1. Sanity check!

1. Alice wants to send a message of length 10 to Bob over a lossy channel. In the general case, what is the degree of the polynomial she uses to encode her message?

Solution: 9

2. Alice sent Bob the values of the above polynomial at 16 distinct points. How many erasure errors can Bob recover from?

Solution: 6

3. How many general errors can Bob recover from?

Solution: 3

2. Where are my packets?

Alice wants to send the message \((a_0, a_1, a_2)\) to Bob, where each \(a_i \in \{0, 1, 2, 3, 4\}\). She encodes it as a polynomial \(P\) of degree \(\leq 2\) over \(GF(5)\) such that \(P(0) = a_0\), \(P(1) = a_0\), and \(P(2) = a_2\), and she sends the packets \((0, P(0)), (1, P(1)), (2, P(2)), (3, P(3)), (4, P(4))\). Two packets are dropped, and Bob only learns that \(P(0) = 4\), \(P(3) = 1\), and \(P(4) = 2\). Help Bob recover Alice’s message.

1. Find the multiplicative inverses of 1, 2, 3 and 4 modulo 5.

Solution: Inverse pairs mod 5: \((1, 1), (2, 3), (4, 4)\).

2. Find the original polynomial \(P\) by using Lagrange interpolation or by solving a system of linear equations.

Solution:

\[
\begin{align*}
\Delta_0 &= \frac{(x - 3)(x - 4)}{(0 - 3)(0 - 4)} = \frac{x^2 - 7x + 12}{(-3)(-4)} = 3(x^2 + 3x + 2) = 3x^2 + 4x + 1 \\
\Delta_3 &= \frac{(x - 0)(x - 4)}{(3 - 0)(3 - 4)} = \frac{x^2 - 4x}{(3)(-1)} = 3(x^2 + x) = 3x^2 + 3x \\
\Delta_4 &= \frac{(x - 0)(x - 3)}{(4 - 0)(4 - 3)} = \frac{x^2 - 3x}{(4)(1)} = 4(x^2 + 2x) = 4x^2 + 3x
\end{align*}
\]

Thus, our original polynomial \(P\) is

\[
4\Delta_0 + 1\Delta_3 + 2\Delta_4 = 4(3x^2 + 4x + 1) + (3x^2 + 3x) + 2(4x^2 + 3x) \\
= (2x^2 + x + 4) + (3x^2 + 3x) + (3x^2 + x) \\
= 3x^2 + 4
\]

Linear equation way: Writing \(P(x) = m_2x^2 + m_1x + m_0\), we solve for the \(m_i\)'s by solving the linear equation

\[
\begin{bmatrix} 0 & 0 & 1 \\ 9 & 3 & 1 \end{bmatrix} \begin{bmatrix} m_2 \\ m_1 \end{bmatrix} = \begin{bmatrix} 4 \\ 1 \end{bmatrix}
\]
This gives the equation
\[ \frac{1}{2}x^2 - \frac{5}{2}x + 4, \]
which, in the modulo 5 world, means \( P(x) = 3x^2 + 4. \)

3. Recover Alice’s original message.

**Solution:** To recover \((a_0, a_1, a_2)\), we compute
\[
P(0) = 4 \\
P(1) = 2 \\
P(2) = 1
\]

3. Berlekamp-Welch for general errors

Suppose that Hector wants to send you a length \( n = 3 \) message, \( m_0, m_1, m_2, \) with the possibility for \( k = 1 \) error. In this world we will work mod 11, so we can encode 11 letters as shown below:

<table>
<thead>
<tr>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
<th>G</th>
<th>H</th>
<th>I</th>
<th>J</th>
<th>K</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
<td>7</td>
<td>8</td>
<td>9</td>
<td>10</td>
</tr>
</tbody>
</table>

Hector encodes the message by finding the degree \( \leq 2 \) polynomial \( P(x) \) that passes through \((0, m_0), (1, m_1), \) and \((2, m_2)\), and then sends you the five packets \( P(0), P(1), P(2), P(3), P(4) \) over a noisy channel. The message you receive is
\[ DHACK \Rightarrow 3, 7, 0, 2, 10 = r_0, r_1, r_2, r_3, r_4 \]
which could have up to 1 error.

1. First locate the error, using an error-locating polynomial \( E(x) \). Let \( Q(x) = P(x)E(x) \). Recall that
\[ Q(i) = P(i)E(i) = r_i E(i), \quad \text{for} \quad 0 \leq i < n + 2k \]
What is the degree of \( E(x) \)? What is the degree of \( Q(x) \)? Using the relation above, write out the form of \( E(x) \) and \( Q(x) \), and then a system of equations to find both these polynomials.

**Solution:** The degree of \( E(x) \) will be 1, since there is at most 1 error. The degree of \( Q(x) \) will be 3, since \( P(x) \) is of degree 2. \( E(x) \) will have the form \( E(x) = x + e \), and \( Q(x) \) will have the form \( Q(x) = ax^3 + bx^2 + cx + d \). We can write out a system of equations to solve for these 5 variables:
\[
d = 3(0 + e) \\
a + b + c + d = 7(1 + e) \\
8a + 4b + 2c + d = 0(2 + e) \\
27a + 9b + 3c + d = 2(3 + e) \\
64a + 16b + 4c + d = 10(4 + e)
\]
Since we are working mod 11, this is equivalent to:
\[
d = 3e \\
a + b + c + d = 7 + 7e \\
8a + 4b + 2c + d = 0 \\
5a + 9b + 3c + d = 6 + 2e \\
9a + 5b + 4c + d = 7 + 10e
\]
2. Ask your GSI for $Q(x)$. What is $E(x)$? Where is the error located?

Solution: Solving this system of linear equations we get

$$Q(x) = 3x^3 + 6x^2 + 5x + 8$$

Plugging this into the first equation (for example), we see that:

$$d = 8 = 3e \quad \Rightarrow \quad e = 8 \cdot 4 = 32 \equiv 10 \text{ mod } 11$$

This means that

$$E(x) = x + 10 \equiv x - 1 \text{ mod } 11.$$ 

Therefore the error occurred at $x = 1$ (so the second number sent in this case).

3. Finally, what is $P(x)$? Use $P(x)$ to determine the original message that Hector wanted to send.

Solution: Using polynomial division, we divide $Q(x) = 3x^3 + 6x^2 + 5x + 8$ by $E(x) = x - 1$:

$$P(x) = 3x^2 + 9x + 3$$

Then $P(1) = 3 + 9 + 3 = 15 \equiv 4 \text{ mod } 11$. This means that our original message was

$$3, 4, 0 \quad \Rightarrow \quad \text{DEA}$$

4. Secret Sharing

Umesh wants to share a secret among 4 TAs and 14 readers, such that a subset of them can reconstruct the secret iff it contains either (i) at least 2 TAs, or (ii) at least 1 TA and at least 2 readers, or (iii) at least 4 readers. Explain how this can be accomplished.

Solution: First note that in this case, a TA essentially counts as 2 readers. Thus, we make a polynomial $p$ of degree 3 such that $p(0) = s$, where $s$ is Tom’s secret. Each reader gets one point in $p$, while each TA gets 2.

Thus, if either 2 TAs, 1 TA and 2 readers, or 4 readers collaborate, they can recover $s$. 

EECS 70, Fall 2015, Discussion 6A