Complexity Theory, WS 13/14: Solution Hints 5.

Markus Bläser, Thatchaphol Saranurak

Exercise 5.1 We will prove only that $t_U = \text{poly}(c_M, t_M(\varphi), |\varphi|)$.

Let M be a DTM that outputs a satisfying assignment for φ in time $t_M(\varphi)$. Let i^* be such that $2^{i^*-1-|M|} < t_M(\varphi) \leq 2^{i^*-|M|}$, then U will halt at iteration i^*.

During the i-th iteration, we simulate $\leq 2^i$ machines, with encoding of length $\leq i$, for $\leq 2^i$ steps, and each step takes $O(i^2 2^i)$ time. After the simulation of each machine, if the machine output an assignment y, we check in time $O(|\varphi|)$ whether y satisfies φ.

We have that

$$\begin{aligned} t_U(\varphi) &\leq \sum_{i=0}^{i^*} 2^i \cdot (2^i \cdot O(i^2 2^i) + O(|\varphi|)) \\ &= O(2^{3i^*} + 2^{i^*}|\varphi|) \\ &= \text{poly}(c_M, t_M(\varphi), |\varphi|), \end{aligned}$$

where $c_M = 2^{|M|}$.

Exercise 5.2 Note: We did not talk about formal proof systems and will not do in the lecture. Therefore, this exercise cannot be answered precisely (intentionally) in the context of this lecture. Nevertheless, you still learn a lot if you use an intuitive notion of "constructive".

We will explicitly describe the algorithm $\hat{U}$ which decides whether $\varphi \in \texttt{SAT}$ in polynomial time for any φ.

Suppose $\texttt{SAT} \in \mathsf{DTime}(n^3) \subset \mathsf{P}$, since $\texttt{SAT}$ is self reducible, there is M that outputs a witness that $\varphi \in \texttt{SAT}$ in time $t_M(\varphi) = \text{poly}(|\varphi|)$ for any given φ.

Moreover, if $\texttt{SAT} \in \mathsf{P}$, then $\mathsf{P} = \mathsf{PH}$. In particular, $\texttt{UNSAT} \in \mathsf{P}$. Therefore, there is M' that outputs a witness that $\varphi \notin \texttt{SAT}$ in time $t_{M'}(\varphi) = \text{poly}(|\varphi|)$ for any given φ.

We define $\hat{U}$ by slightly modifying the algorithm U from the previous exercise, such that for every output y from the simulated machines, we check whether y is a witness for $\varphi \in \texttt{SAT}$ and also for $\varphi \notin \texttt{SAT}$. We can do this in time

$$\begin{aligned} t_U(\varphi) &\leq \min\{\text{poly}(c_M, t_M(\varphi), |\varphi|), \text{poly}(c_{M'}, t_{M'}(\varphi), |\varphi|)\} \\ &= \text{poly}(|\varphi|) \end{aligned}$$

Since we construct $\hat{U}$ explicitly, the proof for $\texttt{SAT} \in \mathsf{P}$ is actually constructive.

Exercise 5.3 For any φ, there is an trivial machine M_φ that does nothing but outputs an satisfying assignment for φ, if it exists. By definition of $|M_\varphi|$, $|M_\varphi| = O(|\varphi|)$ and $t_{M_\varphi}(\varphi) = O(|\varphi|)$.

Suppose we have an algorithm $\hat{U}$ where $c_M = \text{poly}(|M|)$. We have

$$\begin{aligned} t_{\hat{U}}(\varphi) &\leq \text{poly}(c_{M_\varphi}, t_{M_\varphi}(\varphi), |\varphi|)\} \\ &= \text{poly}(|\varphi|). \end{aligned}$$

Since $\hat{U}$ always accept yes-instances within p steps for some polynomial p, we just halt $\hat{U}$ after p steps to obtain a machine which decides $\texttt{SAT}$ in polynomial time, hence $\mathsf{P} = \mathsf{NP}$.