Complexity Theory : Exercise 3

Submit until 8/6

May 25, 2009

Please write clear and precise answers. A 10 point bonus is given for printed solutions.

1. (Existence of functions that cannot be computed by small circuits)
   (a) Show that there are at most \( s^{3s} < 2^{s^2} \) circuits with fan-in 2 of size \( s \).
   (b) Conclude that for any \( n \) there are functions \( f : \{0, 1\}^n \rightarrow \{0, 1\} \) that cannot be computed by circuits of size \( 2^n / 10n \). (In fact most functions cannot be computed by such circuits.)

2. (Directed connectivity in NC)
   (a) Show that given two \( n \times n \) matrices \( A \) and \( B \) the product \( AB \) can be computed in \( NC \).
   (b) Show that given an \( n \times n \) matrix \( A \) the matrix \( A^n \) can be computed in \( NC \).
   (c) Conclude that \( dPATH \) (which is complete for \( NL \)) is in \( NC \). (Hint: Consider the matrix \( A^n \) for the adjacency matrix \( A \) of the given graph).

3. (Amplification of RP)
   note: This is an easy question and you may skip it and go directly to the next question instead.
   Show that \( RP_{1/2^{2n}} = RP_{1/3} = RP_{1/2-1/n} \)

4. (Amplification of BPP using the Chernoff bound) Show that \( BPP_{1/2^{2n}} = BPP_{1/3} = BPP_{1/2-1/n} \).
   You probably want to use the following theorem:

   **Theorem 1** (Additive version of Chernoff’s inequality). Let \( X_1, \ldots, X_n \) be independent random variables taking values in \( \{0, 1\} \). Let \( X = \sum X_i \), then for every \( 0 \leq \delta \leq 1 \)

   \[ \Pr[|X - E(X)| \geq \delta n] \leq 2e^{-\delta^2 n} \]

5. Show that \( ZPP = RP \cap coRP \).