CS 70 Discrete Mathematics and Probability Theory
Fall 2025 Sabin, Hug

HW 06

Due: Saturday, 10/11, 4:00 PM
Grace period until Saturday, 10/11, 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.) If you used an LLM, place transcripts of your chats here.

1 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.

2 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?

3 Counting, Counting, and More Counting

Note 10

The only way to learn counting is to practice, practice, practice, so here is your chance to do so. Although there are many subparts, each subpart is fairly short, so this problem should not take any longer than a normal CS70 homework problem. You do not need to show work, and **Leave your answers as an expression** (rather than trying to evaluate it to get a specific number).

(a) How many ways are there to arrange n 1s and k 0s into a sequence?

(b) How many 19-digit ternary (0,1,2) bitstrings are there such that no two adjacent digits are equal?

(c) A bridge hand is obtained by selecting 13 cards from a standard 52-card deck. The order of the cards in a bridge hand is irrelevant.

(i) How many different 13-card bridge hands are there?

(ii) How many different 13-card bridge hands are there that contain no aces?

(iii) How many different 13-card bridge hands are there that contain all four aces?

(iv) How many different 13-card bridge hands are there that contain exactly 4 spades?

(d) Two identical decks of 52 cards are mixed together, yielding a stack of 104 cards. How many different ways are there to order this stack of 104 cards?

(e) How many 99-bit strings are there that contain more ones than zeros?

(f) An anagram of ALABAMA is any re-ordering of the letters of ALABAMA, i.e., any string made up of the letters A, L, A, B, A, M, and A, in any order. The anagram does not have to be an English word.

(i) How many different anagrams of ALABAMA are there?

(ii) How many different anagrams of MONTANA are there?

(g) How many different anagrams of ABCDEF are there if:

(i) C is the left neighbor of E

(ii) C is on the left of E (and not necessarily E's neighbor)

(h) We have 8 balls, numbered 1 through 8, and 25 bins. How many different ways are there to distribute these 8 balls among the 25 bins? Assume the bins are distinguishable (e.g., numbered 1 through 25).

(i) How many different ways are there to throw 8 identical balls into 25 bins? Assume the bins are distinguishable (e.g., numbered 1 through 25).

(j) We throw 8 identical balls into 6 bins. How many different ways are there to distribute these 8 balls among the 6 bins such that no bin is empty? Assume the bins are distinguishable (e.g., numbered 1 through 6).

(k) There are exactly 20 students currently enrolled in a class. How many different ways are there to pair up the 20 students, so that each student is paired with one other student? Solve this in at least 2 different ways. **Your final answer must consist of two different expressions.**

(l) How many solutions does $x_0 + x_1 + \cdots + x_k = n$ have, if each x must be a non-negative integer?

(m) How many solutions does $x_0 + x_1 = n$ have, if each x must be a *strictly positive* integer?

(n) How many solutions does $x_0 + x_1 + \cdots + x_k = n$ have, if each x must be a *strictly positive* integer?

4 Fermat's Wristband

Note 7
Note 10

Let p be a prime number and let n be a positive integer. We have beads of n different colors, where beads of the same color are indistinguishable from each other.

(a) We place p beads onto a string and have n colors available to us. How many ways are there to color the beads?

(b) How many sequences of p beads on the string are there that use at least two colors?

(c) Now we tie the two ends of the string together, forming a wristband. Two wristbands are equivalent if the sequence of colors on one can be obtained by rotating the beads on the other. (For instance, if we have $n = 3$ colors, red (R), green (G), and blue (B), then the length $p = 5$

necklaces RGGBG, GGBGR, GBGRG, BGRGG, and GRGGB are all equivalent, because these are all rotated versions of each other.)

How many non-equivalent wristbands are there now? Again, the p beads must not all have the same color. (Your answer should be a simple function of n and p.)

[*Hint*: Think about the fact that rotating all the beads on the wristband to another position produces an identical wristband.]

(d) Use your answer to part (c) to prove Fermat's little theorem.

[*Hint*: What must be true about your answer to part (c), in this context?]