Q1 Error Correction
2 Points

Q1.1 Zeroing out
1 Point

The equation $0x = 0y$ is always valid, even if $x \neq y$.

- (●) True
- ( ) False

Explanation
0 times anything is 0

Q1.2 More Intuition on Functions
1 Point

Given two functions, $P(x)$ and $R(x)$ where $P(3) \neq R(3)$. Consider two more functions $Q(x) = (x-3)P(x)$ and $F(x) = (x-3)R(x)$. Then $Q(3) = F(3)$.

- (●) True
- ( ) False

Explanation
$Q(3) = (3-3)P(3) = 0$ regardless of the value of $P(3)$. Similarly $F(x) = 0$.

Q2 More on ECC

3 Points

Q2.1 Erasure Errors

1 Point

Consider a message $m_1, \ldots, m_n$ where each m_i is a number in modular arithmetic with modulus a prime q (in $GF(q)$). One wishes to send the message through a channel that loses as many as k packets.

How many packets does one need to send to always be able to reconstruct the original n packet message? (In terms of n and k.)

- ○ n
- ◉ $n + k$
- ○ $n + 2k$
- ○ None of the above

Explanation

It's necessary since if you lose k packets you still have to recieve n packets to just represent the original message. The polynomial scheme where one sends $n + k$ points on a degree $n - 1$ polynomial formed from the original message allows one to recover the polynomial (and message) with any n points.

Q2.2 General Errors
1 Point

Consider a message $m_1, \ldots, m_n$ where each m_i is a number in modular arithmetic with modulus a prime q (in $GF(q)$). One wishes to send the message through a channel that corrupt as many as k packets.

How many packets does one need to send to always be able to reconstruct the original n packet message? (In terms of n and k.)

- ○ n
- ○ $n + k$
- ◉ $n + 2k$
- ○ None of the above

Explanation

Define a degree $n - 1$ polynomial $P(x)$ that satisfies $P(1) = m_1, \ldots, P(n) = m_n$ and the error-locator polynomial $E(x) = (x - e_1)(x - e_2) \ldots (x - e_k)$, and $Q(x) = P(x)E(x)$. Suppose that the receiver gets $r_1, \ldots, r_{n+2k}$. Then, we know that $P(i)E(i) = r_i E(i)$ for all $1 \leq i \leq n + 2k$ since if $P(i) \neq r_i$, i is a root of $E(x)$, so $P(i)E(i) = 0 = r_i E(i)$. Thus, we get $n + 2k$ equations of the form $Q(i) = r_i E(i)$. Note that the degree of $P(x)$ is $n - 1$, and the degree of $E(x)$ is k, so the degree of $Q(x)$ is $n + k - 1$. There are $n + k$ unknown coefficients in $Q(x)$, and k unknown coefficients in $E(x)$ (since the leading coefficient is 1. So, we have $n + 2k$ unknown variables, $n + 2k$ linear equations of the form $Q(i) = r_i E(i)$, so we can solve the system of linear equations, and retrieve $P(x) = \frac{Q(x)}{E(x)}$.

Q2.3 Both errors
1 Point

Consider a message $m_1, \ldots, m_n$ where each m_i is a number in modular arithmetic with modulus a prime q (in $GF(q)$). One wishes to send the message through a channel that loses as many as k packets and corrupts as many as c packets.

How many packets does one need to send to always be able to reconstruct the original n packet message? (In terms of n, k, and c.)

- ○ $n + 2k + 2c$
- ○ $n + k + c$
- ○ $n + 2k + c$
- ◉ $n + k + 2c$

Explanation

Considering the packets that don't get lost, we already know that we need $n + 2c$ packets to retrieve the original message when there are at most c packets that get corrupted. Taking the packets that do get lost, we need an additional k packets, so we get $n + k + 2c$.