Lecture 10: Polynomials & Error-Correcting Codes 10/1/13

Message: 6 4 4 2 0 5

noisy channel

6 4 2 0 5

Erasure Channel

general channel

6 4 2 1 2 5

packets get corrupted

Repitition code: 6 → 6 6 6 6 6 6
Erasure Error: \( n \) packets. \( P(x) \) - degree \( n-1 \).

Message: \[ 6, 4, 4 \pmod{7} \]

\[ P(x) = x^2 + 2x + 3 \]

\[ P(4) = ? = 4^2 + 8 + 3 \pmod{7} = \frac{16 + 8 + 3}{2} = 6 \]

\[ P(5) = ? = 5^2 + 10 + 3 \pmod{7} = \frac{25 + 10 + 3}{4} = \frac{38}{4} = 3 \]

Send: \[ 6, 4, 4, 6, 3 \]

\[ P(1) = 6 \]
\[ P(4) = 6 \]
\[ P(5) = 3 \]
\[ P(x) \text{ degree 2 polynomial.} \quad P(1) = 6 \quad P(4) = 6 \quad P(5) = 3 \quad (\text{mod 7}). \]

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

\[ \Delta_4(x) = \frac{(x-4)(x-5)}{5} \]

\[ 3(x-4)(x-5) \cdot 5 \quad (\text{mod 7}) \]

\[ \Delta_5(x) = \frac{(x-1)(x-5)}{4} \quad (4-1)(4-5) \]

\[ = -3 = 4. \]

\[ \Delta_5(x) = 2 \frac{(x-1)(x-4)}{4} \quad (5-1)(5-4) \]

\[ = 4. \]

\[ P(x) = 6 \Delta_1(x) + 6 \Delta_4(x) + \overline{3} \Delta_5(x). \]

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

\[ = x^2 + 2x + 3. \]
\( P(1) = 6 \quad P(4) = 6 \quad P(5) = 3 \quad \text{deg } 2 \text{ w/ 7.} \)

\[ a \cdot 1^2 + b \cdot 1 + c = 6 \]

\[ a \cdot 4^2 + b \cdot 4 + c = 6 \]

\[ a \cdot 5^2 + b \cdot 5 + c = 3. \]

\[ a + b + c = 6 \]

\[ 2a + 4b + c = 6 \]

\[ 4a + 5b + c = 3. \]

\[ x^2 + 2x + 3 \]

Solve for \( a, b, c \).
Transmit \( P(1) \), \( P(2) \), \( P(3) \), \( P(4) \), \( P(5) \).

only 1 error.

Claim: The only way to fit a degree 2 polynomial through four out of the five points is to leave off the corrupted point.
General picture: \( P(1), P(2), \ldots, P(n) \).

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 field 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 \( n-1 \).

\( \Rightarrow P(x) = Q(x) \). contradic. .
Berlekamp - Welch

Message: \( 6, 4, 4 \)

Received: \( 6, 4, 4, 1, 3 \)

\[ E(x) = (x-e_1)(x-e_2) \cdots (x-e_k) \]

\[ P(x) E(x) = \sum_{i=1}^{n+k} \eta_i E(i) \]

\[ P(i) \cdot E(i) = \eta_i \cdot E(i) \]

\[ P(x) E(x) = \sum \phi(x) \]

\[ \phi(x) = b_{n+k-1} x^{n+k-1} + b_{n+k-2} x^{n+k-2} + \cdots + b_0 \]

\[ \# \text{coeffs} = \lfloor \frac{n+k-1}{2} \rfloor = \lceil \frac{n+k}{2} \rceil \]
$$P(i) \ E(i) = \gamma_i \ E(i)$$

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

$n+2k$ equations $n+2k$ unknowns.

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

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

$$Q(x) = 4 \ x^2 + 2k + 3$$

Received

$\gamma_1 = 6$ \hspace{0.5cm} $\gamma_2 = 4$ \hspace{0.5cm} $\gamma_3 = 4$ \hspace{0.5cm} $\gamma_4 = 1$ \hspace{0.5cm} $\gamma_5 = 3$

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

$Q(1) = \gamma_1 \ E(1)$

$$b_3 + b_2 + b_1 + b_0 = 6(1 - e)$$

$Q(2) = \gamma_2 \ E(2)$

$$8b_3 + 4b_2 + 2b_1 + b_0 = \frac{48}{5}(2 - e)$$

$Q(3) = \gamma_3 \ E(3)$

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

$Q(4) = $  

$Q(5) = $  

$e = 4$

$b_3 = 1$ \hspace{0.5cm} $b_2 = 5$ \hspace{0.5cm} $b_1 = 2$ \hspace{0.5cm} $b_0 = 2$.  

$n+2k$ values.