Complexity Theory

Homework Set No. 7

Date Due: Dec 30th 2004

Please turn in the homework on time. Preferably - printed.

1. For two $k \times n$ matrices G_1 and G_2 over finite field $\mathcal{F}$ we way that they are equivalent if there exist (i) a $k \times k$ matrix S which is non singular over $\mathcal{F}$ and (ii) An $n \times n$ permutation matrix P Such that $G_1 = S \cdot G2 \cdot P$. This means that if we think of the codewords generated by G_1 and G_2 (i.e. all vector $y = xG_i$), then there is a $1-1$ mapping between them after reordering the bit positions.

Show that the non-equivalent of matrices problem is in IP with constant number of rounds.

2. Recall the method for showing $MA[2] \subseteq AM[2]$. Use it to show that $AM[k] = AM[2]$ and specifically describe what happens to the time analysis as a function of k.

3. For a circuit C with n inputs and m outputs we call the distribution on $\{0,1\}^m$of $C(x)$ when $x \in_R \{0,1\}^n$ the *distribution generated by* C. Given two circuits C_1 and C_2 we would like to check whether these two distributions are close or far from each other.

Consider the *variation distance* (or statistical difference) between distribution D_1 and D_2 on universe U defined as

$$V(D_1, D_2) = max_{S \subseteq U} |\Pr_{D_1}[x \in S] - \Pr_{D_2}[x \in S]|.$$

It is known that

$$V(D_1, D_2) = \frac{1}{2} \sum_{x \in U} |\Pr_{D_1}[x] - \Pr_{D_2}[x]|$$

, i.e. the L_1 distance between the distributions.

We are interested in separating the cases where $V(D_1, D_2) \leq \alpha$ and $V(D_1, D_2) \geq \beta$ when D_1 and D_2 are the distributions generated by C_1 and C_2. Call this problem $VD(\alpha, \beta)$.

(a) Show that if the Graph Non-Isomorphism problem is not in BPP then there is no probabilistic polynomial time algorithm that distinguishes these two cases for all pairs of circuits C_1 and C_2 when $\alpha = 0$ and $\beta = 1$

(b) Show an AM protocol for distinguishing the case where $\alpha = 0$ and $\beta = 1$ (i.e. $VD(0, 1)$).

(c) Let $S_1 = \{x | \Pr_{D_1}[x] > \Pr_{D_2}[x]\}$ and $S_2 = \{x | \Pr_{D_2}[x] > \Pr_{D_1}[x]\}$. Show:

$$V(D_1, D_2) = \sum_{x \in U} (\Pr_{D_1}[x \in S_1] - \Pr_{D_2}[x \in S_1]) = \sum_{x \in U} (\Pr_{D_2}[x \in S_2] - \Pr_{D_1}[x \in S_2]).$$

(d) Show an AM protocol for distinguishing the general case, i.e. $VD(\alpha, \beta)$. What is the complexity of the protocol as a function of $\beta - \alpha$?