Homework 21

Austin Frownfelter Matthew Bialecki

March 14, 2018

1 Problem 35

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

The standard AM protocol that proves the set lower bound has completeness (accepts if x $\in$ L) $\geq \frac{2}{3}$. We already know there is a trivial way to boost this completeness to $1 - \frac{1}{4^n}$ such that it is still an AM protocol. To get to perfect completeness (= 1), we will use the marriage technique from the BPP $\subseteq \Sigma_2^p$.

The Verifier will take a sequence of weddings and will accept if there exists some marriage such that the result makes it accept. More formally, V(y,w) will accept iff $\exists$w (h(x) = y) $\vee$ (h(x) = $w_1 \oplus$ y) $\vee$ ... $\vee$ (h(x) = $w_i \oplus$ y).

This shows there is a perfectly complete AM protocol which proves the set lower bound. Since the marriages Merlin must devise depend solely on y, which Arthur provides in the first question, the protocol is run in AM[$O(1)$].