Computational Complexity

Class Test

March 27, 2008

All problems carry equal weight. You can use results from the class without proving (but do explicitly state the result). Please write your name on each sheet of your solutions.

Problem 1: Show that **NP** is closed under complement if and only if it is closed under Turing reductions: i.e., $\mathbf{co\text{-}NP} \subseteq \mathbf{NP} \iff \mathbf{NP}^{\mathbf{NP}} \subseteq \mathbf{NP}$.

Problem 2: Define a *cautious probabilistic TM* as a Turing machine that makes randomized choices, and has three kinds of terminating states: *yes*, *no*, and *maybe*. We say that a language L is decided by a cautious PTM M in polynomial time if

- on any input x, M terminates within $p(|x|)$ steps, where p is a polynomial;
- on input $x \in L$, M terminates in a *yes* state with probability at least 1/2 and in a *no* state with probability 0,
- on input $x \notin L$, M terminates in a *no* with probability at least 1/2 and in a *yes* state with probability 0,

Show that a language L is decided by a cautious PTM in polynomial time if and only if $L \in \mathbf{ZPP}$.

Problem 3: It can be shown that in an *undirected graph*, if two nodes s and t are in the same connected component (i.e., there is a path between s and t) then a polynomially long random walk starting at s will hit t except with exponentially small probability. This gives a randomized algorithm to solve UPATH (the undirected version of the PATH problem) in logarithmic space. (In fact, now a deterministic logspace algorithm is also known for UPATH.)

Show, however, that in a *directed* graph, the random walk from a node s may take exponentially long to reach a node t. That is, construct an n node graph G, with two nodes s and t such that

- from *each node* in G there is a directed path to t;
- a random walk on G (which, at every node, chooses an outgoing edge uniformly at random) starting at s will hit t within $2^{n/2}$ steps with probability at most $2^{-n/2}$.

Prove that the G you construct indeed has these properties.

(Hint: Depending on the graph you construct, it may be easy or difficult to prove the bound. If it seems difficult, consider modifying the construction. It will also suffice if you show a similar bound: i.e., the probability of hitting t within $2^{\alpha n}$ steps is at most $2^{-\beta n}$ for some constants $\alpha, \beta > 0$.)

Problem 4: Two boolean functions on n bits, $f : \{0,1\}^n \to \{0,1\}$ and $g : \{0,1\}^n \to \{0,1\}$ are said to be ϵ-correlated if $|\Pr_{x \leftarrow \{0,1\}^n}[f(x) = g(x)] - \frac{1}{2}| = \epsilon/2$. (In particular, if f and g are identical or complements of each other, then they are 1-correlated. If they agree on half the points and disagree on the other half, then they are 0-correlated.) We say that f and g are *at least ϵ-correlated* if $|\Pr_{x \leftarrow \{0,1\}^n}[f(x) = g(x)] - \frac{1}{2}| \geq \epsilon/2$.

Show that the functions which are at least ϵ-correlated with a given function f (where $\epsilon > 0$ is a constant) form at most $2^{-\Omega(2^n)}$ fraction of all boolean functions on n bits.

(Hint: Consider a function as a 2^n-bit string. To count the fraction of functions at least ϵ-correlated to f, consider the probability $p(n, \epsilon)$ that a function chosen uniformly at random is at least ϵ-correlated to f. To bound this probability, you can use Chernoff's bound: when N fair coins are tossed, $\Pr[|\text{number of heads} - N/2| \geq \alpha N] \leq 2^{-c\alpha^2 N}$ for some positive constant c. Explain how you can relate the probability in Chernoff's bound to $p(n, \epsilon)$.)

Problem 5: A boolean function $f : \{0,1\}^n \to \{0,1\}$ is said to be *ϵ-predicted by a circuit C* if the function $f_C : \{0,1\}^n \to \{0,1\}$ computed by C is at least ϵ-correlated with f.

Show that for any constant $\epsilon > 0$, for sufficiently large values of n, there exists a function $f : \{0,1\}^n \to \{0,1\}$ such that f is not ϵ-predicted by any circuit of size[1] less than $T = c2^n/n$ for some constant c.

(Hint: Use Problem 4, and a bound on the number of circuits of size T, to derive a bound on the fraction of functions that are ϵ-predicted by such circuits.)

[1] Here the size of the circuit is defined as the number of gates in the circuit; you may assume that the circuit has only fan-in 2 NAND gates.