MAST31213 Complexity theory
Master's Programme in Mathematics and Statistics
Fall 2019
Exercise set 10

Read chapters 3.3 – 3.4 of the book and discuss with a friend/relative/aquaintance what the Baker-Gill-Solovay theorem says about the P vs. NP question.

Exercise 1. Show that the function H defined in the proof of Ladner's theorem is computable in polynomial time.

Exercise 2.

(a) Show that $\mathbf{coNP} \subseteq \mathbf{P}^{\mathbf{NP}}$, where $\mathbf{P}^{\mathbf{NP}} = \bigcup_{A \in \mathbf{NP}} \mathbf{P}^A$.
(b) Show that $\mathbf{P}^{\mathtt{EXPCOM}} \subsetneq \mathbf{EXP}^{\mathtt{EXPCOM}}$. Why does this not contradict $\mathbf{P}^{\mathtt{EXPCOM}} = \mathbf{EXP}$ that we proved in class?

Exercise 3.

(a) Show that if $A \in \mathbf{P}$ then $\mathbf{P}^A = \mathbf{P}$.
(b) Why does the same proof not show that $\mathbf{NP}^{\mathtt{SAT}} = \mathbf{NP}$?
(c) Show that $\mathbf{NP} \subseteq \mathbf{P}^{\mathtt{SAT}}$.
(d) Again, why does this not show that $\mathbf{NP}^{\mathtt{SAT}} \subseteq \mathbf{P}^{\mathtt{SAT}}$?

Exercise 4.

(a) Modify the proof of the Baker-Gill-Solovay theorem to show that there is $B \in \mathbf{EXP}$ such that $\mathbf{NP}^B \neq \mathbf{P}^B$.
(b) Are there oracles B such that if $\mathbf{P}^B \neq \mathbf{NP}^B$ then actually $\mathbf{P} \neq \mathbf{NP}$?

Exercise 5. Let M be a deterministic Turing machine that only queries oracle strings that are shorter than the input string. Show that if $A = L(M^A)$ and $B = L(M^B)$ (where $L(M)$ is the language decided by M) then $A = B$. Hint: induction.

Exercise 6. Show that there is an oracle A and a language $L \in \mathbf{NP}^A$ such that L is not polynomial-time reducible to $\mathtt{3SAT}$ even when the machine computing the reduction is allowed access to A.