TU Dresden, Fakultät Informatik
David Carral, Stephan Mennicke

Winter Term 2020/2021

Complexity Theory

Exercise 5: Diagonalization

Exercise 5.1. Find the fault in the following proof of $\mathrm{P} \neq \mathrm{NP}$.

1. Assume that $\mathrm{P} = \mathrm{NP}$.
2. Then $\mathsf{SAT} \in \mathrm{P}$ and thus there exists a number $k \in \mathbb{N}$ such that $\mathsf{SAT} \in \mathsf{DTime}(n^k)$.
3. Because every language in NP is poly-time reducible to SAT, we have $\mathrm{NP} \subseteq \mathsf{DTime}(n^k)$.
4. It follows that $\mathrm{P} \subseteq \mathsf{DTime}(n^k)$.
5. By the Time Hierarchy Theorem there exist languages in $\mathsf{DTime}(n^{k+1})$ that are not in $\mathsf{DTime}(n^k)$, contradicting $\mathrm{P} \subseteq \mathsf{DTime}(n^k)$.
6. Therefore, $\mathrm{P} \neq \mathrm{NP}$.

Exercise 5.2. Show the following.

1. $\textsc{Time}(2^n) = \textsc{Time}(2^{n+1})$
2. $\textsc{Time}_*(2^n) \subsetneq \textsc{Time}_*(2^{2n})$
3. $\textsc{NTime}(n) \subsetneq \textsc{PSpace}$

Exercise 5.3. Define a function that is computable but not time-constructible.

Exercise 5.4. Consider the function $\mathsf{pad} : \Sigma^* \times \mathbb{N} \to \Sigma^*\#^*$ defined as $\mathsf{pad}(s, l) = s\#^j$, where $j = \max\{0, l - |s|\}$. For some language $\mathbf{A} \subseteq \Sigma^*$ and function $f : \mathbb{N} \to \mathbb{N}$ define $\mathsf{pad}(\mathbf{A}, f) := \{\mathsf{pad}(s, f(|s|) \mid s \in \mathbf{A}\}$.

Show all of the following statements.

1. If $\mathbf{A} \in \mathsf{DTime}(n^6)$, then $\mathsf{pad}(\mathbf{A}, n^2) \in \mathsf{DTime}(n^3)$.
2. If $\textsc{NExpTime} \neq \textsc{ExpTime}$, then $\mathrm{P} \neq \mathrm{NP}$.
3. For every $\mathbf{A} \subseteq \Sigma^*$ and $k \in \mathbb{N}$, $\mathbf{A} \in \mathrm{P}$ iff $\mathsf{pad}(\mathbf{A}, n^k) \in \mathrm{P}$.
4. $\mathrm{P} \neq \mathsf{DSpace}(n)$.
5. $\mathrm{NP} \neq \mathsf{DSpace}(n)$.

Exercise 5.5. You are given two oracles and one of them is the set **TQBF**, but you do not know which one. Design a polynomial algorithm that decides **TQBF** using these oracles.