Error-correcting codes

1. **Find a polynomial of degree at most 2 which passes through the points $(1,2),(2,5),(3,12)$. Use linear equations as opposed to Lagrangian interpolation.** We use the linear equations below to solve for a,b and c:

$$\begin{aligned} a_2+a_1+a_0 &= 2 \\ 4a_2+2a_1+a_0 &= 5 \\ 9a_2+3a_1+a_0 &= 12 \end{aligned}$$

We obtain the first equation by plugging in 1 to $a_2x^2+a_1x+a_0$ and setting it equal to 2, as given by the first point $(1,2)$. We use a similar method to obtain the last two equations. After solving, we obtain $a_2=2, a_1=-3$ and $a_0=3$, giving the polynomial $2x^2-3x+3$.

2. **When working in $GF(11)$, we want to send a message $(5,2)$. The message we send might get corrupted at $k=1$ place.**

   (a) **First find a polynomial $P(x)$ such that $P(1)=5, P(2)=2$.** Using the same technique as above, we obtain the degree 1 polynomial $P(x)=8x+8$.

   (b) **You should be sending more than two characters to ensure that you can recover from 1 general error. How many should you send?** You need to send $n+2k$ characters, where n is the length of the original message (2) and $k=1$, so you need to send 4 characters.

   (c) **Assuming the answer to the previous question was m, find out the actual message you'll be sending by evaluating $P(x)$ at $x=1,2,\ldots,m$.** We'll evaluate $P(x)$ at $x=1,2,3,4$. $P(1)$ and $P(2)$ are given above. $P(3)=10$ and $P(4)=7$. The actual message will be $5,2,10,7$.

   (d) **Assume that the message you send gets corrupted at the 2nd character. Increase the value you computed by 1 to get the corrupted character. Remember that the person receiving the message does not know that it was the 2nd character that got corrupted. What will the error-locating polynomial be here?** The error locating polynomial is $E(x)=x-2$.

   (e) **To decode the message you set-up the polynomial $Q(x)$ as $P(x)E(x)$ where P is the original polynomial and E is the error-locating polynomial. Remember that the receiver does not know what any of these polynomials are yet. What is the degree of Q?** The degree of $Q(x)$ is $n+k-1$. In this example, $n=2$ and $k=1$, so the degree is 2.

   (f) **Remember that the equation $Q(x)=r_xE(x)$ is satisfied where $x=1,\ldots,m$ and r_x is the x-th character received. Why is this true? Give a short justification.** If no error occurs, then since $Q(x)=P(x)E(x)$ and $P(x)=r_x$, the equation is satisfied. If an error occurs, then $Q(x)=0$ as does $E(x)$.

(g) **Now the receiver writes $Q(x)$ and $E(x)$ in the most general format possible (i.e. with arbitrary coefficients). Write $Q(x)$ and $E(x)$ replacing their coefficients with variables. Remember that even though the receiver knows nothing about the message yet, he knows one of the coefficients of $E(x)$. What is that coefficient?** Let $Q(x) = a_2x^2 + a_1x + a_0$ and $E(x) = x + b_0$- the receiver knows that the coefficient of x is 1.

(h) **Now write down the system of linear equations corresponding to $Q(x) = r_xE(x)$. The variables are the coefficients of Q and E.** The first equation will be $a_2 + a_1 + a_0 = 5(1 + b_0)$, which simplifies to $a_2 + a_1 + a_0 + 6b_0 = 5$. We can repeat this process for $x = 2, 3, 4$ to obtain the following equations:

$$\begin{aligned} a_2 + a_1 + a_0 + 6b_0 &= 5 \\ 4a_2 + 2a_1 + a_0 + 8b_0 &= 6 \\ 9a_2 + 3a_1 + a_0 + b_0 &= 8 \\ 5a_2 + 4a_1 + a_0 + 4b_0 &= 6 \end{aligned}$$

(i) **Solve the linear system. Did you get the error-locating polynomial you expected?** After solving, we obtain $b_0 = -2$ and $a_2 = 8, a_1 = 3, a_0 = 6$. Hence $Q(x) = 8x^2 + 3x + 6$ and $E(x) = x - 2$.

(j) **How would one go from knowing E and Q to finding P?** Since $Q(x) = P(x)E(x)$, we can compute $P(x) = \frac{Q(x)}{E(x)}$.

3. **What happens in the error-correcting method if there are actually no errors? Try the previous problem but don't corrupt the 2nd character.** Now our system of equations is:

$$\begin{aligned} a_2 + a_1 + a_0 + 6b_0 &= 5 \\ 4a_2 + 2a_1 + a_0 + 9b_0 &= 4 \\ 9a_2 + 3a_1 + a_0 + b_0 &= 8 \\ 5a_2 + 4a_1 + a_0 + 4b_0 &= 6 \end{aligned}$$

After solving, you can see that we have a degenerate system of linear equations, and b_0 can be any value.