Homework 15

Austin Frownfelter Matthew Bialecki

February 16, 2018

1 Problem 23

"Describe a decidable language in P/poly that is not in P"

Assume $L \notin EXP$.
$L' = \{1^m | m \in L\}$
There exists a family of circuits which decides L' in polynomial gates ($L' \in P/poly$)
If L' runs in polynomial time on input 1^m (relative to m) then L runs in exponential time on input m (relative to $n = \log m$).
This contradicts with the assumption, which means L must be contained in EXP. Therefore, this language is in P/poly but not in P.

2 Problem 24

2.1 Part a

Show for every $k > 0$ that PH contains languages whose circuit complexity is $\Omega(n^k)$

For any given k, construct a TM that decides a Σ_k^p language as such: The input is a quantified boolean formula with k input variables.
There exists a circuit which "simulates" this TM.
This circuit's complexity is greater than n^k.
Therefore, for all k, there exists a language which is decided by a family of circuits where $|C_n| \geq n^k$

2.2 Part b

Solve question 6.5 with PH replaced by Σ_2^p (if your solution didn't already do this).

By the logic in the previous problem, there existed a circuit which decided a Σ_2^p language in complexity $\geq n^k$.

2.3 Part c

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

If P = NP then the Polynomial Time Hierarchy would collapse, having all Σ_k^p and Π_k^p problems be solved in time of a Σ_1^p problem. Since EXP must be a strict superset of PH (per the Time Hierarchy Theorem), the circuit lower boundary of EXP would decrease to $\frac{2^n}{n}$.