Advanced Complexity Theory | Instructor: Madhu Sudan
6.841/18.405J - Spring 2009 | TA: Brendan Juba
Due: Wednesday, March 04, 2007

Problem Set 2 (Revised)

1. **Counting in logarithmic depth:**
   The goal of this question is to give a logarithmic depth circuit to compute the number of ones in the input, i.e., to compute $b = \sum_{i=1}^{n} x_i$. (Assume integers are represented naturally as bits, i.e., so $b = \sum_{j=0}^{\ell} b_j 2^j$ where $b_0, \ldots, b_\ell \in \{0,1\}$.)

   (a) For $k = 1, \ldots, \ell+1$, let $b_k = \sum_{i=1}^{n} x_i (\mod 2^k)$, $c_k = \sum_{i=1}^{n/2} x_i (\mod 2^k)$, and $d_k = \sum_{i=n/2+1}^{n} x_i (\mod 2^k)$. Given c_k, d_k and b_{k-1} (in bits) give an NC^0 circuit (constant depth, binary-and, binary-or, circuit) to compute b_k.

   (b) Using the above (or otherwise) give a logarithmic depth circuit to compute b.

2. **Robustness of $\mathbf{NC}^1$:**
   Prove that a function $f : \{0,1\}^n \to \{0,1\}$ has a logarithmic depth circuit $\Leftrightarrow$ it has a log-depth formula $\Leftrightarrow$ it has a polynomial sized formula $\Leftrightarrow$ it has an $O(1)$-width polynomial sized branching program.

3. **Circuit-Size Hierarchy:**
   Let $f(n) = O(2^n/n)$ be a growing function. For every (sufficiently large) n prove that there is a function $g : \{0,1\}^n \to \{0,1\}$ that is computed by an $f(n)\log f(n)$-size circuit, but not by any $o(f(n))$-size circuit.

4. **Poly-size Circuits (Corrected):**

   - Prove that, unless $\mathrm{P} = \mathrm{NP}$, there exists a decision problem $L \in \mathrm{P}/_{\mathrm{poly}} - \mathrm{P}$ that is not NP-hard.
   - Prove that $\mathrm{TIME}(2^{O(n^{\log n})}) \not\subset \mathrm{P}/_{\mathrm{poly}}$.

5. **CNF, DNF, and Branching Programs:** Prove that if a function $g : \{0,1\}^n \to \{0,1\}$ can be expressed as a k-DNF formula and an ℓ-CNF formula, then it has a branching program of depth $f(k,\ell)$ (independent of n) for some function f.

6. **Majority (Revised):**
   For odd n, define $\mathrm{Maj}_n : \{0,1\}^n \to \{0,1\}$ to be the value taken by a majority of the input bits. Prove that for any constant d, Maj_n does not have a family of depth-d polynomial size circuits with three kinds of allowed gates: AND_∞, OR_∞ and PARITY_∞ (AND with unbounded fan-in, OR with unbounded fan-in and PARITY with unbounded fan-in, respectively). To begin with, try to prove that $\{\mathrm{Maj}_n\}_n \notin AC^0$.

   You may assume that "Parity-Mod-3" (Is the sum of n bits zero mod 3) is not solvable by constant depth poly-sized circuits with AND_∞, OR_∞ and PARITY_∞ gates.