Advanced Complexity Theory — Madhu Sudan
6.841/18.405J
Due: Wednesday, April 3, 2002

Problem Set 3

Problems

1. An $n \times n$ matrix $A = \{a_{i,j}\}$ is a *Toeplitz* matrix if $a_{i+1,j+1} = a_{i,j}$ for every $1 \le i < n$ and $1 \le j < n$. In this question all arithmetic will modulo 2, i.e., in the field $\mathbb{F}_2$.

   For a Toeplitz matrix $A \in \mathbb{F}_2^{n \times n}$, and a vector $b \in \mathbb{F}_2^n$, let $h_{A,b} : \{0,1\}^n \to \{0,1\}^n$ be the function $h_{A,b}(x) = Ax + b$. Let H be the collection of functions $\{h_{A,b} | A \in \mathbb{F}_2^{n \times n}, b \in \mathbb{F}_2^n\}$.

   Prove that H is a nice, pairwise independent family of hash functions.

2. The birthday "paradox" says that if $a_1, \ldots, a_m$ are independent random numbers from the set $\{1, \ldots, N\}$ and $m = \omega(\sqrt{N})$ then, with probability almost one, there exist $i \neq j \in \{1, \ldots, m\}$ such that $a_i = a_j$.

   Derive upper and lower bounds on the probability of this event, as a function of m and n, if $a_1, \ldots, a_m$ are pairwise independent random variables (distributed uniformly from $\{1, \ldots, n\}$.

3. A function $f : \{0,1\}^* \to \mathbb{Z}^{\geq 0}$ is α-approximated by a function $g : \{0,1\}^* \to \mathbb{Z}^{\geq 0}$ if for every $x \in \{0,1\}^*$, $f(x) \le g(x) \le \alpha f(x)$. The α-approximation problem for a function f is that of computing any function g that α-approximates f.

   (a) Define a promise problem that is equivalent to the 2-approximation problem for #SAT (where #SAT maps a 3CNF formula ϕ to the number of satisfying assignments that ϕ has). Include a proof of the equivalence.

   (b) Show that the 2-approximation problem for #SAT is equivalent to the 4-approximation problem.

4. Recall the definition of the permanent of a matrix. Let $S_n = \{\pi : [n] \to [n]$ s.t. π is a permutation$\}$. Then for an $n \times n$ matrix $M = \{m_{ij}\}$ $\text{perm}(M) = \sum_{\pi \in S_n} \prod_{i=1}^{n} m_{i\pi(i)}$.

   Give a polynomial time algorithm to compute the permanent, modulo two, of an $n \times n$ integer matrix.

5. Show that it is #P-complete to compute the number of cycles in a directed graph. You may assume it is #P-complete to compute the number of Hamiltonian cycles in a directed graph.

Instructions:

- Usual rules on collaboration and references.
- Turn in the solutions to the above problems by 11am on Wednesday, April 3, 2002.