CS 221: Computational Complexity **Prof. Salil Vadhan**

Problem Set 3

Assigned: Thu. Mar. 13, 2014 Due: Fri. Mar. 28, 2014 (5 PM sharp)

- You must *type* your solutions. LaTeX, Microsoft Word, and plain ascii are all acceptable. Submit your solutions *via email* to `cs221-hw@seas.harvard.edu`. If you use LaTeX, please submit both the compiled file (`.pdf`) and the source (`.tex`). Please name your files `PS3-yourlastname.*`.
- Strive for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Do not despair if you cannot solve all the problems! Difficult problems are included to stimulate your thinking and for your enjoyment, not to overwork you. *'ed problems are extra credit.

Problem 1. (circuit complexity of a threshold function) Consider the threshold function $\mathrm{Th}_2(x_1, \ldots, x_n)$, defined to be 1 iff at least two of the input variables are 1.

1. Prove that $\mathrm{size}_{\{\wedge,\vee,\neg\}}(\mathrm{Th}_2) \le 4n + O(1)$. (Recall that our measure of circuit size includes the input variables.)
2. Prove that $\mathrm{size}_{B_2}(\mathrm{Th}_2) \ge 3n - O(1)$, where B_2 is the full binary basis. (Hint: show that if two variables are inputs to some binary gate, then at least one of them must be used elsewhere in the circuit.)

Problem 2. (branching programs) A *branching program* over variables $\{x_1, \ldots, x_n\}$ is a directed acyclic graph where every node is labelled with a variable x_i, or is labelled with an output in $\{0, 1\}$. Variable nodes are required to have outdegree 2 and output nodes must have outdegree 0. The two edges leaving every variable node are also labelled 0 and 1. One of the nodes is designated as the start node. Such a branching program defines a function $f : \{0,1\}^n \to \{0,1\}$, where $f(\alpha)$ is defined as follows. We begin at the start node, then follow the path determined by taking the outgoing edge from each variable node v according to the value α assigns to the variable labelling v. Eventually we reach an output node, and set $f(\alpha)$ to be the value at that node.

1. Characterize the class of languages decidable by polynomial-sized branching programs in terms of one of the complexity classes we have seen, augmented with advice.
2. A branching program has *width* w if its nodes can be partitioned into layers $L_1, L_2, \ldots$ each of size up to w, such that every edge leaving a node in layer L_i leads to a node in L_{i+1}.

   Show that every language decidable by a constant-width, polynomial-sized branching program is in $\mathbf{NC^1}$. (*Barrington's Theorem* says that the converse is also true, giving a surprising alternate characterization of $\mathbf{NC^1}$.)

Problem 3. (circuit lower bounds for high classes)

1. Prove that $\mathbf{EXPSPACE} \not\subseteq \mathbf{SIZE}(2^n/2n)$.
2. Prove that for every constant c, $\mathbf{PH} \not\subseteq \mathbf{SIZE}(n^c)$.
3. Prove that for every constant c, $\mathbf{\Sigma_2^p} \not\subseteq \mathbf{SIZE}(n^c)$.

Recall that the best circuit lower bound we have for a function in **NP** is only $6n - o(n)$.

Problem 4. (refined hierarchy theorem for circuit size*) In Arora–Barak (Thm 6.22), a hierarchy theorem for circuit size is proven, showing that a polynomial or even multiplicative factor in circuit size allows computing more functions. Tighten this hierarchy theorem as much as you can; the amount of extra credit will depend on how tight a hierarchy theorem you get.

Problem 5. (different models of randomized computation) Suppose we modify our model of randomized computation to allow the algorithm to obtain a random element of $\{1, \ldots, m\}$ for any number m whose binary representation it has already computed (as opposed to just allowing it access to random bits). Show that this would not change the classes **BPP**, **RP**, and **ZPP**.