CS 70 FALL 2006 — DISCUSSION #6

D. GARMIRE, L. ORECCHIA & B. RUBINSTEIN

1. Administrivia

(1) Course Information
- The midterm is over. Celebrate!
- But don't forget the sixth homework is due October 6^{th} at 4pm in 283 Soda Hall.

2. Error Correcting Codes - 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.

(1) S_II
(2) _TIS
(3) SI_I

Concatenate the 3 character words together. Do you see the message?

Exercise 1. Think about the relationship between this kind of error-correcting scheme and secret sharing.

3. Error Correcting Codes - Unknown Error Positions

In modern day communications, most data is transmitted in the digital domain. This change makes it hard to determine what is noise or an omission in the data, so the error correcting scheme must be improved. Specifically, the error correcting scheme must tell you where the errors occured and allow you to decode the original message. In fact, CDs and other storage devices contain a large amount of redundant data.

The main idea is to add k more characters to the message such that message may be decoded. To follow this procedure, we add another polynomial $E(i) = (x - e_1) * (x - e_2)...(x - e_k)$ whose zeros are at the positions of the errors and then solve $Q(x) = P(x) * E(x)$. Note that E will have k coefficients as well, and that is why we need to extend the size of the message sent to be $n + 2k$ characters long.

Date: October 4, 2006.

The authors gratefully acknowledge Chris Crutchfield and Amir Kamil for the use of their previous notes, which form part of the basis for this handout.

Exercise 2. Try using the examples above and add 1 character to them and then have your partner introduce a random error. See if you can find out where the error was located and what the original message contained.