Solution to question 4(b)

March 14, 2016

Problem 1

Prove that if \( P = NP \) then there is a problem in \( EXP \) that requires circuits of super-polynomial size.

Proof.

Lemma 1. \( EXP \subseteq SIZE(n^{O(1)}) \) implies \( EXP \subseteq \Sigma_2 \).

Proof. (Of Lemma) Let \( L \in EXP \) and let \( M \) be the Turing machine that solves \( L \) in time \( \leq 2^{p(n)} \) on inputs of length \( n \). Fix a representation of the configurations of \( M \) on some \( n \)-bit input \( x \). Each configuration can be written with \( O(2^{p(n)}) \) bits.

There is a machine \( M' \) that, given a string \( x \) of length \( n \), and integers \( t \leq 2^{p(n)} \) and \( i \leq O(2^{p(n)}) \), outputs the \( i \)-th bit of the configuration reached by \( M(x) \) after \( t \) steps. Moreover, \( M' \) is an \( EXP \) machine so by assumption there is a family of polynomial size circuits that simulate \( M' \). Let \( q(n) \) be a polynomial upper bound to the size of these circuits. The \( \Sigma_2 \) verifier of \( M \), on input \( x \), will guess a circuit \( C \) of size \( q(n) \), then it will verify that for every \( i \) and \( t \), the value of \( C(x,t,i) \) is consistent with the (constant number of) values \( C(x,t-1,..) \) that it depends on. Finally, it will accept if and only if \( C \) predicts that after \( 2^{p(n)} \) steps \( M(x) \) accepts.

\[ x \in L \text{ iff } \exists C, |C| \leq q(|x|) \text{ such that } \forall t \leq 2^{p(|x|)} \text{ and } \forall i \leq O(2^{p(x)}) \text{, } C(x,t,i) \text{ is consistent with } C(x,t-1,..) \text{ and } C(x,2^{p(|x|)},..) \text{ describes an accepting configuration} \]

The proof of the homework problem follows by the time hierarchy theorem where we are guaranteed that \( EXP \neq P \) and the conclusion of part (1) of the question where if \( P = NP \) then \( P = \Sigma_2 \).