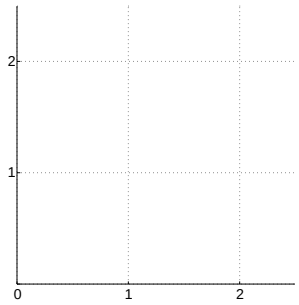
CS 70 Discrete Mathematics and Probability Theory
Summer 2016 Dinh, Psomas, and Ye Discussion 8A

First two questions are rehashes of 7D. Skip if covered already.

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

1. Plot the points represented by the packets Bob received on the grid below.



2. Draw in the unique polynomial $P(x)$ that connects these two points.
3. By visual inspection, find the lost packet $(1,P(1))$.

2. Where are my packets?

Alice wants to send the message (a_0,a_1,a_2) to Bob, where each $a_i \in \{0,1,2,3,4\}$. She encodes it as a polynomial P of degree ≤ 2 over $GF(5)$ such that $P(0)=a_0$, $P(1)=a_1$, and $P(2)=a_2$, 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.

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

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

3. Berlekamp–Welch algorithm

In this question we will go through an example of error-correcting codes with general errors. We will send a message (m_0, m_1, m_2) of length $n = 3$. We will use an error-correcting code for $k = 1$ general error, doing arithmetic modulo 5.

(a) Suppose $(m_0, m_1, m_2) = (4, 3, 2)$. Use Lagrange interpolation to construct a polynomial $P(x)$ of degree 2 (remember all arithmetic is $\bmod 5$) so that $(P(0), P(1), P(2)) = (m_0, m_1, m_2)$. Then extend the message to lengeth $n + 2k$ by appending $P(3), P(4)$. What is the polynomial $P(x)$ and what is the message $(c_0, c_1, c_2, c_3, c_4) = (P(0), P(1), P(2), P(3), P(4))$ that is sent?

(b) Suppose the message is corrupted by changing c_0 to 0. We will locate the error using the Berlekamp–Welsh method. Let $E(x) = x + b_0$ be the error-locator polynomial, and $Q(x) = P(x)E(x) = a_3x^3 + a_2x^2 + a_1x + a_0$ be a polynomial with unknown coefficients. Write down the system of linear equations (involving unknowns a_0, a_1, a_2, a_3, b_0) in the Berlekamp–Welsh method. You need not solve the equations.

(c) The solution to the equations in part (b) is $b_0 = 0, a_0 = 0, a_1 = 4, a_2 = 4, a_3 = 0$. Show how the recipient can recover the original message (m_0, m_1, m_2).

4. **Po(l)lynomial Pranks** Alex and Barb talk to each other via Polly. Knowing her tendency to prank, they use polynomials to ensure they can recover their original messages in case she decides to erase (i.e., replace with a blank) or change some of the packets.

    1. Never the one to run out of ideas, Polly adds an integer offset c to the x values of the packets instead, i.e., each packet (x,y) becomes $(x+c,y)$. Will Alex and Barb be able to get their original messages back without knowing c beforehand? Do they need to modify their scheme to handle this prank? If so, describe the method briefly.

    2. Realizing what you just showed, Polly adds the integer offset c to the y values of the packets instead, i.e., each packet (x,y) becomes $(x,y+c)$. Can Alex and Barb get their original messages back using their current scheme? If not, propose a modified scheme that will work.

3. Polly changes her mind again. Adding a constant offset c is too simple. She now picks a random po(l)lynomial $N(x)$ of degree $\leq d$ and adds it to the y values instead, i.e., each packet (x, y) becomes $(x, y + N(x))$. Note that $N(x)$ can have higher degree than $P(x)$. Suppose Alex and Barb know d, provide a scheme for them to reliably communicate using the minimum number of packets. You only need to give a brief justification.

4. Extend the scheme in part 3 to account for an additional k_e erasure errors. Does your scheme still use the minimum number of packets? If not, come up with a new scheme that does. You should give a brief justification.

5. Modify the scheme in part 4 to account for an additional k_g general errors instead of erasure errors.