Johannes Blömer
Jan Bobolz, Gennadij Liske

27. May 2016
submission due: 06. June 2016, 15:30

Complexity Theory

SS 2016

Homework 7

Exercise 1 can *not* be handed in groups but should be solved by every student individually. (All other Exercises on this sheet can be solved in groups as usual).

Exercise 1 (10 points)**:**
Correct the two randomly assigned solutions to Homework 5, Exercise 2 of your fellow students. At the end of the lecture on May 30th, we will hand out your two assigned solutions to you. If you were not present or did not receive one, please contact Gennadij via email. Please denote your name and matriculation number on the corrected solutions and hand them in next week alongside the other (group-enabled) exercises of this homework sheet.
You do not have to assign points to the solutions. However we do expect you to comment (preferably in a color that is neither red nor black) the solution. In particular, you should check that

- the structure of the proof is clearly stated (or at least easily understandable by itself).
- the argument is convincing, complete, and you can easily follow it.
- the statements made in the proof are technically correct.

Give short explanations (and/or counterexamples) for all corrections you make.

Your correction cannot possibly be taken into account for grading the solutions, because they will already have been corrected by us and returned to you before Homework 6 is due. Consequently you do not have to worry about harming your fellow students' grades.
For your effort, we will award up to 5 points for each of your two corrected solutions, depending on how thoroughly your corrections cover the solutions' errors. If the solution you correct happens to be completely flawless, it suffices to mark it with a "✓" for full points.

Exercise 2 (6 points)**:**
Show that

a) Ladner's theorem can be stated as an equivalence:
There is a language $L \in \mathbf{NP}$ that is neither in $\mathbf{P}$ nor in $\mathbf{NPC}$ if *and only if* $\mathbf{P} \neq \mathbf{NP}$.

b) A slightly modified version of Ladner's theorem applies to co-$\mathbf{NP}$:
If $\mathbf{P} \neq \mathbf{NP}$, then there is a language $L \in$ co-$\mathbf{NP}$ that is neither in $\mathbf{P}$ nor in co-$\mathbf{NPC}$.

For both statements you may use Ladner's theorem without additional proof.

Exercise 3 (8 points)**:**
Let $L \subseteq \{0,1\}^*$ be a language and $f : \{0,1\}^* \to \{0,1\}^*$. We call f a *sublinear self reduction for* L if f is a polynomial time reduction of L to L (i.e. $w \in L \Leftrightarrow f(w) \in L$ for all $w \in \{0,1\}^*$) and $|f(w)| = o(|w|)$ (i.e. images of f have asymptotically sublinear length).

a) Show that if there exists a sublinear self reduction for L, then $L \in \mathbf{P}$.

b) Assume $\mathbf{P} \neq \mathbf{NP}$ and $SAT_H \in \mathbf{NPC}$ (with H like in the lecture). Let f^* be a polynomial time reduction of SAT to SAT_H. For $w \in \{0,1\}^*$, we define $f(w) := \psi$ if $f^*(w) = \psi 01^{|\psi|^{H(|\psi|)}}$ and $f(w) := (A \wedge \neg A)$ if $f^*(w)$ is not of that format.
Show that f is a sublinear self reduction for SAT.

c) Conclude that if $\mathbf{P} \neq \mathbf{NP}$ then $SAT_H \notin \mathbf{NPC}$.