COS 522 Final

Due Jan 11 at the latest in my office, Room 307

Instructions: This exam has seven questions, each worth 20 points. Some questions have subparts.

Finish the test within **96 hours** after first reading it. You can consult any notes/handouts from this class as well as the text. Feel free to quote, without proof, any results from class or the text. You cannot consult any other source or person in any way.

Do not read the test before you are ready to work on it.

Write and sign the honor code pledge on your exam (The pledge is "I pledge my honor that I have not violated the honor code during this exam and followed all instructions.")

I will try to answer all emails about the exam promptly. I will also offer to call you if your confusion does not clear up. In case of unresolved doubt, try to explain your confusion as part of the answer and maybe you will receive partial credit.

1. (20 points) Say whether the following statements are true or false or open (to the best of your knowledge), and give a reason for your answer in a couple of lines.

   (a) NEXPTIME $\neq$ BPP.

   (b) If P $=$ L then P $\neq$ PSPACE

   (c) TQBF is in AM[2].

   (d) If $L \in$ NP is weakly-hard (in the sense defined in connection with the Yao XOR Lemma) then there is a language $L' \in$ NP that is strongly hard.

2. (20 points) We showed that the undirected s-t-connectivity problem can be solved in randomized logspace. Show that the random walk algorithm fails to work for directed graphs. In other words, describe a directed graph in which there is a path from s to t but the random walk takes exponential time to reach t when started in s.

3. Show that for every $k > 1$ there is a language in PH that has circuit complexity greater than n^k. (Hint: Keep in mind the proof of the *existence* of functions with high circuit complexity.)

4. A language is called *unary* if every string in it is of the form 1^i (the string of i ones) for some $i > 0$. Show that if a unary language is NP-complete then P $=$ NP. (Hint: If there is a n^c time reduction f from 3SAT to a unary language L, then f maps every 3SAT instance of size $\leq n$ to some string of the form 1^i where $i \leq n^c$. Also note that if $f(\phi) = f(\psi)$ then either both ϕ and ψ are satisfiable or both are not. Use this to prune the exponential-size search tree.)

5. Show that MA $\subseteq \mathbf{\Sigma}_2^p$. (Here MA refers to public coin interactive proofs where there is only one round of interaction, with the prover speaking to the verifier.)

6. Show that if f is a one-way permutation then so is f^k (namely, $f(f(f(\cdots(f(x)))))$ where f is applied k times). Show that the above fails for one-way functions. (You may assume that one-way functions exist.)

7. The Razborov-Smolenksy proof we did in class showed that PARITY is not in $\text{ACC}^0[3]$. Why does this type of proof break down if the circuit has MOD m gates where m is not a prime? Identify all the places where the proof breaks down.