CS 70 Discrete Mathematics and Probability Theory
Fall 2022 Satish Rao and Babak Ayazifar

# HW 06

Due: —
Grace period until —

## 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 Error-Correcting Codes

(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 $\alpha$ of lost packets (where $0 < \alpha < 1$). At least how many packets do we need to send (as a function of $n$ and $\alpha$)?

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

## 2 Alice and Bob

(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 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.

(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.

(c) Alice wants to send a length 9 message to Bob. There are two communication channels available to her: Channel A and Channel B. When $n$ packets are fed through Channel A, only 6 packets, picked arbitrarily, are delivered. Similarly, Channel B will only deliver 6 packets, picked arbitrarily, 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 two channels once, provide a way for Alice to send her message to Bob so that he can always reconstruct it.

# 3 Error-Detecting Codes

Suppose Alice wants to transmit a message of $n$ symbols, so that Bob is able to *detect* rather than *correct* any errors that have occurred on the way. That is, Alice wants to find an encoding so that Bob, upon receiving the code, is able to either

(I) tell that there are no errors and decode the message, or

(II) realize that the transmitted code contains at least one error, and throw away the message.

Assuming that we are guaranteed a maximum of $k$ errors, how should Alice extend her message (i.e. by how many symbols should she extend the message, and how should she choose these symbols)? You may assume that we work in GF$(p)$ for very large prime $p$. Show that your scheme works, and that adding any lesser number of symbols is not good enough.

# 4 Secret Sharing with Spies

An officer stored an important letter in her safe. In case she becomes unreachable in battle, she decides to share the password (which is a number) with her troops. However, everyone knows that there are 3 spies among the troops, but no one knows who they are except for the three spies themselves. The 3 spies can coordinate with each other and they will either lie and make people not able to open the safe, or will open the safe themselves if they can. Therefore, the officer would like a scheme to share the password that satisfies the following conditions:

- When $M$ of them get together, they are guaranteed to be able to open the safe even if they have spies among them.
- The 3 spies must not be able to open the safe all by themselves.

Please help the officer to design a scheme to share her password. What is the scheme? What is the smallest $M$? Show your work and argue why your scheme works and any smaller $M$ couldn't work. (The troops only have one chance to open the safe; if they fail the safe will self-destruct.)