Zheng Ma *Apr 23, 2005*

Solutions to Problem Set 6

Problem 18 counts 5 points, Problem 19 counts 10, Problem 20 counts 15.
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 π: $\{1, 2, 3\} \rightarrow \{1, 2, 3\}$ 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?

Solution: The maximum probability depends on how close to a 3-coloring the cheating Alice can obtain. If she can produce a coloring in which only k edges have both ends colored the same, then Bob's chance of choosing one of those bad edges is k/e. Bob accepts if he fails to choose a bad edge to examine; hence, the probability with which he accepts in a single iteration is $1 - k/e$. This probability is maximized when k is minimized, so the answer is $1 - k_0/e$, where k_0 is the smallest number of miscolored edges in any coloring that the cheating Alice can produce.

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.

Solution: We consider the graph without isolated nodes, otherwise, the isolated nodes can be colored arbitrarily. Bob won't have any way to discover that. For the graph without any isolated nodes, Bob can ask Alice to reveal the coloring of the nodes of the same edge $\{u, v\}$ many times. He then guess $\chi(u), \chi(v)$ as the most frequent color of u and v. He can then do the same process on other edges until he recover the coloring of the graph.

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.

Solution: We split the 10 shares into 4 groups containing 3,3,3,1 shares, respectively. Then we use the first three groups to recover the secret. The results are s_1, s_2, s_3. At least two results will be the same since any group with three correct shares will recover the correct secret, and there is at most one bad share. Hence, this common result is the secret s.

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

Solution: τ' is 5.

First, we show that 4 shares are not enough. To show this, we construct three good shares and one bad share such that every subset of three shares recovers a different secret, only one of which is correct. Start with four good shares and change the fourth to something different. Then it no longer lies on the polynomial determined by the first three shares. Suppose two different size-3 subsets X and X' nevertheless recover the same secret s' (not necessarily correct). Let $p(x)$ and $p'(x)$ be the polynomials that they interpolate. p and p' have degree at most 2. Since $|X \cap X'| = 2$, then $p(x)$ and $p'(x)$ agree on the two points in the intersection. They also agree on 0, since $p(0) = s' = p'(0)$. Hence, p and p' agree on three points, so they are identical polynomials. But then they must agree on all four points, contradicting the construction of the bad share. Hence, every subset of three shares gives a different secret, any one of which could be the correct secret.

If we have 5 shares, we search for any subset of four shares that interpolate a polynomial of degree at most 2. This polynomial is the correct polynomial, and the secret is its constant coefficient. The subset consisting of the four good shares has this property, so such a subset exists. If two different size-4 subsets X and X' interpolate polynomials p and p', respectively, each having degree at most 2, then p and p' are identical and determine the same secret. This is because $|X \cap X'| = 3$, so the common intersection uniquely determines p and p'.

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

Solution: No. Any two shares will give no information about the secret. However, if we have 4 shares, we do get the information that the secret is among 1 out of the 4 possibilities of reconstruction. With probability of at least 25%, we can guess the secret.