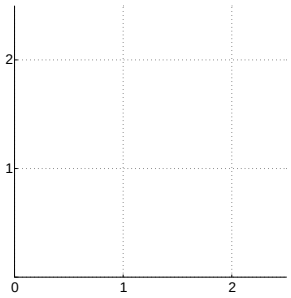
CS 70 Discrete Mathematics and Probability Theory
Summer 2015 Chung-Wei Lin Discussion 3C

1. Visualizing Error Correction

Alice wants to send a message of 2 packets to Bob, and wants to guard against 1 lost packet. So working over $GF(3)$, she finds the unique polynomial $P(x)$ that passes through the points she wants to send, and sends Bob her augmented message of 3 packets: $(0,P(0)),(1,P(1)),(2,P(2))$.

One packet is lost, so Bob receives the following packets: $(0,2),(2,0)$.

(a) Plot the points represented by the packets Bob received on the grid below.



(b) Draw in the unique polynomial $P(x)$ that connects these two points.

(c) By visual inspection, find the lost packet $(1,P(1))$.

$P(x) = -x+2$; the lost packet is $(1,1)$. You should try another case where the received packets are $(0,2),(2,1)$ and see what happens.

2. Erasure Warm-Up

Working over $GF(q)$, you want to send your friend a message of $n = 4$ packets and guard against 2 lost packets. What is the minimum q you can use? What is the maximum degree of the unique polynomial that describes your message?

To guard against 2 lost packets, you want to send $4+2=6$ packets. Since we want q prime, the minimum it can be is 7. Since you have 4 points, your polynomial needs to be degree 3.

3. Aliens, Oh My!

Alice wants to send a plea for help to an alien space ship that is hovering near her city. She knows that at their current distance of 7 miles above ground, no more than 3 general errors can occur during transmission. If she sends a message of length 15, how long must her original message be?

The length of the encrypted message, m, is 15, and number of errors guarded against, k, is 3. Since $m = n+2k$, n, the length of the original message, is 9 packets.

4. Where Are My Packets?

Alice wants to send the message (c_0,c_1,c_2) to Bob, where each $c_i \in \{0,1,2,3,4\}$. She encodes it as a polynomial P of degree ≤ 2 over $GF(5)$ such that $P(0) = c_0$, $P(1) = c_1$, and $P(2) = c_2$, 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.

(a) Find the multiplicative inverses of $1,2,3$ and 4 modulo 5.

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

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

$$\begin{aligned}
\Delta_0 &= \frac{(x-3)(x-4)}{(0-3)(0-4)} = \frac{x^2-7x+12}{(-3)(-4)} = 3(x^2+3x+2) = 3x^2+4x+1;\\
\Delta_3 &= \frac{(x-0)(x-4)}{(3-0)(3-4)} = \frac{x^2-4x}{(3)(-1)} = 3(x^2+x) = 3x^2+3x;\\
\Delta_4 &= \frac{(x-0)(x-3)}{(4-0)(4-3)} = \frac{x^2-3x}{(4)(1)} = 4(x^2+2x) = 4x^2+3x.
\end{aligned}$$

Thus, our original polynomial P is

$$\begin{aligned}
4\Delta_0+1\Delta_3+2\Delta_4 &= 4(3x^2+4x+1)+(3x^2+3x)+2(4x^2+3x)\\
&= (2x^2+x+4)+(3x^2+3x)+(3x^2+x)\\
&= 3x^2+4
\end{aligned}$$

Linear equation way: Writing $P(x)=a_2x^2+a_1x+a_0$, we solve for the a_i's by solving the linear equation

$$\begin{bmatrix} 0 & 0 & 1\\ 9 & 3 & 1\\ 16 & 4 & 1 \end{bmatrix}\begin{bmatrix} a_2\\ a_1\\ a_0 \end{bmatrix} = \begin{bmatrix} 4\\ 1\\ 2 \end{bmatrix}$$

This gives the equation $\frac{1}{2}x^2-\frac{5}{2}x+4$, which, in the modulo 5 world, means $P(x)=3x^2+4$.

(c) Recover Alice's original message.

To recover (c_0,c_1,c_2), we compute $P(0)=4$, $P(1)=2$, and $P(2)=1$.

5. More Erasures!

Consider the alphabet $A=0$, $B=1$, $C=2$, $D=3$, $E=4$. Suppose a message of length 3 is sent using the error correction scheme discussed in class over $GF(5)$. If you receive the following packets, what was the original message?

This problem is the same mechanics as the previous problem, but with less hand-holding.

(a) C _ A A

Let's try the index starting from 1. The packets received are $(1,2),(3,0),(4,0)$ (you can also solve it by the index starting from 0). We use Lagrange Interpolation to find the unique degree 2 polynomial that goes through these points:

$$\Delta_1(x) \equiv \frac{(x-3)(x-4)}{(-2)(-3)} \equiv \frac{(x-3)(x-4)}{6} \equiv \frac{(x-3)(x-4)}{1} \equiv (x-3)(x-4).$$

Notice that the y values of the second and third points are 0, so when we compute the polynomial, it won't matter what $\Delta_3(x)$ and $\Delta_4(x)$ are, so no need to compute them. The polynomial is then

$$P(x) = 2\Delta_1(x) = 2(x-3)(x-4) \equiv 2x^2 + x + 4,$$

and we plug in $x = 2$ to find the lost packet: $P(2) = 4$, so the missing letter is E.

(b) _ A C C

Let's try the index starting from 0. The packets received are $(1,0),(2,2),(3,2)$. We use Lagrange Interpolation to find the unique degree 2 polynomial that goes through these points. We skip finding $\Delta_0(x)$ since we know it will just get multiplied by a 0 y value.

$$\Delta_1(x) \equiv \frac{(x-1)(x-3)}{(1)(-1)} \equiv \frac{(x-1)(x-3)}{4} \equiv 4(x-1)(x-3) \equiv 4x^2 + 4x + 2;$$
$$\Delta_2(x) \equiv \frac{(x-1)(x-2)}{(2)(1)} \equiv \frac{(x-1)(x-2)}{2} \equiv 3(x-1)(x-2) \equiv 3x^2 + x + 1.$$

The polynomial is then

$$P(x) = 2(4x^2 + 4x + 2) + 2(3x^2 + x + 1) \equiv 3x^2 + 3x + 4 + x^2 + 2x + 2 \equiv 4x^2 + 1,$$

and we plug in $x = 0$ to find the lost packet: $P(0) = 1$, so the missing letter is B.

(c) Can you determine the original message if you only receive C E _ _? Either find the original message or explain why you can't.

You can't! Because only 4 packets were sent, we can only tolerate $4 - 3 = 1$ erasures to recover a message of length 3.