Problem Set 6

Due by 5:30 pm on Friday, April 15, 2005.

Problems 18 and 19 refer to the **zero knowledge interactive proof of three-colorability** described below.

Let G be an undirected graph. A *3-coloring* of G is a mapping χ from the vertices of G to the set of "colors" $\{1, 2, 3\}$ such that for all edges $\{u, v\}$ in G, $\chi(u) \neq \chi(v)$. In words, χ describes a coloring of the vertices using three colors such that the two ends of every edge are colored differently. There is no known polynomial-time algorithm for determining if a given graph G is 3-colorable or for finding a 3-coloring if one exists.

Consider the following protocol. Alice has a 3-colorable graph G for which she knows a 3-coloring χ. She wants to convince Bob that she knows a 3-coloring of G without revealing what the 3-coloring is. They proceed as follows:

(a) Alice chooses a random permutation $\pi\colon \{1, 2, 3\} \to \{1, 2, 3\}$ and constructs a new 3-coloring $\chi'(v) = \pi(\chi(v))$. For each vertex v in G, she commits to the color $\chi'(v)$ by using a bit-commitment protocol. She sends the commitments for all vertices to Bob.

(b) Bob choose an edge $\{u, v\}$ of G at random and sends it to Alice.

(c) Alice reveals the colors $\chi'(u)$ and $\chi'(v)$ to Bob using the reveal protocol.

(d) Bob checks that $\chi'(u)$ and $\chi'(v)$ were revealed correctly and that $\chi'(u) \neq \chi'(v)$. He accepts if all checks are okay.

As usual, this protocol is iterated many times.

Problem 18: (Probability that Cheating Alice Escapes Detection)

Suppose Alice is dishonest and does not really know a 3-coloring of G. (This means that however she tries to color the graph, she always ends up with at least one edge for which both ends are colored the same.) Assume G has n vertices and e edges. What is the maximum probability by which Alice can make Bob accept in a single iteration of the protocol? Explain how you derive this number?

Problem 19: (Effects of Non-Randomness in Alice's Protocol)

Suppose now Alice is honest, but her random number generator is faulty so that the six permutations $\pi\colon \{1, 2, 3\} \to \{1, 2, 3\}$ are not equally likely. For definiteness, suppose that the identity permutation gets chosen half the time and the other five permutations each get chosen with probability $1/10$. Explain how a dishonest Bob can discover χ with high probability after sufficiently many iterations of the protocol.

Problem 20: (Secret-Sharing)

Consider a $(3, 10)$ Shamir secret-sharing scheme over $\mathbf{Z}_p$ for some large prime p. That is, a secret $s \in \mathbf{Z}_p$ is split into 10 shares, any three of which allow for its recovery, but no pair of shares gives any information about s. Suppose an adversary corrupts one of the 10 shares, but nobody knows which share is bad.

(a) Describe a method to recover s given all 10 shares and explain why it works.

(b) Let τ' be the smallest number such that τ' shares are always sufficient to recover s. How big is τ'? Explain.

(c) Is it the case that any collection of fewer than τ' shares gives no information about s? Why or why not?