CS 70 Discrete Mathematics and Probability Theory
Spring 2026 Sinclair, Song

HW 05

Due: Saturday, 2/28, 4:00 PM
Grace period until Saturday, 2/28, 6:00 PM
Remember to show your work for all problems!

Sundry

Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Equivalent Polynomials

Note 7
Note 8

This problem is about polynomials with coefficients in GF(p) for some prime $p \in \mathbb{N}$. We say that two such polynomials f and g are *equivalent* if $f(x) \equiv g(x) \pmod{p}$ for every $x \in \text{GF}(p)$.

(a) Show that $f(x) = x^{p-1}$ and $g(x) = 1$ are **not** equivalent polynomials under GF(p).

(b) Use Fermat's Little Theorem to find a polynomial with degree strictly less than 13 that is equivalent to $f(x) = x^{13}$ over GF(13); then find a polynomial with degree strictly less than 7 that is equivalent to $g(x) = 2x^{74} + 6x^7 + 3$ over GF(7).

(c) In GF(p), prove that whenever $f(x)$ has degree $\geq p$, it is equivalent to some polynomial $\tilde{f}(x)$ with degree $< p$.

2 Lagrange's Residents

Note 8

A group of humans has settled at the Earth–Moon L5 point, a Lagrange Point near earth. They have a message for their friends on Earth, and its your job to decode it.

A four packet message is sent using a degree 3 polynomial $P(x)$, where $P(0) = m_1$, $P(1) = m_2$, $P(2) = m_3$, and, $P(3) = m_4$. $P(4)$ and $P(5)$ are also sent.

Unfortunately, the channel lost $P(0)$ and $P(3)$, so the earthlings only received:

$(1,3), (2,7), (4,-90), (5,-335)$

Using Lagrange interpolation and a graphical calculator (eg. Desmos), recover $P(0)$ and $P(3)$ to unlock the space explorers' message.

3 Cal Football's Secrets

Note 8

After a tough defeat, the Cal Football team has created a new set of top-secret plays. They're worried about leaks, however, and have asked you to devise a secret sharing scheme to protect their strategy.

The team has one head coach, six assistant coaches, and thirty two players. All plays are encrypted and we know that:

- The head coach along with one assistant coach should be able to access the plays.
- The majority (4+) of assistant coaches should be able to access the plays.
- All of the players should be able to access the plays together.
- Sixteen players and two assistant coaches should be able to access the plays.

Design a secret sharing scheme to make this work.

4 Alice and Bob

Note 8
Note 9

(a) Alice decides that instead of encoding her message as the values of a polynomial, she will encode her message as the coefficients of a degree 2 polynomial $P(x)$. For her message $[m_1, m_2, m_3]$, she creates the polynomial $P(x) = m_1x^2 + m_2x + m_3$ and sends the five packets $(0, P(0))$, $(1, P(1))$, $(2, P(2))$, $(3, P(3))$, and $(4, P(4))$ to Bob. However, one of the packet y-values (one of the $P(i)$ terms; the second attribute in the pair) is changed by Eve before it reaches Bob. If Bob receives

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

and knows Alice's encoding scheme and that Eve changed one of the packets, can he recover the original message? If so, find it as well as the x-value of the packet that Eve changed. If he can't, explain why. Work in mod 7. Also, feel free to use a calculator or online systems of equations solver, but make sure it can work under mod 7.

(b) Bob gets tired of decoding degree 2 polynomials. He convinces Alice to encode her messages on a degree 1 polynomial. Alice, just to be safe, continues to send 5 points on her polynomial even though it is only degree 1. She makes sure to choose her message so that it can be encoded on a degree 1 polynomial. However, Eve changes two of the packets. Bob receives $(0,5)$, $(1,7)$, $(2,x)$, $(3,5)$, $(4,0)$. If Alice sent $(0,5)$, $(1,7)$, $(2,9)$, $(3,-2)$, $(4,0)$, for what values of x will Bob not uniquely be able to determine Alice's message? Assume that Bob knows Eve changed two packets. Work in mod 13. Again, feel free to use a calculator or graphing calculator software.

Hint: Observe that since Bob knows that Eve changed two packets, he's looking for a polynomial that passes through at least 3 of the given points. Think about what must happen in order for Bob to be unable to uniquely identify the original polynomial.

(c) Alice wants to send a length n message to Bob. There are two communication channels available to her: Channel X and Channel Y. Only 6 packets can be sent through channel X. Similarly, Channel Y will only deliver 6 packets, but it will also corrupt (change the value) of one of the delivered packets. Using each of the two channels once, what is the largest message length n Alice can send such that Bob so that he can always reconstruct the message?

5 Error-Correcting Codes

Note 9

(a) Recall from class the error-correcting code for erasure errors, which protects against up to k lost packets by sending a total of $n+k$ packets (where n is the number of packets in the original message). Often the number of packets lost is not some fixed number k, but rather a *fraction* of the number of packets sent. Suppose we wish to protect against a fraction α of lost packets (where $0 < \alpha < 1$). At least how many packets do we need to send (as a function of n and α)?

(b) Repeat part (a) for the case of general errors.