EECS 70 Discrete Mathematics and Probability Theory
Fall 2014 Anant Sahai **Discussion 7M-S**

1. Lagrange Interpolation

In this question we will find $p(x)$ using the Lagrange interpolation method. Recall from last discussion that we are given the three points $\{(-1,2),(1,-2),(2,5)\}$ we wish to find the unique polynomial $p(x) = a_2x^2 + a_1x + a_0$ such that $p(x_i) = y_i$.

(a) Find $p_{-1}(x)$ where $p_{-1}(1) = p_{-1}(2) = 0$ and $p_{-1}(-1) = 1$.

(b) Find $p_1(x)$ where $p_1(-1) = p_1(2) = 0$ and $p_1(1) = 1$.

(c) Find $p_2(x)$ where $p_2(-1) = p_2(1) = 0$ and $p_2(2) = 1$.

(d) Find $q_{-1}(x)$ where $q_{-1}(1) = q_{-1}(2) = 0$ and $q_{-1}(-1) = 2$.

(e) Find $q_1(x)$ where $q_1(-1) = q_1(2) = 0$ and $q_1(1) = -2$.

(f) Find $q_2(x)$ where $q_2(-1) = q_2(1) = 0$ and $q_2(2) = 5$.

(g) Why does $q_{-1}(x) + q_1(x) + q_2(x)$ pass through $(-1,2)$, $(1,-2)$ and $(2,5)$?

2. Secret Sharing

Suppose you are in charge of setting up a secret sharing scheme where you want to distribute $n = 5$ shares to 5 officials such that any $k = 3$ or more people can figure out the secret, but two or fewer cannot. Suppose we are working over $GF(7)$.

(a) How many values can the secret take on?

(b) What is the degree of the polynomial you will use to distribute the shares, and why?

(c) You randomly choose the polynomial: $P(x) = 5x^2 + 3x + 3$. What is the secret?
$P(0) =$

(d) What is the share given to the first official?
$P(1) =$

(e) What is the share given to the second official?
$P(2) =$

(f) What is the share given to the third official?
$P(3) =$

(g) What is the share given to the fourth official?

$P(4) =$

(h) What is the share given to the fifth official?
$P(5) =$

(i) Suppose officials 1, 2, and 5 get together, and try to recover the secret. Using Lagrange interpolation, compute their delta functions $\Delta_1(x), \Delta_2(x), \Delta_5(x)$.

(j) Compute their final polynomial.

(k) Could officials 1 and 2 recover the secret with official 4 instead of collaborating with official 5? Why or why not?

(l) Could officials 1 and 2 recover the secret by only collaborating with each other? Why or why not?