Theory of Computer Science to Msc Students, Spring 2006

Exercise 5

Lecturer: Dorit Aharonov *Hand in date: 11.06.07 -* ***not mandatory***

1. Show that if $\mathbf{P} = co\mathbf{NP}$ then $\mathbf{P} = \mathbf{PH}$.

2. In class we described a tree for a given instance of TQFT, whose value is the value of the formula. (We viewed this tree as describing a game corresponding to the formula.) We then used the tree description of the problem to show that TQFT is in **PSPACE**.

   a) Now, consider the problem of finding the optimal next step for the game of GO, where by optimal we mean the step that maximizes the number of points at the end of the game. It turns out that this problem is **EXP** complete. Can you describe the problem as finding the value of a tree? to do this, describe what should be in the nodes and what should be in the leafs, and how is the value calculated.

   For the rules of GO you can have a look at
   `http://en.wikipedia.org/wiki/Go_%28board_game%29`

   Obviously, the answer to the question does not need to include all the exact rules of the game... Just say abstractly how the tree looks like and how its value is calculated.

   b) In class, we used the tree construction to show that TQFT is in **PSPACE**. Why doesn't a very similar proof apply here to show that the above GO problem is in **PSPACE**?

3. Show that if $\mathbf{P} = \mathbf{NP}$ then one way functions and Pseudo Random Genrators do not exist.

4. In the derandomization lemma shown in class, where we applied the existence of PRG to get $\mathbf{BPP} = \mathbf{P}$, we assumed that the generators G_m are secure against circuits of size m^2. Does the proof go through if we assume security against circuits of size m? what about m^3?

5. Prove that for every natural numbers n and k

$$\binom{n}{k} \geq 2^{H(\frac{k}{n})n}/(n+1)$$

6. A family of Linear codes C_n, where C_n is a $[n,k,d]$-code, is a good code if we have k/n (the rate of the code) and d/n (the percentage of correctable errors) both larger than some constant > 0 independent of n. Consider the Reed-Solomon codes encoded in binary by converting each field element to binary representation. Are they good codes?