CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 00

Due: Saturday, 1/20, 4:00 PM
Grace period until Saturday, 1/20, 6:00 PM

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 Administrivia

(a) Make sure you are on the course Ed (for Q&A) and Gradescope (for submitting homeworks, including this one). Find and familiarize yourself with the course website. What is its homepage's URL?

(b) Read the policies page on the course website.

(i) What is the breakdown of how your grade is calculated, for both the homework and the no-homework option?

(ii) What is the attendance policy for discussions?

(iii) When are homeworks released and when are they due?

(iv) How many "drops" do you get for homeworks? How many mini-vitamins will contribute to your grade?

(v) When is the midterm? When is the final?

(vi) What percentage score is needed to earn full credit on a homework?

2 Course Policies

Go to the course website and read the course policies carefully. Leave a followup on Ed if you have any questions. Are the following situations violations of course policy? Write "Yes" or "No", and a short explanation for each.

(a) Alice and Bob work on a problem in a study group. They write up a solution together and submit it, noting on their submissions that they wrote up their homework answers together.

(b) Carol goes to a homework party and listens to Dan describe his approach to a problem on the board, taking notes in the process. She writes up her homework submission from her notes, crediting Dan.

(c) Erin comes across a proof that is part of a homework problem while studying course material. She reads it and then, after she has understood it, writes her own solution using the same approach. She submits the homework with a citation to the website.

(d) Frank is having trouble with his homework and asks Grace for help. Grace lets Frank look at her written solution. Frank copies it onto his notebook and uses the copy to write and submit his homework, crediting Grace.

(e) Heidi has completed her homework using LaTeX. Her friend Irene has been working on a homework problem for hours, and asks Heidi for help. Heidi sends Irene her PDF solution, and Irene uses it to write her own solution with a citation to Heidi.

(f) Joe found homework solutions before they were officially released, and every time he got stuck, he looked at the solutions for a hint. He then cited the solutions as part of his submission.

3 Use of Ed

Ed is incredibly useful for Q&A in such a large-scale class. We will use Ed for all important announcements. You should check it frequently. We also highly encourage you to use Ed to ask questions and answer questions from your fellow students.

(a) Read the Ed Etiquette section of the course policies and explain what is wrong with the following hypothetical student question: "Can someone explain the proof of Theorem XYZ to me?" (Assume Theorem XYZ is a complicated concept.)

(b) When are the weekly posts released? Are they required reading?

(c) If you have a question or concern not directly related to the course content, where should you direct it?

4 Academic Integrity

Please write or type out the following pledge in print, and sign it.

> I pledge to uphold the university's honor code: to act with honesty, integrity, and respect for others, including their work. By signing, I ensure that all written homework I submit will be in my own words, that I will acknowledge any collaboration or help received, and that I will neither give nor receive help on any examinations.

5 Propositional Practice

Note 1

In parts (a)-(b), convert the English sentences into propositional logic. In parts (c) - (d), convert the propositions into English. For parts (b) and (d), use the notation $a \mid b$ to denote the statement "a divides b", and use the notation $P(x)$ to denote the statement "x is a prime number".

(a) For every real number k, there is a unique real solution to $x^3 = k$.

(b) If p is a prime number, then for any two natural numbers a and b, if p doesn't divide a and p divides ab, then p divides b.

(c) $(\forall x, y \in \mathbb{R})\,[(xy = 0) \implies ((x = 0) \vee (y = 0))]$

(d) $\neg((\exists y \in \mathbb{N})\,[(\forall x \in \mathbb{N})\,[(x > y) \implies ((y \mid x) \vee P(x))]])$

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 01

Due: Saturday, 1/27, 4:00 PM
Grace period until Saturday, 1/27, 6:00 PM

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 Logical Equivalence?

Note 1

Decide whether each of the following logical equivalences is correct and justify your answer.

(a) $\forall x\ (P(x) \wedge Q(x)) \stackrel{?}{\equiv} \forall x\, P(x) \wedge \forall x\, Q(x)$

(b) $\forall x\ (P(x) \vee Q(x)) \stackrel{?}{\equiv} \forall x\, P(x) \vee \forall x\, Q(x)$

(c) $\exists x\ (P(x) \vee Q(x)) \stackrel{?}{\equiv} \exists x\, P(x) \vee \exists x\, Q(x)$

(d) $\exists x\ (P(x) \wedge Q(x)) \stackrel{?}{\equiv} \exists x\, P(x) \wedge \exists x\, Q(x)$

2 Prove or Disprove

Note 2

For each of the following, either prove the statement, or disprove by finding a counterexample.

(a) $(\forall n \in \mathbb{N})$ if n is odd then $n^2 + 4n$ is odd.

(b) $(\forall a, b \in \mathbb{R})$ if $a + b \leq 15$ then $a \leq 11$ or $b \leq 4$.

(c) $(\forall r \in \mathbb{R})$ if r^2 is irrational, then r is irrational.

(d) $(\forall n \in \mathbb{Z}^+)\ 5n^3 > n!$. (Note: $\mathbb{Z}^+$ is the set of positive integers)

(e) The product of a non-zero rational number and an irrational number is irrational.

3 Twin Primes

Note 2

(a) Let $p > 3$ be a prime. Prove that p is of the form $3k+1$ or $3k-1$ for some integer k.

(b) *Twin primes* are pairs of prime numbers p and q that have a difference of 2. Use part (a) to prove that 5 is the only prime number that takes part in two different twin prime pairs.

4 Airport

Note 3

Suppose that there are $2n+1$ airports, where n is a positive integer. The distances between any two airports are all different. For each airport, exactly one airplane departs from it and is destined for the closest airport. Prove by induction that there is an airport which has no airplanes destined for it.

5 A Coin Game

Note 3

Your "friend" Stanley Ford suggests you play the following game with him. You each start with a single stack of n coins. On each of your turns, you select one of your stacks of coins (that has at least two coins) and split it into two stacks, each with at least one coin. Your score for that turn is the product of the sizes of the two resulting stacks (for example, if you split a stack of 5 coins into a stack of 3 coins and a stack of 2 coins, your score would be $3 \cdot 2 = 6$). You continue taking turns until all your stacks have only one coin in them. Stan then plays the same game with his stack of n coins, and whoever ends up with the largest total score over all their turns wins.

Prove that no matter how you choose to split the stacks, your total score will always be $\frac{n(n-1)}{2}$. (This means that you and Stan will end up with the same score no matter what happens, so the game is rather pointless.)

6 Grid Induction

Note 3

Pacman is walking on an infinite 2D grid. He starts at some location $(i, j) \in \mathbb{N}^2$ in the first quadrant, and is constrained to stay in the first quadrant (say, by walls along the x and y axes).

Every second he does one of the following (if possible):

(i) Walk one step down, to $(i, j-1)$.

(ii) Walk one step left, to $(i-1, j)$.

For example, if he is at $(5,0)$, his only option is to walk left to $(4,0)$; if Pacman is instead at $(3,2)$, he could walk either to $(2,2)$ or $(3,1)$.

Prove by induction that no matter how he walks, he will always reach $(0,0)$ in finite time.

(*Hint*: Try starting Pacman at a few small points like $(2,1)$ and looking all the different paths he could take to reach $(0,0)$. Do you notice a pattern in the number of steps he takes? Try to use this to strengthen the inductive hypothesis.)

7 (Optional) Calculus Review

In the probability section of this course, you will be expected to compute derivatives, integrals, and double integrals. This question contains a couple examples of the kinds of calculus you will encounter.

(a) Compute the following integral:

$$\int_0^\infty \sin(t)e^{-t}\,\mathrm{d}t\,.$$

(b) Compute the values of $x \in (-2,2)$ that correspond to local maxima and minima of the function

$$f(x) = \int_0^{x^2} t\cos\left(\sqrt{t}\right)\mathrm{d}t\,.$$

Classify which x correspond to local maxima and which to local minima.

(c) Compute the double integral

$$\iint_R 2x + y\,\mathrm{d}A\,,$$

where R is the region bounded by the lines $x = 1$, $y = 0$, and $y = x$.

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 02

Due: Saturday, 2/3, 4:00 PM
Grace period until Saturday, 2/3, 6:00 PM

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 Universal Preference

Note 4

Suppose that preferences in a stable matching instance are universal: all n jobs share the preferences $C_1 > C_2 > \cdots > C_n$ and all candidates share the preferences $J_1 > J_2 > \cdots > J_n$.

(a) What pairing do we get from running the algorithm with jobs proposing? Can you prove this happens for all n?

(b) What pairing do we get from running the algorithm with candidates proposing?

(c) What does this tell us about the number of stable pairings?

2 Pairing Up

Note 4

Prove that for every even $n \geq 2$, there exists an instance of the stable matching problem with n jobs and n candidates such that the instance has at least $2^{n/2}$ distinct stable matchings.

3 Upper Bound

Note 4

(a) In the notes, we show that the stable matching algorithm terminates in at most n^2 days. Prove the following stronger result: the stable matching algorithm will always terminate in at most $(n-1)^2 + 1 = n^2 - 2n + 2$ days.

(b) Provide a set of preference lists for 4 jobs and 4 candidates that will result in the upper bound from part (a) when running the Propose-and-Reject algorithm. Verify this by running the Propose-and-Reject algorithm on your preference lists.

4 Build-Up Error?

Note 5

What is wrong with the following "proof"? In addition to finding a counterexample, you should explain what is fundamentally wrong with this approach, and why it demonstrates the danger of build-up error.

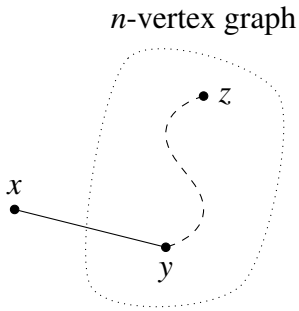
False Claim: If every vertex in an undirected graph has degree at least 1, then the graph is connected.

Proof? We use induction on the number of vertices $n \geq 1$.

Base case: There is only one graph with a single vertex and it has degree 0. Therefore, the base case is vacuously true, since the if-part is false.

Inductive hypothesis: Assume the claim is true for some $n \geq 1$.

Inductive step: We prove the claim is also true for $n+1$. Consider an undirected graph on n vertices in which every vertex has degree at least 1. By the inductive hypothesis, this graph is connected. Now add one more vertex x to obtain a graph on $(n+1)$ vertices, as shown below.



All that remains is to check that there is a path from x to every other vertex z. Since x has degree at least 1, there is an edge from x to some other vertex; call it y. Thus, we can obtain a path from x to z by adjoining the edge $\{x, y\}$ to the path from y to z. This proves the claim for $n+1$. □

5 Proofs in Graphs

Note 5

(a) On the axis from San Francisco traffic habits to Los Angeles traffic habits, Old California is more towards San Francisco: that is, civilized. In Old California, all roads were one way streets. Suppose Old California had n cities ($n \geq 2$) such that for every pair of cities X and Y, either X had a road to Y or Y had a road to X.

Prove that there existed a city which was reachable from every other city by traveling through at most 2 roads.

[*Hint:* Induction]

(b) Consider a connected graph G with n vertices which has exactly $2m$ vertices of odd degree, where $m > 0$. Prove that there are m walks that *together* cover all the edges of G (i.e., each

edge of G occurs in exactly one of the m walks, and each of the walks should not contain any particular edge more than once).

[*Hint:* In lecture, we have shown that a connected undirected graph has an Eulerian tour if and only if every vertex has even degree. This fact may be useful in the proof.]

(c) Prove that any graph G is bipartite if and only if it has no tours of odd length.

[*Hint:* In one of the directions, consider the lengths of paths starting from a given vertex.]

6 (Optional) Nothing Can Be Better Than Something

Note 4

In the stable matching problem, suppose that some jobs and candidates have hard requirements and might not be able to just settle for anything. In other words, each job/candidate prefers being unmatched rather than be matched with those below a certain point in their preference list. Let the term "entity" refer to a candidate/job. A matching could ultimately have to be partial, i.e., some entities would and should remain unmatched.

Consequently, the notion of stability here should be adjusted a little bit to capture the autonomy of both jobs to unilaterally fire employees and/or employees to just walk away. A matching is stable if

- there is no matched entity who prefers being unmatched over being with their current partner;
- there is no matched/filled job and unmatched candidate that would both prefer to be matched with each other over their current status;
- there is no matched job and matched candidate that would both prefer to be matched with each other over their current partners; and
- similarly, there is no unmatched job and matched candidate that would both prefer to be matched with each other over their current status;
- there is no unmatched job and unmatched candidate that would both prefer to be with each other over being unmatched.

(a) Prove that a stable pairing still exists in the case where we allow unmatched entities.

(HINT: You can approach this by introducing imaginary/virtual entities that jobs/candidates "match" if they are unmatched. How should you adjust the preference lists of jobs/candidates, including those of the newly introduced imaginary ones for this to work?)

(b) As you saw in the lecture, we may have different stable matchings. But interestingly, if an entity remains unmatched in one stable matching, they must remain unmatched in any other stable matching as well. Prove this fact by contradiction.

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 03

Due: Saturday, 2/10, 4:00 PM
Grace period until Saturday, 2/10, 6:00 PM

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 Short Tree Proofs

Note 5

Let $G = (V, E)$ be an undirected graph with $|V| \geq 1$.

(a) Prove that every connected component in an acyclic graph is a tree.

(b) Suppose G has k connected components. Prove that if G is acyclic, then $|E| = |V| - k$.

(c) Prove that a graph with $|V|$ edges contains a cycle.

2 Touring Hypercube

Note 5

In the lecture, you have seen that if G is a hypercube of dimension n, then

- The vertices of G are the binary strings of length n.
- u and v are connected by an edge if they differ in exactly one bit location.

A *Hamiltonian tour* of a graph is a sequence of vertices $v_0, v_1, \ldots, v_k$ such that:

- Each vertex appears exactly once in the sequence.
- Each pair of consecutive vertices is connected by an edge.
- v_0 and v_k are connected by an edge.

(a) Show that a hypercube has an Eulerian tour if and only if n is even.

(b) Show that every hypercube has a Hamiltonian tour.

3 Planarity and Graph Complements

Note 5

Let $G = (V, E)$ be an undirected graph. We define the complement of G as $\overline{G} = (V, \overline{E})$ where $\overline{E} = \{(i, j) \mid i, j \in V, i \neq j\} - E$; that is, $\overline{G}$ has the same set of vertices as G, but an edge e exists is $\overline{G}$ if and only if it does not exist in G.

(a) Suppose G has v vertices and e edges. How many edges does $\overline{G}$ have?

(b) Prove that for any graph with at least 13 vertices, G being planar implies that $\overline{G}$ is non-planar.

(c) Now consider the converse of the previous part, i.e., for any graph G with at least 13 vertices, if $\overline{G}$ is non-planar, then G is planar. Construct a counterexample to show that the converse does not hold.

Hint: Recall that if a graph contains a copy of K_5, then it is non-planar. Can this fact be used to construct a counterexample?

4 Modular Practice

Note 6

Solve the following modular arithmetic equations for x and y.

(a) $9x + 5 \equiv 7 \pmod{13}$.

(b) Show that $3x + 12 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $5x + 4y \equiv 0 \pmod{7}$ and $2x + y \equiv 4 \pmod{7}$.

(d) $13^{2023} \equiv x \pmod{12}$.

(e) $7^{62} \equiv x \pmod{11}$.

5 Short Answer: Modular Arithmetic

Note 6

(a) What is the multiplicative inverse of $n - 1$ modulo n? (Your answer should be an expression that may involve n)

(b) What is the solution to the equation $3x \equiv 6 \pmod{17}$?

(c) Let $R_0 = 0; R_1 = 2; R_n = 4R_{n-1} - 3R_{n-2}$ for $n \geq 2$. Is $R_n \equiv 2 \pmod{3}$ for $n \geq 1$? (True or False)

(d) Given that $(7)(53) - m = 1$, what is the solution to $53x + 3 \equiv 10 \pmod{m}$? (Answer should be an expression that is interpreted $\pmod{m}$, and shouldn't consist of fractions.)

6 Wilson's Theorem

Note 6

Wilson's Theorem states the following is true if and only if p is prime:

$$(p-1)! \equiv -1 \pmod{p}.$$

Prove both directions (it holds if AND only if p is prime).

Hint for the if direction: Consider rearranging the terms in $(p-1)! = 1 \cdot 2 \cdot \cdots \cdot (p-1)$ to pair up terms with their inverses, when possible. What terms are left unpaired?

Hint for the only if direction: If p is composite, then it has some prime factor q. What can we say about $(p-1)! \pmod{q}$?

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 04

Due: Saturday, 2/17, 4:00 PM
Grace period until Saturday, 2/17, 6:00 PM

Sundry

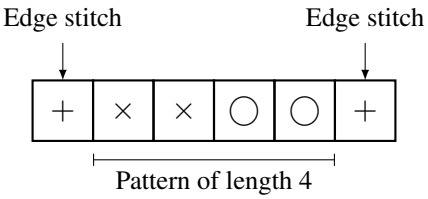
Before you start writing your final homework submission, state briefly how you worked on it. Who else did you work with? List names and email addresses. (In case of homework party, you can just describe the group.)

1 Celebrate and Remember Textiles

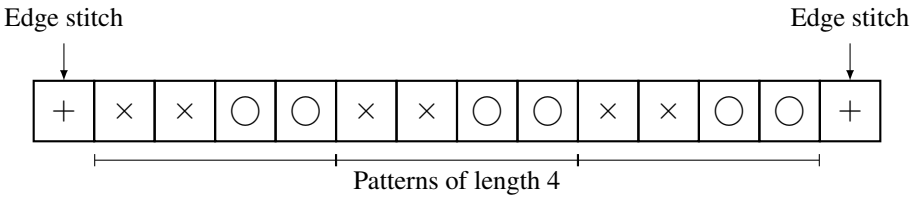
Note 6

Mathematics and computing both owe an immense debt to textiles, where many key ideas originated.

Instructions for knitting patterns will tell you to begin by "casting on" the needle some multiple of m plus r, where m is the number of stitches to create one repetition of the pattern and r is the number of stitches needed for the two edges of the piece. For example, in the simple rib stitch pattern below, the repeating pattern is of length $m = 4$, and you need $r = 2$ stitches for the edges.



Thus, to make the final piece wider, you can add as many multiples of the pattern of length 4 as you like; for example, if you want to repeat the pattern 3 times, you need to cast on a total of $3m + r = 3(4) + 2 = 14$ stitches (shown below).



You've decided to knit a 70-themed baby blanket as a gift for your cousin and want to incorporate rows from three different stitch patterns with the following requirements:

- Alternating Link: Multiple of 7, plus 4
- Double Broken Rib: Multiple of 4, plus 2
- Swag: Multiple of 5, plus 2

You want to be able to switch between knitting these different patterns without changing the number of stitches on the needle, so you must use a number of stitches that simultaneously meets the requirements of all three patterns.

Find the *smallest number of stitches* you need to cast on in order to incorporate all three patterns in your baby blanket.

2 Euler's Totient Theorem

Note 6
Note 7

Euler's Totient Theorem states that, if n and a are coprime,

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

where $\phi(n)$ (known as Euler's Totient Function) is the number of positive integers less than or equal to n which are coprime to n (including 1). Note that this theorem generalizes Fermat's Little Theorem, since if n is prime, then $\phi(n) = n-1$.

(a) Let the numbers less than n which are coprime to n be $m_1, m_2, \ldots, m_{\phi(n)}$. Argue that the set

$$\{am_1, am_2, \ldots, am_{\phi(n)}\}$$

is a permutation of the set

$$\{m_1, m_2, \ldots, m_{\phi(n)}\}.$$

In other words, prove that

$$f : \{m_1, m_2, \ldots, m_{\phi(n)}\} \to \{m_1, m_2, \ldots, m_{\phi(n)}\}$$

is a bijection, where $f(x) \coloneqq ax \pmod{n}$.

(b) Prove Euler's Theorem. (Hint: Recall the FLT proof.)

3 Sparsity of Primes

Note 6

A prime power is a number that can be written as p^i for some prime p and some positive integer i. So, $9 = 3^2$ is a prime power, and so is $8 = 2^3$. $42 = 2 \cdot 3 \cdot 7$ is not a prime power.

Prove that for any positive integer k, there exists k consecutive positive integers such that none of them are prime powers.

Hint: This is a Chinese Remainder Theorem problem. We want to find n such that $(n+1)$, $(n+2)$, $\ldots$, and $(n+k)$ are all not powers of primes. We can enforce this by saying that $n+1$ through $n+k$ each must have two distinct prime divisors. In your proof, you can choose these prime divisors arbitrarily.

4 RSA Practice

Note 7

Consider the following RSA scheme and answer the specified questions.

(a) Assume for an RSA scheme we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$, what is the decryption key d? Calculate the exact value.

(b) If the receiver gets 4, what was the original message?

(c) Encode your answer from part (b) to check its correctness.

5 Tweaking RSA

Note 7

You are trying to send a message to your friend, and as usual, Eve is trying to decipher what the message is. However, you get lazy, so you use $N = p$, and p is prime. Similar to the original method, for any message $x \in \{0, 1, \ldots, N-1\}$, $E(x) \equiv x^e \pmod{N}$, and $D(y) \equiv y^d \pmod{N}$.

(a) Show how you choose e and d in the encryption and decryption function, respectively. Prove the correctness property: the message x is recovered after it goes through your new encryption and decryption functions, $E(x)$ and $D(y)$.

(b) Can Eve now compute d in the decryption function? If so, by what algorithm?

(c) Now you wonder if you can modify the RSA encryption method to work with three primes ($N = pqr$ where p, q, r are all prime). Explain the modifications made to encryption and decryption and include a proof of correctness showing that $D(E(x)) = x$.

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 05

Due: Saturday, 2/24, 4:00 PM
Grace period until Saturday, 2/24, 6:00 PM

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 5 that is equivalent to $f(x) = x^5$ over GF(5); then find a polynomial with degree strictly less than 11 that is equivalent to $g(x) = 4x^{70} + 9x^{11} + 3$ over GF(11).

(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 Secret Sharing

Note 8

Suppose the Oral Exam questions are created by 2 TAs and 3 Readers. The answers are all encrypted, and we know that:

- Two TAs together should be able to access the answers
- Three Readers together should be able to access the answers
- One TA and one Reader together should also be able to access the answers
- One TA by themself or two Readers by themselves should not be able to access the answers.

Design a Secret Sharing scheme to make this work.

3 One Point Interpolation

Note 8

Suppose we have a polynomial $f(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_2x^2 + c_1x + c_0$.

(a) Can we determine $f(x)$ with k points? If so, provide a set of inputs $x_0, x_1, \ldots, x_{k-1}$ such that knowing points $(x_0, f(x_0)), (x_1, f(x_1)), \ldots, (x_{k-1}, f(x_{k-1}))$ allows us to uniquely determine $f(x)$, and show how $f(x)$ can be determined from such points. If not, provide a proof of why this is not possible.

(b) Now, assume each coefficient is an integer satisfying $0 \leq c_i < 100 \quad \forall i \in [0, k-1]$. Can we determine $f(x)$ with one point? If so, provide an input x_* such that knowing the point $(x_*, f(x_*))$ allows us to uniquely determine $f(x)$, and show how $f(x)$ can be determined from this point. If not, provide a proof of why this is not possible.

4 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.

5 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.

(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 such that Bob so that he can always reconstruct the message?

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 06

Due: Saturday, 3/1, 4:00 PM
Grace period until Saturday, 3/1, 6:00 PM

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 Unions and Intersections

Note 11

Given:

- X is a countable, non-empty set. For all $i \in X$, A_i is an uncountable set.
- Y is an uncountable set. For all $i \in Y$, B_i is a countable set.

For each of the following, decide if the expression is "Always countable", "Always uncountable", "Sometimes countable, Sometimes uncountable".

For the "Always" cases, prove your claim. For the "Sometimes" case, provide two examples – one where the expression is countable, and one where the expression is uncountable.

(a) $X \cap Y$

(b) $X \cup Y$

(c) $\bigcup_{i \in X} A_i$

(d) $\bigcap_{i \in X} A_i$

(e) $\bigcup_{i \in Y} B_i$

(f) $\bigcap_{i \in Y} B_i$

2 Count It!

Note 11

For each of the following collections, determine and briefly explain whether it is finite, countably infinite (like the natural numbers), or uncountably infinite (like the reals):

(a) The integers which divide 8.

(b) The integers which 8 divides.

(c) The functions from $\mathbb{N}$ to $\mathbb{N}$.

(d) The set of strings over the English alphabet. (Note that the strings may be arbitrarily long, but each string has finite length. Also the strings need not be real English words.)

(e) The set of finite-length strings drawn from a countably infinite alphabet, $\mathscr{A}$.

(f) The set of infinite-length strings over the English alphabet.

3 Fixed Points

Note 12

Consider the problem of determining if a program P has any fixed points. Given any program P, a fixed point is an input x such that $P(x)$ outputs x.

(a) Prove that the problem of determining whether a program has a fixed point is uncomputable.

(b) Consider the problem of outputting a fixed point of a program if it has one, and outputting "Null" otherwise. Prove that this problem is uncomputable.

(c) Consider the problem of outputting a fixed point of a program F if the fixed point exists *and* is a natural number, and outputting "Null" otherwise. If an input is a natural number, then it has no leading zero before its most significant bit.

Show that if this problem can be solved, then the problem in part (b) can be solved. What does this say about the computability of this problem? (You may assume that the set of all possible inputs to a program is countable, as is the case on your computer.)

4 Unprogrammable Programs

Note 12

Prove whether the programs described below can exist or not.

(a) A program $P(F,x,y)$ that returns true if the program F outputs y when given x as input (i.e. $F(x) = y$) and false otherwise.

(b) A program P that takes two programs F and G as arguments, and returns true if F and G halt on the same set of inputs (or false otherwise).

Hint: Use P to solve the halting problem, and consider defining two subroutines to pass in to P, where one of the subroutines always loops.

5 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 19-digit ternary (0,1,2) bitstrings are there such that no two adjacent digits are equal?

(b) 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?

(c) 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?

(d) 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)

(e) 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).

(f) 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.**

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 08

Due: Saturday, 3/16, 4:00 PM
Grace period until Saturday, 3/16, 6:00 PM

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 Probability Warm-Up

Note 13

(a) Suppose that we have a bucket of 30 green balls and 70 orange balls. If we pick 15 balls uniformly out of the bucket, what is the probability of getting exactly k green balls (assuming $0 \leq k \leq 15$) if the sampling is done **with** replacement, i.e. after we take a ball out the bucket we return the ball back to the bucket for the next round?

(b) Same as part (a), but the sampling is **without** replacement, i.e. after we take a ball out the bucket we **do not** return the ball back to the bucket.

(c) If we roll a regular, 6-sided die 5 times. What is the probability that at least one value is observed more than once?

2 Five Up

Note 13

Say you toss a coin five times, and record the outcomes. For the three questions below, you can assume that order matters in the outcome, and that the probability of heads is some p in $0 < p < 1$, but *not* that the coin is fair ($p = 0.5$).

(a) What is the size of the sample space, $|\Omega|$?

(b) How many elements of Ω have exactly three heads?

(c) How many elements of Ω have three or more heads?

For the next three questions, you can assume that the coin is fair (i.e. heads comes up with $p = 0.5$, and tails otherwise).

(d) What is the probability that you will observe the sequence HHHTT? What about HHHHT?

(e) What is the probability of observing at least one head?

(f) What is the probability you will observe more heads than tails?

For the final three questions, you can instead assume the coin is biased so that it comes up heads with probability $p = \frac{2}{3}$.

(g) What is the probability of observing the outcome HHHTT? What about HHHHT?

(h) What about the probability of at least one head?

(i) What is the probability you will observe more heads than tails?

3 Aces

Note 13
Note 14

Consider a standard 52-card deck of cards:

(a) Find the probability of getting an ace or a red card, when drawing a single card.

(b) Find the probability of getting an ace or a spade, but not both, when drawing a single card.

(c) Find the probability of getting the ace of diamonds when drawing a 5 card hand.

(d) Find the probability of getting exactly 2 aces when drawing a 5 card hand.

(e) Find the probability of getting at least 1 ace when drawing a 5 card hand.

(f) Find the probability of getting at least 1 ace or at least 1 heart when drawing a 5 card hand.

4 Independent Complements

Note 14

Let Ω be a sample space, and let $A, B \subseteq \Omega$ be two independent events.

(a) Prove or disprove: $\overline{A}$ and $\overline{B}$ must be independent.

(b) Prove or disprove: A and $\overline{B}$ must be independent.

(c) Prove or disprove: A and $\overline{A}$ must be independent.

(d) Prove or disprove: It is possible that $A = B$.

5 Faulty Lightbulbs

Note 13
Note 14

Box 1 contains 1000 lightbulbs of which 10% are defective. Box 2 contains 2000 lightbulbs of which 5% are defective.

(a) Suppose a box is given to you at random and you randomly select a lightbulb from the box. If that lightbulb is defective, what is the probability you chose Box 1?

(b) Suppose now that a box is given to you at random and you randomly select two light- bulbs from the box. If both lightbulbs are defective, what is the probability that you chose from Box 1?

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 09

Due: Saturday, 3/23, 4:00 PM
Grace period until Saturday, 3/23, 6:00 PM

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 Symmetric Marbles

Note 14

A bag contains 4 red marbles and 4 blue marbles. Rachel and Brooke play a game where they draw four marbles in total, one by one, uniformly at random, without replacement. Rachel wins if there are more red than blue marbles, and Brooke wins if there are more blue than red marbles. If there are an equal number of marbles, the game is tied.

(a) Let A_1 be the event that the first marble is red and let A_2 be the event that the second marble is red. Are A_1 and A_2 independent?

(b) What is the probability that Rachel wins the game?

(c) Given that Rachel wins the game, what is the probability that all of the marbles were red?

Now, suppose the bag contains 8 red marbles and 4 blue marbles. Moreover, if there are an equal number of red and blue marbles among the four drawn, Rachel wins if the third marble is red, and Brooke wins if the third marble is blue. All other rules stay the same.

(d) What is the probability that the third marble is red?

(e) Given that there are k red marbles among the four drawn, where $0 \leq k \leq 4$, what is the probability that the third marble is red? Answer in terms of k.

(f) Given that the third marble is red, what is the probability that Rachel wins the game?

2 Man Speaks Truth

Note 14

Consider a man who speaks the truth with probability $\frac{3}{4}$.

(a) Suppose the man flips a biased coin that comes up heads $1/3$ of the time, and reports that it is heads.

(i) What is the probability that the coin actually landed on heads?

(ii) Unconvinced, you ask him if he just lied to you, to which he replies "no". What is the probability now that the coin actually landed on heads?

(iii) Did the probability go up, go down, or stay the same with this new information? Explain in words why this should be the case.

(b) Suppose the man rolls a fair 6-sided die. When you ask him if the die came up with a 6, he answers "yes".

(i) What is the probability that the die actually came up with a 6?

(ii) Skeptical, you also ask him whether the die came up with a 1, to which he replies "yes". What is the probability now that the die actually came up with a 6?

(iii) Did the probability go up, go down, or stay the same with this new information? Explain in words why this should be the case.

3 Cliques in Random Graphs

Note 13
Note 14

Consider the graph $G = (V, E)$ on n vertices which is generated by the following random process: for each pair of vertices u and v, we flip a fair coin and place an (undirected) edge between u and v if and only if the coin comes up heads.

(a) What is the size of the sample space?

(b) A k-clique in a graph is a set S of k vertices which are pairwise adjacent (every pair of vertices is connected by an edge). For example, a 3-clique is a triangle. Let E_S be the event that a set S forms a clique. What is the probability of E_S for a particular set S of k vertices?

(c) Suppose that $V_1 = \{v_1, \ldots, v_\ell\}$ and $V_2 = \{w_1, \ldots, w_k\}$ are two arbitrary sets of vertices. What conditions must V_1 and V_2 satisfy in order for E_{V_1} and E_{V_2} to be independent? Prove your answer.

(d) Prove that $\binom{n}{k} \leq n^k$. (You might find this useful in part (e)).

(e) Prove that the probability that the graph contains a k-clique, for $k \geq 4\log_2 n + 1$, is at most $1/n$. *Hint:* Use the union bound.

4 Combined Head Count

Note 19

Suppose you flip a fair coin twice.

(a) What is the sample space Ω generated from these flips?

(b) Define a random variable X to be the number of heads. What is the distribution of X?

(c) Define a random variable Y to be 1 if you get a heads followed by a tails and 0 otherwise. What is the distribution of Y?

(d) Compute the conditional probabilities $\mathbb{P}[Y = i \mid X = j]$ for all i, j.

(e) Define a third random variable $Z = X + Y$. Use the conditional probabilities you computed in part (d) to find the distribution of Z.

5 Max/Min Dice Rolls

Note 15

Yining rolls three fair six-sided dice.

(a) Let X denote the maximum of the three values rolled. What is the distribution of X (that is, $\mathbb{P}[X = x]$ for $x = 1,2,3,4,5,6$)? You can leave your final answer in terms of "x". [*Hint*: Try to first compute $\mathbb{P}[X \leq x]$ for $x = 1,2,3,4,5,6$]. If you want to check your answer, you can solve this problem using counting and make sure it matches with the formula you derived.

(b) Let Y denote the minimum of the three values rolled. What is the distribution of Y?

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 11

Due: Saturday, 4/6, 4:00 PM
Grace period until Saturday, 4/6, 6:00 PM

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 Fishy Computations

Note 19

Assume for each part that the random variable can be modelled by a Poisson distribution.

(a) Suppose that on average, a fisherman catches 20 salmon per week. What is the probability that he will catch exactly 7 salmon this week?

(b) Suppose that on average, you go to Fisherman's Wharf twice a year. What is the probability that you will go at most once in 2024?

(c) Suppose that in March, on average, there are 5.7 boats that sail in Laguna Beach per day. What is the probability there will be *at least* 3 boats sailing throughout the *next two days* in Laguna?

(d) Denote $X \sim \text{Pois}(\lambda)$. Prove that

$$\mathbb{E}[Xf(X)] = \lambda\,\mathbb{E}[f(X+1)]$$

for any function f.

2 Such High Expectations

Note 19

Suppose X and Y are independently drawn from a Geometric distribution with parameter p.

(a) Compute $\mathbb{E}[\min(X,Y)]$.

(b) Compute $\mathbb{E}[\max(X,Y)]$.

3 Diversify Your Hand

Note 15
Note 16

You are dealt 5 cards from a standard 52 card deck. Let X be the number of distinct values in your hand. For instance, the hand (A, A, A, 2, 3) has 3 distinct values.

(a) Calculate $\mathbb{E}[X]$. (Hint: Consider indicator variables X_i representing whether i appears in the hand.)

(b) Calculate $\text{Var}(X)$.

4 Swaps and Cycles

Note 15

We'll say that a permutation $\pi = (\pi(1), \ldots, \pi(n))$ contains a *swap* if there exist $i, j \in \{1, \ldots, n\}$ so that $\pi(i) = j$ and $\pi(j) = i$, where $i \neq j$.

(a) What is the expected number of swaps in a random permutation?

(b) In the same spirit as above, we'll say that π contains a *k-cycle* if there exist $i_1, \ldots, i_k \in \{1, \ldots, n\}$ with $\pi(i_1) = i_2, \pi(i_2) = i_3, \ldots, \pi(i_k) = i_1$. Compute the expectation of the number of k-cycles.

5 Double-Check Your Intuition Again

Note 16

(a) You roll a fair six-sided die and record the result X. You roll the die again and record the result Y.

(i) What is $\text{cov}(X+Y, X-Y)$?

(ii) Prove that $X+Y$ and $X-Y$ are not independent.

For each of the problems below, if you think the answer is "yes" then provide a proof. If you think the answer is "no", then provide a counterexample.

(b) If X is a random variable and $\text{Var}(X) = 0$, then must X be a constant?

(c) If X is a random variable and c is a constant, then is $\text{Var}(cX) = c\,\text{Var}(X)$?

(d) If A and B are random variables with nonzero standard deviations and $\text{Corr}(A, B) = 0$, then are A and B independent?

(e) If X and Y are not necessarily independent random variables, but $\text{Corr}(X, Y) = 0$, and X and Y have nonzero standard deviations, then is $\text{Var}(X+Y) = \text{Var}(X) + \text{Var}(Y)$?

The two subparts below are **optional** and will not be graded but are recommended for practice.

(f) If X and Y are random variables then is $\mathbb{E}[\max(X, Y)\min(X, Y)] = \mathbb{E}[XY]$?

(g) If X and Y are independent random variables with nonzero standard deviations, then is

$$\text{Corr}(\max(X, Y), \min(X, Y)) = \text{Corr}(X, Y)?$$

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 12

Due: Saturday, 4/13, 4:00 PM
Grace period until Saturday, 4/13, 6:00 PM

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 Tellers

Note 17

Imagine that X is the number of customers that enter a bank at a given hour. To simplify everything, in order to serve n customers you need at least n tellers. One less teller and you won't finish serving all of the customers by the end of the hour. You are the manager of the bank and you need to decide how many tellers there should be in your bank so that you finish serving all of the customers in time. You need to be sure that you finish in time with probability at least 95%.

(a) Assume that from historical data you have found out that $\mathbb{E}[X] = 5$. How many tellers should you have?

(b) Now assume that you have also found out that $\text{Var}(X) = 5$. Now how many tellers do you need?

2 Polling Numbers

Note 17

Suppose the whole population of California has Democrats, Republicans, and no other parties. You choose N people independently and uniformly at random from the Californian population, and for each person, you record whether they are a Democrat or a Republican. We want to estimate the true percentage of Democrats among the polled Californians to within 1% with 95% confidence. According to Chebyshev's inequality, what is the minimum number of people you need to poll?

3 Tightness of Inequalities

Note 17

(a) Show by example that Markov's inequality is tight; that is, show that given some fixed $k > 0$, there exists a discrete non-negative random variable X such that $\mathbb{P}[X \geq k] = \mathbb{E}[X]/k$.

(b) Show by example that Chebyshev's inequality is tight; that is, show that given some fixed $k \geq 1$, there exists a random variable X such that $\mathbb{P}[|X - \mathbb{E}[X]| \geq k\sigma] = 1/k^2$, where $\sigma^2 = \text{Var}(X)$.

4 Max of Uniforms

Note 21

Let $X_1, ...X_n$ be independent Uniform$(0,1)$ random variables, and let $X = \max(X_1, ...X_n)$. Compute each of the following in terms of n.

(a) What is the cdf of X?

(b) What is the pdf of X?

(c) What is $\mathbb{E}[X]$?

(d) What is $\text{Var}(X)$?

5 Darts with Friends

Note 21

Michelle and Alex are playing darts. Being the better player, Michelle's aim follows a uniform distribution over a disk of radius 1 around the center. Alex's aim follows a uniform distribution over a disk of radius 2 around the center.

(a) Let the distance of Michelle's throw from the center be denoted by the random variable X and let the distance of Alex's throw from the center be denoted by the random variable Y.

(i) What's the cumulative distribution function of X?

(ii) What's the cumulative distribution function of Y?

(iii) What's the probability density function of X?

(iv) What's the probability density function of Y?

(b) What's the probability that Michelle's throw is closer to the center than Alex's throw? What's the probability that Alex's throw is closer to the center?

(c) What's the cumulative distribution function of $U = \max(X, Y)$?

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 13

Due: Saturday, 4/20, 4:00 PM
Grace period until Saturday, 4/20, 6:00 PM

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 Uniform Uniform Computation

Note 21

Suppose $X \sim \text{Uniform}[0,1]$ and $Y \sim \text{Uniform}[0,X]$. That is, conditioned on $X = x$, Y has a $\text{Uniform}[0,x]$ distribution.

(a) What is $\mathbb{P}[Y > 1/2]$?

(b) Calculate $\text{Cov}(X,Y)$.

2 Moments of the Gaussian

Note 21

For a random variable X, the quantity $\mathbb{E}[X^k]$ for $k \in \mathbb{N}$ is called the *kth moment* of the distribution. In this problem, we will calculate the moments of a standard normal distribution.

(a) Prove the identity

$$\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left(-\frac{tx^2}{2}\right) dx = t^{-1/2}$$

for $t > 0$.

Hint: Consider a normal distribution with variance $\frac{1}{t}$ and mean 0.

(b) For the rest of the problem, X is a standard normal distribution (with mean 0 and variance 1). Use part (a) to compute $\mathbb{E}[X^{2k}]$ for $k \in \mathbb{N}$.

Hint: Try differentiating both sides with respect to t, k times. You may use the fact that we can differentiate under the integral without proof.

(c) Compute $\mathbb{E}[X^{2k+1}]$ for $k \in \mathbb{N}$.

3 Exponential Median

Note 21

(a) Prove that if $X_1, X_2, ..., X_n$ are mutually independent exponential random variables with parameters $\lambda_1, \lambda_2, ..., \lambda_n$, then $\min(X_1, X_2, ..., X_n)$ is exponentially distributed with parameter $\sum_{i=1}^{n} \lambda_i$.

Hint: Recall that the CDF of an exponential random variable with parameter λ is $1 - e^{-\lambda t}$.

(b) Given that the minimum of three i.i.d exponential variables with parameter λ is m, what is the probability that the difference between the median and the smallest is at least s? Note that the exponential random variables are mutually independent.

(c) What is the expected value of the median of three i.i.d. exponential variables with parameter λ?

Hint: Part (b) may be useful for this calculation.

4 Chebyshev's Inequality vs. Central Limit Theorem

Note 17
Note 21

Let n be a positive integer. Let $X_1, X_2, \ldots, X_n$ be i.i.d. random variables with the following distribution:

$$\mathbb{P}[X_i = -1] = \frac{1}{12}; \qquad \mathbb{P}[X_i = 1] = \frac{9}{12}; \qquad \mathbb{P}[X_i = 2] = \frac{2}{12}.$$

(a) Calculate the expectations and variances of X_1, $\sum_{i=1}^{n} X_i$, $\sum_{i=1}^{n} (X_i - \mathbb{E}[X_i])$, and

$$Z_n = \frac{\sum_{i=1}^{n} (X_i - \mathbb{E}[X_i])}{\sqrt{n/2}}.$$

(b) Use Chebyshev's Inequality to find an upper bound b for $\mathbb{P}[|Z_n| \geq 2]$.

(c) Use b from the previous part to bound $\mathbb{P}[Z_n \geq 2]$ and $\mathbb{P}[Z_n \leq -2]$.

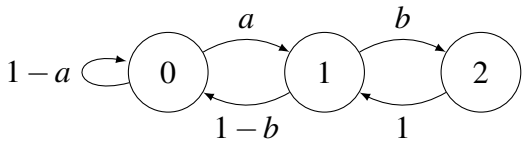
(d) As $n \to \infty$, what is the distribution of Z_n?

(e) We know that if $Z \sim \mathcal{N}(0,1)$, then $\mathbb{P}[|Z| \leq 2] = \Phi(2) - \Phi(-2) \approx 0.9545$. As $n \to \infty$, provide approximations for $\mathbb{P}[Z_n \geq 2]$ and $\mathbb{P}[Z_n \leq -2]$.

5 Analyze a Markov Chain

Note 22

Consider a Markov chain with the state diagram shown below where $a, b \in (0,1)$.



Here, we let $X(n)$ denote the state at time n.

(a) Show that this Markov chain is aperiodic.

(b) Calculate $\mathbb{P}[X(1) = 1, X(2) = 0, X(3) = 0, X(4) = 1 \mid X(0) = 0]$.

(c) Calculate the invariant distribution.

CS 70 Discrete Mathematics and Probability Theory
Spring 2024 Seshia, Sinclair

HW 14

Due: Saturday, 4/27, 4:00 PM
Grace period until Saturday, 4/27, 6:00 PM

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 Rahil's Dilemma

Note 22

Youngmin and Rahil decided to play a game: A fair coin is flipped until either the last two flips were all heads - then Youngmin wins, or the last three flips were all tails - then Rahil wins. Compute the probability that Rahil wins.

2 A Bit of Everything

Suppose that $X_0, X_1, \ldots$ is a Markov chain with finite state space $S = \{1, 2, \ldots, n\}$, where $n > 2$, and transition matrix P. Suppose further that

$$P(1,i) = \frac{1}{n} \quad \text{for all states } i \text{ and}$$
$$P(j, j-1) = 1 \quad \text{for all states } j \neq 1,$$

with $P(i,j) = 0$ everywhere else.

(a) Prove that this Markov chain is irreducible and aperiodic.

(b) Suppose you start at state 1. What is the distribution of T, where T is the number of transitions until you leave state 1 for the first time?

(c) Again starting from state 1, what is the expected number of transitions until you reach state n for the first time?

(d) Again starting from state 1, what is the probability you reach state n before you reach state 2?

(e) Compute the stationary distribution of this Markov chain.

3 Playing Blackjack

Note 22

Suppose you start with \$1, and at each turn, you win \$1 with probability p, or lose \$1 with probability $1-p$. You will continually play games of Blackjack until you either lose all your money, or you have a total of n dollars.

(a) Formulate this problem as a Markov chain.

(b) Let $\alpha(i)$ denote the probability that you end the game with n dollars, given that you started with i dollars.

Notice that for $0 < i < n$, we can write $\alpha(i+1) - \alpha(i) = k(\alpha(i) - \alpha(i-1))$. Find k.

(c) Using part (b), find $\alpha(i)$, where $0 \leq i \leq n$. (You will need to split into two cases: $p = \frac{1}{2}$ or $p \neq \frac{1}{2}$.)

Hint: Try to apply part (b) iteratively, and look at a telescoping sum to write $\alpha(i)$ in terms of $\alpha(1)$. The formula for the sum of a finite geometric series may be helpful when looking at the case where $p \neq \frac{1}{2}$:

$$\sum_{k=0}^{m} a^k = \frac{1-a^{m+1}}{1-a}.$$

Lastly, it may help to use the value of $\alpha(n)$ to find $\alpha(1)$ for the last few steps of the calculation.

(d) As $n \to \infty$, what happens to the probability of ending the game with n dollars, given that you start with i dollars, with the following values of p?

(i) $p > \frac{1}{2}$

(ii) $p = \frac{1}{2}$

(iii) $p < \frac{1}{2}$