Endsem : CC2019

25 April 2019

Instruction

Answer as much as you can. Maximum you can score is 100. All questions carry equal marks.

1 Problems

1. Let s be any polynomial function from $\mathbb{N} \to \mathbb{N}$. Show that there exists a boolean function $f : \{0,1\}^n \to \{0,1\}$ that does not have circuits of size $s(n)$.

2. Let ZTIME($T(n)$) contains all the languages for which there exists a probabilistic Turing Machine which runs in expected-time $O(T(n))$ such that for every input x, whenever the machine halts it answers correctly whether $x \in L$ or not. Define $ZPP = \cup_c ZTIME(n^c)$. Prove that $ZPP \subseteq RP$.

3. Discuss the construction of a pairwise independent hash family from $\{0,1\}^n$ to $\{0,1\}^k$.

4. Describe the notion of Hadamard encoding g of a vector v over $\{0,1\}^n$. How do you locally check if g is the Hadamard encoding for $u \otimes u$ for some vector u.

5. Can you identify and discuss why the Razborov-Smolensky method does not work when the circuit has MOD_m gates where m is composite.