

## Computational Complexity – Homework 7

Discussed on Tuesday 31.05.2016.

Recall that  $L \in \mathbf{RP}$  if there exists a polynomial  $p$  and a polynomial-time TM  $M(x; u)$  using certificates  $u$  of length  $p(|x|)$  such that for every  $x \in \{0, 1\}^*$

$$x \in L \Rightarrow \Pr[A_{M;x} \geq 3/4] \text{ and } x \notin L \Rightarrow \Pr[A_{M;x}] = 0$$

Further  $\mathbf{co-RP} = \{\bar{L} \mid L \in \mathbf{RP}\}$  and  $\mathbf{ZPP} = \mathbf{RP} \cap \mathbf{co-RP}$ .

### Exercise 7.1

- (a) Show that  $\mathbf{RP}$  does not change if we replace in the definition  $\geq 3/4$  by  $\geq n^{-k}$  or  $\geq 1 - 2^{-n^k}$  (with  $k > 0$ ).
- (b) Let  $L \in \mathbf{NP}$  be decided by a poly-time TM  $M(x, u)$  with certificates  $u$  of length  $p(|x|)$ .

Prove or disprove that  $x \in L \Rightarrow \Pr[A_{M;x}] \geq n^{-k}$  needs to hold for some  $k > 0$  if a polynomial number  $r(|x|)$  of reruns should suffice to reduce the probability of false negatives below any given bound  $c \in (0, 1)$ .

*Remark:* Use that  $(1 - 1/k)^k \approx e^{-1}$  for large  $k$ .

### Exercise 7.2

Show that  $L \in \mathbf{ZPP}$  if and only if  $L$  is decided by some PTM in expected polynomial time.

### Exercise 7.3

For a given  $c > 0$  let a language  $L$  be in  $\mathbf{PP}_{\geq c}$  if  $x \in L \Leftrightarrow \Pr[A_{M;x}] \geq c$ . Similarly, the class  $\mathbf{PP}_{> c}$  is defined.

Show that

- (a)  $\mathbf{PP}_{> 1/2} = \mathbf{PP}_{\geq 1/2}$ .
- (b)  $\mathbf{PP}_{> 1/2}$  is closed under complement and symmetric difference.

*Remark:* The symmetric difference  $A \Delta B$  of two sets  $A, B$  is defined by  $A \Delta B := (A \setminus B) \cup (B \setminus A)$ .

- (c) MAJSAT is  $\mathbf{PP}_{> 1/2}$ -complete.

*Remark:* MAJSAT is the following problem: Given a Boolean expression with  $n$  variables, is it true that the majority of the  $2^n$  truth assignments to its variables, i.e., at least  $2^{n-1} + 1$  of them, satisfy it?

- \*(d)  $\mathbf{PP}_{\geq 3/4} = \mathbf{PP}_{\geq 1/2}$ .