CS 70 Discrete Mathematics and Probability Theory
Spring 2015 Vazirani Discussion 7W

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?

   Answer: 9

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

   Answer: 6

3. How many general errors can Bob recover from?

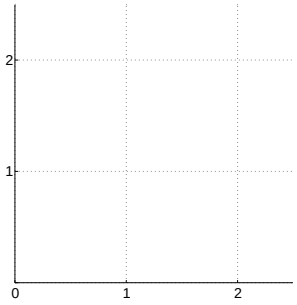
   Answer: 3

2. Visualizing erasure errors

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: $(0,2),(2,0)$.

1. Plot the points represented by the packets Bob received on the grid to the right.
2. Draw in the unique polynomial $P(x)$ that connects these two points.
3. By visual inspection, find the lost packet $(1,P(1))$.

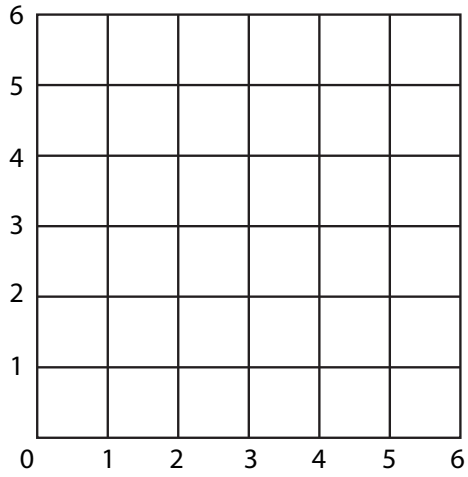


Answer: The lost packet is $(1,1)$.

3. Visualizing general errors

Alice wants to send Bob the same two packets as in the previous question, except that this time the channel may have general errors. To allow for stronger error correction she chooses to work in $GF(7)$. Let P denote the unique degree-1 polynomial that encodes Alice's message.

1. Plot P on the grid below.



Answer: $P(x) = 6x + 2$

2. Suppose Alice sends Bob the following four packets: $(0, P(0)), (1, P(1)), (2, P(2)), (3, P(3))$. First, convince yourself that Bob can recover from any one general error. Provide an example that shows that Bob may not be able to recover from more than one general error.

   Answer: For example, $(1,3), (2,4)$.

3. Suppose Alice sends Bob the following six packets: $(0, P(0)), (1, P(1)), (2, P(2)), (3, P(3)), (4, P(4)), (5, P(5))$. Convince yourself that Bob can recover from any two general errors. Provide an example that shows that Bob may not be able to recover from more than two general errors.

   Answer: For example, $(1,3), (2,4), (3,5)$.

4. 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:

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

Hector encodes 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 sends you the five packets $P(0), P(1), P(2), P(3), P(4)$ over a noisy channel. The message you receive is

$$\text{DHACK} \Rightarrow 3, 7, 0, 2, 10 = r_0, r_1, r_2, r_3, r_4$$

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.

   Answer: 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:

$$\begin{aligned} d &= 3(0+e) \\ a+b+c+d &= 7(1+e) \\ 8a+4b+2c+d &= 0(2+e) \\ 27a+9b+3c+d &= 2(3+e) \\ 64a+16b+4c+d &= 10(4+e) \end{aligned}$$

Since we are working mod 11, this is equivalent to:

$$\begin{aligned} d &= 3e \\ a+b+c+d &= 7+7e \\ 8a+4b+2c+d &= 0 \\ 5a+9b+3c+d &= 6+2e \\ 9a+5b+4c+d &= 7+10e \end{aligned}$$

2. Ask your GSI for $Q(x)$. What is $E(x)$? Where is the error located?

   Answer: 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:

   $$d = 8 = 3e \quad \Rightarrow \quad e = 8 \cdot 4 = 32 \equiv 10 \bmod 11$$

   This means that

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

   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.

   Answer: 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 $P(1) = 3 + 9 + 3 = 15 \equiv 4 \bmod 11$. This means that our original message was

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