CS 70 SPRING 2008 — DISCUSSION #6

LUQMAN HODGKINSON, AARON KLEINMAN, MIN XU

1. Polynomials and Interpolation

Exercise 1. Find (and prove) an upper-bound on the number of times two degree d polynomials can intersect. What if the polynomials' degrees differ?

Exercise 2. Use the Lagrange interpolation method to determine the polynomial of degree at most 2 that fits the points $(-1, 2), (0, 1), (1, 2)$. What is the (exact) degree of this polynomial?

2. Secret Sharing

Professor Wagner and the three GSIs of CS70 want to password-protect the software that lets them alter student midterm grades. To prevent malicious tinkering, they don't want to allow anyone to access the system alone. Instead, they would like it so that the system can be entered only with the consent of either (1) Professor Wagner and any one GSI, or (2) all three GSIs together. Suppose the password is some message m, and let p be a prime.

Exercise 3. Professor Wagner asks you to help implement the following scheme: generate two numbers s_1 and s_2 at random and choose s_3 such that $s_1 + s_2 + s_3 \equiv m \pmod{p}$. Let $t_1 = s_2 + s_3, t_2 = s_1 + s_3$, and $t_3 = s_1 + s_2$. Give s_1 to Aaron, s_2 to Luqman and s_3 to Min, and give t_1, t_2 and t_3 to Professor Wagner. If the three GSIs want to compute the password, they can pool their information to compute $s_1 + s_2 + s_3 \equiv m \pmod{p}$. If a GSI and Professor Wagner want to comptue the password, they can compute $s_i + t_i \equiv m \pmod{p}$.

Is this a valid solution? Why or why not?

Exercise 4. Modify the above scheme to make it more secure.

Date: March 12, 2008.

The authors gratefully acknowledge the TA's of CS70 Past for the use of their previous notes: Chris Crutchfield, Alex Fabrikant, David Garmire, Assane Gueye, Amir Kamil, Lorenzo Orecchia, Vahab Pournaghshband, Ben Rubinstein. Their notes form the basis for this handout.