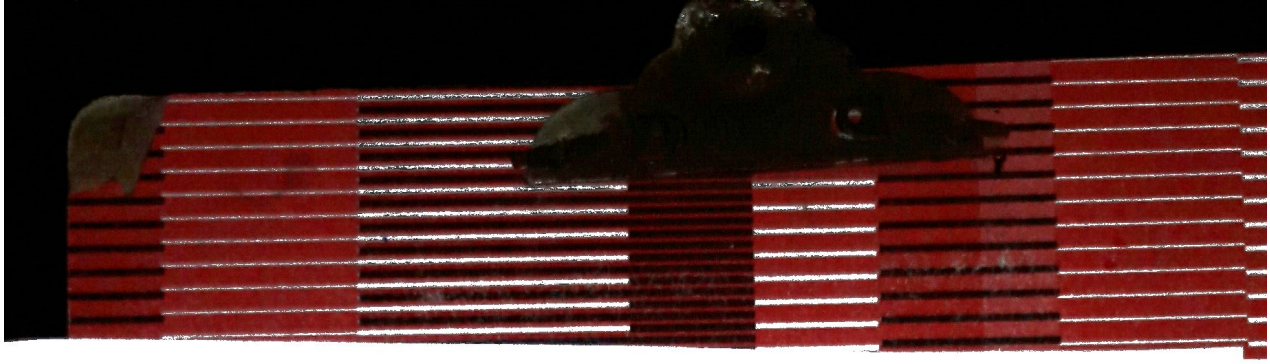

Assignment 3

1. ZPP is the complexity class which contains all the languages L for which there is a machine M that runs in expected polynomial time but never makes mistake on any input. Prove that $ZPP = RP \cap coRP$

2. B reduces to C under a randomized polynomial time reduction, denoted by $B \leq_p C$ if there is a probabilistic TM M s.t $\forall x$: $Pr[B(M(x)) = C(x)] \geq$
$BP \cdot NP = \{ L : L \leq_p 3SAT \}$.
Prove that $BP \cdot NP \subseteq NP/poly$.

3. Prove that there exists a perfectly complete $AM[O(1)]$ protocol for proving a lower bound on set size.

4. Let $k \leq n$. Construct a family $H_{n,k}$ of a pairwise independent functions : $\{0,1\}^n \rightarrow \{0,1\}^k$ as discussed in class.

5. Prove QUADEQ is NP - complete.