Homework #5

1. 1. We have an expected-polynomial time algorithm M for any language in BPP. Here goes an exchange protocol as follow:
      1. For an input sequence x, V apply an algorithm M and sends a random bit form to P.
      2. P sends the inverse bit back to V.
      3. V ignore the bit , and apply algorithm to generate answer.
   2. For the protocol , it is a perfect zero-knowledge property because
      1. M is in expected polynomial time.
      2. M on any x has the same probability distribution as the one that can be observed.
   3. Therefore, we claim that zero-knowledge proofs exist for every language in BPP.
2. 1. Construct a Turning Machine T has the property follow:

We know the satisfied cluster at most achieve 89.1% of all clusters if the Boolean expression is unsatisfiable, so we set the threshold at 90%. Thus, we can decide any x is satisfiable or not in polynomial time. If there is more than 90% clusters is satisfy, than x is belong to SAT, otherwise, it isn’t. Therefore, under our assumption.