CSE531: Complexity Theory

Midterm

Anup Rao Due: May 22

The midterm is take home, but collaboration is not allowed. You may use anything in the class notes without proof. No other materials may be used to solve the midterm.

1. Prove that if $\mathbf{NP} \subseteq \mathbf{BPP}$, then $\mathbf{NP} \subseteq \mathbf{RP}$.

2. Give an example of a function that is computable in exponential space (space $2^{n^{O(1)}}$) yet does not have polynomial sized circuits. HINT: The space is enough to enumerate over all circuits of a certain size.

3. Someone shows that there is a logspace algorithm that takes as input a directed graph G and a number c and determines whether the shortest cycle in the graph (if it exists) is of length c. Show that this implies that $\mathbf{NL} = \mathbf{L}$.

4. Show that if there is an $\mathbf{NP}$-complete function $f : \{0,1\}^* \to \{0,1\}$ and a number k such that for every n,
$$|\{x : |x| = n, f(x) = 1\}| \leq n^k,$$
then $\mathbf{P} = \mathbf{NP}$. HINT: Consider the following variant of SAT. The input is a formula ϕ and an assignment to the variables w. The output is 1 if and only if there is an assignment a such that $\phi(a) = 1$ and $a \leq w$ in the lexicographic ordering on assignments. Since this problem is in $\mathbf{NP}$, there is a polynomial time computable function g such that $f(g(\phi, w))$ computes the answer. Now if the output length of g on n-bit inputs is at most n^c, pick $w_0, \ldots, w_{n^{kc+c}}$ evenly spaced in the ordering, and consider the values $f(g(\phi, w_i))$ for each i. Since there are at most n^{kc+c} inputs to f of length $1, 2, \ldots, n^c$ that evaluate to 1, either one of these values is 0, or $g(\phi, w_i) = g(\phi, w_j)$ for some $i \neq j$. Conclude by giving a polynomial time algorithm for deciding whether or not ϕ is satisfiable. (It migth be useful to use the fact that $1 - \epsilon \leq e^{-\epsilon}$ for all ϵ.)