6.841: Advanced Complexity Theory Spring 2016

Problem Set 2

Due Date: March 15th, 2016

Turn in your solution to each problem on a separate piece of paper. Mark the top of each sheet with the following: (1) your name, (2) the question number, (3) the names of any people you worked with on the problem, or "Collaborators: none" if you solved the problem individually. We encourage you to spend time on each problem individually before collaborating!

Problem 1 – AC0 Lower Bound for Majority

Define the function MAJ$(x) = 1$ iff $|x| \geq n/2$, where $|x|$ denotes the number of 1s in the n-bit string x.

Prove that any circuit of constant depth d computing the function MAJ requires size $\exp(\Omega(n^{2^{-d-O(1)}}))$. Hint: Use the fact that depth d circuits computing PARITY require size $\exp(\Omega(n^{2^{-d}}))$.

Problem 2 – Hardness of Counting over $\mathbb{Z}$

Fix some small $\epsilon < 1$. Consider the following computational problem: given a polynomial time computable function $f : \{0,1\}^n \to \mathbb{Z}$, estimate $\sum_x f(x)$ to within a factor $(1 \pm \epsilon)$. Show that given an oracle for this problem, one can solve any $\#\mathsf{P}$ problem in polynomial time.

Problem 3 – Computing OR Exactly with Polynomials

Let q be any prime. Show that any polynomial over $GF(q)$ that exactly agrees with the n-bit OR function on $\{0,1\}^n$ must have degree at least n.[1]

Problem 4 – (Another) Alternate Characterization of PH

In the first problem set, we saw that $\Sigma_2^P = NP^{NP}$. Extrapolating this, we get an alternate characterization of the polynomial heirarchy in terms of *oracle machines*. In this problem, we will give another characterization of the polynomial heirarchy in terms of circuit families.

Definition 1. *(DC-Uniform Circuits) Let $\{C_n\}_{n\geq 1}$ be a circuit family. We say that $\{C_n\}$ is a* Direct Connect uniform *(DC uniform) family iff the following functions are computable in polynomial time:*

[1] Notice that this means that using approximations of OR gates was in a sense *necessary* to get a low degree polynomial to represent the circuit in the proof of Razborov-Smolensky.

- SIZE(n) - *returns the size S of the circuit C_n in binary.*
- TYPE(n, i) - *returns the type of the ith gate of C_n, i.e. $\wedge$, $\vee$, $\neg$, or $NONE$.*
- EDGE(n, i, j) - *returns 1 if there is a directed edge in C_n from the ith gate to the jth gate.*

Show that $L \in PH$ iff L can be computed by a DC uniform circuit family $\{C_n\}$ that satisfies the following:

1. Uses AND, OR, and NOT gates
2. has size $2^{n^{O(1)}}$ and constant depth
3. its gates can have unbounded (exponential) fan-in
4. its NOT gates appear only at the input level

You may additionally assume that the underlying labeling of gates is such that, if the depth of one gate is greater than another, then it has a higher label. Furthermore, it is okay to assume that the DC uniform circuit has AND and OR layers like we are used to from class.

Problem 5: Practice with Larger Complexity Classes

In the proof of NEXP $\not\subseteq$ ACC0, Williams deals with large complexity classes like E^{NP} and NEXP. We will use the complexity class E = DTIME($2^{O(n)}$), the corresponding nondeterministic class NE = NTIME($2^{O(n)}$), and the class NEXP = NTIME($2^{\mathrm{poly}(n)}$) below to build some intuition about larger complexity classes.

a) Show that NEXP $\subseteq \mathrm{E}^{\mathrm{NP}}$. [2]

b) Show that NEXP $\not\subseteq P/\mathrm{poly} \Rightarrow$ NE $\not\subseteq P/\mathrm{poly}$

c) We say a Turing Machine M *nondeterministically generates* the truth table of a function $f_n : \{0,1\}^n \to \{0,1\}$ if, on input 1^n, we have the following. Given an advice string of length n, M should:

- Have at least one accepting branch of computation.
- Whenever M accepts, it should contain the truth table of f_n in the output tape.

Show that $NEXP \not\subseteq P/\mathrm{poly}$ implies there is a poly(2^n)-time TM which, on input 1^n and given an advice string x_n of length n, nondeterministically generates 2^n-bit truth tables of n-variable Boolean functions f_n satisfying the following: for every $d \in \mathbb{N}$ and infinitely many $n \in \mathbb{N}$, f_n has circuit complexity greater than n^d.

[2] In "A Casual Tour Around a Circuit Lower Bound," Williams first proves that $\mathrm{E}^{\mathrm{NP}} \not\subset ACC0$ before improving it to NEXP $\not\subset ACC0$.

Note: The characterization of languages $L \in \text{PH}$ as DC-uniform circuit families allows us to interpret lower bounds on circuit families as lower bounds on the oracleized polynomial hierarchy. In fact, Furst, Saxe, and Sipser proved that if their lower bound on the size of circuits in AC0 that compute Parity was improved from super-polynomial to super-quasi-polynomial then this would yield an oracle A such that $\text{PH}^A \neq \text{PSPACE}^A$. Indeed, this was accomplished by works of Yao '85 and Håstad '86.

Results have also been translated from PH to circuit families. In fact, using this correspondence and similar ones for $\oplus$P and #P it is possible to reinterpret Toda's theorem in the land of circuits. This intuitive line of reasoning comes up in the Yao-Beigel-Tarui theorem, which is used in the Ryan Williams's proof that NEXP $\not\subset$ ACC0.

18.405J / 6.841J Advanced Complexity Theory

Spring 2016