Homework 23

Austin Frownfelter Matthew Bialecki

March 19, 2018

1 Problem 39

Prove CoNP $\subseteq$ IP to show IP = PSPACE

1.1 Part a

Since the definition of the QBF formula in the problem states universal quantifiers exists at most once for each variable x_j before the final occurrence of x_i where $j > i$, there is a blowup in the degree of the resulting polynomial of at most 2 for each universal quantifier. This blowup is at most 2 because this quantifier will exist only once with previous variables considered. Thus, the degree for each previous variable will increase by 1, and as a result the degree will double at worst. Since variables multiplied by themselves are effectively the same as just the value of the single variable, the degree will be, at worst, O(n).

1.2 Part b

If there is a conflicting variable (one which causes the ψ QBF function to not fit the y QBF definition), then start at the right and add a new variable with a corresponding universal quantifier for each conflict. Repeat this for all conflicting variables. Using this algorithm, there are at most n-i conflicts for each ith (of n) variable, which will yield a formula with n*n variables. Therfore, this algorithm yields a formula of size O(n^2)

2 Problem 40

A one-time pad is equivalent to a truly random number to any function which does not know it. A function can therefore do no better than flipping a random coin to guess a given bit, therefore the probability of guessing any given bit is $\leq \frac{1}{2}+$ negligible.

3 Problem 41

If P=NP, then there exists a way to invert a one-way function in polynomial time (by attempting all possibilities in polynomial time).