EECS 70 Discrete Mathematics and Probability Theory
Fall 2014 Anant Sahai

Discussion 8M-S

1. Decoding with General Errors

Suppose Alice wants to send Bob a message of $n = 3$ packets and she wants to guard against $k = 1$ corrupted packets. Further assume that packets can be coded up as integers between 0 and 6.

a) Alice can work over $GF(q)$. What is the minimum prime q can be?

b) Suppose Alice wants to send Bob the message $m = (m_1, m_2, m_3)$. What is the maximum degree of the unique polynomial described by these points, which are of the form (i, m_i)?

c) What is the minimum number of extra points Alice must send to Bob so that he can correctly reconstruct her message m?

d) Bob receives a message $r = (3,3,3,2,0)$. In order to check whether there the message is corrupted, Bob needs to solve $Q(x) = r_i E(x)$, where $Q(x) = P(x)E(x)$, $P(x)$ is the original polynomial for sending the message, and $E(x)$ is the error-locator polynomial in the Berlekamp-Welch algorithm.

- What is the degree of $Q(x)$?
- What is the degree of $E(x)$?
- What does $E(x)$ look like?

By letting $x = i, 1 < i < 5$ in $Q(x) = r_i E(x)$, we obtain the following system of linear equations:

$$a_3 + a_2 + a_1 + a_0 = 3 + 3b_0 \quad (1)$$
$$a_3 + 4a_2 + 2a_1 + a_0 = 6 + 3b_0 \quad (2)$$
$$6a_3 + 2a_2 + 3a_1 + a_0 = 2 + 3b_0 \quad (3)$$
$$a_3 + 2a_2 + 4a_1 + a_0 = 1 + 2b_0 \quad (4)$$
$$6a_3 + 4a_2 + 5a_1 + a_0 = 0 \quad (5)$$

What are the coefficients?

e) What is the original polynomial $P(x) = ax^2 + bx + c$?

f) Which packet is corrupted?

g) What is the orignal value?