CS 70 FALL 2007 — DISCUSSION #5

ASSANE GUEYE, LUQMAN HODGKINSON, AND VAHAB POURNAGHSHBAND

1. Administrivia

(1) Course Information
- The homework box will be emptied on Monday, 10/15. We will bring all the uncollected homeworks to the final review session and the final exam session.

(2) Discussion Information
- The first midterm is graded and will be distributed in section.

2. Polynomials on the Reals

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?

3. Polynomial Interpolation on the Reals and Finite Fields

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?

Exercise 3. Use the Lagrange interpolation method to determine the polynomial of degree at most 2 that fits the points $(-1, 2), (0, 1), (1, 2)$ in $GF(3)$.

4. Secret Sharing

Exercise 4. Suppose (!) you're a CS70 student, and your GSI has distributed a secret s to 10 students including yourself and your neighbor. The GSI picked a polynomial $P(x)$ of degree 2 (and so s/he hopes that no fewer than $k = 3$ students could reconstruct s) modular $q = 11$. Suppose the two of you are told that $P(6) = 7 \mod 11$ and that $P(7) = 5 \mod 11$. What can you say about s?

Exercise 5. What if you make friends with another student who tells you that $P(8) = 7 \mod 11$? If possible, determine s.

Date: October 9, 2007.

5. Error Correcting Codes - Erasure Errors or Known Error Positions

In lecture, we learned an error-correcting scheme that allows us to correct k errors by adding k more characters to the transmitted message. This ability is quite useful in communications where we know we lost characters (such as noise or random disconnections on a line where it is very clear what noise is, etc...).

Let us review how this process works. Reconstruct the following statements in the alphabet $A = 0$, $I = 1$, $N = 2$, $S = 3$, and $T = 4$, knowing that the message size is 3 (the number of acceptable erasures is 1). Note that you are solving for a quadratic polynomial modulo 5.

Exercise 6. Figure out the dropped letter in S_II.

6. Error Correcting Codes - General Errors or Unknown Error Positions

Exercise 7. Suppose you received 42045 through a noisy channel that changes a packet in every five packets. What's the length of the initial message? Figure out the initial message, knowing that you are working on GF(7).