CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 00

1 Implication

Which of the following implications are always true, regardless of P? Give a counterexample for each false assertion (i.e. come up with a statement $P(x,y)$ that would make the implication false).

(a) $\forall x \forall y P(x,y) \implies \forall y \forall x P(x,y)$.

(b) $\forall x \exists y P(x,y) \implies \exists y \forall x P(x,y)$.

(c) $\exists x \forall y P(x,y) \implies \forall y \exists x P(x,y)$.

2 Equivalences with Quantifiers

Evaluate whether the expressions on the left and right sides are equivalent in each part, and briefly justify your answers.

(a)	$\forall x \left((\exists y\, Q(x,y)) \Rightarrow P(x)\right)$	$\forall x\, \exists y \left(Q(x,y) \Rightarrow P(x)\right)$
(b)	$\neg\exists x\, \forall y \left(P(x,y) \Rightarrow \neg Q(x,y)\right)$	$\forall x \left((\exists y\, P(x,y)) \wedge (\exists y\, Q(x,y))\right)$
(c)	$\forall x\, \exists y \left(P(x) \Rightarrow Q(x,y)\right)$	$\forall x \left(P(x) \Rightarrow (\exists y\, Q(x,y))\right)$

3 XOR

The truth table of XOR (denoted by $\oplus$) is as follows.

A	B	A $\oplus$ B
F	F	F
F	T	T
T	F	T
T	T	F

1. Express XOR using only $(\wedge, \vee, \neg)$ and parentheses.

2. Does $(A \oplus B)$ imply $(A \vee B)$? Explain briefly.

3. Does $(A \vee B)$ imply $(A \oplus B)$? Explain briefly.

4 Truth Tables

Determine whether the following equivalences hold, by writing out truth tables. Clearly state whether or not each pair is equivalent.

(a) $P \wedge (Q \vee P) \equiv P \wedge Q$

(b) $(P \vee Q) \wedge R \equiv (P \wedge R) \vee (Q \wedge R)$

(c) $(P \wedge Q) \vee R \equiv (P \vee R) \wedge (Q \vee R)$

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 01A

1 Proof Practice

(a) Prove that $\forall n \in \mathbb{N}$, if n is odd, then n^2+1 is even. (Recall that n is odd if $n = 2k+1$ for some natural number k.)

(b) Prove that $\forall x, y \in \mathbb{R}$, $\min(x,y) = (x+y-|x-y|)/2$. (Recall, that the definition of absolute value for a real number z, is

$$|z| = \begin{cases} z, & z \geq 0 \\ -z, & z < 0 \end{cases}$$

(c) Suppose $A \subseteq B$. Prove $\mathscr{P}(A) \subseteq \mathscr{P}(B)$. (Recall that $A' \in \mathscr{P}(A)$ if and only if $A' \subseteq A$.)

2 Preserving Set Operations

For a function f, define the image of a set X to be the set $f(X) = \{y \mid y = f(x) \text{ for some } x \in X\}$. Define the inverse image or preimage of a set Y to be the set $f^{-1}(Y) = \{x \mid f(x) \in Y\}$. Prove the following statements, in which A and B are sets. By doing so, you will show that inverse images preserve set operations, but images typically do not.

Recall: For sets X and Y, $X = Y$ if and only if $X \subseteq Y$ and $Y \subseteq X$. To prove that $X \subseteq Y$, it is sufficient to show that $(\forall x)\ ((x \in X) \implies (x \in Y))$.

(a) $f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$.

(b) $f(A \cup B) = f(A) \cup f(B)$.

3 Fermat's Contradiction

Prove that $2^{1/n}$ is not rational for any integer $n \geq 3$. (*Hint*: Use Fermat's Last Theorem. It states that there exists no positive integers a, b, c s.t. $a^n + b^n = c^n$ for $n \geq 3$.)

4 Pebbles

Suppose you have a rectangular array of pebbles, where each pebble is either red or blue. Suppose that for every way of choosing one pebble from each column, there exists a red pebble among the chosen ones. Prove that there must exist an all-red column.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 01B

1 Induction

Prove the following using induction:

(a) Let a and b be integers with $a \neq b$. For all natural numbers $n \geq 1$, $(a^n - b^n)$ is divisible by $(a-b)$.

(b) For all natural numbers n, $(2n)! \leq 2^{2n}(n!)^2$. [Note that 0! is defined to be 1.]

2 Make It Stronger

Suppose that the sequence $a_1, a_2, \ldots$ is defined by $a_1 = 1$ and $a_{n+1} = 3a_n^2$ for $n \geq 1$. We want to prove that

$$a_n \leq 3^{2^n}$$

for every positive integer n.

(a) Suppose that we want to prove this statement using induction, can we let our induction hypothesis be simply $a_n \leq 3^{2^n}$? Show why this does not work.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 02A

1 Stable Matching

Consider the set of candidates $C = \{1, 2, 3\}$ and the set of jobs $J = \{A, B, C\}$ with the following preferences.

C	J		
1	A	B	C
2	B	A	C
3	A	B	C

J	C		
A	2	1	3
B	1	2	3
C	1	2	3

Run the applicant propose-and-reject algorithm on this example. How many days does it take and what is the resulting pairing? (Show your work)

2 Good, Better, Best

In a particular instance of the stable marriage problem with n applicants and n jobs, it turns out that there are exactly three distinct stable matchings, S_1, S_2, and S_3. Also, each applicant m has a different partner in the three matchings. Therefore each applicant has a clear preference ordering of the three matchings (according to the ranking of his partners in his preference list). Now, suppose for applicant m_1, this order is $S_1 > S_2 > S_3$.

Prove that every applicant has the same preference ordering $S_1 > S_2 > S_3$.

Hint: Recall that a applicant-optimal matching always exists and can be generated using applicant proposes matching algorithm. By reversing the roles of stable matching algorithm, what other matching can we generate?

(b) Try to instead prove the statement $a_n \leq 3^{2^n-1}$ using induction. Does this statement imply what you tried to prove in the previous part?

3 Binary Numbers

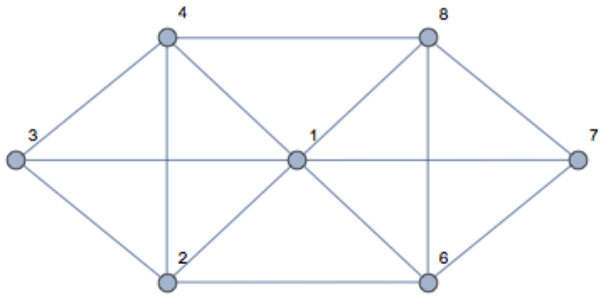
Prove that every positive integer n can be written in binary. In other words, prove that we can write

$$n = c_k \cdot 2^k + c_{k-1} \cdot 2^{k-1} + \cdots + c_1 \cdot 2^1 + c_0 \cdot 2^0,$$

where $k \in \mathbb{N}$ and $c_k \in \{0, 1\}$.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 DIS 02B

1 Eulerian Tour and Eulerian Walk



(a) Is there an Eulerian tour in the graph above? If no, give justification. If yes, provide an example.

(b) Is there an Eulerian walk in the graph above? An Eulerian walk is a walk that uses each edge exactly once. If no, give justification. If yes, provide an example.

(c) What is the condition that there is an Eulerian walk in an undirected graph? Briefly justify your answer.

2 Banquet Arrangement

In the words of the great Ana Lynch, "Let's have a kiki."

Suppose n people are attending a kiki, and each of them has at least m friends ($2 \leq m \leq n$), where friendship is mutual. Prove that we can put at least $m+1$ of the attendants on the same round table, so that each person sits next to his or her friends on both sides.

3 Not everything is normal: Odd-Degree Vertices

Claim: Let $G = (V, E)$ be an undirected graph. The number of vertices of G that have odd degree is even.

Prove the claim above using:

(i) Direct proof (e.g., counting the number of edges in G). *Hint: in lecture, we proved that* $\sum_{v \in V} \deg v = 2|E|$.

(ii) Induction on $m = |E|$ (number of edges)

(iii) Induction on $n = |V|$ (number of vertices)

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 03A

1 Cube Dual

We define a graph G by letting the vertices be the corners of a cube and having edges connecting adjacent corners. Define the *dual* of a planar graph G to be a graph G', constructed by replacing each face in G with a vertex, and an edge between every vertex in G' if the respective faces are adjacent in G.

(a) Draw a planar representation of G and the corresponding dual graph. Is the dual graph planar? (Hint: think about the act of drawing the dual)

(b) Is G' bipartite?

2 True or False

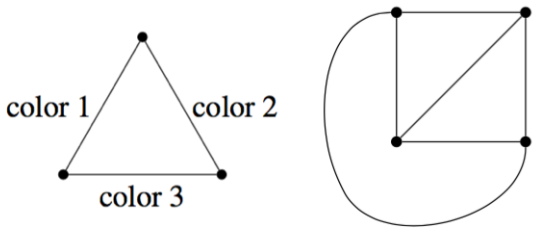
(a) Any pair of vertices in a tree are connected by exactly one path.

(b) Adding an edge between two vertices of a tree creates a new cycle.

(c) Adding an edge in a connected graph creates exactly one new cycle.

3 Edge Colorings

An edge coloring of a graph is an assignment of colors to edges in a graph where any two edges incident to the same vertex have different colors. An example is shown on the left.



(a) Show that the 4 vertex complete graph above can be 3 edge colored. (Use the numbers $1, 2, 3$ for colors. A figure is shown on the right.)

(b) Prove that any graph with maximum degree $d \geq 1$ can be edge colored with $2d - 1$ colors.

(c) Show that a tree can be edge colored with d colors where d is the maximum degree of any vertex.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 3B

1 Modular Inverses

Recall the definition of inverses from lecture: let $a, m \in \mathbb{Z}$ and $m > 0$; if $x \in \mathbb{Z}$ satisfies $ax \equiv 1 \pmod{m}$, then we say x is an **inverse of** a **modulo** m.

Now, we will investigate the existence and uniqueness of inverses.

(a) Is 3 an inverse of 5 modulo 10?

(b) Is 3 an inverse of 5 modulo 14?

(c) Is each $3 + 14n$ where $n \in \mathbb{Z}$ an inverse of 5 modulo 14?

(d) Does 4 have inverse modulo 8?

(e) Suppose $x, x' \in \mathbb{Z}$ are both inverses of a modulo m. Is it possible that $x \not\equiv x' \pmod{m}$?

2 Paper GCD

Given a sheet of paper such as this one, and no rulers, describe a method to find the GCD of the width and the height of the paper. You can fold or tear the paper however you want, and ultimately you should produce a square piece whose side lengths are equal to the GCD.

3 Amaze Your Friends

It's been a long week, and you're finally in the Friday Zoom hangout that you've been looking forward to. You eschew conversations about Professor Rao's updated facial hair, that sourdough starter that's all the rage, or the new season of "Pose". Instead, you decide to invoke wonder (or

possibly fear) in your friends by tricking them into thinking you can perform mental arithmetic with very large numbers.

So, what are the last digit of the following numbers?

(a) 11^{2017}

(b) 9^{10001}

(c) $3^{987654321}$

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 04A

1 Chinese Remainder Theorem Practice

In this question, you will solve for a natural number x such that,

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 4 \pmod 7 \end{aligned} \tag{1}$$

(a) Suppose you find 3 natural numbers a, b, c that satisfy the following properties:

$$a \equiv 2 \pmod 3 \; ; \; a \equiv 0 \pmod 5 \; ; \; a \equiv 0 \pmod 7, \tag{2}$$
$$b \equiv 0 \pmod 3 \; ; \; b \equiv 3 \pmod 5 \; ; \; b \equiv 0 \pmod 7, \tag{3}$$
$$c \equiv 0 \pmod 3 \; ; \; c \equiv 0 \pmod 5 \; ; \; c \equiv 4 \pmod 7. \tag{4}$$

Show how you can use the knowledge of a, b and c to compute an x that satisfies (1).

In the following parts, you will compute natural numbers a, b and c that satisfy the above 3 conditions and use them to find an x that indeed satisfies (1).

(b) Find a natural number a that satisfies (2). In particular, an a such that $a \equiv 2 \pmod 3$ and is a multiple of 5 and 7. It may help to approach the following problem first:

(b.i) Find a^*, the multiplicative inverse of 5×7 modulo 3. What do you see when you compute $(5 \times 7) \times a^*$ modulo 3, 5 and 7? What can you then say about $(5 \times 7) \times (2 \times a^*)$?

(c) Find a natural number b that satisfies (3). In other words: $b \equiv 3 \pmod 5$ and is a multiple of 3 and 7.

(d) Find a natural number c that satisfies (4). That is, c is a multiple of 3 and 5 and $\equiv 4 \pmod 7$.

(e) Putting together your answers for Part (a), (b), (c) and (d), report an x that indeed satisfies (1).

2 CRT Decomposition

In this problem we will find $3^{302} \mod 385$.

(a) Write 385 as a product of prime numbers in the form $385 = p_1 \times p_2 \times p_3$.

(b) Use Fermat's Little Theorem to find $3^{302} \mod p_1$, $3^{302} \mod p_2$, and $3^{302} \mod p_3$.

(c) Let $x = 3^{302}$. Use part (b) to express the problem as a system of congruences (modular equations $\mod 385$). Solve the system using the Chinese Remainder Theorem. What is $3^{302} \mod 385$?

3 Baby Fermat

Assume that a does have a multiplicative inverse mod m. Let us prove that its multiplicative inverse can be written as $a^k \pmod m$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \ldots \pmod m$. Prove that this sequence has repetitions. (**Hint:** Consider the Pigeonhole Principle.)

(b) Assuming that $a^i \equiv a^j \pmod m$, where $i > j$, what can you say about $a^{i-j} \pmod m$?

(c) Prove that the multiplicative inverse can be written as $a^k \pmod m$. What is k in terms of i and j?

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 04B

1 RSA Practice

Consider the following RSA schemes and solve for asked variables.

(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.

2 RSA Practice

Bob would like to receive encrypted messages from Alice via RSA.

(a) Bob chooses $p = 7$ and $q = 11$. His public key is (N, e). What is N?

(b) What number is e relatively prime to?

(c) e need not be prime itself, but what is the smallest prime number e can be? Use this value for e in all subsequent computations.

(d) What is $\gcd(e, (p-1)(q-1))$?

(e) What is the decryption exponent d?

(f) Now imagine that Alice wants to send Bob the message 30. She applies her encryption function E to 30. What is her encrypted message?

(g) Bob receives the encrypted message, and applies his decryption function D to it. What is D applied to the received message?

3 RSA Lite

Woody misunderstood how to use RSA. So he selected prime $P = 101$ and encryption exponent $e = 67$, and encrypted his message m to get $35 = m^e \bmod P$. Unfortunately he forgot his original message m and only stored the encrypted value 35. But Carla thinks she can figure out how to recover m from $35 = m^e \bmod P$, with knowledge only of P and e. Is she right? Can you help her figure out the message m? Show all your work.

4 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where p, q, r are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \pmod{N}$.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

Dis 05A

1 Polynomial Practice

(a) If f and g are non-zero real polynomials, how many roots do the following polynomials have at least? How many can they have at most? (Your answer may depend on the degrees of f and g.)

(i) $f+g$

(ii) $f \cdot g$

(iii) f/g, assuming that f/g is a polynomial

(b) Now let f and g be polynomials over GF(p).

(i) We say a polynomial $f = 0$ if $\forall x, f(x) = 0$. If $f \cdot g = 0$, is it true that either $f = 0$ or $g = 0$?

(ii) How many f of degree *exactly* $d < p$ are there such that $f(0) = a$ for some fixed $a \in \{0, 1, \ldots, p-1\}$?

(c) Find a polynomial f over GF(5) that satisfies $f(0) = 1, f(2) = 2, f(4) = 0$. How many such polynomials are there?

2 Rational Root Theorem

The rational root theorem states that for a polynomial

$$P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0,$$

$a_0, \cdots, a_n \in \mathbb{Z}$, if $a_0, a_n \neq 0$, then for each rational solution $\frac{p}{q}$ such that $\gcd(p,q) = 1$, $p|a_0$ and $q|a_n$. Prove the rational root theorem.

3 Secret Sharing Practice

Consider the following secret sharing schemes and solve for asked variables.

(a) Suppose there is a bag of candy locked with a passcode between 0 and an integer n. Create a scheme for 5 trick-or-treaters such that they can only open the bag of candy if 3 of them agree to open it.

(b) Create a scheme for the following situation: There are 4 cats and 3 dogs in the neighborhood, and you want them to only be able to get the treats if the majority of the animals of each type are hungry. The treats are locked by a passcode between 0 and an integer n.

4 Old Secrets, New Secrets

In order to share a secret number s, Alice distributed the values $(1, p(1)), (2, p(2)), \ldots, (n+1, p(n+1))$ of a degree n polynomial p with her friends $\text{Bob}_1, \ldots, \text{Bob}_{n+1}$. As usual, she chose p such that $p(0) = s$. Bob_1 through Bob_{n+1} now gather to jointly discover the secret. Suppose that for some reason Bob_1 already knows s, and wants to play a joke on $\text{Bob}_2, \ldots, \text{Bob}_{n+1}$, making them believe

that the secret is in fact some fixed $s' \neq s$. How could he achieve this? In other words, what value should he report in order to make the others believe that the secret is s'?

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 DIS 06A

1 Zerg Player

A Zerg player wants to produce an army to fight against Protoss in early game, and he wants to have a small army which consumes exactly 10 supply. And he has the following choices:

- Zerglings: consumes 1 supply
- Hydralisk: consumes 2 supply
- Roach: consumes 2 supply

How many different compositions can the player's army have? Note that Zerglings are indistinguishable, as are Hydralisks and Roachs.

2 Strings

What is the number of strings you can construct given:

(a) n ones, and m zeroes?

(b) n_1 A's, n_2 B's and n_3 C's?

(c) $n_1, n_2, \ldots, n_k$ respectively of k different letters?

3 Counting Game

RPG games are all about explore different mazes. Here is a weird maze: there are 2^n rooms, where each room is the vertex on a the n-dimensional hypercube, labeled by a n bit binary string.

For each room, there are n different doors, each door corresponding to an edge on the hypercube. If you are at room i, and choose door j, then you will go to room $i \oplus 2^j$ (flips the $j+1$-th bit in number i).

(a) How many different shortest path are there from room 0 to room $2^n - 1$?

(b) How many different paths of $n+2$ steps are there to go from room 0 to room $2^n - 1$?

(c) If $n = 8$, how many different shortest pathes are there from room 0 to room 63 that pass through 3 and 19?

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 6B

1 Count it

Let's get some practice with counting!

(a) How many sequences of 15 coin-flips are there that contain exactly 4 heads?

(b) An anagram of HALLOWEEN is any re-ordering of the letters of HALLOWEEN, i.e., any string made up of the letters H, A, L, L, O, W, E, E, N in any order. The anagram does not have to be an English word.
How many different anagrams of HALLOWEEN are there?

(c) How many solutions does $y_0 + y_1 + \cdots + y_k = n$ have, if each y must be a non-negative integer?

(d) How many solutions does $y_0 + y_1 = n$ have, if each y must be a positive integer?

(e) How many solutions does $y_0 + y_1 + \cdots + y_k = n$ have, if each y must be a positive integer?

2 Inclusion and exclusion

What is total number of positive numbers that smaller than 100 and coprime to 100?

3 Identities

(a) $\sum_{i=0}^{n}(-1)^i\binom{n}{i} = 0$

(b) $\sum_{i=0}^{n}\binom{r+i}{i} = \binom{r+n+1}{n}$

(c) $\sum_{i=0}^{n}\binom{r}{i}\binom{s}{n-i} = \binom{r+s}{n}$ (Note: Assuming $r > n, s > n$)

4 Largest binom

For which value(s) of k is $\binom{n}{k}$ maximum? Prove your answer.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 DIS 8A

1 Graph Isomorphic

In graph theory, an isomorphism of graphs G and H is a bijection between the vertex sets of G and H

$$f : V(G) \to V(H)$$

such that any two vertices u, v of G are adjacent in G if and only if $f(u), f(v)$ are adjacent in H.

Prove the following:

1. The degrees of corresponding nodes $u, f(u)$ are the same.
2. There is a bijection between edges.
3. If G is connected, then H is also connected.

2 Countability Practice

(a) Do $(0,1)$ and $\mathbb{R}_+ = (0,\infty)$ have the same cardinality? If so, either give an explicit bijection (and prove that it is a bijection) or provide an injection from $(0,1)$ to $(0,\infty)$ and an injection from $(0,\infty)$ to $(0,1)$ (so that by Cantor-Bernstein theorem the two sets will have the same cardinality). If not, then prove that they have different cardinalities.

(b) Is the set of strings over the English alphabet countable? (Note that the strings may be arbitrarily long, but each string has finite length. Also the strings need not be real English words.) If so, then provide a method for enumerating the strings. If not, then use a diagonalization argument to show that the set is uncountable.

(c) Consider the previous part, except now the strings are drawn from a countably infinite alphabet $\mathscr{A}$. Does your answer from before change? Make sure to justify your answer.

3 Python Functions

(a) The set $F = \{f : \mathbb{N} \to \{0,1\}\}$ is not countable.

(b) Prove that the set of all python functions that output $\{0,1\}$ is countable. (Python functions have the same power as Turing machines, but people are more familiar with python.)

(c) The set of Python functions that take in input x and output either 0 or 1 appears to be the same as F in (a), but the set of Python function is countable. Why?

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 8B

1 Countability and the Halting Problem

Prove the Halting Problem using the set of all programs and inputs.

a) What is a reasonable representation for a computer program? Using this definition, show that the set of all programs are countable. *(Hint: Python Code)*

b) We consider only finite-length inputs. Show that the set of all inputs are countable.

c) Assume that you have a program that tells you whether or not a given program halts on a specific input. Since the set of all programs and the set of all inputs are countable, we can enumerate them and construct the following table.

	x_1	x_2	x_3	x_4	...
p_1	H	L	H	L	...
p_2	L	L	L	H	...
p_3	H	L	H	L	...
p_4	L	H	L	L	...
⋮	⋮	⋮	⋮	⋮	⋱

An H (resp. L) in the ith row and jth column means that program p_i halts (resp. loops) on input x_j. Now write a program that is not within the set of programs in the table above.

d) Find a contradiction in part a and part c to show that the halting problem can't be solved.

2 Fixed Points

Consider the problem of determining if a function F has any fixed points. That is, given a function F that takes inputs from some (possibly infinite) set $\mathscr{X}$, we want to know if there is any input $x \in \mathscr{X}$ such that $F(x)$ outputs x. Prove that this problem is undecidable.

3 Computability

Decide whether the following statements are true or false. Please justify your answers.

(a) The problem of determining whether a program halts in time 2^{n^2} on an input of size n is undecidable.

(b) There is no computer program `Line` which takes a program P, an input x, and a line number L, and determines whether the L^{th} line of code is executed when the program P is run on the input x.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 DIS 9A

1 Venn Diagram

Out of 1,000 computer science students, 400 belong to a club (and may work part time), 500 work part time (and may belong to a club), and 50 belong to a club and work part time.

(a) Suppose we choose a student uniformly at random. Let C be the event that the student belongs to a club and P the event that the student works part time. Draw a picture of the sample space Ω and the events C and P.

(b) What is the probability that the student belongs to a club?

(c) What is the probability that the student works part time?

(d) What is the probability that the student belongs to a club AND works part time?

(e) What is the probability that the student belongs to a club OR works part time?

2 Flippin' Coins

Suppose we have an unbiased coin, with outcomes H and T, with probability of heads $\mathbb{P}[H] = 1/2$ and probability of tails also $\mathbb{P}[T] = 1/2$. Suppose we perform an experiment in which we toss the coin 3 times. An outcome of this experiment is (X_1, X_2, X_3), where $X_i \in \{H, T\}$.

(a) What is the *sample space* for our experiment?

(b) Which of the following are examples of *events*? Select all that apply.

- $\{(H,H,T),(H,H),(T)\}$
- $\{(T,H,H),(H,T,H),(H,H,T),(H,H,H)\}$
- $\{(T,T,T)\}$
- $\{(T,T,T),(H,H,H)\}$
- $\{(T,H,T),(H,H,T)\}$

(c) What is the complement of the event $\{(H,H,H),(H,H,T),(H,T,H),(H,T,T),(T,T,T)\}$?

(d) Let A be the event that our outcome has 0 heads. Let B be the event that our outcome has exactly 2 heads. What is $A \cup B$?

(e) What is the probability of the outcome (H,H,T)?

(f) What is the probability of the event that our outcome has exactly two heads?

(g) What is the probability of the event that our outcome has at least one head?

3 Counting & Probability

Consider the equation $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 70$, where each x_i is a non-negative integer. We choose one of these solutions uniformly at random.

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

(b) What is the probability that both $x_1 \geq 30$ and $x_2 \geq 30$?

(c) What it the probability that either $x_1 \geq 30$ or $x_2 \geq 30$?

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 9B

1 Box of Marbles

You are given two boxes: one of them containing 900 red marbles and 100 blue marbles, the other one contains 500 red marbles and 500 blue marbles.

(a) If we pick one of the boxes randomly, and pick a marble what is the probability that it is blue?

(b) If we see that the marble is blue, what is the probability that it is chosen from box 1?

(c) Suppose we pick one marble from box 1 and without looking at its color we put it aside. Then we pick another marble from box 1. What is the probability that the second marble is blue?

2 Duelling Meteorologists

Tom is a meteorologist in New York. On days when it snows, Tom correctly predicts the snow 70% of the time. When it doesn't snow, he correctly predicts no snow 95% of the time. In New York, it snows on 10% of all days.

(a) If Tom says that it is going to snow, what is the probability it will actually snow?

(b) Let A be the event that, on a given day, Tom predicts the weather correctly. What is $\mathbb{P}(A)$?

(c) Tom's friend Jerry is a meteorologist in Alaska. Jerry claims that she is a better meteorologist than Tom even though her overall accuracy is lower. After looking at their records, you determine that Jerry is indeed better than Tom at predicting snow on snowy days and sun on sunny day. Give an instance of the situation described above. *Hint: what is the weather like in Alaska?*

3 Binary Conditional Probabilities

Let us consider a sample space $\Omega = \{\omega_1, \ldots, \omega_N\}$ of size $N > 2$, and two probability functions $\mathbb{P}_1$ and $\mathbb{P}_2$ on it. That is, we have two probability spaces: $(\Omega, \mathbb{P}_1)$ and $(\Omega, \mathbb{P}_2)$.

If for every subset $A \subset \Omega$ of size $|A| = 2$ and every outcome $\omega \in \Omega$ it is true that $\mathbb{P}_1(\omega \mid A) = \mathbb{P}_2(\omega \mid A)$, then is it necessarily true that $\mathbb{P}_1(\omega) = \mathbb{P}_2(\omega)$ for all $\omega \in \Omega$? That is, if $\mathbb{P}_1$ and $\mathbb{P}_2$ are equal conditional on events of size 2, are they equal unconditionally? (*Hint*: Remember that probabilities must add up to 1.)

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 10A

1 Probability Potpourri

Prove a brief justification for each part.

(a) For two events A and B in any probability space, show that $\mathbb{P}(A \setminus B) \geq \mathbb{P}(A) - \mathbb{P}(B)$.

(b) If $|\Omega| = n$, how many distinct events does the probability space have?

(c) Suppose $\mathbb{P}(D \mid C) = \mathbb{P}(D \mid \overline{C})$, where $\overline{C}$ is the complement of C. Prove that D is independent of C.

2 Aces

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.

3 Balls and Bins

Throw n balls into n labeled bins one at a time.

(a) What is the probability that the first bin is empty?

(b) What is the probability that the first k bins are empty?

(c) Let A be the event that at least k bins are empty. Notice that there are $m = \binom{n}{k}$ sets of k bins out of the total n bins. If we assune A_i is the event that the i^{th} set of k bins is empty. Then we can write A as the union of A_i's.

$$A = \bigcup_{i=1}^{m} A_i.$$

Write the union bound for the probability A.

(d) Use the union bound to give an upper bound on the probability A from part (c).

(e) What is the probability that the second bin is empty given that the first one is empty?

(f) Are the events that "the first bin is empty" and "the first two bins are empty" independent?

(g) Are the events that "the first bin is empty" and "the second bin is empty" independent?

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 10B

1 Pullout Balls

Suppose you have a bag containing six balls numbered $1, 2, 3, 4, 5, 6$.

(a) You perform the following experiment: pull out a single ball and record its number. What is the expected value of the number that you record?

(b) You repeat the experiment from part (a), except this time you pull out two balls together and record the product of their numbers. What is the expected value of the total that you record?

2 How Many Queens?

You shuffle a standard 52-card deck, before drawing the first three cards from the top of the pile. Let X denote the number of queens you draw.

(a) What is $\mathbb{P}(X = 0)$, $\mathbb{P}(X = 1)$, $\mathbb{P}(X = 2)$ and $\mathbb{P}(X = 3)$?

(b) What do your answers you computed in part a add up to?

(c) Compute $\mathbb{E}(X)$ from the definition of expectation.

(d) Are the X_i indicators independent?

3 Head Count

Consider a coin with $\mathbb{P}(\text{Heads}) = 2/5$. Suppose you flip the coin 20 times, and define X to be the number of heads.

(a) Name the distribution of X and what its parameters are.

(b) What is $\mathbb{P}(X = 7)$?

(c) What is $\mathbb{P}(X \geq 1)$? Hint: You should be able to do this without a summation.

(d) What is $\mathbb{P}(12 \leq X \leq 14)$?

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 DIS 11A

1 Linearity

Solve each of the following problems using linearity of expectation. Explain your methods clearly.

(a) In an arcade, you play game A 10 times and game B 20 times. Each time you play game A, you win with probability $1/3$ (independently of the other times), and if you win you get 3 tickets (redeemable for prizes), and if you lose you get 0 tickets. Game B is similar, but you win with probability $1/5$, and if you win you get 4 tickets. What is the expected total number of tickets you receive?

(b) A monkey types at a 26-letter keyboard with one key corresponding to each of the lower-case English letters. Each keystroke is chosen independently and uniformly at random from the 26 possibilities. If the monkey types 1 million letters, what is the expected number of times the sequence "book" appears?

2 Joint Distributions

(a) Give an example of discrete random variables X and Y with the property that $\mathbb{E}[XY] \neq \mathbb{E}[X]\mathbb{E}[Y]$. You should specify the joint distribution of X and Y.

(b) Give an example of discrete random variables X and Y that (i) are *not independent* and (ii) have the property that $\mathbb{E}[XY] = 0$, $\mathbb{E}[X] = 0$, and $\mathbb{E}[Y] = 0$. Again you should specify the joint distribution of X and Y.

3 Ball in Bins

You are throwing k balls into n bins. Let X_i be the number of balls thrown into bin i.

(a) What is $\mathbb{E}[X_i]$?

(b) What is the expected number of empty bins?

(c) Define a collision to occur when two balls land in the same bin (if there are n balls in a bin, count that as $n-1$ collisions). What is the expected number of collisions?

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 DIS 11B

1 Variance Proofs

(a) Let X be a random variable. Prove that:

$$\text{Var}(X) \geq 0$$

(b) Let $X_1, \ldots, X_n$ be random variables. Prove that:

$$\text{Var}(X_1 + \cdots + X_n) = \sum_{i=1}^{n} \text{Var}(X_i) + 2 \sum_{1 \leq i < j \leq n} \text{cov}(X_i, X_j)$$

Hint: Without loss of generality we can assume that $\mathbb{E}[X_1] = \cdots = \mathbb{E}[X_n] = 0$. Why?

(c) Let $a_1, \ldots, a_n \in \mathbb{R}$, and $X_1, \ldots, X_n$ be random variables. Prove that:

$$\sum_{i=1}^{n} a_i^2 \cdot \text{Var}(X_i) + 2 \sum_{1 \leq i < j \leq n} a_i \cdot a_j \cdot \text{cov}(X_i, X_j) \geq 0$$

2 Subset Card Game

Jonathan and Yiming are playing a card game. Jonathan has $k > 2$ cards, and each card has a real number written on it. Jonathan tells Yiming (truthfully), that the sum of the card values is 0, and that the sum of squares of the values on the cards is 1. Specifically, if the card values are $c_1, c_2, \ldots, c_k$, then we have $\sum_{i=1}^{k} c_i = 0$ and $\sum_{i=1}^{k} c_i^2 = 1$.

The cards are then going to be dealt randomly in the following fashion: for each card in the deck, a fair coin is flipped. If the coin lands heads, then the card goes to Yiming, and if the coin lands tails, the card goes to Jonathan. Note that it is possible for either player to end up with no cards/all the cards.

Calculate $\text{Var}(S)$, where S is the sum of value of cards in Yiming's hand. The answer should not include a summation.

3 Variance

A building has n upper floors numbered $1, 2, \ldots, n$, plus a ground floor G. At the ground floor, m people get on the elevator together, and each person gets off at one of the n upper floors uniformly at random and independently of everyone else. What is the *variance* of the number of floors the elevator *does not* stop at?

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 12A

1 Inequality Practice

(a) X is a random variable such that $X > -5$ and $\mathbb{E}[X] = -3$. Find an upper bound for the probability of X being greater than or equal to -1.

(b) Y is a random variable such that $Y < 10$ and $\mathbb{E}[Y] = 1$. Find an upper bound for the probability of Y being less than or equal to -1.

(c) You roll a die 100 times. Let Z be the sum of the numbers that appear on the die throughout the 100 rolls. Compute $\text{Var}(Z)$. Then use Chebyshev's inequality to bound the probability of the sum Z being greater than 400 or less than 300.

2 Vegas

On the planet Vegas, everyone carries a coin. Many people are honest and carry a fair coin (heads on one side and tails on the other), but a fraction p of them cheat and carry a trick coin with heads on both sides. You want to estimate p with the following experiment: you pick a random sample of n people and ask each one to flip his or her coin. Assume that each person is independently likely to carry a fair or a trick coin.

1. Given the results of your experiment, how should you estimate p?
   (*Hint:* Construct an (unbiased) estimator for p such that $E[\hat{p}] = p$.)

2. How many people do you need to ask to be 95% sure that your answer is off by at most 0.05?

3 Working with the Law of Large Numbers

(a) A fair coin is tossed multiple times and you win a prize if there are more than 60% heads. Which number of tosses would you prefer: 10 tosses or 100 tosses? Explain.

(b) A fair coin is tossed multiple times and you win a prize if there are more than 40% heads. Which number of tosses would you prefer: 10 tosses or 100 tosses? Explain.

(c) A fair coin is tossed multiple times and you win a prize if there are between 40% and 60% heads. Which number of tosses would you prefer: 10 tosses or 100 tosses? Explain.

(d) A fair coin is tossed multiple times and you win a prize if there are exactly 50% heads. Which number of tosses would you prefer: 10 tosses or 100 tosses? Explain.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 12B

1 Planetary Party

(a) Suppose we are at party on a planet where every year is 2849 days. If 30 people attend this party, what is the exact probability that two people will share the same birthday? You may leave your answer as an unevaluated expression.

(b) From lecture, we know that given n bins and m balls, $\mathbb{P}\left[\text{no collision}\right] \approx \exp(-m^2/(2n))$. Using this, give an approximation for the probability in part (a).

(c) What is the minimum number of people that need to attend this party to ensure that the probability that any two people share a birthday is at least 0.5? You can use the approximation you used in the previous part.

(d) Now suppose that 70 people attend this party. What the is probability that none of these 70 individuals have the same birthday? You can use the approximation you used in the previous parts.

2 Throwing Balls into a Depth-Limited Bin

Say you want to throw n balls into n bins with depth $k-1$ (they can fit $k-1$ balls, after that the bins overflow). Suppose that n is a large number and $k = 0.1n$. You throw the balls randomly into the bins, but you would like it if they don't overflow. You feel that you might expect not too many balls to land in each bin, but you're not sure, so you decide to investigate the probability of a bin overflowing.

(a) Count the number of ways we can select k balls to put in the first bin, and then throw the remaining balls randomly. You should assume that the balls are distinguishable.

(b) Argue that your answer in (a) is an upper bound for the number of ways that the first bin can overflow.

(c) Calculate an upper bound on the probability that the first bin will overflow.

(d) Upper bound the probability that some bin will overflow. [*Hint*: Use the union bound.]

(e) How does the above probability scale as n gets really large?

3 The Memoryless Property

Let X be a discrete random variable which takes on values in $\mathbb{Z}_+$. Suppose that for all $m, n \in \mathbb{N}$, we have $\mathbb{P}(X > m+n \mid X > n) = \mathbb{P}(X > m)$. Prove that X is a geometric distribution. Hint: In order to prove that X is geometric, it suffices to prove that there exists a $p \in [0,1]$ such that $\mathbb{P}(X > i) = (1-p)^i$ for all $i > 0$.

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 13A

1 Continuous Joint Densities

The joint probability density function of two random variables X and Y is given by $f(x,y) = Cxy$ for $0 \leq x \leq 1, 0 \leq y \leq 2$, and 0 otherwise (for a constant C).

(a) Find the constant C that ensures that $f(x,y)$ is indeed a probability density function.

(b) Find $f_X(x)$, the marginal distribution of X.

(c) Find the conditional distribution of Y given $X = x$.

(d) Are X and Y independent?

2 Uniform Distribution

You have two fidget spinners, each having a circumference of 10. You mark one point on each spinner as a needle and place each of them at the center of a circle with values in the range $[0, 10)$ marked on the circumference. If you spin both (independently) and let X be the position of the first spinner's mark and Y be the position of the second spinner's mark, what is the probability that $X \geq 5$, given that $Y \geq X$?

3 Darts with Friends

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

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

- What's the cumulative distribution function of X?
- What's the cumulative distribution function of Y?
- What's the probability density function of X?
- 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 $U = \min\{X, Y\}$?

(d) What's the cumulative distribution function of $V = \max\{X, Y\}$?

(e) What is the expectation of the absolute difference between Michelle's and Alex's distances from the center, that is, what is $\mathbb{E}[|X - Y|]$? [*Hint*: Use parts (c) and (d), together with the continuous version of the tail sum formula, which states that $\mathbb{E}[Z] = \int_0^\infty P(Z \geq z)dz$.]

CS 70 Discrete Mathematics and Probability Theory
Fall 2020

DIS 14A

1 First Exponential to Die

Let X and Y be Exponential(λ_1) and Exponential(λ_2) respectively, independent. What is

$$\mathbb{P}\big(\min(X,Y) = X\big),$$

the probability that the first of the two to die is X?

2 Chebyshev's Inequality vs. Central Limit Theorem

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) Can you use b 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 $n \to \infty$, can you provide approximations for $\mathbb{P}[Z_n \geq 2]$ and $\mathbb{P}[Z_n \leq -2]$?

3 Why Is It Gaussian?

Let X be a normally distributed random variable with mean μ and variance σ^2. Let $Y = aX + b$, where $a > 0$ and b are non-zero real numbers. Show explicitly that Y is normally distributed with mean $a\mu + b$ and variance $a^2\sigma^2$. The PDF for the Gaussian Distribution is $\frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$. One approach is to start with the cumulative distribution function of Y and use it to derive the probability density function of Y.

[1.You can use without proof that the pdf for any gaussian with mean and sd is given by the formula $\frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$ where μ is the mean value for X and σ^2 is the variance. 2. The drivative of CDF gives PDF.]

CS 70 Discrete Mathematics and Probability Theory
Fall 2020 DIS 14B

1 Markov Chains: Prove/Disprove

Prove or disprove the following statements, using the definitions from the previous question.

(a) There exists an irreducible, finite Markov chain for which there exist initial distributions that converge to different distributions.

(b) There exists an irreducible, aperiodic, finite Markov chain for which $\mathbb{P}(X_{n+1} = j \mid X_n = i) = 1$ or 0 for all i, j.

(c) There exists an irreducible, non-aperiodic Markov chain for which $\mathbb{P}(X_{n+1} = j \mid X_n = i) \neq 1$ for all i, j.

(d) For an irreducible, non-aperiodic Markov chain, any initial distribution not equal to the invariant distribution does not converge to any distribution.

2 Can it be a Markov Chain?

(a) A fly flies in a straight line in unit-length increments. Each second it moves to the left with probability 0.3, right with probability 0.3, and stays put with probability 0.4. There are two spiders at positions 1 and m and if the fly lands in either of those positions it is captured. Given that hte fly starts between positions 1 and m, model this process as a Markov Chain.

(b) Take the same scenario as in the previous part with $m = 4$. Let $Y_n = 0$ if at time n the fly is in position 1 or 2 and let $Y_n = 1$ if at time n the fly is in position 3 or 4. Is the process Y_n a Markov chain?

3 Allen's Umbrella Setup

Every morning, Allen walks from his home to Soda, and every evening, Allen walks from Soda to his home. Suppose that Allen has two umbrellas in his possession, but he sometimes leaves his

umbrellas behind. Specifically, before leaving from his home or Soda, he checks the weather. If it is raining outside, he will bring his umbrella (that is, if there is an umbrella where he currently is). If it is not raining outside, he will forget to bring his umbrella. Assume that the probability of rain is p.

(a) Model this as a Markov chain. What is $\mathscr{X}$? Write down the transition matrix.

(b) What is the transition matrix after 2 trips? n trips? Determine if the distribution of X_n converges to the invariant distribution, and compute the invariant distribution. Determine the long-term fraction of time that Allen will walk through rain with no umbrella.

4 Three Tails

You flip a fair coin until you see three tails in a row. What is the average number of heads that you'll see until getting TTT?

Hint: How is this different than the number of *coins* flipped until getting TTT?