COS 522 Complexity — Homework 3.

Boaz Barak

Total of 120 points. Due March 27th, 2006.

Exercise 1 (25 points)**.** For every directed graph G, let $\#\mathsf{CYCLE}(G)$ be the number of simple (no repeated vertices) directed cycles in G. Prove that if there's a polynomial-time algorithm A such that

$$\frac{1}{2} \leq \frac{A(G)}{\#\mathsf{CYCLE}(G)} \leq 2$$

for every directed G then $\mathbf{P} = \mathbf{NP}$.

Exercise 2 (25 points)**.** Let f be any function in $\#\mathbf{P}$. Prove that for every $\epsilon > 0$, there exists a probabilistic polynomial time algorithm A such that

$$1 - \epsilon \leq \frac{A^{\Sigma_5\mathsf{SAT}}(x)}{f(x)} \leq 1 + \epsilon$$

for every $x \in \{0,1\}^*$, where for every function $g : \{0,1\}^* \to \{0,1\}$, A^g denotes executing A with access to an oracle that computes g, and $\Sigma_5\mathsf{SAT}$ denotes the function that on input a quantified Boolean formula with at most 5 alternations and the outside quantifier being $\exists$, returns 1 iff the formula is true. (We note that 5 is actually an overkill, and this can be done using 3 levels and a deterministic algorithm A.)

Exercise 3 (25 points)**.** Show that $\mathbf{IP} \subseteq \mathbf{PSPACE}$.

Exercise 4 (25 points)**.** Show that $AM[k] = AM[2]$ for every constant $k \geq 2$. That is, show that if L has a k-round public coin interactive proof then it has a two round proof, consisting of the verifier sending a random string and the prover responding. (Hint: do this by showing that $AM[k+1] \subseteq AM[k]$ for all $k \geq 2$.)

Exercise 5 (20 points)**.** Let L be a language. We say that L is *downward self-reducible* if there exists a deterministic polynomial-time Turing machine M such that **(a)** if M is executed with access to an oracle solving L, then it also solves L: that is for every $x \in \{0,1\}^*$, $M^L(x) = L(x)$.[1] and **(b)** on input $x \in \{0,1\}^*$, M only asks its oracle queries that are shorter than x (of length at most $|x| - 1$).

1. Show that the languages SAT (satisfiable CNF formulas with clauses of any length, not necessarily 3) and TQBF (true quantified Boolean formulas) are downward self-reducible. (Hint: this may seem to depend heavily on the particular representation of formulas as strings, but in fact once you show this for one reasonable representation it's not hard to generalize the algorithms for others as well. You can pick any reasonable representation to solve this question.)

2. Show that if L is downward self-reducible then $L \in \mathbf{PSPACE}$.

[1] Note that without another condition, it is trivial to find such M since M could simply ask its oracle on the input x.