Complexity Theory, WS 13/14: Solution Hints 8.

Markus Bläser, Thatchaphol Saranurak

Exercise 8.1 Given a language L with $L \in \mathsf{RP} \cap \mathsf{co\text{-}RP}$. We construct a probabilistic machine with polynomial runtime. We run both machines M_{RP} and $M_{\mathsf{co\text{-}RP}}$ at the same time. Now we have different cases:

$\mathsf{ZPP} \to$ *0 probability: One accepts, one rejects* We know the accepting machine is correct with probability 1.

Both accept This is impossible as either $x \in L$ or $x \notin L$ and our machines do not make a errors in this case.

Both reject If both reject we run our machine again. We need to make sure that this doesn't violate our expected polynomial runtime. We now look at the expected runtime. The probability that we run more than c rounds is:

$$\Pr[t \geq cp(n)] \leq \left(\frac{1}{4}\right)^c$$

where $p(n)$ is the runtime of our RP machine. This gives us the expected runtime

$$\begin{aligned} E[t] \leq& \Pr[t \leq c'p(n)]c'p(n) + \int_{c'}^{\infty} \Pr[t = xp(n)]x dx \\ \leq& c'p(n) + \int_{c'}^{\infty} \Pr[t \geq xp(n)]x dx \\ \leq& c'p(n) + n^{\mathrm{O}(1)} \end{aligned}$$

for some constant c'. The last inequality can be easily calculated.

0 probability $\to$ ZPP*:* Let our 0 probability machine have an expected running time of $t(n)$. We build a TM $M \in \mathsf{RP}$ in the following way. We simulate our 0 probability machine M' for $t(n)$ steps. If we halt in $t(n)$ steps we accept if M' accepts and rejects if M' rejects. If we run over our timebound we reject. Let $x \notin L$, we reject with probability 1 by either straight forward rejecting or running over the time bound. If $x \in L$ we need to use Markov's Inequality. Let $t'(n)$ be the runtime of our machine and $t(n)$ such that M' has expected runtime $t(n)$. We know that

$$\Pr[t'(n) \geq a] \leq \frac{t(n)}{a}.$$

If we set our runtime to be $2t(n)$ which gives us a bound on the missed number of results of $\Pr[t'(n) \geq 2t(n)] \leq \frac{t(n)}{2t(n)} \leq 1/2$.

Exercise 8.2 First we do probability amplification. We now build a TM $M' \in \mathsf{RP}$. We test with M if the formula is satisfiable. If yes, we set one variable to a value and check the remaining formula. We do this until only one variable is left. Here we check deterministically if this is satisfiable. If yes we accept else reject.

If $x \notin \mathsf{SAT}$ we will always reject. Let us look at the $x \in \mathsf{SAT}$ case. Assume our TM M makes after probability amplification a twosided error of 2^{-m}.

$$\Pr[\text{we make no mistake in } n \text{ tests}] \geq (1 - 2^{-m})^n.$$

For $m = n$ our probability is larger than $(1 - 2^{-n})^n \leq e^{-2}$ which is larger than $1/2$.

The runtime is obviously polynomial. We run only n tests which gives us a runtime $np(n, n)$ which is polynomial where $p(n, n)$ is the runtime of M after probability amplification with n which gives us a polynomial runtime.