(d) $\mathsf{P} \neq \mathsf{coNP}$

Solutions:

(a) No such oracle exists, because the Deterministic Time Hierarchy Theorem is relativizing and states that $\mathsf{DTIME}(n^2) \subsetneq \mathsf{DTIME}(n^3)$. So for all oracles O it holds that $\mathsf{DTIME}^O(n^2) \subsetneq \mathsf{DTIME}^O(n^3)$

(b) Yes, in fact, for all oracles this is the case—by the Deterministic Time Hierarchy Theorem, which is a relativizing result.

(c) and (d) Since P is closed under taking the complement of languages, $\mathsf{P} = \mathsf{coNP}$ if and only if $\mathsf{P} = \mathsf{NP}$. This is a relativizing result (because it also works for oracle Turing machines), so for each oracle O, it holds that $\mathsf{P}^O = \mathsf{coNP}^O$ if and only if $\mathsf{P}^O = \mathsf{NP}^O$. So we can take the oracles A and B from the Baker-Gill-Solovay Theorem for this.

Exercise 2. Show that if $\mathsf{NTIME}(n) \subseteq \mathsf{DTIME}(n)$, then $\mathsf{P} = \mathsf{NP}$.

- $\mathsf{NTIME}(n)$ can be characterized as the set of all decision problems that can be verified in linear time with a linear-size certificate. That is, $A \in \mathsf{NTIME}(n)$ 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 $\mathbb{M}(x,u) = 1$.
- *Hint:* Use a padding argument.

Solutions:

Suppose that $\mathsf{NTIME}(n) \subseteq \mathsf{DTIME}(n)$. We will show that then $\mathsf{NP} \subseteq \mathsf{P}$. Take an arbitrary language $L \in \mathsf{NP}$. Then there must exist a polynomial p and a polynomial-time TM $\mathbb{M}$ such that for each x, $x \in L$ if and only if there exists some $u \in \{0,1\}^{p(|x|)}$ such that $\mathbb{M}(x,u) = 1$. Suppose also, without loss of generality, that p also bounds the running time of $\mathbb{M}$.

Consider the following language $L' = \{ (x, 1^{p(|x|)}) \mid x \in L \}$. We claim that $L' \in \mathsf{NTIME}(n)$. We describe a linear-time deterministic TM $\mathbb{M}'$ that verifies linear-size certificates for L'. On input $((x, 1^m), u')$, with $u' \in \{0,1\}^{|(x,1^m)|}$, it first checks whether $m = p(|x|)$. If not, it rejects. If so, it continues, and does whatever $\mathbb{M}$ does on (x,u), where u consists of the first m bits of u'—in other words, it 'simulates' $\mathbb{M}$ on (x,u), but since $\mathbb{M}$ is fixed, we don't need any overhead for this simulation. And then $\mathbb{M}'$ accepts $((x,1^m),u')$ if and only if $\mathbb{M}$ accepts (x,u).

You can show that the machine $\mathbb{M}'$ runs in linear time, and the length of the certificates u' is exactly the length of the input, so in particular, it is linear in the length of the input.

You can also show that, for each x, there is some u of size $p(|x|)$ such that $\mathbb{M}(x, u) = 1$ if and only if there is some u' of length $|(x, 1^{p(|x|)})|$ such that $\mathbb{M}'((x, 1^{p(|x|)}), u') = 1$. Thus, L polynomial-time reduces to L', by the reduction f that maps x to $(x, 1^{p(|x|)})$.

Since $L' \in \mathsf{NTIME}(n)$ and $\mathsf{NTIME}(n) \subseteq \mathsf{DTIME}(n)$, we know that $L' \in \mathsf{DTIME}(n) \subseteq \mathsf{P}$. Then, since L polynomial-time reduces to a problem in P, we know that $L \in \mathsf{P}$. Since L was an arbitrary problem in NP, we get that $\mathsf{NP} \subseteq \mathsf{P}$.