Computational Complexity

Homework Sheet 5

Hand in before March 13, 17:00

By email to `J.Czajkowski@uva.nl`

Exercise 1 (3pt)**.** Define:

$$\mathrm{P}_{/\log} = \bigcup_{c,d \in \mathbb{N}} \mathrm{DTIME}(n^c)/(d \log n).$$

That is, $\mathrm{P}_{/\log}$ is the class of all languages that can be decided in polynomial time with $O(\log n)$ bits of advice. Prove that $\mathrm{SAT} \notin \mathrm{P}_{/\log}$, unless $\mathrm{P} = \mathrm{NP}$.

- *Hint:* iterate over all possible advice strings of length $O(\log n)$.
- *Hint:* you may assume that for any string x that represents a propositional formula φ and any truth assignment α to (some of) the variables of φ, one can in polynomial-time encode the formula $\varphi[\alpha]$ as a string x' that is of the same length as x—where $\varphi[\alpha]$ is obtained from φ by instantiating each variable z in the domain of α by $\alpha(z)$.

Exercise 2 (2pt)**.** Let $\mathrm{P}_{/1}$ be the class of languages that can be decided in polynomial time with a single bit of advice (for each input size). That is $\mathrm{P}_{/1} = \bigcup_{c \in \mathbb{N}} \mathrm{DTIME}(n^c)/1$. Prove that $\mathrm{P} \subsetneq \mathrm{P}_{/1}$.

- *Hint:* use the following undecidable language UHALT:

$$\begin{aligned}\mathrm{UHALT} = \{\ 1^n \mid\ & n\text{'s binary expansion encodes a pair } \langle M, x\rangle \\ & \text{such that } M \text{ is a Turing machine that halts on input } x\ \}.\end{aligned}$$

Exercise 3 (2pt)**.** Show that $\mathrm{RP} \subseteq \mathrm{NP}$.

Exercise 4 (3pt)**.** Show that $\mathrm{ZPP} = \mathrm{RP} \cap \mathrm{coRP}$.

- *Hint:* use Markov's inequality for showing that $\mathrm{ZPP} \subseteq \mathrm{RP} \cap \mathrm{coRP}$. If X is a non-negative random variable and $a > 0$, then:

$$\mathbb{P}(X \geq a) \leq \frac{\mathbb{E}(X)}{a}.$$