TU Dresden, Fakultät Informatik
David Carral, Stephan Mennicke

Complexity Theory

Exercise 8: Probabilistic Turing Machines and Complexity Classes

Exercise 8.1. Show that **MajSat** is in PP.

$$\textbf{MajSat} = \left\{ \varphi \;\middle|\; \begin{array}{l} \varphi \text{ is a propositional logic formula that is satisfied} \\ \text{by more than half of its assignments} \end{array} \right\}$$

Exercise 8.2. Show $\mathrm{BPP} = \mathrm{coBPP}$.

$*$ **Exercise 8.3.** Show $\mathrm{BPP}^{\mathrm{BPP}} = \mathrm{BPP}$.

Exercise 8.4. Find the error in the following proof that shows $\mathrm{PP} = \mathrm{BPP}$: *Let $\mathbf{L} \in \mathrm{PP}$. Then there is a poly-time bounded PTM accepting $\mathbf{L}$ with error probability smaller than $\frac{1}{2}$. Using error amplification, we can make this error arbitrarily small, and in particular smaller than $\frac{1}{3}$. Hence, $\mathbf{L} \in \mathrm{BPP}$.*

Exercise 8.5. Let $\mathcal{M}$ be a polynomial-time probabilistic Turing machine. We say that $\mathcal{M}$ has *error probability smaller than* $\frac{1}{3}$ if and only if

$$Pr[\mathcal{M} \text{ accepts } w] < \frac{1}{3} \quad \text{or} \quad Pr[\mathcal{M} \text{ accepts } w] \geq \frac{2}{3}$$

for all inputs w. Show that the problem whether a polynomial-time probabilistic Turing machine has error probability smaller than $\frac{1}{3}$ is undecidable.

Exercise 8.6. Let $0 < p < 1$ and let $(X_i \mid i \in \mathbb{N})$ be a sequence of independent random variables $X_i \colon \Omega_i \to \{0, 1\}$ such that $P(X_i = 1) = p$ for all $i \in \mathbb{N}$. Describe a way how to transform the sequence $(X_i \mid i \in \mathbb{N})$ into a sequence $(Y_i \mid i \in \mathbb{N})$ such that $P(Y_i = 1) = P(Y_i = 0) = 1/2$. The construction may have a zero probability to fail.

Exercise 8.7. Consider the following alternative definition of ZPP:
A language **L** is in ZPP if and only if there exists some polynomial time PTM $\mathcal{M}$ that answers Accept (A), Reject (R), or Inconclusive (I), and all of the following hold.

- For all $w \in \mathbf{L}$, $\mathcal{M}$ always returns A or I.
- For all $w \notin \mathbf{L}$, $\mathcal{M}$ always returns R or I.
- For all $w \in \Sigma^*$, $\Pr[\mathcal{M}(w) = \mathsf{I}] < \frac{1}{2}$.

Exercise 8.8. Prove Theorem 17.26 (see slide 44 of lecture 17).