1 Error-Correcting Polynomials

(a) Alice wishes to send a message to Bob as the coefficients of a degree 2 polynomial P. For a message $[m_1, m_2, m_3]$, she creates polynomial $P = m_1x^2 + m_2x + m_3$ and sends 5 packets: $(0, P(0)), (1, P(1)), (2, P(2)), (3, P(3)), (4, P(4))$. However, Eve interferes and changes one of the values of a packet before it reaches Bob. If Bob receives

$$(0,3),(1,0),(2,3),(3,0),(4,3),$$

and knows Alice's encoding scheme and that Eve changed one of the packets, can he still figure out what the original message was? If so find it as well as the x-value of the packet that Eve changed, if not, explain why he can not. (Work in mod 11.)

(b) After getting tired of decoding degree 2 polynomials, Bob convinces Alice to send messages using a degree 1 polynomial instead. To be on the safer side, Alice decides to continue to send 5 points on the polynomial even though it is only degree 1 (Alice makes sure to choose her message in such a way that it can be encoded in a polynomial of degree 1). She encodes and sends a length 5 message. Eve however, decides to change 2 of the packets. After Eve interferes, Bob receives $(0,-3),(1,-1),(2,x),(3,-3),(4,5)$. If Alice sent $(0,-3),(1,-1),(2,1),(3,3),$ $(4,5)$, for what values of x will Bob not be able to uniquely determine Alice's message? (Assume Bob knows that Eve changed 2 of the packets and **work in mod 13.**)

(c) Finally, Alice has a length 8 message to Bob. There are 2 communication channels available. When n packets are fed through channel A, the channel will only deliver 5 packets (picked at random). Similarly, channel B will only deliver 5 packets (picked at random), but it will also corrupt (change the value) of one of the delivered packets. Each channel will only work if at least 10 packets are sent through it. Using each of the 2 channels once, how can Alice send the message to Bob?

Solution:

(a) We can use Berlekamp and Welch. We have: $Q(x) = P(x)E(x)$. $E(x)$ has degree 1 since we know we have at most 1 error. $Q(x)$ is degree 3 since $P(x)$ is degree 2. We can write a system of linear equations and solve:

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

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

$$\begin{aligned} d &= -3e \\ a+b+c+d &= 0 \\ 8a+4b+2c+d &= 6-3e \\ 5a+9b+3c+d &= 0 \\ 9a+5b+4c+d &= 1-3e \end{aligned}$$

Solving yields:

$$Q(x) = x^3+5x^2+5, E(x) = x-2$$

To find $P(x)$ we divide $Q(x)$ by $E(x)$ and get $P(x) = x^2+7x+3$. So Alice's message is $m_1 = 1, m_2 = 7, m_3 = 3$.

Alternative solution: Since we have 5 points, we have to find a polynomial of degree 2 that goes through 4 of those points. The point that the polynomial does not go through will be the packet that Eve changed. Since 3 points uniquely determine a polynomial of degree 2, we can pick 3 points and check if a 4th point goes through it. (It may be the case that we need to try all sets of 3 points.) We pick the points $(0,3),(1,0),(3,0)$. Lagrange interpolation can be used to create the polynomial but we can see that for the polynomial that goes through these 3 points, it has 0's at $x = 1$ and $x = 3$. Thus the polynomial is $(x-1)(x-3) = x^2-4x+3 \pmod{11} = x^2+7x+3 \pmod{11}$. We then check to see if the this polynomial goes through one of the 2 points that we didn't use. Plugging in 4 for x, we get 3. The packet that Eve changed is the point that our polynomial does not go through which has x-value 2. Alice's original message was $m_1 = 1, m_2 = 7, m_3 = 3$.

(b) Since Bob knows that Eve changed 2 of the points, the 3 remaining points will still be on the degree 1 polynomial that Alice encoded her message on. Thus if Bob can find a degree 1 polynomial that passes through at least 3 of the points that he receives, he will be able to uniquely recover Eve's message. The only time that Bob cannot uniquely determine Alice's message is if there are 2 polynomials with degree 1 that pass through 3 of the 5 points that he receives. Since we are working with degree 1 polynomials, we can plot the points that Bob receives and then see which values of x will cause 2 sets of 3 points to fall on a line. $(0,-3),(1,-1),(4,5)$ already fall on a line. If $x = -2$, $(1,-1),(2,-2),(3,-3)$ also falls on a line. If $x = -3$, $(0,-3),(2,-3),(3,-3)$ also falls on a line. If $x = 1$, $(0,-3),(2,1),(4,5)$ falls on the original line, so here Bob can decode the message. If $x = 2$, $(2,2),(3,-3),(4,5)$

also falls on a line. So if $x = -3, -2, 2$, Bob will not be able to uniquely determine Alice's message.

(c) Channel A will deliver 5 packets so we can send a message of length 5 encoded on a polynomial of degree 4 though it. If we send 10 points though channel A, it doesn't matter which 5 points bob gets, he will still be able to reconstruct our degree 4 polynomial. Since the channel B has 1 general error, we can only send a message of length 3 encoded on a degree 2 polynomial through it. If we send 10 points, Bob will get 5 points to calculate a degree 2 polynomial with 1 general error, which he is able to do. Thus to send our length 8 message, we can send the character 1 - 5 through a channel A and the characters 6 - 8 through channel B.
Alternative Solution: Alice can interpolate a polynomial of degree 7 encoding the message of length 8. She sends 10 points from that polynomial through channel A and another 10 points from the same polynomial through channel B. Bob will receive 5 points from channel A and 5 points from channel B, with one of them corrupted. He can use Berlekamp Welch with $n = 8$ and $k = 1$ to recover the original polynomial. He retrieves the message by evaluating the polynomial on relevant points.

2 Berlekamp-Welch Algorithm with Fewer Errors

In class we derived how the Berlekamp-Welch algorithm can be used to correct k general errors, given $n+2k$ points transmitted. In real life, it is usually difficult to determine the number of errors that will occur. What if we have less than k errors? This is a follow up to the exercise posed in the notes.

Suppose Alice wants to send 1 message to Bob and wants to guard against 1 general error. She decides to encode the message with $P(x) = 4$ (on GF(7)) such that $P(0) = 4$ is the message she want to send. She then sends $P(0), P(1), P(2) = (4, 4, 4)$ to Bob.

(a) Suppose Bob receives the message $(4, 5, 4)$. Without performing Gaussian elimination explicitly, find $E(x)$ and $Q(x)$.

(b) Now, suppose there were no general errors and Bob receives the original message $(4, 4, 4)$. Show that the $Q(x), E(x)$ that you found in part (a) still satisfies $Q(i) = r_i E(i)$ for all $i = 0, 1, 2$.

(c) Verify that $E(x) = x$, $Q(x) = 4x$ is another possible set of polynomials that satisfies $Q(i) = r_i E(i)$ for all $i = 0, 1, 2$.

(d) Suppose you're actually trying to decode the received message $(4, 4, 4)$. Based on what you showed in the previous two parts, what will happen during row reduction when you try to solve for the unknowns?

(e) Prove that in general, no matter what the solution of $Q(x)$ and $E(x)$ are though, the recovered $P(x)$ will always be the same.

Solution:

(a) $E(x) = x - 1$ and $Q(x) = P(x)E(x) = 4x - 4$.

(b) This is true because there were no errors, so $P(i) = r_i$ for $i = 0, 1, 2$.

(c) Since $Q(x) = P(x)E(x)$ and $P(i) = r_i$ for $i = 0, 1, 2$, we must have $Q(i) = r_i E(i)$ for all $i = 0, 1, 2$.

(d) There are multiple solutions to the system of equations.

(e) Suppose we got two solutions $Q'(x), E'(x)$ and $Q(x), E(x)$. Since they are both solutions, by definition, we have $Q'(i) = r_i E'(i)$ and $Q(i) = r_i E(i)$ for $1 \leq i \leq n + 2k$. Therefore, $Q'(i)E(i) = Q(i)E'(i) = r_i E(i)E'(i)$. However, $Q'(x)E(x) - Q(x)E'(x)$ is a degree $n + 2k - 1$ polynomial, which is 0 at $n + 2k$ points. Thus, $Q'(x)E(x) = Q(x)E'(x)$ for all x, so we arrive at

$$\frac{Q'(x)}{E'(x)} = \frac{Q(x)}{E(x)}.$$

This proves that the final solution for $P(x)$ is the same.

3 Orpheus' Adventures in the Halls of Time

You're designing a new role-playing game for a mathematically themed production house. Your eccentric colleague comes to you with an idea for a key scene and he wants you to think about it.

The backstory is that the mortal Orpheus wants to gain knowledge of the dates of certain key events in the year to come: call these the prophecies of interest. He has heard that in the Halls of Time, these things are already known so he quests through the underworld until he comes upon them.

In the Halls of Time, he encounters the Guardians. They have access to the knowledge of the Fates.

The game behaves as follows. There are 12 guardians (corresponding to the 12 constellations of the Zodiac or the 12 months) and each knows all the prophecies, but they have a peculiar property. Half of them are honest and answer questions posed to them exactly. One quarter of them consider mortals to be beneath them and will simply say "Begone mortal!" And one quarter despise mortals and will answer maliciously.

But mortals do not know the secret forms of the guardians and so Orpheus doesn't know who he is talking to.

On this setting, Orpheus can only ask questions (he can invoke arithmetic operations in $GF(367)$ if he wants) whose answer is a number from $\{0, 1, 2, \ldots, 366\}$.

(The prophecies he wants are answers to questions like: "When will my child be born?" The answers can be viewed as numbers: 1, ..., 365 for the days in the coming year. 0 for the past. 366 to represent the future beyond this coming year. Fortunately for Orpheus, 367 happens to be prime.)

All guardians are good at math and can answer any question as long as the answer is from 0 to 366 (not limited to just a simple answer to a prophecy). Orpheus can only ask any individual guardian one question. After that, that particular guardian will magically leave the room. He gets to question all 12 guardians.

How many prophecies can Orpheus reliably extract from the 12 guardians? How can he do it? (Be explicit) Why will this work?

Solution:

Orpheus can reliably extract 3 prophecies.
Suppose the answers of the three prophecies Orpheus is interested are a_1, a_2 and a_3 (note that Orpheus does not know the answers in advance). Orpheus can ask the Guardians by either ways as follows:

- **Method 1:** Orpheus can ask the i-th Guardian to form a polynomial of degree≤ 2 over $GF(367)$ with a_1, a_2, a_3 as coefficients, i.e. $P(x) = a_3x^2 + a_2x + a_1$, and to tell him what is $P(i)$.
- **Method 2:** Orpheus can ask the i-th Guardian to form a polynomial $P(x)$ of degree≤ 2 over $GF(367)$ such that $P(1) = a_1, P(2) = a_2$ and $P(3) = a_3$, and to tell him what is $P(i)$.

Let r_i be the i-th answer Orpheus got from the Guardians. He knows that among all r_i's, there are only 9 valid answers because 3 of the Guardians will always answer 'Begone mortal'. Among the 9 valid answers, there are 3 malicious answers. Collecting all the answers r_i's from every Guardian, he can recover the polynomial $P(x)$ by ignoring the 3 missing answers and using Berlekamp-Welch algorithm with the remaining 9 answers (3 of them may be wrong).

If Orpheus uses **method 1**, he can find out a_1, a_2, a_3 by just looking at the coefficients of $P(x)$.
If Orpheus uses **method 2**, he can find out a_1, a_2, a_3 by $a_1 = P(1), a_2 = P(2), a_3 = P(3)$.

We can analogize the 12 answers as a message of 12 packets which subjects to $k_e = 3$ erasure errors and $k_g = 3$ general errors, so the above framework can recover a polynomial of degree at most $n = 12 - k_e - 2k_g = 3$.

4 Make Your Own Question

You must make your own question on this week's material and solve it.

5 Homework Process and Study Group

You must describe your homework process and study group in order to receive credit for this question.