Lecture 10 Polynomials & Error Correcting Codes. 10/1/13

message: $\boxed{6}$ $\boxed{4}$ $\boxed{4}$ $\boxed{2}$ $\boxed{0}$ $\boxed{5}$

noisy channel.

Erasure Channel.

$\boxed{6}$ $\boxed{\phantom{0}}$ $\boxed{4}$ $\boxed{2}$ $\boxed{\phantom{0}}$ $\boxed{5}$

general channel.

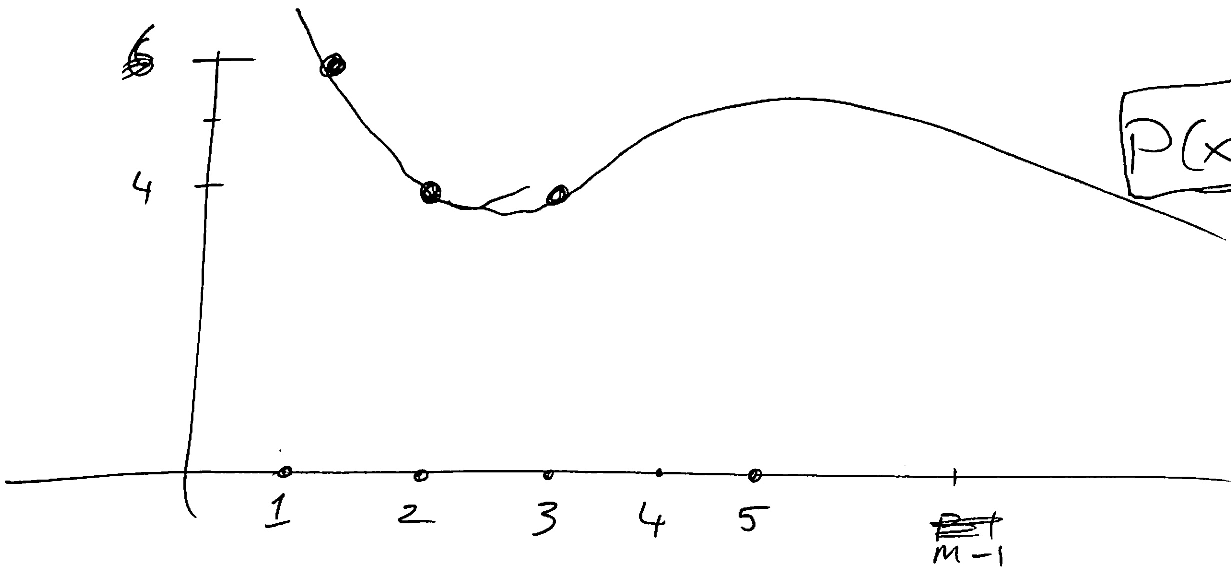
packets get corrupted.

$\boxed{6}$ $\boxed{4}$ $\boxed{2}$ $\boxed{2}$ $\boxed{3}$ $\boxed{5}$

Repitition code: $\boxed{6} \rightarrow \boxed{6}\ \boxed{6}\ \boxed{6}\ \boxed{6}\ \boxed{6}$

Erasure Errors : message $n$ packets. $P(x)$ — degree $n-1$.
Protect against $k$ erasures.
Transmit: $P(1), P(2), \ldots, P(n), P(n+1), \ldots, P(n+k)$.

Message : 6, 4, 4. (mod 7).




$\boxed{P(x) = x^2 + 2x + 3}$

$P(4) = ? = 4^2 + 8 + 3 \pmod 7 = \underbrace{16}_{2} + \underbrace{8}_{1} + 3 = 6$

$P(5) = ? = 5^2 + 10 + 3 = \underbrace{25}_{4} + \underbrace{10}_{3} + \underbrace{3}_{3} = 3$

Send: $6, \cancel{4}, \cancel{4}, 6, 3$.

$P(1) = 6$
$P(4) = 6$
$P(5) = 3$.

$P(x)$ degree 2 polynomial. $P(1)=6$ $P(4)=6$ $P(5)=3$ (mod 7).

<u>Lagrange</u>:

$$\Delta_1(x) = \begin{cases} 1 & \text{at } x=1. \\ 0 & \text{at } x=4,5. \end{cases}$$

polynomial of degree 2.

$$\frac{(x-4)(x-5)}{5} = 3(x-4)(x-5).$$

$(1-4)(1-5) = 12 = 5$

$5^{-1}$ (mod 7)

$$\Delta_4(x) = \frac{(x-1)(x-5)}{4} = 2(x-1)(x-5)$$

$(4-1)(4-5) = -3 = 4.$

$$\Delta_5(x) = \frac{2(x-1)(x-4)}{}$$

$(5-1)(5-4) = 4$

$$P(x) = 6\Delta_1(x) + 6\Delta_4(x) + 3\Delta_5(x).$$

$$= 6\cdot 3(x-4)(x-5) + 6\cdot 2(x-1)(x-5) + 3\cdot 2(x-1)(x-4)$$

$$= x^2 + 2x + 3.$$

$P(1) = 6 \qquad P(4) = 6 \qquad P(5) = 3 \qquad \deg 2 \qquad \text{mod } 7.$

$ax^2 + bx + c$ Solve for $a, b, c$.

$P(1) \qquad a \cdot 1^2 + b \cdot 1 + c = 6$

$P(4) \qquad a \cdot 4^2 + b \cdot 4 + c = 6$

$P(5) \qquad a \cdot 5^2 + b \cdot 5 + c = 3.$

$a + b + c = 6$

$2a + 4b + c = 6$

$4a + 5b + c = 3.$

$-2 \times [\; a + 3b = 0$

$2a + b = 4$

$-5b = 4$

$2b = 4$

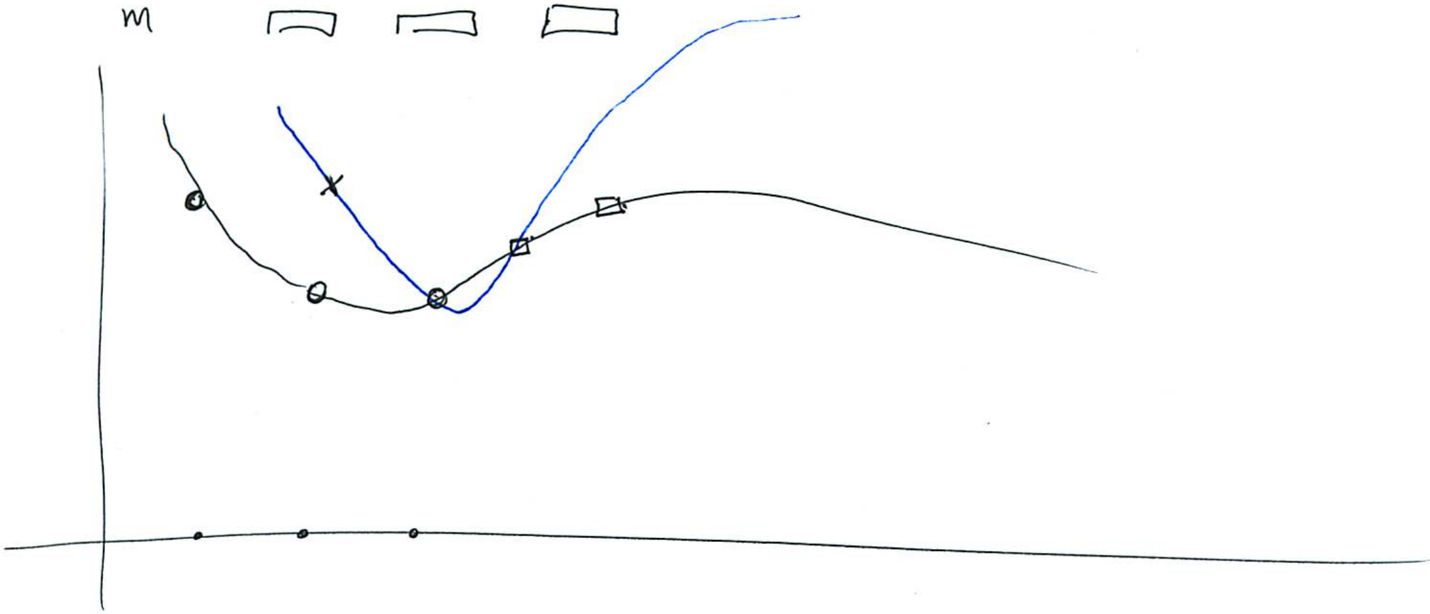
$b = 2.$

$2a + 2 = 4$

$2a = 2 \qquad a = 1$

$a + b + c = 6 \Rightarrow c = 3.$

$x^2 + 2x + 3$




Transmit P(1) P(2) P(3) P(4) P(5).

only 1 error.

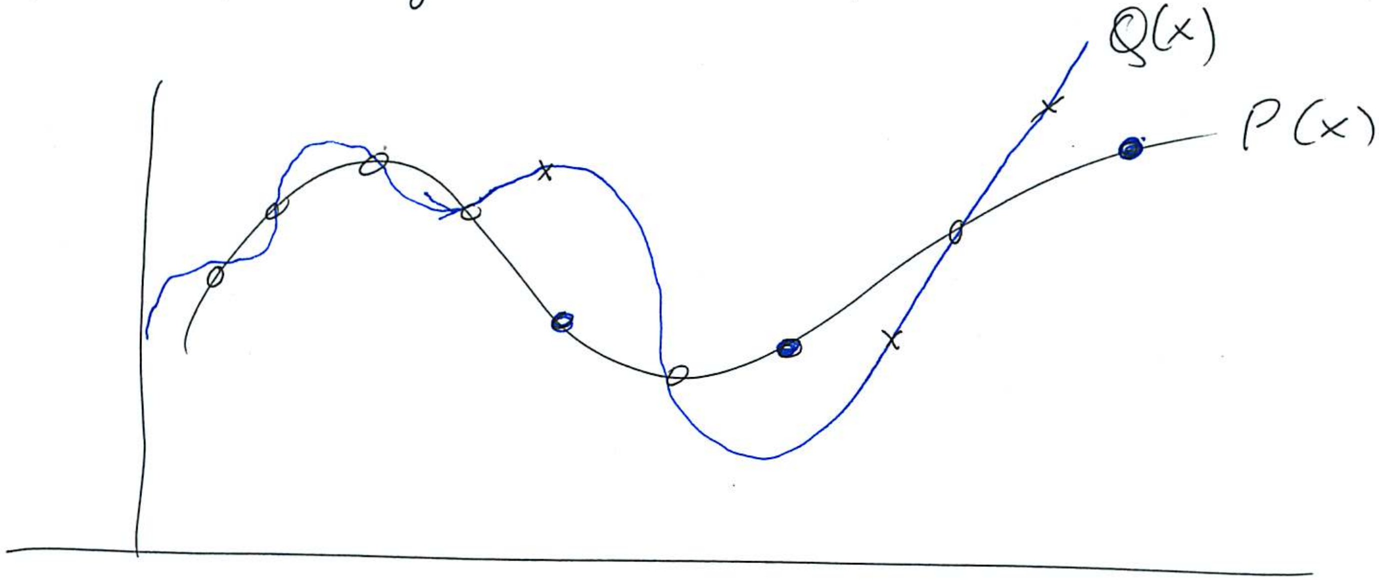
<u>Claim</u>: The only way to fit a degree 2 polynomial through four out of the five received points is to leave off the ~~[illegible]~~ corrupted point.

General picture: $P(1), P(2), \ldots, P(n)$.

~~E~~ message : $n$ packets $=$ degree $n-1$ polynomial.

$\leq k$ packets corrupted.

Transmitted message: $P(1), P(2), \ldots, P(n), P(n+1), \ldots, P(n+2k)$.




Claim : succeed ~~iff~~ in finding polynomial that goes through $n+k$ points iff leave off the $k$ x's.

# points on both curves $P(x)$ & $Q(x)$ $= n$.

But $P(x)$ & $Q(x)$ are polynomials of degree $n-1$.

$\therefore$ $P(x) = Q(x)$. contradiction.

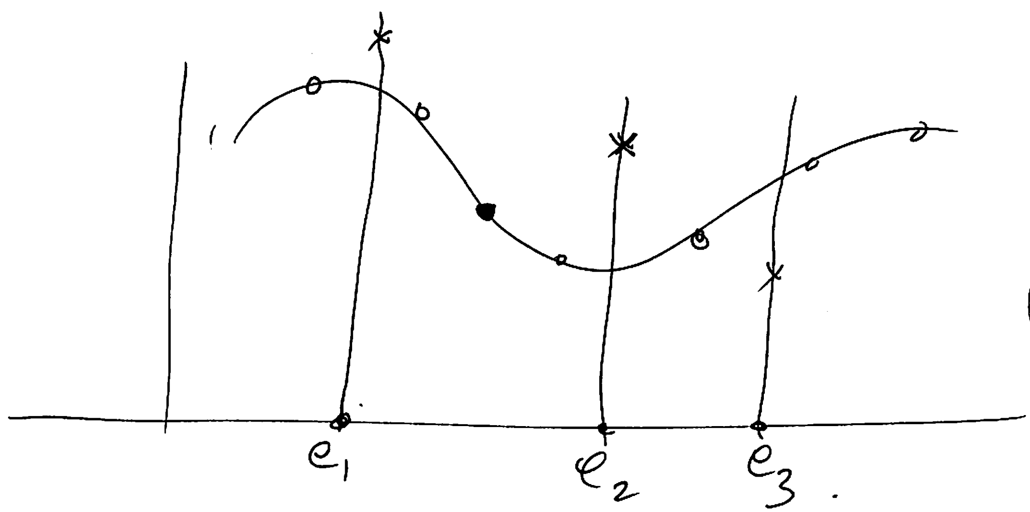
Berlekamp - Welch

$x^2 + 2x + 3$ (mod 7)

message 6, 4, 4.

received : 6, 4, 4, 1, 3.

| sent | received. |
| --- | --- |
| $P(1) = 6$ | $r_1$ |
| $P(2) = 4$ | $r_2$ |
| $P(3) = 4$ | $r_3$ |
| $P(4) = \cancel{2}\,6$ | $r_4 = 1$ |
| $P(5) = 3.$ | $r_5$ |




$\boxed{n + 2k}$

$P(x) = a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$

$\underbrace{e_1 \cdots e_k}_{}$. Solve for.

$E(x) = (x - e_1)(x - e_2) \cdots (x - e_k).$

$P(\cancel{x}\, i)\, E(\cancel{x}\, i) = r_i\, E(i).$ for $i = 1$ to $n + 2k$.

$n + k \begin{cases} k \text{ unknowns.} \\ n \text{ unknowns} = a_0, \ldots a_{n-1} \end{cases}$

$P(i)\, E(i) = r_i\, E(i).$

equations. $= n + 2k$

$P(x)\, E(x) = Q(x).$ $\deg(Q(x)) = \cancel{n+k}$ $n - 1 + k.$

$= n + k - 1.$

$Q(x) = b_{n+k-1}x^{n+k-1} + b_{n+k-2}x^{n+k-2} + \cdots + b_0$ unknowns.

$\#$ coeffs $= |\{b_{n+k-1}, \ldots, b_0\}| = n + k$

$P(i)\, E(i) = r_i\, E(i)$

$i = 1, \dots, n+2k$.

variables:

$e_1, e_2, \dots, e_k \} k$

$b_{n+k+1}, \dots, b_0 \} n+k$.

$n+2k$ vars.

$n+2k$ eqns $n+2k$ unknowns.

solve for $Q(x)$ & $E(x)$

$P(x) = \frac{Q(x)}{E(x)}$.

$\| $

$x^2+2x+3$

received $r_1 = 6$ $r_2 = 4$, $r_3 = 4$, $r_4 = 1$, $r_5 = 3$

$\cancel{Q(x) = b}\ E(x) = (x - e)$ one error.

$Q(x) = P(x)\,E(x) = b_3 x^3 + b_2 x^2 + b_1 x + b_0$

$Q(1) = r_1 E(1)$ $b_3 + b_2 + b_1 + b_0 = 6(1-e)$.

$Q(2) = r_2 E(2)$ $8b_3 + 4b_2 + 2b_1 + b_0 = 4(2-e)$.

$Q(3) = r_3 E(3)$ $27b_3 + 9b_2 + 3b_1 + b_0 = 4(3-e)$

$Q(4) =$

$Q(5) =$

$b_3 = 1$ $b_2 = 5$, $b_1 = 2$, $b_0 = 2$.

$e = 4$.