Homework 15

Joe Baker, Brett Schreiber, Brian Knotten

February 15, 2018

23

Problem 6.3 Describe a decidable language in $P/_{poly}$ that is not in P

From the Time Hierarchy Theorem we know there exists a decidable language $L \notin EXP$. Using L, we can construct the unary language $L' = \{1^n | n \in L\}$. Clearly, by the proof of claim 6.8 in the book, $L' \in P/_{poly}$. To show that $L' \notin P$, assume the opposite: therefore $\exists$ TM M that decides L' in time $O(n^k)$. We could then use M to construct the TM M' that decides L in time $O((2^n)^k)$, meaning that $L \in EXP$ - a contradiction. All that remains is to show that L' is decidable; this is trivial however, as L is decidable so we merely define L' to reject all inputs not of the form 1^n and accept only if $n \in L$. Therefore $\exists$ decidable language L' such that $L' \in P_{poly}$ and $L' \notin P$.

24

a

Problem 6.5: Show for every $k > 0$ that PH contains languages whose circuit complexity is $\Omega\left(n^k\right)$.

Proof:
Let C be a circuit with complexity at of at least n^k. We know that such a circuit must exist by Theorem 6.22 from the book. We can construct a boolean formula F from the gates of C with k quantifiers over the boolean formula. Now let L be the language of all variable assignments for k which satisfy F. Since $|C|$ is polynomial, C can decide if an input is valid for F in polynomial time. So there must exist a TM M with k advice tapes (from the quantifiers) that can decide the input with its advice tapes in polynomial time. Thus for each $k > 0$, there is a language in PH whose circuit complexity is $\Omega\left(n^k\right)$.

b

Problem 6.6: Show for every $k > 0$ that Σ_2^p contains languages whose circuit complexity is $\Omega\left(n^k\right)$.

Proof:
Consider the circuit C from problem 6.5. Now construct the same formula F, but only use two quantifiers. One $\exists$ over the tuple of some of the variables and one $\forall$ for the remaining tuple of variables. Again let L be the language of all variable assignments for k which satisfy F. Since $|C|$ is polynomial, C can decide if an input is valid for F in polynomial time. So there must exist a TM M with 2 advice tapes (from the quantifiers) that can decide the input with its advice tapes in polynomial time. Thus for each $k > 0$, there is a language in Σ_2^p whose circuit complexity is $\Omega\left(n^k\right)$.

c

Problem 6.7: Show that if P = NP, then there is a language in EXP that requires circuits of size $\frac{2^n}{n}$.

Proof:
Assume P = NP and let $L \in$ EXP. If L is decidable by a circuit of complexity n^k, then because the polynomial hierarchy is collapsible and by problem 6.6, L is in P. So any L in EXP that is not in P must have a circuit with complexity $\frac{2^n}{n}$.