

## 4 Berlekamp-Welch for General Errors

(a)  $\deg(E(x)) = 1, \deg(Q(x)) = 3$ .

Since there's only one error, so  $k = 1$  here, so the degree of  $E(x) = k = 1$

Now, since Hector wants to send a length  $n = 3$  message, so the degree of  $Q(x) = n + k - 1 = 3$

Using the given relation, so we can write:

$$\begin{aligned} E(x) &= x - e_1 \\ Q(x) &= a_3x^3 + a_2x^2 + a_1x + a_0 \end{aligned}$$

Then, since  $Q(i) = r_i E(i)$  for  $0 \leq i < 5$ , and with  $E(x) = x - e_i = x + b_0$ , so we have that:

$$\begin{aligned} Q(0) &= r_0 E(0), \text{ which gives: } a_0 = 3(0 + b_0) = 3b_0 \\ Q(1) &= r_1 E(1), \text{ which gives: } a_3 + a_2 + a_1 + a_0 = 7(1 + b_0) = 7 + 7b_0 \\ Q(2) &= r_2 E(2), \text{ which gives: } 8a_3 + 4a_2 + 2a_1 + a_0 = 0(2 + b_0) = 0 \\ Q(3) &= r_3 E(3), \text{ which gives: } 27a_3 + 9a_2 + 3a_1 + a_0 = 2(3 + b_0) = 6 + 2b_0 \\ Q(4) &= r_4 E(4), \text{ which gives: } 64a_3 + 16a_2 + 4a_1 + a_0 = 10(4 + b_0) = 40 + 10b_0 \end{aligned}$$

(b)  $Q(x) = 3x^3 + 6x^2 + 5x + 8, E(x) = x - 1$ ; error located at position 1.

Suppose we're working over  $GF(11)$ , and with the system of equations derived above, we can translate them into:

$$\begin{aligned} a_0 + 8b_0 &= 0 \\ a_3 + a_2 + a_1 + a_0 + 4b_0 &= 7 \\ 8a_3 + 4a_2 + 2a_1 + a_0 &= 0 \\ 5a_3 + 9a_2 + 3a_1 + a_0 + 9b_0 &= 6 \\ 9a_3 + 5a_2 + 4a_1 + a_0 + b_0 &= 7 \end{aligned}$$

Since  $2 \cdot 6 = 12 = 11 + 1$ , so  $2^{-1} \equiv 6 \pmod{11}$ . Thus, solving this system of linear equations (with the help of Jupyter Notebook) would yield:

$$\begin{aligned} a_3 &= -\frac{5}{2} \equiv -5 \cdot 6 = -3 \cdot 11 + 3 \equiv 3 \pmod{11}, \\ a_2 &= \frac{1}{2} \equiv 1 \cdot 6 = 6 \pmod{11}, \\ a_1 &= 5 \pmod{11}, \\ a_0 &= 8 \pmod{11}, \\ b_0 &= -1 \pmod{11}. \end{aligned}$$

Thus,  $Q(x) = 3x^3 + 6x^2 + 5x + 8$  and  $E(x) = x - 1$ ; the location of this error is at position  $e_1 = -b_0 = 1$ .

(c)  $P(x) = 3x^2 + 9x + 3$ ; message = "DEA".

Then, since we're working over  $GF(11)$ , with  $Q(x) = 3x^3 + 6x^2 + 5x + 8$  and  $E(x) = x - 1$ , so we can calculate  $P(x) = \frac{Q(x)}{E(x)} = \frac{3x^3 + 6x^2 + 5x + 8}{x - 1} = 3x^2 + 9x + 3$ .

Since we noticed that the first character was corrupted as  $e_1 = 1$ , so we calculate  $P(1) = 3 + 9 + 3 = 4 = \text{"E"}$ , which means that