EECS 70 Discrete Mathematics and Probability Theory
Fall 2014 Anant Sahai

Discussion 7W-S

1. Decoding with Erasure Errors

Suppose Alice wants to send Bob a message of $n = 5$ packets and she wants to guard against $k = 1$ lost 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 $m = (2,3,5,1,6)$, where e.g., $m_2 = 3$. What is the maximum degree of the unique polynomial described by these points, which are of the form (i, m_i)?

(c) What are the coefficients of the polynomial $P(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4$ described by these 5 points, $(i, m_i)\ \forall\ i \in \{1,\ldots,5\}$?

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

(e) Suppose Alice evaluates $P(x)$ at the extra point $i = 6$. What is the polynomial evaluated at this new point?

(f) Alice sends her final message: $c_1 = 2$, $c_2 = 3$, $c_3 = 5$, $c_4 = 1$, $c_5 = 6$, $c_6 = 6$. But, the second packet is dropped, so Bob only receives: $c_1 = 2$, $c_3 = 5$, $c_4 = 1$, $c_5 = 6$, $c_6 = 1$. Recover m_2.

(g) Could Bob have still correctly decoded Alice's message if both c_2 and c_6 were dropped?