Karlsruhe Institute of Technology

Stefan Walzer, Stefan Hermann
ITI Prof. Sanders
winter term 2025/2026

Exercise Sheet 5 – Randomized Complexity Classes

Probability and Computing

Exercise 1 – Relations between Complexity Classes

Justify the following inclusions:

(i) $\mathbf{ZPP} \subseteq \mathbf{RP}$ and $\mathbf{ZPP} \subseteq \text{co}-\mathbf{RP}$

(ii) $\mathbf{P} \subseteq \mathbf{ZPP}$

(iii) $\mathbf{RP} \subseteq \mathbf{NP}$ and $\text{co}-\mathbf{RP} \subseteq \text{co}-\mathbf{NP}$

(iv) $\mathbf{RP} \subseteq \mathbf{BPP}$ and $\text{co}-\mathbf{RP} \subseteq \mathbf{BPP}$

(v) $\mathbf{BPP} \subseteq \mathbf{PP}$

Solution 1

(i) This follows directly from the definition $\mathbf{ZPP} := \mathbf{RP} \cap \text{co}-\mathbf{RP}$.

(ii) Let $L \in \mathbf{P}$. We show that $L \in \mathbf{ZPP}$. Let T be a deterministic polynomial-time Turing machine for L. Using the "typecasting" argument from the lecture, we can formally regard T as a probabilistic Turing machine (which in fact uses no randomness) that still decides L and still runs in polynomial time. In particular, this PTM witnesses that $L \in \mathbf{RP}$. We have $\bar{L} \in \mathbf{P}$ because $\mathbf{P} = \text{co}-\mathbf{P}$, and by the same reasoning, $\bar{L} \in \mathbf{RP}$. Therefore, $L \in \text{co}-\mathbf{RP}$. Altogether we obtain $L \in \mathbf{RP} \cap \text{co}-\mathbf{RP} = \mathbf{ZPP}$.

(iii) Let $L \in \mathbf{RP}$ and let T be an $\mathbf{RP}$-PTM for L. By "forgetting" the probabilistic choices, we obtain a nondeterministic Turing machine T'. Since for every $w \in L$ we have $\Pr[T(w) = \text{YES}] \geq \frac{1}{2}$, there exists at least one accepting computation path for w. Thus $T'(w) = \text{YES}$. For every $w \notin L$ we have $\Pr[T(w) = \text{YES}] = 0$, hence there exists no accepting computation for w. Therefore $T'(w) = \text{NO}$. Consequently, T' decides L, and we have $L \in \mathbf{NP}$. As L was arbitrary, it follows that $\mathbf{RP} \subseteq \mathbf{NP}$.

For the symmetric case we conclude analogously:

$$L \in \text{co}-\mathbf{RP} \Leftrightarrow \bar{L} \in \mathbf{RP} \Rightarrow \bar{L} \in \mathbf{NP} \Leftrightarrow L \in \text{co}-\mathbf{NP}.$$

(iv) Let $L \in \mathbf{RP}$ and let T be an **RP**-PTM for L. Define a PTM T' that runs T three times independently and accepts if at least one of the three runs of T accepts. Then, for all $w \in L$,

$$\Pr[T'(w) = \text{NO}] = \Pr[T(w) = \text{NO}]^3.$$

Hence for $w \in L$ we have:

$$\begin{aligned}\Pr[T'(w) = \text{YES}] &= 1 - \Pr[T'(w) = \text{NO}] = 1 - \Pr[T(w) = \text{NO}]^3 \\ &= 1 - (1 - \Pr[T(w) = \text{YES}])^3 \geq 1 - \left(1 - \frac{1}{2}\right)^3 = 1 - \frac{1}{8} > \frac{3}{4}.\end{aligned}$$

For $w \notin L$ we obtain:

$$\Pr[T'(w) = \text{YES}] = 1 - \Pr[T'(w) = \text{NO}] = 1 - \Pr[T(w) = \text{NO}]^3 = 1 - 1^3 = 0 < \frac{1}{4}.$$

Thus, T' is a **BPP**-PTM for L. Hence $L \in \mathbf{BPP}$. Since L was arbitrary, we have $\mathbf{RP} \subseteq \mathbf{BPP}$.

The symmetric case follows analogously, since $\mathbf{BPP} = \text{co}-\mathbf{BPP}$.

(v) There is nothing to prove here. Every **BPP**-PTM is also a **PP**-PTM, as the acceptance requirement is merely relaxed. Hence, for every language L that has a **BPP**-PTM, there also exists a **PP**-PTM.

Exercise 2 – Las Vegas Algorithm for L implies $L \in$ ZPP

Let **LV** (for Las Vegas) denote the class of all languages L for which there exists a probabilistic Turing machine T with the following properties:

- T decides L (that is, T outputs 1 for all $x \in L$ and 0 for all $x \notin L$).
- There exists a polynomial $p(n)$ such that the *expected* runtime of T on input x is bounded by $p(|x|)$.

In the lecture we proved that $\mathbf{ZPP} \subseteq \mathbf{LV}$. Show that also $\mathbf{LV} \subseteq \mathbf{ZPP}$ holds. Thus, the two classes are identical.

Hint: Definition of **ZPP**, Markov inequality.

Solution 2

Let $L \in \mathbf{LV}$. We first show that $L \in \mathbf{RP}$. Let T be an **LV**-TM for L with associated polynomial $p(n)$. We consider the following Turing machine T':

Algorithm $T'(w)$**:**

```
t_max ← 2p(|w|)
simulate T on input w for t_max steps
if T has terminated with output r then
    return r
else // T has not yet terminated
    return NO
```

We now show that T' is an **RP**-TM for L. Due to the choice of $t_{\max}$, the runtime of $T'(w)$ is clearly bounded by some polynomial $q(|w|)$. Concerning the outputs of T':

- For $w \notin L$, the output of $T'(w)$ is always NO, either because T decided so or because we reached the else-case. Hence, $\Pr[T'(w) = \text{YES}] = 0$.
- For $w \in L$, let $t(w)$ denote the random runtime of T on w. By assumption, $\mathbb{E}[t(w)] \leq p(|w|)$. By Markov's inequality it follows that:

$$\Pr[t(w) > t_{\max}] \leq \frac{\mathbb{E}[t(w)]}{t_{\max}} \leq \frac{p(|w|)}{2p(|w|)} \leq \frac{1}{2}.$$

  Thus, T terminates on w within the given time limit (with the correct result) with probability at least $1/2$. Therefore, $\Pr[T'(w) = \text{YES}] \geq \frac{1}{2}$.

Hence, T' is an **RP**-TM for L. Thus, $L \in \mathbf{RP}$. Analogously, $L \in \text{co}-\mathbf{RP}$ follows (by returning YES in the non-termination case). Therefore, $L \in \mathbf{ZPP}$. Since L was arbitrary, we obtain $\mathbf{LV} \subseteq \mathbf{ZPP}$.

Exercise 3 – Bonus: Probability Amplification for BPP

Look up on Wikipedia what the complexity class **P/poly** means. Show that $\mathbf{BPP} \subseteq \mathbf{P/poly}$. This insight is also known as *Adleman's Theorem*.

Hint: Make the error probability smaller than 2^{-n}. Transform the PTM into a DTM and show that there exists a random string that yields the correct result for all inputs.

Solution 3

No solution for the bonus exercise.