Sandra Kiefer, Pascal Schweitzer **SS 16**

Exercises for Computational Complexity Theory

Assignment 9 Deadline: Thursday, June 30th, 2016

Exercise 33 (*Error Reduction for* RP) [Exercise 7.4 in AB]

Let $L \subseteq \{0,1\}^*$ be such that there is a polynomial-time PTM M satisfying for every $x \in \{0,1\}^*$: **(1)** If $x \in L$, then $\Pr[M(x) = 1] \geq n^{-c}$ and **(2)** if $x \notin L$, then $\Pr[M(x) = 1] = 0$.

Prove that for every $d > 0$ there is a polynomial-time PTM M' such that for every $x \in \{0,1\}^*$: **(1)** If $x \in L$ then $\Pr[M'(x) = 1] \geq 1 - 2^{-n^d}$ and **(2)** if $x \notin L$ then $\Pr[M'(x) = 1] = 0$.

Exercise 34 (*Alternative definition of* ZPP) [Exercise 7.6 in AB]

a) Prove that a language L is in ZPP if and only if there exists a polynomial-time PTM M with outputs in $\{0, 1, \star\}$ such that for every $x \in \{0,1\}^*$, with probability 1, it holds that $M(x) \in \{L(x), \star\}$ and $\Pr[M(x) = \star] \leq 1/2$.

b) Show that ZPP $=$ RP $\cap$ coRP.

Exercise 35 (*Two-sided and one-sided error*)

Show that the assumption NP $\subseteq$ BPP implies NP $\subseteq$ RP.

Exercise 36 (*Non-specialists and primes*)

Your economist friend works in the banking sector. They tell you that the bank's new software library requires a test to check whether a given number is prime. What would you tell your friend? Can you provide them with a *practical* solution?