CS 1511 Homework 19

Mathew Varughese, Justin Kramer, Zach Smith

Wednesday, March 27

36.

AM = { (M, p, q, I) | ∃ TM M, ∃ polynomial p ∃ polynomial q and input I such that:
M runs in poly-time
if x ∈ L, then $Pr_{y\in\{0,1\}^{p(n)}}(\exists z \in \{0,1\}^{q(n)} M(x,y,z) = 1) \geq 2/3$
if x ∉ L, then $Pr_{y\in\{0,1\}^{p(n)}}(\forall z \in \{0,1\}^{q(n)} M(x,y,z) = 0) \geq 2/3$
MAM = { (M, x, y, R, I) | ∃ TM M, ∃ polynomial x ∃ polynomial y and input I such that:
M runs in poly-time
if x ∈ L, then $Pr_{y\in\{0,1\}^{x(n)}}(\exists z \in \{0,1\}^{y(n)} M(x,R,y) = 1) \geq 2/3$
if x ∉ L, then $Pr_{y\in\{0,1\}^{x(n)}}(\forall z \in \{0,1\}^{y(n)} M(x,R,y) = 0) \geq 2/3$

Where in MAM Merlin send an x, Arthur replies with a random bits R, and Merlin sends back a y.

L ∈ MAM
When Arthur sends random bits to Merlin in the MAM protocol, there's a chance that he sends bits that are incorrect. If Arthur sends m^2 bits back, the chance the he is wrong is $1/4^m$. Here is how we do this. According to the Chernoff bound, with k independent unfair coin flips with our probability of 2/3 correctness, the expected number of heads is $2k/3$. Our chances that there's more than 10% more or less than 10% less is at most $2 * e^{-(p)^2 * k/3}$. Thus, the chances that we get more than 10% more would be $2/(\sqrt[27]{e^{4k}})$, which will be equal to one in a polynomial amount of coin tosses k. The expected number of tails would be $1k/3$, so we have a majority of heads. If through a union bound we continue to take the majority each time we do these coin flips, the probability that we send an incorrect answer is less than one. In this way, we do not need Merlin to send us a first x, and our language is now just Arthur sending a ton of coin flips in parallel at once to Merlin and having Merlin still respond since he already does that in MAM, which is in AM.
L ∈ AM