1. How many polynomials?

Let $P(x)$ be a polynomial of degree 2 over GF(5). As we saw in lecture, we need $d+1$ distinct points to determine a unique d-degree polynomial.

1. Assume that we know $P(0)=1$, and $P(1)=2$. Now we consider $P(2)$. How many values can $P(2)$ have? List all possible polynomials of degree 2. How many distinct polynomials are there?
   Solution: 5 polynomials, each for different values of $P(2)$.
2. Now assume that we only know $P(0)=1$. We consider $P(1)$, and $P(2)$. How many different $(P(1),P(2))$ pairs are there? How many different polynomials are there?
   Solution: Now there are 5^2 different polynomials.
3. How many different polynomials of degree d over $GF(p)$ are there if we only know k values, where $k \leq d$?
   Solution: p^{d+1-k} different polynomials. For $k=d+1$, there should only be 1 polynomial.

2. Erasures: Lagrange or Linear System

Say we do the erasure coding scheme discussed in note 10, where a three packet message is sent using a polynomial $P(x)$, where $P(0)=m_1, P(1)=m_2$, and $P(2)=m_3$, and $P(3)$ and $P(4)$ are also sent. The channel loses $P(0)$ and $P(4)$.

In this exercise, we will try to find the polynomial $P(x)$ of degree at most 2 with coefficients in GF(5) such that $P(1)=2 \pmod 5$, $P(2)=4 \pmod 5$, and $P(3)=3 \pmod 5$ and recover the original message.

1. Find the $\Delta_i(x)$ polynomials for $i \in \{1,2,3\}$.
   Solution:

$$\begin{aligned}
\Delta_1(x) &= \frac{(x-2)(x-3)}{(1-2)(1-3)} = 3x^2+3 \\
\Delta_2(x) &= \frac{(x-1)(x-3)}{(2-1)(2-3)} = 4x^2+4x+2 \\
\Delta_3(x) &= \frac{(x-1)(x-2)}{(3-1)(3-2)} = 3x^2+x+1
\end{aligned}$$

2. Combine the Δ_is with the right coefficients to find the polynomial $P(x)$.
   Solution: We have $P(x) = 2\Delta_1(x)+4\Delta_2(x)+3\Delta_3(x) = x^2+4x+2$.
3. Now we will try a different approach. Write the polynomial $P(x)$ as $c_0+c_1x+c_2x^2$. Treating c_is as variables, what do the equations $P(1)=2 \pmod 5$, $P(2)=4 \pmod 5$, and $P(3)=3 \pmod 5$ tell us about the c_is?

Solution: They give us a system of linear equations.

$$\begin{aligned} P(1) = 2 &\implies c_0 + c_1 + c_2 = 2 \pmod 5 \\ P(2) = 4 &\implies c_0 + 2c_1 + 4c_2 = 4 \pmod 5 \\ P(3) = 3 &\implies c_0 + 3c_1 + 9c_2 = 3 \pmod 5 \end{aligned}$$

4. Solve the system of equations you got from the last part to solve for the c_is. What is the resulting polynomial $P(x)$?

   Solution: The answer given by the system of linear equations is the same as the one gotten by Lagrange; i.e. $c_0 = 2, c_1 = 4, c_2 = 1$.

5. What was the original message that was sent?

   Solution: The message was $2,2,4$, since $P(0) = 2$, $P(1) = 2$, and $P(2) = 4$.

3. Berlekamp-Welch for general errors

Suppose you want to send your friend a length $n = 3$ message, m_0, m_1, m_2, with advice on a cool place to visit. Unfortunately your only way to communicate with her is via a channel with the possibility for $k = 1$ error. We will work mod 13, so we can encode 13 letters as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

You encode the message by finding the degree ≤ 2 polynomial $P(x)$ that passes through $(0, m_0)$, $(1, m_1)$, and $(2, m_2)$, and then send your friend the five packets $P(0), P(1), P(2), P(3), P(4)$ over the noisy channel. The message your friend receives is

$$\text{CELJH} \Rightarrow 2,4,11,9,7 = r_0, r_1, r_2, r_3, r_4$$

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:

   $$\begin{aligned} d &= 2(0+e) \\ a+b+c+d &= 4(1+e) \\ 8a+4b+2c+d &= 11(2+e) \\ 27a+9b+3c+d &= 9(3+e) \\ 64a+16b+4c+d &= 7(4+e) \end{aligned}$$

Since we are working mod 13, this is equivalent to:

$$\begin{aligned} d &= 2e \\ a+b+c+d &= 4+4e \\ 8a+4b+2c+d &= 9+11e \\ 1a+9b+3c+d &= 1+9e \\ 12a+3b+4c+d &= 2+7e \end{aligned}$$

Solution, which students do not need to find by hand:
$a = -91/82, b = -108/41, c = 211/82, d = -212/41, e = -106/41 (mod 13)$
$a \equiv 0, b \equiv 9 \cdot 7 \equiv 11, c \equiv 3 \cdot 10 \equiv 4, d \equiv 9 \cdot 7 \equiv 11 (mod 13)$

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

$$Q(x) = 0x^3 + 11x^2 + 4x + 11 = 11x^2 + 4x + 11$$

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

$$d = 11 = 2e \quad \Rightarrow \quad e = 11 \cdot 7 = 77 \equiv 12 \text{ mod } 13$$

This means that
$$E(x) = x + 12 \equiv x - 1 \quad \text{mod } 13.$$

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 (and awesome) message that you sent your friend.
Solution: Using polynomial division, we divide $Q(x) = 11x^2 + 4x + 11$ by $E(x) = x - 1$:

$$P(x) = 0x^2 + 11x + 2 = 11x + 2$$

Then $P(1) = 11 + 2 \equiv 0 (mod 13)$. This means that our original message was

$$2, 0, 11 \quad \Rightarrow \quad \text{CAL}$$