CS 70 Discrete Mathematics and Probability Theory
Spring 2020 HW 6

Due: Friday, March 6, 2020 at 11:59 PM
Grace period until Sunday, March 8, 2020 at 11:59 PM

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?

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.

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?

4 Make Your Own Question

Make your own question on this week's material and solve it.

5 Homework Process and Study Group

Citing sources and collaborators are an important part of life, including being a student! We also want to understand what resources you find helpful and how much time homework is taking, so we can change things in the future if possible.

1. **What sources (if any) did you use as you worked through the homework?**
2. **If you worked with someone on this homework, who did you work with?** List names and student ID's. (In case of homework party, you can also just describe the group.)
3. **How did you work on this homework?** (For example, *I first worked by myself for 2 hours, but got stuck on problem 3, so I went to office hours. Then I went to homework party for a few hours, where I finished the homework.*)
4. **Roughly how many total hours did you work on this homework?**