CS 1511 Homework 18

Mathew Varughese, Justin Kramer, Zach Smith

Sunday, March 25

33. a)

33. b)

33. c)

33. d)

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

Hint: First note that in the current set lower bound protocol we can have the prover choose the hash function. Consider the easier case of constructing a protocol to distinguish between the case $|S| \geq$ K and $|S| \leq$ 1K where c¿2 can even be a function of K. c If c is large enough, we can allow the prover to use several hash functions h1 , . . . , hi , and it can be proven that if i is large enough, well have $\cup_i hi(S) = 0, 1k$.The gap can be increased by considering instead of S the set Sl, that is the l times cartesian product of S.