

Error Correcting Code

CS 70 Discussion 5A

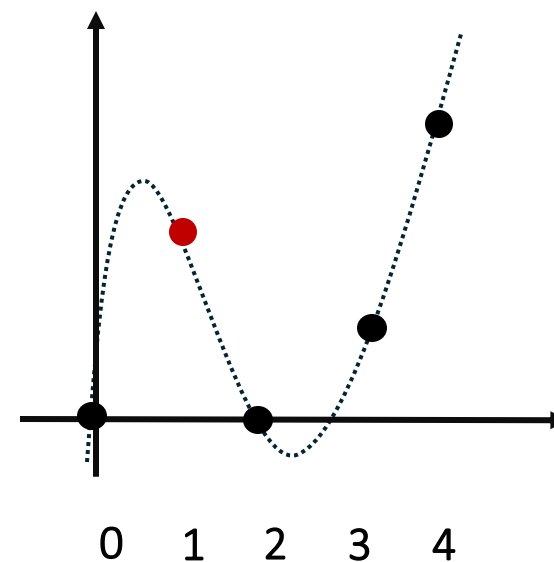
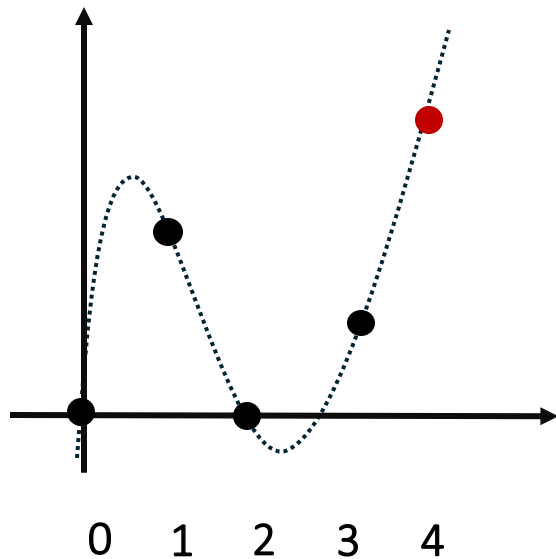
Raymond Tsao

2025-02-26

Note: These slides are unofficial course materials. Please use the notes as the only single source of truth.

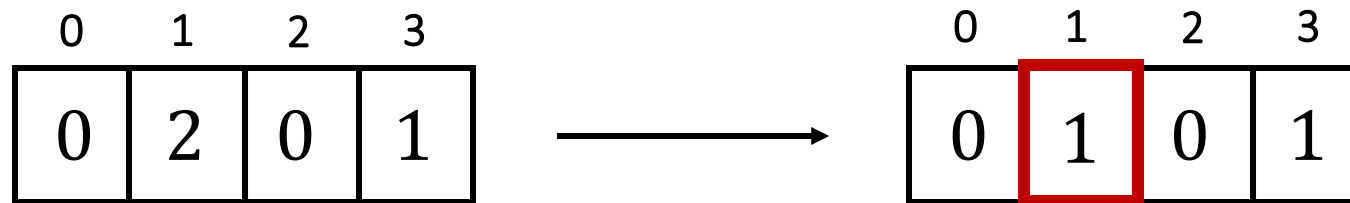
Erasure Errors

- Send 4 packets, with 1 erasure error



Difficult Case: Corruption Error

- Send 4 packets, with 1 corruption error



- Berlekamp Welch algorithm!

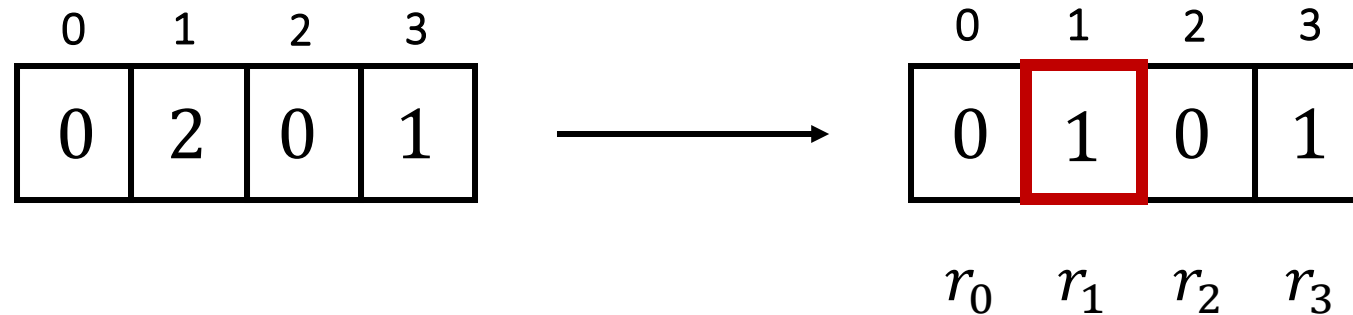
Berlekamp-Welch Algorithm

Some terminology...

- $P(x)$: Polynomial passing through the original messages $\deg(P) = n - 1$
- $E(x) = (x - e_1)(x - e_2) \dots (x - e_k) = (x - 1)$ $\deg(E) = k$
- Define $Q(x) = P(x)E(x)$ $\deg(Q) = n + k - 1$

 Indices where corruption occurs

If we know Q and E , then we know P !



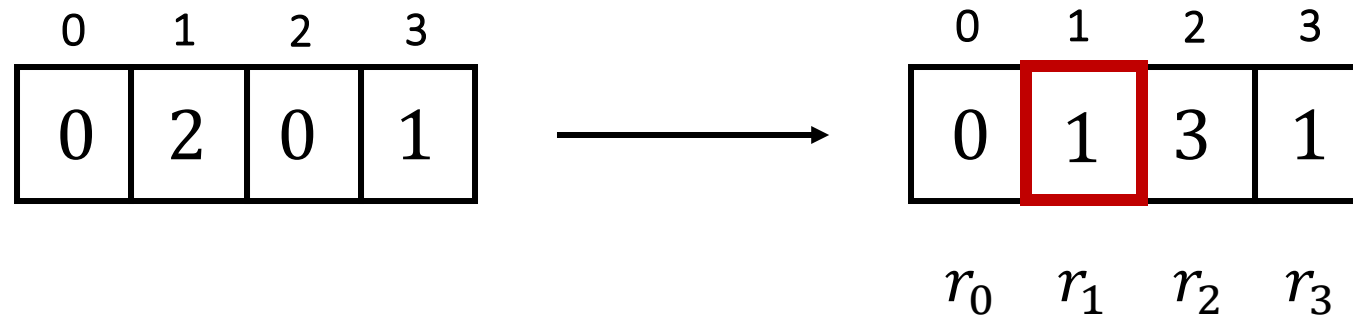
Berlekamp-Welch Algorithm

Crucial fact: $Q(i) = r_i E(i)$ for all index i

$$Q(0) = r_0 E(0) = 0 \cdot E(0)$$

$$Q(1) = r_1 E(1) = 1 \cdot E(1)$$

$$Q(2) = r_2 E(2) = 3 \cdot E(2) \quad \text{And so on...}$$



Berlekamp-Welch Algorithm

Crucial fact: $Q(i) = r_i E(i)$ for all index i

$$Q(x) = a_{n+k-1}x^{n+k-1} + \dots + a_1x + a_0$$

$n + k$ unknowns

$$E(x) = (x - e_1)(x - e_2) \dots (x - e_k)$$

k unknowns

$$= x^k + b_{k-1}x^{k-1} + \dots + b_0$$

$$Q(0) = r_0 E(0)$$

$$Q(1) = r_1 E(1)$$

$$Q(2) = r_2 E(2)$$

\vdots

Need $n + 2k$ equations

Send $n + 2k$ packages!

Problem 1: Berlekamp-Welch Warm Up

(a) Degree of P : $n - 1$

(b) $P(i) = r_i$ if no error on index i

(c) Erasure error: send $n + k$ packages

General error: send $n + 2k$ packages

(e) Key behind Berlekamp-Welch

$$Q(i) = P(i)E(i) = r_i E(i)$$

- Case 1: There's no error on index i $P(i) = r_i$
- Case 2: There's an error on index i $P(i) \neq r_i$ but $E(i) = 0$

Problem 2: Berlekamp-Welch Algorithm

(a) From the perspective of sender

0	1	2	3	4
1	1	4	0	4

Need to find a polynomial passing these points $(0, 1), (1, 1), (2, 4)$

$$\begin{aligned} & 1 \cdot \frac{(x-1)(x-2)}{(0-1)(0-2)} + 1 \cdot \frac{(x-0)(x-2)}{(1-1)(1-2)} + 4 \cdot \frac{(x-0)(x-1)}{(2-0)(2-1)} \\ &= 4x^2 + x + 1 \end{aligned}$$

Problem 2: Berlekamp-Welch Algorithm

(b) From the perspective of receiver

0	1	2	3	4
0	1	4	0	4

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

$$E(x) = (x - e)$$

$$Q(0) = r_0E(0) = 0 \cdot E(0)$$

$$a_0 = 0$$

$$Q(1) = r_1E(1) = 1 \cdot E(1)$$

$$a_3 + a_2 + a_1 + a_0 = 1 - e$$

$$Q(2) = r_2E(2) = 4 \cdot E(2)$$

$$8a_3 + 4a_2 + 2a_1 + a_0 = 4(2 - e)$$

$$Q(3) = r_3E(3) = 0 \cdot E(3)$$

$$27a_3 + 9a_2 + 3a_1 + a_0 = 0$$

$$Q(4) = r_4E(4) = 4 \cdot E(4)$$

$$64a_3 + 16a_2 + 4a_1 + a_0 = 4(4 - e)$$

Problem 2: Berlekamp-Welch Algorithm

(c) Solving gives $Q(x) = 4x^3 + x^2 + x$ and $E(x) = x$

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

Plug in $P(0), P(1), \dots$ to get recovered messages

1	1	4	0	4
---	---	---	---	---

Problem 3: Berlekamp-Welch Algorithm with Fewer Errors

(d) Claim: The $P(x)$ solved is still correct even if there are multiple solutions

Suppose there are two distinct solutions $(Q(x), E(x)), (Q'(x), E'(x))$

Want to show

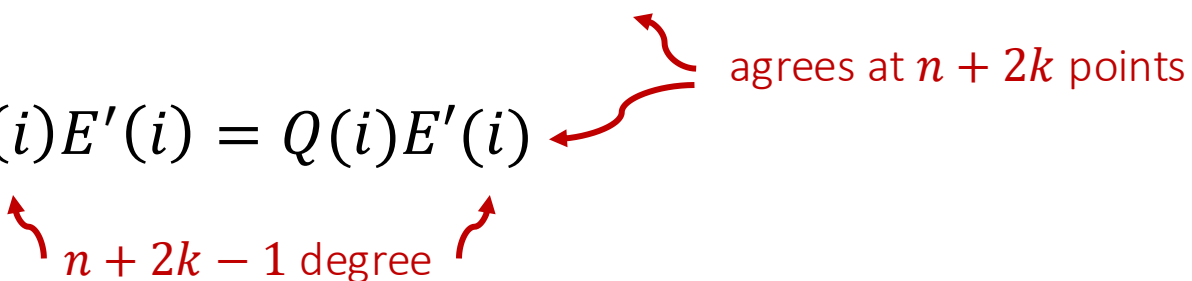
$$\frac{Q(x)}{E(x)} = \frac{Q'(x)}{E'(x)} \quad \text{i.e.} \quad Q(x)E'(x) = Q'(x)E(x)$$

We know

$$Q(i) = r_i E(i) \quad Q'(i) = r_i E'(i)$$

Cross multiply:

$$Q(i)E'(i) = Q'(i)E(i)$$



$n + 2k - 1$ degree

agrees at $n + 2k$ points

Since two $n + 2k - 1$ degree polynomial agree at $n + 2k$ points, they must be the same