1 Berlekamp-Welch Warm Up

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

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

(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.

(d) What do the roots of the error polynomial $E(x)$ tell you? 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 $Q(x) = P(x)E(x)$?

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

(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?

2 Berlekamp-Welch Algorithm

In this question we will send the message $(m_0, m_1, m_2) = (4, 3, 2)$ 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

$$P(0) = 4, \qquad P(1) = 3, \qquad P(2) = 2.$$

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

(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 $E(x)$.

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

3 Bijections

Consider the function

$$f(x) = \begin{cases} x, & \text{if } x \geq 1; \\ x^2, & \text{if } -1 \leq x < 1; \\ 2x + 3, & \text{if } x < -1. \end{cases}$$

(a) If the domain and range of f are $\mathbb{N}$, is f injective (one-to-one), surjective (onto), bijective?

(b) If the domain and range of f are $\mathbb{Z}$, is f injective (one-to-one), surjective (onto), bijective?

(c) If the domain and range of f are $\mathbb{R}$, is f injective (one-to-one), surjective (onto), bijective?

4 Count It!

For each of the following collections, determine and briefly explain whether it is finite, countably infinite (like the natural numbers), or uncountably infinite (like the reals):

(a) $\mathbb{N}$, the set of all natural numbers.

(b) $\mathbb{Z}$, the set of all integers.

(c) $\mathbb{Q}$, the set of all rational numbers.

(d) $\mathbb{R}$, the set of all real numbers.

(e) The integers which divide 8.

(f) The integers which 8 divides.

(g) The functions from $\mathbb{N}$ to $\mathbb{N}$.

(h) Computer programs that halt.

(i) Numbers that are the roots of nonzero polynomials with integer coefficients.