CS 70 Discrete Mathematics and Probability Theory
Fall 2025 Sabin, Hug **HW 06**

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.

Solution: We will create polynomials that satisfy each condition and distribute points to coaches / players appropriately.

$S_i(x)$ will represent a polynomial with a y-intercept that contains the secret code for the plays.

First, we will create a polynomial that the coaches can use to get the secret code. $S_1(x)$ will be a degree 3 polynomial that coaches can use to access the secret code. The head coach will get three points on $S_1(x)$ and each assistant coach will get one point on $S_1(x)$. This allows our scheme to satisfy the first two requirements.

Next, we will create a polynomial that the players can use to get the secret code. $S_2(x)$ will be a degree 31 polynomial. Each player will get one point on $S_2(x)$. This allows our scheme to satisfy the third requirement.

Lastly, we need a way for two coaches and sixteen players to access the secret code. $S_3(x)$ will be a degree 1 polynomial. The players will be able to access one point on this polynomial $(1,a)$. The assistant coaches will be able to access another point on this polynomial $(2,b)$.

For the players to be able to access their point on $S_3(x)$, we will create $P_1(x)$, a degree 15 polynomial. $P_1(0) = a$. Each player will get one point and 16 players will be able to recover the polynomial, and therefore, the y-intercept (which stores their point, a).

For the assistant coaches to be able to access their point on $S_3(x)$, we will create $P_2(x)$, a degree 1 polynomial. $P_2(0) = b$. Each assistant coaches will get one point and 2 coaches will be able to recover the polynomial, and therefore, the y-intercept (which stores their point, b).

When the players have recovered a and the coaches have recovered b, they can recover $S_3(x)$ together using their two points. This allows our scheme to satisfy the final requirement.

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?

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 for the coefficients of $Q(x) = ax^3 + bx^2 + cx + d$ and $E(x) = (x - e)$ by writing the equation $Q(i) = r_i \cdot E(i)$ for $0 \le i \le 4$, where r_i is the ith received point.

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

Since we are working in mod 7, this is equivalent to:

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

Solving yields:

$$Q(x) = x^3+5x^2+5x+4, E(x) = x-3$$

To find $P(x)$ we divide $Q(x)$ by $E(x)$ and get $P(x) = x^2+x+1$. So Alice's message is $m_1 = 1, m_2 = 1, m_3 = 1$. The x-value of the packet Eve changed is 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 it goes through a 4th point. (It may be the case that we need to try all sets of 3 points.)

We pick the points $(1,3),(2,0),(4,0)$. 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 0s at $x = 2$ and $x = 4$. Thus the polynomial is $k(x-2)(x-4) = k(x^2-6x+8) \pmod 7 \equiv k(x^2+x+1) \pmod 7$. We find $k \equiv 1$ by plugging in the point $(1,3)$, so our polynomial is x^2+x+1. We then check to see if this polynomial goes through one of the 2 points that we didn't use. Plugging in 0 for x, we get 1. The packet that Eve changed is the point that our polynomial does not go through which has x-value 3. Alice's original message was $m_1 = 1, m_2 = 1, m_3 = 1$.

(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. $(0,5),(1,7),(4,0)$ already fall on a line. If $x = 6$, $(1,7),(2,6),(3,5)$ also falls on a line. If $x = 5$, $(0,5),(2,5),(3,5)$ also falls on a line. If $x = 9$, $(0,5),(2,9),(4,0)$ falls on the original line, so here Bob can decode the message. If $x = 10$, $(2,10),(3,5),(4,0)$ also falls on a line. So if $x = 6,5,10$, Bob will not be able to uniquely determine Alice's message.

(c) Channel X can send 6 packets, so the first 6 characters of the message can be send through Channel X. Channel Y can send 6 packets, but 1 will be corrupted, thus only a message of length 4 can be sent. Thus, a total of $m = 6+4 = 10$ characters can effectively sent.

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?

Solution:

(a) $\binom{n+k}{k}$

(b) There are 3 options for the first digit. For each of the next digits, they only have 2 options because they cannot be equal to the previous digit. Thus, $3 \cdot 2^{18}$

(c) (i) We have to choose 13 cards out of 52 cards, so this is just $\binom{52}{13}$.

(ii) We now have to choose 13 cards out of 48 non-ace cards. So this is $\binom{48}{13}$.

(iii) We now require the four aces to be present. So we have to choose the remaining 9 cards in our hand from the 48 non-ace cards, and this is $\binom{48}{9}$.

(iv) We need our hand to contain 4 out of the 13 spade cards, and 9 out of the 39 non-spade cards, and these choices can be made separately. Hence, there are $\binom{13}{4}\binom{39}{9}$ ways to make up the hand.

(d) If we consider the 104! rearrangements of 2 identical decks, since each card appears twice, we would have overcounted each distinct rearrangement. Consider any distinct rearrangement of the 2 identical decks of 52 cards and see how many times this appears among the rearrangement of 104 cards where each card is treated as different. For each identical pair (such as the two Ace of spades), there are two ways they could be permuted among each other (since $2! = 2$). This holds for each of the 52 pairs of identical cards. So the number 104! overcounts the actual number of rearrangements of 2 identical decks by a factor of 2^{52}. Hence, the actual number of rearrangements of 2 identical decks is $\frac{104!}{2^{52}}$.

(e) **Answer 1:** There are $\binom{99}{k}$ 99-bit strings with k ones and $99-k$ zeros. We need $k > 99-k$, i.e. $k \geq 50$. So the total number of such strings is $\sum_{k=50}^{99}\binom{99}{k}$.

This expression can however be simplified. Since $\binom{99}{k} = \binom{99}{99-k}$, we have

$$\sum_{k=50}^{99} \binom{99}{k} = \sum_{k=50}^{99} \binom{99}{99-k} = \sum_{l=0}^{49} \binom{99}{l}$$

by substituting $l = 99 - k$.

Now $\sum_{k=50}^{99} \binom{99}{k} + \sum_{l=0}^{49} \binom{99}{l} = \sum_{m=0}^{99} \binom{99}{m} = 2^{99}$. Hence, $\sum_{k=50}^{99} \binom{99}{k} = \frac{1}{2} \cdot 2^{99} = 2^{98}$.

Answer 2 (Symmetry): Since the answer from above looked so simple, there must have been a more elegant way to arrive at it. Since 99 is odd, no 99-bit string can have the same number of zeros and ones. Let A be the set of 99-bit strings with more ones than zeros, and B be the set of 99-bit strings with more zeros than ones. Now take any 99-bit string x with more ones than zeros i.e. $x \in A$. If all the bits of x are flipped, then you get a string y with more zeros than ones, and so $y \in B$. This operation of bit flips creates a one-to-one and onto function (called a bijection) between A and B. Hence, it must be that $|A| = |B|$. Every 99-bit string is either in A or in B, and since there are 2^{99} 99-bit strings, we get $|A| = |B| = \frac{1}{2} \cdot 2^{99}$. The answer we sought was $|A| = 2^{98}$.

(f) ALABAMA: The number of ways of rearranging 7 distinct letters and is 7!. In this 7 letter word, the letter A is repeated 4 times while the other letters appear once. Hence, the number 7! overcounts the number of different anagrams by a factor of 4! (which is the number of ways of permuting the 4 A's among themselves). Aka, we only want 1/4! out of the total rearrangements. Hence, there are $\frac{7!}{4!}$ anagrams.

MONTANA: In this 7 letter word, the letter A and N are each repeated 2 times while the other letters appear once. Hence, the number 7! overcounts the number of different anagrams by a factor of $2! \times 2!$ (one factor of 2! for the number of ways of permuting the 2 A's among themselves and another factor of 2! for the number of ways of permuting the 2 N's among themselves). Hence, there are $\frac{7!}{(2!)^2}$ different anagrams.

(g) (i) Suppose we consider CE to be a new letter X; with this replacement, the question is just to count the number of rearrangements of 5 distinct letters, which is 5!.

(ii) Symmetry: Let A be the set of all the rearranging of ABCDEF with C on the left side of E, and B be the set of all the rearranging of ABCDEF with C on the right side of E. $|A \cup B| = 6!, |A \cap B| = 0$. There is a bijection between A and B by construct a operation of exchange the position of C and E. Thus $|A| = |B| = \frac{6!}{2}$.

(h) Each ball has a choice of which bin it should go to. So each ball has 25 choices and the 8 balls can make their choices separately. Hence, there are 25^8 ways.

(i) Since there is no restriction on how many balls a bin needs to have, this is just the problem of throwing k identical balls into n distinguishable bins, which can be done in $\binom{n+k-1}{k}$ ways. Here $k = 8$ and $n = 25$, so there are $\binom{32}{8}$ ways.

(j) **Answer 1:** Since each bin is required to be non-empty, let's throw one ball into each bin at the outset. Now we have 2 identical balls left which we want to throw into 6 distinguishable bins. There are 2 cases to consider:

Case 1: The 2 balls land in the same bin. This gives 6 ways.

Case 2: The 2 balls land in different bins. This gives $\binom{6}{2}$ ways of choosing 2 out of the 6 bins for the balls to land in. Note that it is *not* 6×5 since the balls are identical and so there is no order on them.

Summing up the number of ways from both cases, we get $6 + \binom{6}{2}$ ways.

Answer 2: Since each bin is required to be non-empty, let's throw one ball into each bin at the outset. Now we have 2 identical balls left which we want to throw into 6 distinguishable bins. From class (see note 10), we already saw that the number of ways to put k identical balls into n distinguishable bins is $\binom{n+k-1}{k}$. Taking $k = 2$ and $n = 6$, we get $\binom{7}{2}$ ways to do this.

EXERCISE: Can you give an expression for the number of ways to put k identical balls into n distinguishable bins such that no bin is empty?

(k) **Answer 1:** Let's number the students from 1 to 20. Student 1 has 19 choices for her partner. Let i be the smallest index among students who have not yet been assigned partners. Then no matter what the value of i is (in particular, i could be 2 or 3), student i has 17 choices for her partner. The next smallest indexed student who doesn't have a partner now has 15 choices for her partner. Continuing in this way, the number of pairings is $19 \times 17 \times 15 \times \cdots \times 1 = \prod_{i=1}^{10}(2i-1)$.

Answer 2: Arrange the students numbered 1 to 20 in a line. There are 20! such arrangements. We pair up the students at positions $2i-1$ and $2i$ for i ranging from 1 to 10. You should be able to see that the 20! permutations of the students doesn't miss any possible pairing. However, it counts every different pairing multiple times. Fix any particular pairing of students. In this pairing, the first pair had freedom of 10 positions in any permutation that generated it, the second pair had a freedom of 9 positions in any permutation that generated it, and so on. There is also the freedom for the elements within each pair i.e. in any student pair (x, y), student x could have appeared in position $2i-1$ and student y could have appeared in position $2i$ and also vice versa. This gives 2 ways for each of the 10 pairs. Thus, in total, these freedoms cause $10! \times 2^{10}$ of the 20! permutations to give rise to this particular pairing. This holds for each of the different pairings. Hence, 20! overcounts the number of different pairings by a factor of $10! \times 2^{10}$. Hence, there are $\frac{20!}{10! \cdot 2^{10}}$ pairings.

Answer 3: In the first step, pick a pair of students from the 20 students. There are $\binom{20}{2}$ ways to do this. In the second step, pick a pair of students from the remaining 18 students. There are $\binom{18}{2}$ ways to do this. Keep picking pairs like this, until in the tenth step, you pick a pair of students from the remaining 2 students. There are $\binom{2}{2}$ ways to do this. Multiplying all these, we get $\binom{20}{2}\binom{18}{2}\ldots\binom{2}{2}$. However, in any particular pairing of 20 students, this pairing could have been generated in 10! ways using the above procedure depending on which pairs in the pairing got picked in the first step, second step, ..., tenth step. Hence, we have to divide the above number by 10! to get the number of different pairings. Thus there are $\binom{20}{2}\binom{18}{2}\cdots\binom{2}{2}/10!$ different pairings of 20 students.

You may want to check for yourself that all three methods are producing the same integer, even though they are expressed very differently.

(l) $\binom{n+k}{k}$. This is just n indistinguishable balls into $k+1$ distinguishable bins (stars and bars). There is a bijection between a sequence of n ones and k plusses and a solution to the equation: x_0 is the number of ones before the first plus, x_1 is the number of ones between the first and second plus, etc. A key idea is that if a bijection exists between two sets they must be the same size, so counting the elements of one tells us how many the other has. Note that this is the exact same answer as part (a) — make sure you understand why!

(m) $n-1$. It's easiest just to enumerate the solutions here. x_0 can take values $1,2,\dots,n-1$ and this uniquely fixes the value of x_1. So, we have $n-1$ ways to do this. But, this is just an example of the more general question below.

(n) $\binom{(n-(k+1))+k}{k} = \binom{n-1}{k}$. This is just $n-(k+1)$ indistinguishable balls into distinguishable $k+1$ bins. By subtracting 1 from all $k+1$ variables, and $k+1$ from the total required, we reduce it to problem with the same form as the previous problem. Once we have a solution to that we reverse the process, and adding 1 to all the non-negative variables gives us positive variables.

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?]

Solution:

(a) n^p. For each of the p beads, there are n possibilities for its colors. Therefore, by the first counting principle, there are n^p different sequences.

(b) $n^p - n$. You can have n sequences of a beads with only one color.

(c) Since p is prime, rotating any sequence by less than p spots will produce a new sequence. As in, there is no number x smaller than p such that rotating the beads by x would cause the pattern to look the same. This is because every other rotation of $x < p$ would only have the sequence and its rotated sequence being equivalent if the sequence was monochromatic (the sequence was just a repetition of one number). If we have a sequence $a_0, a_1, \ldots, a_{p-1}$ and rotate it by x to get $a_x, a_{x+1}, \ldots, a_{x-1}$, the two sequences would only be equal if $a_0 = a_x = a_{2x} = \ldots$, and thus each element would have to be the same. For example, if we had the sequence a_1, a_2, a_3, a_4, a_5, and rotated it by 2 to get a_3, a_4, a_5, a_1, a_2, we can analyze each position of the string. Looking at this first position, this implies that $a_1 = a_3$. Then, looking at the third position, this implies that $a_3 = a_5$, and then $a_5 = a_2$, and $a_2 = a_4$, thus they all have to be equal. This cannot happen in our count, because we are only considering wristbands for which there are at least 2 different colors.

So, every pattern which has more than one color of beads can be rotated to form $p-1$ other patterns. So the total number of patterns equivalent with some bead sequence is p. Thus, the total number of non-equivalent patterns are $(n^p - n)/p$.

(d) $(n^p - n)/p$ must be an integer, because from the previous part, it is the number of ways to count something. Hence, $n^p - n$ has to be divisible by p, i.e., $n^p \equiv n \pmod{p}$, which is Fermat's Little Theorem.