Computer Science 345
The Efficient Universe

Homework 6
Due Wednesday, April 12, 2006

You may collaborate with other students, but you should write up the solutions entirely on your own.

1 Complexity

Problem 1 Prove or disprove the following statements:

1. If $A, B \in \mathcal{NP}$, then $A \cap B \in \mathcal{NP}$ and $A \cup B \in \mathcal{NP}$.
2. If A and B are two $\mathcal{NP}$-complete languages, then $A \cap B$ is $\mathcal{NP}$-complete.
3. If A and B are two $\mathcal{NP}$-complete languages, then $A \cup B$ is $\mathcal{NP}$-complete.

Definition 1 (Circuit Minimization Problem) *Given a circuit C determine if there exists a smaller circuit that computes the same function as C.*

Problem 2 Prove that if the *SAT* problem is in $\mathcal{P}$, then the *Circuit Minimization Problem* is solvable in polynomial time. On the other hand, try to argue intuitively why *Circuit Minimization Problem* does not seem to be in $\mathcal{NP}$ or *co*$\mathcal{NP}$.

Problem 3 First we will describe the one-time pad cipher. Alice and Bob pick a random binary string K (*the key*) of length n in advance. When Alice wants to send a message M to Bob, she computes $C = M \oplus K$, where $\oplus$ denotes the XOR of two binary strings (i.e. $C_i = M_i + K_i \mod 2$) and sends C to Bob. Bob receives C and recovers M by computing $K \oplus M$. Alice and Bob use the key K only once.

Come up with a definition of a secure cipher and prove that one-time pad is secure. In other wards, imagine that an adversary Carl is listening on the channel between Alice and Bob, and reads the message C. In what sense doesn't Carl learn anything about the message M? Try to define it, and prove that it holds in this setting.

Problem 4 In this problem we define a secret sharing scheme (this scheme is due to Shamir). Alice, the owner of a bank, needs to share a secret message (e.g. the secret combination for a safe) m between N managers $B_1, \ldots, B_N$. However she does not trust the managers. So she wants to ensure that any d managers together can decipher the message m, but even $d-1$ managers cannot gain any information about the message.

Consider the following scheme.

- Alice picks a prime number p, which is greater than m and N. The number p is publicized and is known to everybody. You can also think that this number is chosen in advance.
- Alice picks $d-1$ random uniform numbers $a_1, \dots, a_{d-1}$ in $\mathbb{Z}_p$.
- Define the polynomial $f(x)$ over the field $\mathbb{Z}_p$:

$$f(x) = a_{d-1}x^{d-1} + \cdots + a_2x^2 + a_1x + m.$$

- For each $i = 1, \dots, N$, Alice sends $f(i)$ to the manager B_i.

1. Describe how any d managers together can decipher the message.
2. Prove, that fewer than d managers cannot gain any information about the secret message (use the definition from the previous problem).

2 Finite Automata

In class we discussed randomized and non-randomized finite automata. We constructed a randomized finite automaton that recognizes the language $L = \{a^n b^n : n \in \mathbb{N}\}$; and proved that no non-randomized finite automaton can recognize this language (i.e. L is not a regular language). In the next exercise you need to prove the same properties for another language.

Remark: If you forget the definition of a finite automaton, you can think of it as of a Turing Machine with a read-only tape.

Problem 5 Consider the language $L = \{a^n b^n c^n : n \in \mathbb{N}\}$ in the alphabet $\Sigma = \{a, b, c\}$.

1. Prove that L cannot be recognized by a finite (non-randomized) automaton.
2. Construct a randomized finite automaton that recognizes L.