Complexity Theory
Problem Set 6

1. Describe a real number ρ such that a PTM that chooses δ_0 with probability ρ and δ_1 with probability $1 - \rho$ can decide an undecidable language in (probabilistic) polynomial time.

2. Complexity class **BPL** is the set of languages that can be decided by a logspace PTM that gives the right answer with probability at least $2/3$. Prove that **BPL** ⊆ **P**.

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

4. Show that if **NP** ⊆ **BPP**, then **NP** = **RP**. (Use the idea of self-reducibility)

Solutions

1. *https://cstheory.stackexchange.com/questions/43831/how-to-use-a-coin-so-a-tm-can-decide-an-undecidable-language-in-polynomial-ti*

2. Let M be a **BPL** machine. We will design a polynomial time TM M' such that $L(M) = L(M')$. On input x, M' will first construct the configuration graph $G_{M,x}$.

For every $v \in G_{M,x}$, let $prob(v)$ denote the probability of reaching an accepting configuration from v. M' computes the $prob(v)$ for every vertex in the following way.

1) Set $prob(v) = 1$, if v is an accepting configuration and $prob(v) = 0$ if v is a rejecting configuration.
2) For every vertex v whose $prob(v)$ is still not computed, set $prob(v) = \frac{1}{2} . prob(v_1) + \frac{1}{2} . prob(v_2)$, if $prob(v_1)$ and $prob(v_2)$ are already computed and there is an edge from v to both v_1 and v_2.
3) Repeat 2 until $prob(v)$ is computed for all $v \in G_{M,x}$.

In the end, M' accepts x if and only if $prob(v_{init}) \geq \frac{2}{3}$, where v_{init} is the initial configuration. The procedure to compute $prob(v)$s can easily be done by M' in time polynomial in $|G_{M,x}|$ and since M is a BPL machine, $|G_{M,x}|$ is also polynomial in the length of x.

3. Let's call the new class as **ZPP**$'$. **ZPP**$' \subseteq$ **ZPP** can be proven by repeating the **ZPP**$'$ machine inside a **ZPP** machine again and again until you get a non "?" output. The expected time of **ZPP** machine will clearly be polynomial. **ZPP** $\subseteq$ **ZPP**$'$ can be proven by running **ZPP** machine inside a **ZPP**$'$ machine for $2T$ steps, where T is **ZPP** machine's expected time. Within $2T$ time if **ZPP** machine answers something, **ZPP**$'$ machine will answer the same, else it will output "?". The probability analysis can be done using Markov's inequality.

4. *https://cs.stackexchange.com/questions/80509/show-that-if-np-subseteq-bpp-then-also-np-rp-considerations-about-solution*