End Semester Examination, Autumn 2003-04

Total points: 50 | April 25, 2004 | Total time: 3 hours

[*Solve four NP-easy, four NP-complete and the NP-hard problems. Each problem carries six points.*]

NP-Easy problems

1. Prove that the language $\{0^m 1^k \mid m \text{ has a divisor } d \text{ with } 2 \leqslant d \leqslant k\}$ is in P.

2. Show that each NC^j is closed under complementation.

3. Let $f : \Sigma^* \to \Sigma^*$ be a function with the property that $f(f(\alpha)) = f(\alpha)$ for every $\alpha \in \Sigma^*$. Argue that f is *not* a one-way function.

4. Suppose that $\mathrm{NP} \neq \mathrm{coNP}$. Show that there exist languages A and B such that A is not poly-time reducible to B and B is not poly-time reducible to A.

5. Design an NC^2 circuit to compute the product of two n-bit unsigned integers given in binary representation.

NP-Complete problems

(View the hints as certificates)

6. Prove that $\mathrm{TIME}(n) \neq \mathrm{NL}$. (**Hint:** Suppose that $\mathrm{TIME}(n) = \mathrm{NL}$. Then use padding (cf. Exercise 2.3.4) to show that $\mathrm{TIME}(n^2) \subseteq \mathrm{NL}$.)

7. Show that PP is closed under symmetric difference, i.e., if the languages L_1 and L_2 (over the same alphabet) are in PP, then so also is the language $L_1 \triangle L_2 := (L_1 \setminus L_2) \cup (L_2 \setminus L_1) = (L_1 \cup L_2) \setminus (L_1 \cap L_2)$.

8. Show that the language

$$\text{THRESHOLD-SAT} := \{\langle \phi, k \rangle \mid \phi \text{ is a Boolean formula with more than } k \text{ satisfying assignments}\}$$

is PP-complete. (**Hint:** Assume that MAJSAT is PP-complete. To prove THRESHOLD-SAT $\in$ PP, first make a coin toss. If the outcome is 'Head', evaluate ϕ, otherwise forget ϕ and make some more coin tosses.)

9. A NAND gate takes two input bits (call them x and y) and outputs the bit $x \mathbin{\overline{\wedge}} y := \overline{x \wedge y} = \overline{x} \vee \overline{y}$. Let us call a Boolean circuit consisting only of NAND gates a NAND circuit. Show that the language

$$\text{NAND-CIRCUIT-VALUE} := \{\langle C, \alpha \rangle \mid C \text{ is a NAND circuit and } C(\alpha) = 1\}$$

is P-complete. (**Hint:** Assume that CIRCUIT-VALUE is P-complete.)

10. Show that if there exists a *bijective* one-way function, then $\mathrm{NP} \cap \mathrm{coNP} \neq \mathrm{P}$. (**Hint:** For a one-way function f look at the language L_f discussed in the proof of the theorem relating the existence of one-way functions with the hypothesis that $\mathrm{P} \neq \mathrm{UP}$.)

NP-Hard problem

11. Write a short feedback about this course. Your essay may not exceed 200 words. Please avoid being unduly praising or abusing, but comment on the relevance, coverage and effectiveness of the course and its teaching.

Dr. Abhijit Das, Dept. of Computer Science & Engg, Indian Institute of Technology, Kharagpur 721 302