E0 224 : Computational Complexity Theory
Assignment 3

Due Date : 1 December 2016 **TOTAL MARKS : 85**

1. Prove that any language L that has a PCP verifier using r coins and q adaptive queries, has a PCP verifier using r coins and 2^q non-adaptive queries. **[5 marks]**

2. Prove that there exists an deterministic polytime algorithm which when given a $3CNF$ formula with exactly 3 variables per clause outputs an assignment that satisfies at least 7/8 of the clauses. **[7 marks]**

3. Let G be an undirected graph. Associate with each edge (v_i, v_j) an indeterminate x_{ij} if $i < j$. Define the Tutte matrix A with entries $A_{ij} = x_{ij}$ and $A_{ji} = -x_{ij}$ if (v_i, v_j) is an edge with $i < j$ and all other entries are zero.

   (a) Prove that $det(A) \neq 0$ if and only if G has a perfect matching. **[6 marks]**

   (b) Use the above result, to provide a randomized algorithm to check if a graph has a perfect matching. **[2 marks]**

   (c) Prove that the rank of the Tutte matrix is twice the size of the maximum matching. **[7 marks]**

4. Consider a PCP system with proof length $poly(n)$, where the verifier flips $O(\log(n))$ coins but looks at just one bit of the proof. Prove that for any soundness s and completeness c with $0 < s < c < 1$, the set of languages with such a proof system is in P. **[6 marks]**

5. Let Q be a probability mass function on $\{0,1\}^n$ with $H_\infty(Q) = b$, where $H_\infty(Q) = -\log(\max_x Q(x))$. Let $G : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^l$ be a family of pairwise independent hash functions. Let x be chosen according to Q and s be chosen uniformly, then prove that the distribution of $F(x,s) = (s, G(s,x))$ is $2^{-(b-l)/2}$ close to uniform i.e. $\frac{1}{2}\Sigma_{y\in\{0,1\}^{k+l}} \left|\Pr[F(s,x) = y] - 2^{-(l+k)}\right| \leq 2^{-(b-l)/2}$.

   Hint: Consider the collision probability of P in relation to $||P||_2$, where $||P||_2 = \left(\sum P(x)^2\right)^{1/2}$ **[8 marks]**

6. Let $r(n) = o(\log(n))$, where n denotes the size of the input.

   (a) If $\texttt{SAT} \in \mathsf{PCP}(r(n), 1)$, then $\mathsf{P} = \mathsf{NP}$. **[7 marks]**

   (b) $\mathsf{NP} \subseteq \mathsf{PCP}(r(n), r(n))$, then $\mathsf{P} = \mathsf{NP}$. **[9 marks, BONUS]**

7. (a) Prove that finding the nth order partial derivatives of a polynomial is #P-Hard, where the input polynomial is given in the form $\prod_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_j$. Specifically, consider **[5 marks]**

$$\frac{\partial^n}{\partial x_1 \ldots \partial x_n}\left[\prod_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_j\right]$$

   where a_{ij} are integers.

   (b) Prove that #2-SAT is #P-complete. **[8 marks]**

8. (a) Define $\oplus\texttt{PERM} = \{A | A$ is an $m \times m$ integer matrix and $perm(A)$ is odd.$\}$ Prove that $\oplus\texttt{PERM}$ is in P. **[5 marks]**

   (b) Prove that for any $n \times n$ matrix A, **[6 marks]**

$$perm(A) = \sum_{S\subseteq[n]} (-1)^{n-|S|} \prod_{i=1}^{n}\sum_{j\in S} A_{ij}$$

   Use this to provide an algorithm to compute the permanent in time $2^n poly(n)$.

9. If $\mathsf{P} = \mathsf{NP}$, prove that for all $f \in \#\mathsf{P}$ there exists a deterministic polytime algorithm that approximates f to within a factor of $1 + \epsilon$ for each $\epsilon > 0$.

[8 marks]

10. Prove that the class PP is closed under complementation and unions. **[5 marks]**

Practice Problems

1. Prove that for each $\mathtt{L} \in \mathsf{AC}^0$, there is a depth three circuit of size $n^{poly(\log(n))}$ decides the language on $1 - 1/poly(n)$ inputs and has the following structure : It has a $\oplus$ gate on top and the other gates are $\wedge$ and $\vee$ and have fan in $poly(\log(n))$.

2. Let H_n be the hypercube $\{0,1\}^n$. Prove that every subset of size 2^{n-1} has at least 2^{n-1} edges leaving from it. Also, prove that if a subset S of size 2^{n-1} has exactly 2^{n-1} edges leaving from it, then there is an i and a $\beta \in \{0,1\}$ such that $S = \{x | x_i = \beta\}$.