$Q(x) = P(x)E(x)$

CS 70 Disc 3D: tinyurl.com/frank-discussion 7/9/2020

1 (a) Construct $P(x)$ mod 5 of degree ≤ 2 such that $P(0)=1$, $P(1)=1$, $P(2)=4$

$2(3) \equiv 1 \pmod 5$

$$\Delta_0(x) = \frac{(x-1)(x-2)}{(0-1)(0-2)} = \frac{x^2-3x+2}{+2} = 3(x^2-3x+2)$$

$4(-1) \equiv 1 \pmod 5$

$$\Delta_1(x) = \frac{x(x-2)}{1(1-2)} = \frac{x^2-2x}{-1} = 4(x^2-2x)$$

$$\Delta_2(x) = \frac{x(x-1)}{2(2-1)} = \frac{x^2-x}{2} = 3(x^2+x)$$

$$P(x) = 1(\Delta_0(x)) + 1(\Delta_1(x)) + 4(\Delta_2(x))$$

$$= 4x^2 + x + 1 \pmod 5$$

$P(3) = 0 \quad P(4) = 4$

(b) Suppose $c_0 = 0$, set up system of linear equations to find $Q(x)$ and $E(x)$

$Q(x) = P(x)E(x) = r_x E(x)$

$P(x)$: message polynomial; $E(x)$: error-locator polynomial; r_x: received value @ every x coordinate

$E(x) = x - b_0$?

$Q(x) = a_3x^3 + a_2x^2 + a_1x + a_0$

$\forall x \; 0 \leq x \leq 4$:

$$\begin{cases} a_3(0) + a_2(0) + a_1(0) + a_0 = 0 \cdot (0 - b_0) \\ \quad Q(0) \qquad\qquad = r_0 \cdot E(0) \\ a_3 + a_2 + a_1 + a_0 = 1 \cdot (1 - b_0) \\ 8a_3 + 4a_2 + 2a_1 + a_0 = 4(2 - b_0) \\ 27a_3 + 9a_2 + 3a_1 + a_0 = 0(3 - b_0) \\ 64a_3 + 16a_2 + 4a_1 + a_0 = 4(4 - b_0) \end{cases}$$

(c) Suppose $Q(x) = 4x^3 + x^2 + x$ and $E(x) = x$; show how to recover original msg from Q, E

$Q(x) = E(x)P(x)$

$$P(x) = \frac{4x^3 + x^2 + x}{x} = 4x^2 + x + 1$$

2 (a) Will group discover secret if ℓ individuals lie amongst $(k+\ell)$ representatives?

$k+\ell$ packets sent, ℓ corruptions occur

no, Berlekamp Welch does not work here; would have to brute-force and try out many different subsets of k representatives to find secret

(b) Repeat part (a) except now, there are only $\ell/2$ representatives in opposition.

$k+\ell$ packets sent, $\frac{\ell}{2}$ corruptions occur

we need a min. of k representatives to agree for us to decode the secret

yes, can recover secret via Berlekamp-Welch

if I expect k corruptions, I should send an extra $2k$ packets to recover