Decoding with Erasure Errors

1. Suppose Alice wants to send Bob a message of $n = 5$ packets and she wants to guard against $k = 1$ lost packets. Further assume that packets can be coded up as integers between 0 and 6.

   (a) Alice can work over $GF(q)$. What is the minimum prime q can be?
   $q =$
   Recall that $q > n + k$.
   $q = 7$. Alice needs to be able to send the original 5 packets, plus one redundant packet to guard against one erasure, so q must be a prime greater than 6.

   (b) Suppose Alice wants to send Bob the message $m = (2, 3, 5, 1, 6)$, where e.g., $m_2 = 3$. What is the maximum degree of the unique polynomial described by these points, which are of the form (i, m_i)?
   $d =$
   4 — we have 5 points, which can uniquely determine a polynomial of degree at most 4.

   (c) What are the coefficients of the polynomial $P(x) = a_0+a_1x+a_2x^2+a_3x^3+a_4x^4$ described by these 5 points, $(i, m_i)\ \forall\ i \in \{1, \ldots, 5\}$?
   $a_0 =$
   $a_0 = 3$. For full solution, see solution to a_4.
   $a_1 =$
   $a_1 = 5$. For full solution, see solution to a_4.
   $a_2 =$
   $a_2 = 4$. For full solution, see solution to a_4.
   $a_3 =$
   $a_3 = 6$. For full solution, see solution to a_4.
   $a_4 =$
   $a_4 = 5$. The packets m_1 through m_5 gives us a system of 5 linear equations

$$\begin{aligned} P(1) &= a_0 + a_1 + a_2 + a_3 = 2 \\ P(2) &= a_0 + 2a_1 + 4a_2 + a_3 = 3 \\ P(3) &= a_0 + 3a_1 + 2a_2 + 6a_3 = 5 \\ P(4) &= a_0 + 4a_1 + 2a_2 + a_3 = 1 \\ P(5) &= a_0 + 5a_1 + 4a_2 + 6a_3 = 6 \end{aligned}$$

   Notice that none of the coefficients are greater than 6 — we're always working in $GF(7)$! Thus the i^{th} term of $P(x)$ is always $a_i \times (x^i \bmod 7)$.

   Solving this system of linear equations will give us the coefficients found above. We can then easily check our work by plugging each i into

$$P(x) = 3 + 5x + 4x^2 + 6x^3 + 5x^4 \mod 7$$

   and verifying that we get out m_i in each case.

   (d) What is the minimum number of extra points Alice must send to Bob so that he can correctly reconstruct her message m?
   6 — we want to make sure that even if one packet is lost, we still have enough points to reconstruct a degree-4 polynomial, which means we need 5 points left after a loss of 1.

   (e) Suppose Alice evaluates $P(x)$ at the extra point $i = 6$. What is the polynomial evaluated at this new point?
   $P(6) =$
   We plug $x = 6$ into the polynomial found above:

$$P(6) = 3 + 6 \times 5 + 6^2 \times 4 + 6^3 \times 6 + 6^4 \times 5 \mod 7$$

   First we find $6^2 \bmod 7 = 36 \bmod 7 = 1$. Using this, we can find $6^3 \bmod 7 = 6^2 \times 6 \bmod 7 = 1 \times 6 \bmod 7 = 6$. Finally, $6^4 \bmod 7 = 6^2 \times 6^2 \bmod 7 = 1 \times 1 \bmod 7 = 1$. Plugging these values back in,

$$P(6) = 3 + 6 \times 5 + 1 \times 4 + 6 \times 6 + 1 \times 5 \mod 7$$

   From here we compute $6 \times 5 = 30 \equiv 2 \bmod 7$ and $6 \times 6 = 1 \bmod 7$:

$$P(6) = 3 + 2 + 4 + 1 + 5 \mod 7$$

   This is equivalent to

$$P(6) = 15 \bmod 7 = 1$$

   (f) Alice sends her final message: $c_1 = 2$, $c_2 = 3$, $c_3 = 5$, $c_4 = 1$, $c_5 = 6$, $c_6 = 1$. But, the second packet is dropped, so Bob only receives: $c_1 = 2$, $c_3 = 5$, $c_4 = 1$, $c_5 = 6$, $c_6 = 1$. Bob can correctly recover the second packet via polynomial interpolation.

   - True
   - False
     True, Bob still has 5 distinct points from the same degree-4 polynomial, so the polynomial can be recovered, and $P(2)$ can be recomputed.

   (g) Bob decides to solve a system of linear equations to recover the second packet. How many linear equations are in his system?
   There are 5 equations.

   (h) Bob's j^{th} linear equation is of the form $\sum_{i=0}^{4} g_i^{(j)} \cdot a_i = g_5^{(j)}$. What are the coefficients $g_i^{(1)}, g_i^{(2)}, \ldots, g_i^{(5)}$? Enter your answers in the form: $g^{(j)} = [g_4^{(j)}\ g_3^{(j)}\ g_2^{(j)}\ g_1^{(j)}\ g_0^{(j)}\ g_5^{(j)}]$.
   $g^{(1)} =$
   [1 1 1 1 1 2]. To find the $g_i^{(1)}$, we simply plug 1 into the expression for $P(x)$:

$$P(1) = 1^4 \times a_4 + 1^3 \times a_3 + 1^2 \times a_2 + 1 \times a_1 + a_0 = 2 \mod 7$$

   This simplifies to

$$a_4 + a_3 + a_2 + a_1 + a_0 = 2$$

   meaning our coefficients are all 1 and our result is 2.
   $g^{(2)} =$
   [4 6 2 3 1 5]. To find the $g_i^{(2)}$, we plug 3 into the expression for $P(x)$ (m_3 is the second m_i we received intact):

$$P(3) = 3^4 \times a_4 + 3^3 \times a_3 + 3^2 \times a_2 + 3 \times a_1 + a_0 = 5 \mod 7$$

   This simplifies to

$$4a_4 + 6a_3 + 2a_2 + 3a_1 + a_0 = 5$$

   $g^{(3)} =$
   [4 1 2 4 1 1]. To find the $g_i^{(3)}$, we plug in 4 into the expression for $P(x)$:

$$P(4) = 4^4 \times a_4 + 4^3 \times a_3 + 4^2 \times a_2 + 3 \times a_1 + a_0 = 1 \bmod 7$$

   This simplifies to

$$4a_4 + a_3 + 2a_2 + 4a_1 + a_0 = 1$$

   $g^{(4)} =$
   [2 6 4 5 1 6] To find the $g_i^{(4)}$, we plug in 5 into the expression for $P(x)$:

$$P(5) = 5^4 \times a_4 + 5^3 \times a_3 + 5^2 \times a_2 + 5 \times a_1 + a_0 = 6 \bmod 7$$

   This simplifies to

$$2a_4 + 6a_3 + 4a_2 + 5a_1 + a_0 = 6$$

   $g^{(5)} =$
   [1 6 1 6 1 1]

   (i) Bob solves this system by Gaussian elimination. He starts by subtracting equation 2 from equation 3 to get a new equation 3. What are the coefficients of the new equation 3? Again, enter your answer in the form: $g^{(j)} = [g_4^{(j)}\ g_3^{(j)}\ g_2^{(j)}\ g_1^{(j)}\ g_0^{(j)}\ g_5^{(j)}]$.
   $g^{(3)} = [0\ 2\ 0\ 1\ 0\ 3]$

   (j) Bob continues with Gaussian elimination, and solves for $a_4, \ldots, a_0$. What are the coefficients $a_4, \ldots, a_0$? Enter your answer in the form: $a = [a_4\ a_3\ a_2\ a_1\ a_0]$.
   $a =$
   [5 6 4 5 3]

   (k) Bob evaluates his polynomial to decode the dropped packet m_2 as:
   $P(2) =$
   [5 6 4 5 3]

   (l) Bob could have still correctly decoded Alice's message if both c_2 and c_6 were dropped.

   - True
   - False

Decoding with General Errors

2. Suppose Alice wants to send Bob a message of $n = 3$ packets and she wants to guard against $k = 1$ corrupted packets. Further assume that packets can be coded up as integers between 0 and 6.

   (a) Alice can work over $GF(q)$. What is the minimum prime q can be?
   $q =$
   Recall that $q > n + 2k$.
   7

   (b) Suppose Alice wants to send Bob the message $m = (m_1, m_2, m_3)$. What is the maximum degree of the unique polynomial described by these points, which are of the form (i, m_i)?
   $d =$
   2

   (c) What is the minimum number of extra points Alice must send to Bob so that he can correctly reconstruct her message m?
   2

   (d) Bob receives a message $r = (3, 3, 3, 2, 0)$. In order to check whether there the message is corrupted, Bob needs to solve $Q(x) = r_iE(x)$, where $Q(x) = P(x)E(x)$, $P(x)$ is the original polynomial for sending the message, and $E(x)$ is the error-locator polynomial in the Berlekamp-Welch algorithm.

   What is the degree of $Q(x)$?
   3
   What is the degree of $E(x)$?
   1
   What does $E(x)$ look like?

   - $x + b_0$
   - $b_1x + b_0$

   By letting $x = i, 1 < i < 5$ in $Q(x) = r_iE(x)$, we obtain the following system of linear equations:

$$\begin{aligned} a_3 + a_2 + a_1 + a_0 &= 3 + 3b_0 && (1) \\ a_3 + 4a_2 + 2a_1 + a_0 &= 6 + 3b_0 && (2) \\ 6a_3 + 2a_2 + 3a_1 + a_0 &= 2 + 3b_0 && (3) \\ a_3 + 2a_2 + 4a_1 + a_0 &= 1 + 2b_0 && (4) \\ 6a_3 + 4a_2 + 5a_1 + a_0 &= 0 && (5) \end{aligned}$$

   What is the solution of $a_0 - a_3$ and b_0?
   $a_0 =$
   $a_0 = 0$
   $a_1 =$
   $a_1 = 1$
   $a_2 =$
   $a_2 = 3$
   $a_3 =$
   $a_3 = 3$
   $b_0 =$
   $b_0 = 6$

   (e) What is the original polynomial $P(x) = ax^2 + bx + c$?
   $a =$
   $a = 3$. For full solution, see solution to c.
   $b =$
   $b = 6$. For full solution, see solution to c.
   $c =$
   $c = 0$. We solve for the coefficients a, b, and c by solving the equation

$$P(x) = ax^2 + bx + c = \frac{Q(x)}{E(x)}$$

   We plug in the expressions found for $Q(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ and $E(x) = x + b_0$:

$$P(x) = \frac{3x^3 + 3x^2 + x}{x + 6} \mod 7$$

   Carrying out the long division mod7, we find

$$P(x) = 3x^2 + 6x$$

   (f) Which packet is corrupted?

   - 1st
   - 2nd
   - 3rd

   To find out which packet was corrupted, we find the index i for which $P(i)$ differs from r_i. When $i = 1$, we see that $P(i) = 3 + 6 \bmod 7 = 2$, but $r_1 = 3$.

   (g) What is the orignal value?
   As stated above, the original answer is 2.