Assignment 4, Complexity Theory, WiSe 16/17

Markus Bläser, Anurag Pandey, Harry Zisopoulos
`http://www-cc.cs.uni-saarland.de/course/56/`

Due: May 27, 2015, 11:00

Exercise 4.1 Show that, if A is downward self-reducible, then $A \in \mathsf{PSPACE}$.

Exercise 4.2 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 $B = L(M^B)$, then $A = B$.
Hint: prove by induction over n that $A^{\leq n} = B^{\leq n}$ holds.

Exercise 4.3 Prove the following:

a) $\texttt{FACTOR} \in \mathsf{NP}$.

b) $\texttt{FACTOR} \in \textsf{co-NP}$. (You can use the result by Agrawal, Kayal, and Saxena that $\texttt{PRIMES} \in \mathsf{P}$; that is, we can determine in polynomial time whether a given positive integer x is a prime number or not, where the integer x is encoded in binary)

Exercise 4.4 Let CMP (circuit minimization problem) be the language of the encodings of all minimal (with respect to size) Boolean circuits.

a) Show that $\texttt{CMP} \in \Pi_2^{\mathsf{P}}$.

b) Show that if $\texttt{SAT} \in \mathsf{P}$, then $\texttt{CMP} \in \mathsf{P}$.

This is a somewhat paradox situation. In the second case, we are given an algorithm for SAT and this places CMP into P. In the first case, we are essentially given an oracle for SAT ($\Pi_2^{\mathsf{P}} = \textsf{co-NP}^{\mathsf{NP}}$). This oracle solves the same problem as the algorithm above, but it is not clear whether this is enough to solve CMP in polynomial time (most likely not).