

May 9

COURSE WEBSITE: [www.cs.umd.edu/~gasarch/858/858.html](http://www.cs.umd.edu/~gasarch/858/858.html)

1. (50 points) Assume there is a set of hash functions  $H_{n,k}$  such that the following hold.
  - (a)  $H_{n,k}$  has functions from  $\{0, 1\}^n$  to  $\{0, 1\}^k$ .
  - (b) Arthur can pick an  $h \in H_{n,k}$  randomly.
  - (c) For all  $k, n$ , for all  $X \subseteq \{0, 1\}^n$ , if Arthur picks  $h \in H_{n,k}$  at random, and  $S = |\{x \in X : h(x) = 0^k\}|$ , then  $E(S) = |X| - 2^{-\sqrt{k}}$  and  $Var(S) \leq 2$ .

Let PROMISE( $\phi$ ) be “ $\#(\phi(x_1, \dots, x_n)) \leq 2^{n-1}$  OR  $\#(\phi(x_1, \dots, x_n)) \geq 2^{n-1} + n$ ”.

Let  $A = \{\phi : \#(\phi(x_1, \dots, x_n)) \geq 2^{n-1} + n\}$ .

Use the  $H_{k,n}$  to come up with an AM protocol for  $A$  assuming that, for all inputs  $\phi$ , PROMISE( $\phi$ ) holds. Prove that it works.

HINT: The answer should be of the following form (you need to fill in the blanks).

PROTOCOL:

- (a) Input( $\phi(x_1, \dots, x_n)$ ) (We assume PROMISE( $\phi(x_1, \dots, x_n)$ ) holds.)
- (b) Arthur picks a random  $h \in H_{k,n}$  where  $k = XXX$ . Arthur sends this  $h$  to Merlin.
- (c) Merlin sends Arthur YYY elements  $z \in \{0, 1\}^n$ .
- (d) Arthur checks that, for each  $z \in \{0, 1\}^n$  that Merlin send, ZZZ holds. If so, he accepts. If not he rejects.

PROOF OF CORRECTNESS:

If  $\#\phi \geq 2^{n-1} + n$  then FILL THIS IN hence  $\Pr(\text{Arthur accepts}) \geq \frac{3}{4}$ .

If  $\#\phi \leq 2^{n-1}$  then FILL THIS IN hence  $\Pr(\text{Arthur accepts}) \leq \frac{1}{4}$ .

2. (50 points) Show that  $PCP(5, \log n, \frac{1}{4}) \subseteq NP$ .
3. (0 points- don't hand in) What is your favorite theorem from this course? Why?