Assignment 4 solutions

Exercise 7.4

$M'(x)$ runs $M(x)$ k *independent* times and accepts x iff $M(x) = 1$ at least once. Obviously, if $x \notin L$ we have $M(x) = 0$ for all k times, and $Pr[M'(x) = 0] = 1$. If $x \in L$,

$$Pr[M'(x) = 0] = Pr[M(x) = 1 \forall k \text{ times}] \leq (1 - n^{-c})^k. \tag{1}$$

If we set $k := dn^c \ln n$ then, since for large enough n we have $(1 - n^{-c})^{n^c} \leq 1/e$ (1) implies $Pr[M'(x) = 0] \leq n^{-d}$.

Exercise 7.6

(a) First assume that M exists, and its running time is at most n^c. We construct a new TM M', which runs $M(x)$ repeatedly, until it gets something other than ?. If $M'(x)$ terminates, then it terminates with $L(x)$ by definition. To calculate its *expected* running time, we note that it runs $M(x)$ i times iff $M(x) =?$ for the first $i-1$ times, and $M(x) \neq ?$ the i-th time. Then the running time is in^c, and the probability that this event happens is

$$Pr[\text{repeat } M(x)\ i \text{ times}] \leq \frac{1}{2^{i-1}} Pr[M(x) \neq ?] \leq \frac{1}{2^{i-1}}.$$

So, the expected running time for $M'(x)$ is at most $\sum_{i=1}^{\infty} \frac{in^c}{2^{i-1}} = 2n^c \sum_{i=1}^{\infty} \frac{i}{2^i} \leq 2Dn^c = O(n^c)$, where D is the constant of exercise 7.2. Therefore $L \in ZPP$.

Now assume that $L \in ZPP$. Then there is a probabilistic TM M' that outputs the correct answer *if* it terminates, and runs in *expected* polynomial time. If $T_{M'}(n)$ is the running time of M', then $E[T_{M'}(n)] = \sum_{i=1}^{\infty} iPr[T_{M'}(n) = i] = n^c$. We apply Markov's inequality (Lemma A.7 for $k := l/E[T_{M'}(n)]$) for some l (to be determined), and get

$$Pr[T_{M'}(n) \geq l] \leq \frac{E[T_{M'}(n)]}{l} = \frac{n^c}{l}. \tag{2}$$

If we set $l := 2n^c$, the probability of (2) is $\leq 1/2$. Let M be the probabilistic TM that runs $M'(x)$ for at most $l = 2n^c$ steps. If it terminates at some point with an answer $M'(x) = 0$ or 1, then output the answer, else output ?. Because of (2), $Pr[M(x) =?] \leq 1/2$.

(b) See lecture notes.

Exercise 7.8

(a) As described at the beginning of the proof for Theorem 7.14, we have a polynomial-time probabilistic TM M that, given input $|x| = n$, uses $m = p(n)$ random bits for some polynomial p so that $Pr_r[3SAT(M(x,r)) \neq \overline{3SAT}(x)] \leq \frac{1}{2^{-n-1}}$. Continuing with the argument of Theorem 7.14, there is a random string r_0 with $|r_0| = m$, such that $3SAT(M(x,r)) \neq \overline{3SAT}(x)$, $\forall x$.

(b) Modify the proof in (a) to show how it works if the input is not just x, but (x, u), where you know that $u \in \{0,1\}^{q(|x|)}$ for a polynomial q. (*Hint:* The only change is that r_0 will now be of size polynomial in $q(|x|)$, which is still polynomial in $|x|$.)

(c) Σ_4^p languages have polynomial-time TM M' s.t.

$$\exists u_1 \forall u_2 \exists u_3 \forall u_4 : M'(x, u_1, u_2, u_3, u_4) = 1.$$

The inner statement $\forall u_4 : M'(x, u_1, u_2, u_3, u_4) = 1$ is an $coNP$ statement, which can be reduced (deterministically in poly-time) to a $\overline{3SAT}$ statement for fixed u_1, u_2, u_3, i.e., it is equivalent to $\overline{3SAT}(R(x, u_1, u_2, u_3))$. We guess the random string r_0 that works for any u_1, u_2, u_3, to reduce *deterministically* this $\overline{3SAT}$ statement to $3SAT(M(R(x, u_1, u_2, u_3), r_0))$, i.e., the statement becomes

$$\exists r_0 \exists u_1 \forall u_2 \exists u_3 \exists v_4 : M''(M(R(x, u_1, u_2, u_3), r_0), v_4) = 1$$

for a polynomial certifier M'' of $3SAT$, which is a Σ_3^p statement.

Exercise 7.10

Consider the directed graph that consists of a path $s \to v_1 \to v_2 \to \ldots \to v_{n-2} \to t$, plus the edges $(v_i, s),\ i = 1, \ldots, n-2$. Each edge can be taken with probability 1/2, except for (s, v_1) that is taken with probability 1. Then the expected time to reach t can be calculated recursively

$$E[s \to t] = E[s \to v_{n-2}] + \frac{1}{2}1 + \frac{1}{2}E[s \to v_{n-2}], E[s \to v_1] = 1$$

or

$$\frac{1}{2}E_n = E_{n-1} + \frac{1}{2},\ E_1 = 1$$

which implies $E_n = \Omega(2^n)$.