

# CS 1511 Homework 18

Mathew Varughese, Justin Kramer, Zach Smith

Sunday, March 25

**33. a)** The verifier could simulate say 1000 trials of the prover and pick the majority answer. Since the verifier is a BPP machine it still will error with low probability if the prover sends an incorrect result.

**33. b)** We have polynomial space so verifier writes down every possible thing to ask. This can be done in polynomial space. Then, it keeps track of the maximum probability.

**33. c)** IP is in PSPACE. So, changing the  $2/3$  to 1 does not matter.

**33. d)** This means that the verifier always rejects when a string is not in the language. Since the verifier can ask a polynomial number questions, this means that enough trials can be made to know if it is the language. So,  $IP' = NP$ .

**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  $K$ . If  $c$  is large enough, we can allow the prover to use several hash functions  $h_1, \dots, h_i$ , and it can be proven that if  $i$  is large enough, we'll have  $\cup_i h_i(S) = [0, 1K]$ . The gap can be increased by considering instead of  $S$  the set  $S^l$ , that is the  $l$  times cartesian product of  $S$ .