

CS401 - Problem Set 10 - the last one!

This problem set is a little challenging, so give yourself time to think!

1. Prove that if $3\text{SAT} \leq_p \overline{3\text{SAT}}$, then $\mathbf{PH} = \mathbf{NP}$. (The \mathbf{PH} collapses to \mathbf{NP}).
2. The class \mathbf{ZPP} (zero-error probabilistic polynomial time) is another variant on \mathbf{BPP} :

Definition. $L \in \mathbf{ZPP}$ if there exists a probabilistic TM (PTM) M such that if

$$x \in L \leftrightarrow \Pr[(M(x) = 1)] = 1 \tag{1}$$

$$x \notin L \leftrightarrow \Pr[(M(x) = 1)] = 0 \tag{2}$$

and for all x , $M(x)$ terminates in polynomial time on average.

The idea with \mathbf{ZPP} is that it always outputs the right answer, and usually it takes polynomial time, but it can sometimes take much longer. However, the likelihood of it taking a long time is small.

- (a) Prove that $L \in \mathbf{ZPP}$ iff \exists a polytime probabilistic TM M that outputs $\{0, 1, ?\}$ such that for every $x \in \{0, 1\}^*$, $M(x) \in \{L(x), ?\}$, and $\Pr[M(x) = ?] \leq 1/2$, where this probability is over the random choices that M makes. (Note that unlike in \mathbf{ZPP} , M will always terminate in polynomial time.)
- (b) Explain the significance of part (a).
- (c) Prove $\mathbf{ZPP} \in \mathbf{RP} \cap \mathbf{coRP}$