CS 70 Discrete Mathematics and Probability Theory
Spring 2022 Koushik Sen and Satish Rao **DIS 5A**

1 Berlekamp-Welch Warm Up

Let $P(i)$, a polynomial applied to the input i, be the original encoded polynomial before sent, and let r_i be the received info for the input i which may or may not be corrupted.

(a) If you want to send a length-n message, what should the degree of $P(x)$ be? Why?

$n-1$

(b) When does $r_i = P(i)$? When does r_i not equal $P(i)$?

$r_i = P(i)$ when there is no corruption at i

$r_i \neq P(i)$ when there is a corruption at i

(c) If there are at most k erasure errors, how many packets should you send? If there are at most k general errors, how many packets should you send? (We will see the reason for this later.) Now we will only consider general errors.

k erasure errors: $n+k$ packets

k general errors: $n+2k$ packets

(d) What do the roots of the error polynomial $E(x)$ represent? Does the receiver know the roots of $E(x)$? If there are at most k errors, what is the maximum degree of $E(x)$? Using the information about the degree of $P(x)$ and $E(x)$, what is the degree of $Q(x) = P(x)E(x)$?

The roots of $E(x) = (x-e_1)\cdots(x-e_k)$ represent the locations of the errors.

The receiver does not know the roots of $E(x)$.

$\deg(P) = n-1$ $\deg(E) = k$ $\deg(Q) = n+k-1$

(e) Why is the equation $Q(i) = P(i)E(i) = r_iE(i)$ always true? (Consider what happens when $P(i) = r_i$, and what happens when $P(i)$ does not equal r_i.)

If there is no error at i, then $P(i) = r_i$ so $P(i)E(i) = r_iE(i)$.

If there is an error at i, then $E(i) = 0$ so $P(i)E(i) = r_iE(i)$.

(f) In the polynomials $Q(x)$ and $E(x)$, how many total unknown coefficients are there? (These are the variables you must solve for. Think about the degree of the polynomials.) When you receive packets, how many equations do you have? Do you have enough equations to solve for all of the unknowns?

(Think about the answer to the earlier question - does it make sense now why we send as many packets as we do?)

$Q(x) = a_{n+k-1} x^{n+k-1} + \ldots + a_1 x + a_0$ $\quad$ $n+k$ unknowns

$E(x) = x^k + b_{k-1} x^{k-1} + \ldots + b_1 x + b_0$ $\quad$ k unknowns

We have $n+2k$ equations, so there are enough equations to solve for all unknowns.

(g) If you have $Q(x)$ and $E(x)$, how does one recover $P(x)$? If you know $P(x)$, how can you recover the original message?

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

Original message is $P(1), \ldots, P(n)$.

2 Berlekamp-Welch Algorithm

In this question we will send the message $(m_0, m_1, m_2) = (1, 1, 4)$ of length $n = 3$. We will use an error-correcting code for $k = 1$ general error, doing arithmetic over GF(5).

(a) Construct a polynomial $P(x) \pmod 5$ of degree at most 2, so that

$$P(0) = 1, \qquad P(1) = 1, \qquad P(2) = 4.$$

What is the message $(c_0, c_1, c_2, c_3, c_4)$ that is sent?

$P_0(x) = 3(x-1)(x-2) = 3x^2 + x + 1$

$P_1(x) = 4x(x-2) = 4x^2 + 2x$

$P_2(x) = 3x(x-1) = 3x^2 + 2x$

$P(x) = P_0(x) + P_1(x) + 4P_2(x)$

$= 4x^2 + x + 1$

$(1, 1, 4, 0, 4)$

(b) Suppose the message is corrupted by changing c_0 to 0. Set up the system of linear equations in the Berlekamp-Welch algorithm to find $Q(x)$ and $E(x)$.

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

$E(x) = x + b_0$

$Q(i) = r_i E(i)$ for $0 \le i \le 4$

$$Q(i) = a_3 i^3 + a_2 i^2 + a_1 i + a_0 = r_i(i + b_0)$$

$$Q(0) = a_0 = 0$$

$$Q(1) = a_3 + a_2 + a_1 + a_0 = 1 + b_0$$

$$Q(2) = 8a_3 + 4a_2 + 2a_1 + a_0 = 8 + 4b_0$$

$$Q(3) = 27a_3 + 9a_2 + 3a_1 + a_0 = 0$$

$$Q(4) = 64a_3 + 16a_2 + 4a_1 + a_0 = 16 + 4b_0$$

(c) Assume that after solving the equations in part (b) we get $Q(x) = 4x^3 + x^2 + x$ and $E(x) = x$. Show how to recover the original message from Q and E.

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

$$(P(0), P(1), P(2)) = (1, 1, 4)$$

3 Berlekamp-Welch Algorithm with Fewer Errors

In class we derived how the Berlekamp-Welch algorithm can be used to correct k general errors, given $n+2k$ points transmitted. In real life, it is usually difficult to determine the number of errors that will occur. What if we have less than k errors? This is a follow up to the exercise posed in the notes.

Suppose Alice wants to send 1 message to Bob and wants to guard against 1 general error. She decides to encode the message with $P(x) = 4$ (on GF(7)) such that $P(0) = 4$ is the message she want to send. She then sends $P(0), P(1), P(2) = (4,4,4)$ to Bob.

(a) Suppose Bob receives the message $(4,5,4)$. Without performing Gaussian elimination explicitly, find $E(x)$ and $Q(x)$.

$E(x) = x - 1$

$Q(x) = 4(x-1) = 4x + 3$

(b) Now, suppose there were no general errors and Bob receives the original message $(4,4,4)$. Show that the $Q(x), E(x)$ that you found in part (a) still satisfies $Q(i) = r_i E(i)$ for all $i = 0,1,2$.

$4x + 3 = r_x(x-1)$

$i = 0: \quad 3 = 3$

$i = 1: \quad 4+3 = 0$

$i = 2: \quad 8+3 = 4$

(c) Verify that $E(x) = x$, $Q(x) = 4x$ is another possible set of polynomials that satisfies $Q(i) = r_i E(i)$ for all $i = 0,1,2$.

(Skipped.)

(d) Suppose you're actually trying to decode the received message $(4,4,4)$. Based on what you showed in the previous two parts, what will happen during row reduction when you try to solve for the unknowns?

There will be multiple solutions.

(e) Prove that in general, no matter what the solution of $Q(x)$ and $E(x)$ are though, the recovered $P(x)$ will always be the same.

Suppose $Q(x), E(x)$ and $Q'(x), E'(x)$ were both solutions.

$$Q(i) = r_i E(i)$$
$$Q'(i) = r_i E'(i) \quad \text{for all } 1 \le i \le n+2k$$

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

$$Q(i)E'(i) = Q'(i)E(i) \quad \text{for all } 1 \le i \le n+2k$$

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