CS 70 Discrete Mathematics and Probability Theory
Summer 2019 James Hulett and Elizabeth Yang

Final

PRINT your name: _____ _____
(First) (Last)

SIGN your name: _____

PRINT your student ID: _____

CIRCLE your exam room: VLSB 2050 VLSB 2060 Soda 320 Soda 380 Soda 405

Name of the person sitting to your left: _____

Name of the person sitting to your right: _____

- We will not grade anything outside of the space provided for a problem unless we are clearly told in the space provided for the question to look elsewhere.
- We will not be collecting scratch paper. Write everything you want to be graded on the exam itself.
- For problems with answers modulo m, only answers between 0 and $m-1$ will receive full credit.
- Assume all graphs are undirected and have no self-loops or parallel edges unless otherwise specified.
- Assume independence means *mutual independence* unless otherwise noted.
- You may use binomial coefficients in your answers, unless the question otherwise specifies an answer form (e.g. fraction, decimal).
- Unless otherwise specified, you may use any variables from the problem in your answer.
- Unless otherwise specified, summations and integrals are not allowed in short answer boxes.
- You may consult three handwritten double-sided sheets of notes. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronics devices are prohibited.
- There are 22 pages (11 sheets) on the exam. Notify a proctor immediately if a page is missing.
- There are 10 questions on this exam, worth a total of 270 points.
- **You may, without proof, use theorems and facts that were proven in the notes, lecture, discussion, or homework.**
- **You have 180 minutes.**

Do not turn this page until your instructor tells you to do so.

1 True/False [3 Points Each, 36 Total]

1 point for True/False marking, 2 points for justification.

For each statement, mark whether it is true or false and give a brief justification (maximum 1 sentence, must fit in box) in the adjacent box.

(a) $(\neg P \implies \neg Q) \equiv (Q \implies P)$

◯ **True**

◯ **False**

Answer: True. $Q \implies P$ is the contrapositive of $(\neg P) \implies (\neg Q)$.

(b) An irreducible Markov Chain with a self-loop must be aperiodic.

◯ **True**

◯ **False**

Answer: True. At the vertex with the self-loop, there exists a cycle of length 1, so the gcd of all cycle lengths must be 1.

(c) Suppose that for random variables X and Y, if $\mathbb{P}(X = x, Y = y) = \mathbb{P}(X = x)\mathbb{P}(Y = y)$ for all x and y. Then $\mathbb{E}[XY] = \mathbb{E}[X]\mathbb{E}[Y]$.

◯ **True**

◯ **False**

Answer: True. Independence of two random variables implies they are uncorrelated.

(d) Let $G = (V, E)$ be a simple, connected, bipartite graph. If we create a Markov Chain with state space V that transitions to any neighbor of the current state with equal probability, the chain will be periodic.

◯ **True**

◯ **False**

Answer: True. All cycles in a bipartite graph have even length, so the gcd of the cycle lengths must be a multiple of 2 and therefore not 1.

(e) Suppose you throw n balls in n bins uniformly at random. Let X be the number of balls in bin 1 and let Y be the number of balls in bin 2. Then $\mathbb{E}[XY] > \mathbb{E}[X]\mathbb{E}[Y]$.

◯ **True**

◯ **False**

Answer: False. If there are more balls in bin 1, there are fewer balls available to be in bin 2, so we must have that $\text{cov}(X,Y) < 0$, where $\text{cov}(X,Y) = \mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y]$.

(f) Let $X \sim \text{Bin}(n,p)$ and $Y \sim \text{Bin}(m,p)$ be independent. Then $X+Y \sim \text{Bin}(n+m,p)$.

◯ **True**

◯ **False**

Answer: True. We are adding the number of successes in n independent Bernoulli trials with that in m other independent trials, which is just the number of successes in $n+m$ independent trials.

(g) Suppose X has distribution given by $\mathbb{P}[X=1] = \mathbb{P}[X=-1] = \frac{1}{2}$, and $Y = X^2$. Then, $\text{Cov}(X,Y) = 0$.

◯ **True**

◯ **False**

Answer: True. Y always takes on the value 1, and everything has zero correlation with a constant. Alternatively, we could find it directly. $E[X] = \frac{1}{2} * 1 + \frac{1}{2} * (-1) = 0$, so we only need to find $E[XY]$. $E[XY] = 1 * 1 * \frac{1}{2} + 1 * (-1) * \frac{1}{2} = 0$. Therefore $\text{Cov}(X,Y) = E[XY] - E[X]E[Y] = 0$.

(h) Working over $GF(7)$, the polynomials $x^8 - 1$ and $(x+1)(x-1)$ are equivalent.

◯ **True**

◯ **False**

Answer: True. We know that $x^7 \equiv x \pmod 7$, so $x^8 - 1 \equiv x^2 - 1 \equiv (x+1)(x-1) \pmod 7$.

(i) There exists integers a, b such that $39a + 15b = 7$.

◯ **True**

◯ **False**

Answer: False. Both 39 and 15 are divisible by 3, so any linear combination of them needs to be as well.

(j) If a problem A reduces to the Halting Problem, then A is recognizable.

◯ **True**

◯ **False**

Answer: False. We can trivially use the Halting Problem to solve the Looping Problem, but the Looping Problem is not recognizable.

(k) If A is uncountable and $A - B$ is countable, then B must be uncountable.

◯ **True**

◯ **False**

Answer: True. If B were countable, then $(A - B) \cup B$, which is a superset of A, would be the union of two countable sets, and hence countable.

(l) If the public key of an RSA scheme is $(N = 11 \cdot 13, e = 7)$, $d = 41$ is a valid decryption key.

◯ **True**

◯ **False**

Answer: False. $7 \cdot 41 = 287 = 47 \pmod{10 \cdot 12}$, which is not equal to $1 \pmod{10 \cdot 12}$.

2 Short Answer [3 Points Each, 87 Total]

Logic

(a) Consider the propositional formula $[(\neg A) \wedge B] \vee [A \wedge C]$. Write an equivalent formula that uses **only** $\vee$ and $\neg$ (ie, does not use $\wedge$).

Answer: $\big(\neg[A \vee (\neg B)]\big) \vee \big(\neg[(\neg A) \vee (\neg C)]\big)$. We use De Morgan's laws to convert anything of the form $P \wedge Q$ to $\neg[(\neg P) \vee (\neg Q)]$.

(b) Let P be the set of all basketball players in the NBA, C be the set of all coaches in the NBA, and $\mathbf{R}(c)$ be the set of all players on the team that coach c coaches. Define the following statements:

$B(c,x,y)$: "Coach c thinks player x is **better** than or equal to player y"

$F(c,x)$: "Coach c's **favorite** player on his own team is player x"

Write each statement below in terms of propositional logic.

(i) There is not a player that every coach thinks is the best player in the NBA.

Answer: $\neg[\exists p \in P, \forall c \in C, \forall p' \in P, B(c,p,p')]$

(ii) Every coach thinks that their favorite player on their team is the best player on their team or the best player in the NBA.

Answer: $(\forall c \in C, \forall p \in \mathbf{R}(c))[F(c,p) \implies [(\forall p' \in \mathbf{R}(c), B(c,p,p')) \vee (\forall p' \in P, B(c,p,p'))]]$

Polynomials

(c) If the error polynomial in the Berlekamp-Welch procedure is $E(x) = x$, where is the error? Assume that there is one corruption.

Answer: $E(x)$ has a single root at 0, so that is where the error is.

(d) What's the maximum number of roots a polynomial can have in $GF(p)$, where p is a prime?

Answer: p. There are only p points to plug into the polynomial, so a polynomial can certainly never have more than p roots. To see that one can acheive this maximum, consider the zero polynomial or something like $x^p - x$.

(e) Let $P(x)$ and $Q(x)$ be two **distinct** polynomials of degrees d_P and d_Q. If P and Q intersect at k points that all lie on a degree exactly $k-1$ polynomial, what is the smallest possible value of $d_P + d_Q$?

Answer: $2k-1$. First, we note that there is a unique degree at most $k-1$ polynomial passing through the k points of intersection, which the problem tells us is in fact degree exactly $k-1$. Hence, since both P and Q pass through all those points, they must both be degree at least $k-1$. But they cannot both be degree $k-1$, since then they would be the same polynomial. Hence, one of them must be degree at least k, so the sum of their degrees must be at least $(k-1)+k = 2k-1$.

Graphs

(f) If a connected planar graph has 3 faces and 10 vertices, how many edges does it have?

Answer: 11. Applying Euler's formula, we have that $10+3 = e+2$, so $e = 10+3-2 = 11$.

(g) What is the maximum number of edges we can have in a bipartite graph on $2n$ vertices?

Answer: n^2. If the two sides have m and $2n-m$ vertices, there are $m(2n-m)$ potential edges that could exist. This quantity is maximized when we set $m = n$, at which point we have n^2 edges that can exist.

Modular Arithmetic

(h) Find 3^{13} mod 13.

Answer: From FLT we get this is equal to $3^{13} \equiv 3 \bmod 13$.

(i) Find $42^{63} \pmod{11}$.

Answer: 3. First we can reduce the base of the exponent to $-2 \bmod 11$. Then, by FLT, we can reduce $(-2)^{63} \equiv (-2)^3 \pmod{11}$ Evaluating this, we get $-8 \equiv 3 \pmod{11}$.

(j) For two distinct primes p, q, find $p^{q-1} + q^{p-1} \bmod pq$.

Answer: 1. We can use the CRT to help our calculations. In particular, we know that $p^{q-1} + q^{p-1} \equiv 0^{q-1} + q^{p-1} \equiv q^{p-1} \pmod{p}$; by FLT, this is equivalent to 1 modulo p. We can repeat the calculation with p and q reversed to get $p^{q-1} + q^{p-1} \equiv 1 \pmod{q}$. By inspection, we know that $x \equiv 1 \pmod{pq}$

(k) Let m and n be coprime. If we know that $x \equiv m-1 \pmod{m}$ and $x \equiv n-1 \pmod{n}$, what is the value of x modulo mn? *Simplify* your answer.

Answer: $mn-1$. We can rewrite the constraints as $x \equiv -1 \pmod{m}$ and $x \equiv -1 \pmod{n}$. By inspection, we see that $x \equiv -1 \pmod{mn}$ satisfies both of these constraints. By the CRT, we know that any solution to the two constraints must be equivalent to this modulo mn; the only such value in the range $0, 1, \ldots, mn-1$ is $mn-1$.

(l) Find all primes p such that $70^p \equiv 1 \bmod p$.

Answer: We know from FLT that $a^p \equiv a \bmod p$, so we know that $70^p \equiv 70 \bmod p$. This would mean $70 \equiv 1 \bmod p$ which only happens when $69 \equiv 0 \bmod p$. Therefore, p can only be 23 or 3 since those are the only prime factors of 69.

Bijections

(m) For each function below, fill in the *one* bubble that most completely describes the function.

(i) $f : \mathbb{Z}^+ \to \mathbb{N}$, where $f(x) = x$.

◯ **1-1** ◯ **Onto** ◯ **Both** ◯ **Neither**

Answer: One-to-one. No two elements of $\mathbb{Z}^+$ map to the same element of $\mathbb{N}$, but nothing maps to 0.

(ii) $f : [1, \infty) \to [0, 1]$, where $f(x) = \frac{1}{x}$.

◯ **1-1** ◯ **Onto** ◯ **Both** ◯ **Neither**

Answer: One-to-one. No two elements of $\mathbb{R}^+$ map to the same element of $[0, 1]$, but nothing maps to 0.

(iii) $f : \mathbb{R} \to \mathbb{R}$, where $f(x) = x - 1$ for $x \leq 2$, and $f(x) = 2x^2 - 5$ for $x > 2$.

◯ **1-1** ◯ **Onto** ◯ **Both** ◯ **Neither**

Answer: One-to-one. No two elements of $\mathbb{R}$ map to the same element of $\mathbb{R}$, but nothing maps to the interval $(1, 3]$.

(iv) $f : GF(65) \to GF(65)$, where $f(x) = x^5$. Note that $65 = 5 \cdot 13$.

◯ **1-1** ◯ **Onto** ◯ **Both** ◯ **Neither**

Answer: Both. This is a valid RSA encoding function; 5 is coprime to $(5-1)(13-1) = 48$.

Counting

(n) How many ways can I order the string "BROCCOLI"?

Answer: $\frac{8!}{2!2!}$. 8! ways to order, divide by the 2 O's and divide by the 2 C's.

(o) How many 5-(English) letter strings are there with exactly 3 vowels and 2 consonants? Note that there are 5 vowels and 21 consonants in the alphabet.

Answer: $\binom{5}{3} \cdot 5^3 \cdot 21^2$. There are $\binom{5}{3}$ ways to place the vowels, and for each placement, there are $5^3 \cdot 21^2$ ways to fill the letters.

(p) How many solutions to $x+y+z \leq 30$ where x, y, and z are non-negative integers? *Hint: Introduce a fourth variable, w.*

Answer: Add another variable to get $x+y+z+w = 30$. All 4 variables are non-negative so we can see that this is just stars and bars with 30 stars and 3 bars so the answer is $\binom{33}{3}$

Bounds

(q) Let X be a random variable such that $\mathbb{E}[X] = 10$ and X is always at least -3. Give a non-trivial upper bound on $\mathbb{P}(X \geq 20)$.

Answer: Since X is negative, we cannot apply Markov's inequality directly. We define $Y = X+3 \geq 0$. We see that $\mathbb{E}[Y] = \mathbb{E}[X]+3 = 13$. Since Y is non-negative, we can use Markov's inequality. We see that: $\mathbb{P}(X \geq 20) = \mathbb{P}(X+3 \geq 23) = \mathbb{P}(Y \geq 23) \leq \frac{\mathbb{E}[Y}{23} = \frac{13}{23}$.

(r) I have a random variable Y, and I only know $\mathbb{E}[Y^2] = 6$. Provide the best possible upper bound on $\mathbb{P}(|Y - \mathbb{E}[Y]| \geq 8)$.

Answer: $\frac{3}{32}$. We know that $\text{Var}(Y) = \mathbb{E}[Y^2] - \mathbb{E}[Y]^2 \leq \mathbb{E}[Y^2] = 6$. Hence, by Chebyshev's inequality, we have that $\mathbb{P}(|Y - \mathbb{E}[Y]| \geq 8) \leq \frac{\text{Var}(Y)}{8^2} \leq \frac{6}{64} = \frac{3}{32}$.

Random Variables

(s) Suppose I have the PDF $f_X(x) = cx$ for when $x \in [0,1]$ and 0 elsewhere. Find c.

Answer: $\int_0^1 cx\,dx = 1$, and we solve the integral to see that $\frac{c}{2} = 1$ or $c = 2$.

(t) Suppose $X \sim \mathcal{N}(0,4)$ and $Y \sim \mathcal{N}(1,5)$ are independent. What is $\mathbb{P}(X < Y)$? You may leave your answer in terms of Φ, the CDF of the standard normal distribution.

Answer: $\Phi(\frac{1}{3})$. Since the normal distribution is symmetric, we have that $-Y \sim N(-1,5)$, so $X-Y = X+(-Y) \sim N(-1,9)$. This means that $\frac{X-Y+1}{3} \sim N(0,1)$. Hence, we have $\mathbb{P}(X<Y) = \mathbb{P}(X-Y<0) = \mathbb{P}(\frac{X-Y+1}{3} < \frac{1}{3}) = \Phi(\frac{1}{3})$.

(u) Let X and Y be independent random variables with $\mathbb{E}[X]=1$, $\mathrm{Var}(X)=3$, $\mathbb{E}[Y]=1$, and $\mathrm{Var}(Y)=2$. What is $\mathbb{E}[(X+Y)^2]$?

Answer: $E[X^2+Y^2+2XY] = E[X^2]+E[Y^2]+2E[XY]$. We see that $E[X^2] = \mathrm{Var}(X)+E[X]^2 = 3+1^2 = 4$. We have $E[XY] = E[X]E[Y] = 1*1 = 1$ since X and Y are independent. Finally, we have $E[Y^2] = \mathrm{Var}(Y)+E[Y]^2 = 2+1^2 = 3$.

Therefore, we have the final answer to be: $4+3+2*1 = 9$.

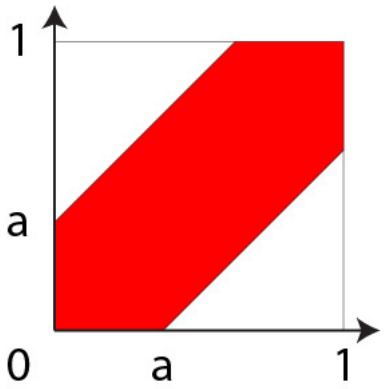
(v) Let X be uniform in the range $[0,1]$ and let $Y = \max(X, 1-X)$. What is the PDF of Y?

Answer: $f_Y(y) = 2$ for $y \in [\frac{1}{2}, 1]$ and $f_Y(y) = 0$ otherwise. We first note that one of X and $1-X$ must always be at least $\frac{1}{2}$, but neither of them can be larger than 1, so the maximum of the two must always be in the range $[\frac{1}{2}, 1]$.

Knowing this, we now attempt to find the cdf of Y; that is, we want to find $\mathbb{P}(Y \le y)$ for $y \in [\frac{1}{2}, 1]$. In order for the maximum of $1-X$ and X to be y or smaller, we must have that $X \le y$ and $1-X \le y$, where the latter can be rewritten as $X \ge 1-y$. Hence, $\mathbb{P}(Y \le y) = \mathbb{P}(1-y \le X \le y)$. Since X is uniform, this last probability is just the length of the interval $[1-y, y]$ (which is $y-(1-y) = 2y-1$) divided by the length of the interval $[0,1]$ (which is 1). Hence, the cdf of Y is $2y-1$, so we take the derivative to get the pdf $f_Y(y) = 2$ for $y \in [\frac{1}{2}, 1]$.

(w) Let X, Y be independent uniform random variables over the $[0,1]$ interval. Find the CDF of $|Y-X|$.

Answer: For $a \in [0,1]$, $\mathbb{P}(|Y-X| \ge a) = 1-(1-a^2)$ (and is zero outside this range). We can find this probability by calculating the area of the following region:



Here, we notice that the area of the overall square is 1, while each of the two white triangles have an area of $\frac{1}{2}(1-a)(1-a)$. Hence, the area of the red shape is $1-\frac{1}{2}(1-a)^2-\frac{1}{2}(1-a)^2 = 1-(1-a)^2$.

(x) Let X, Y be independent exponential random variables with means $\lambda_X = 1$ and $\lambda_Y = 2$.

(i) What is the PDF of $\min(X,Y)$?

Answer: First, we compute the CDF of $\min(X,Y)$:

$$\begin{aligned}\mathbb{P}[\min(X,Y) \le t] &= 1-\mathbb{P}[\min(X,Y) \ge t] \\ &= 1-\mathbb{P}[X \ge t, Y \ge t] \\ &= 1-\mathbb{P}[X \ge t]\mathbb{P}[Y \ge t] \\ &= 1-e^{-(\lambda_X+\lambda_Y)t}\end{aligned}$$

We differentiate with respect to t to compute the PDF, so we obtain $f_{\min(X,Y)}t = (\lambda_X+\lambda_Y)e^{-(\lambda_X+\lambda_Y)t} = 3e^{-3t}$

(ii) What is $\mathbb{E}[\min(X,Y)]$?

Answer: Using the PDF from above, $\min(X,Y) \sim \text{Expo}(3)$ so the expectation should be $\frac{1}{3}$.

3 A Midsummer Light's Dream [3/3/3/5/4/3/3 Points, 24 Total]

Any correct answer will receive full credit. Partial credit may be awarded if work is shown. Parts (e)-(g) do not rely on (a)-(d), and vice versa.

On Bernoulli Ave., there are $(n+1)$ lamps in a line, spaced 1 block apart. We treat the lamps as the locations $\{0,1,2,\ldots,n\}$ on a number line, and the "blocks" as the intervals $(0,1),(1,2),\ldots,(n-1,n)$.

Each lamp is turned on independently with probability p. A block $(i,i+1)$ is "illuminated" if both the light at i and the light at $(i+1)$ are on. Let X_i be an indicator for the block $(i,i+1)$ being illuminated, and let X be the total number of illuminated blocks. *Your answers may be in terms of n, p.*

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

Answer: np^2. We have $X = X_1 + X_2 + \ldots + X_n$, so $\mathbb{E}[X] = \mathbb{E}[X_1] + \mathbb{E}[X_2] + \ldots + \mathbb{E}[X_n]$. Each X_i is a Bernoulli where $\mathbb{P}[X_i = 1] = p^2$, so $\mathbb{E}[X_i] = p^2$ for all i. We conclude the answer.

(b) Consider i, j where $|i-j| = 1$. What is $\mathbb{E}[X_iX_j]$?

Answer: p^3. If $|i-j| = 1$, then the two intervals share a lamp. The event $X_iX_j = 1$ corresponds to 3 different lamps being lit, which occurs with probablity p^3.

(c) Now consider i, j where $|i-j| > 1$. What is $\mathbb{E}[X_iX_j]$?

Answer: p^4. If $|i-j| > 1$, then the two intervals do not share any lamps. The event $X_iX_j = 1$ corresponds to 4 different lamps being lit, which occurs with probablity p^4.

(d) Compute $\text{Var}(X)$. You may leave your answers in terms of a, b, c, the answers from Parts (a), (b), (c), respectively.

(Problem continued on the next page.)

Answer: $a+2(n-1)b+(n-1)(n-2)(c)-a^2$. Alternate form: $p^2(n+2(n-1)p-(3n-2)p^2)$.

We note that $\mathbb{E}[X^2]=\sum_{i=1}^n \mathbb{E}[X_i^2]+\sum_{i\neq j}\mathbb{E}[X_iX_j]$.
The first sum is equivalent to $\mathbb{E}[X]=\sum_{i=1}^n \mathbb{E}[X_i^2]$, as X_i^2 has the same distribution as X_i.
The second sum is $2(n-1)b+(n-1)(n-2)c$, because there are $2(n-1)$ pairs (i,j) with $|i-j|=1$, leaving $(n-1)(n-2)$ pairs (i,j) with $|i-j|>1$.
Lastly, we need to subtract $\mathbb{E}[X]^2$.

Now, imagine that every evening, each lamp is turned on independently with probability p. Each evening, a different set of lamps may be lit. A (questionably effective) lamp inspector is assigned to Bernoulli Ave. Initially, all blocks are unapproved.

Every evening, the inspector samples a block uniformly at random among *all* blocks. If it is not illuminated or it is already approved, the inspector does nothing. Otherwise, if the block is not already approved and is illuminated, he is satisfied and approves it. Let N be the number of evenings that the inspector needs until he approves all blocks.

(e) Suppose the inspector has already approved exactly $(i-1)$ blocks. What is the probability q_i that the inspector approves a new block tonight? *(Your answer may be in terms of n,p,i,k.)*

Answer: $\frac{n-i+1}{n}\cdot p^2$. In order for the inspector to approve a new block, they need to (1) choose a block that isn't already approved, and (2) have that block be illuminated. (1) occurs with probability $\frac{n-i+1}{n}$, and (2) occurs independently with probability p^2; these events are independent of one another.

(f) What is $\mathbb{E}[N]$? You may leave your answer in terms of the variables q_i for $i=1,\ldots,n$, where q_i is the answer to Part (e). *You may use a summation, but you may not use expectations in your answer.*

Answer: $\sum_{i=1}^n \frac{1}{q_i}$. Alternate form: $\frac{n}{p^2}\ln n$. This is a variant of the coupon collector problem.

If we let N_i be the number of nights between the $(i-1)$st and ith approvals, we'll have that $N=N_1+N_2+\ldots+N_n$. From the previous part, we know that N_i is a Geometric RV with parameter q_i, so $\mathbb{E}[N_i]=\frac{1}{q_i}=\frac{n}{p^2(n-i+1)}$. Hence, we have $\mathbb{E}[N]=\mathbb{E}[N_1]+\ldots+\mathbb{E}[N_n]=\sum_{i=1}^n\frac{1}{q_i}=\sum_{i=1}^n\frac{n}{p^2(n-i+1)}=\frac{n}{p^2}\sum_{i=1}^n\frac{1}{(n-i+1)}\approx\frac{n}{p^2}\ln n$.

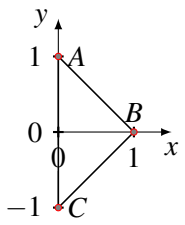
(g) What is $\mathrm{Var}[N]$? You may leave your answer in terms of q_i for $i=1,\ldots,n$, where q_i is the answer to Part (e). *You may use a summation, but you may not use expectations or variances in your answer.*

Answer: $\sum_{i=1}^{n} \frac{1-q_i}{q_i^2}$. The N_i are mutually independent. Thus, we can write $\text{Var}(N) = \text{Var}(N_1) + \ldots + \text{Var}(N_n) = \sum_{i=1}^{n} \frac{1-q_i}{q_i^2}$.

4 It Can't Hurt To Try-angle [3/3/4/5 Points, 15 Total]

Suppose we have the triangle as below. It is defined by 3 vertices A, B, C. The coordinates are: $A : (0,1), B : (1,0), C : (0,-1)$.

We choose a point uniformly at random in the triangle. Let the random variable X be the x-coordinate of the point and let the random variable Y be the y-coordinate of the point.



(a) Find $f_{X,Y}(x,y)$, i.e. the joint density of X and Y.

Answer: The area of the triangle is 1, so the joint density within the triangle will be $\frac{1}{1} = 1$; outside the triangle, the density is zero.

(b) Find $\mathbb{E}[Y]$.

Answer: 0 by symmetry. Y is symmetric around the x-axis, so on average it should be equal to 0.

(c) Find the PDF of X.

Answer: We first find the cdf or $P(X \leq x)$. We see that if we draw a vertical line at $X = x$, then the area is the total area minus the area of the triangle. The base of the triangle is $2(1-x)$ and the height of the triangle is $(1-x)$. Therefore, the area of the triangle is $(1-x)^2$. Thus, the cdf is $1-(1-x)^2$. We take the derivative to get the pdf which is $2(1-x)$.

(d) Let $Z = |X| + |Y|$. Find the PDF of Z.

Answer: $P(Z \leq z) = 0$ if $z < 0$ and $P(Z \leq z) = 1$ if $z > 1$. We can see that $|X| + |Y|$ is at most 1.

If we look at the region $|X| + |Y| \leq z$, it's just the triangle with vertices $(z,0)$, $(0,z)$, $(0,-z)$. The area of this triangle is $\frac{1}{2}z \cdot 2z = z^2$. Thus, the pdf is $2z$ for $0 < z < 1$ and 0 elsewhere.

5 Staff Curry [2/2/2/3/3/3/3/3/3/3/3 Points, 30 Total]

(a) Vishnu and James are playing basketball! Vishnu, a secret NBA prodigy, scores on half of all shots he takes; James, who hasn't played since high school, has only a $\frac{1}{4}$ chance of scoring on each shot. Assume that each shot is independent of all others.

Vishnu and James play the following game: in each round, they both try to take a shot. If one of them scores and the other doesn't, the player that scored wins. Otherwise (if neither of them score or both of them score), the game moves on to the next round.

(i) What is the probability that Vishnu wins *in the first round*?

Answer: $\frac{3}{8}$. In order for Vishnu to win in the first round, we need him to make his shot and James to miss his. The former happens with probability $\frac{1}{2}$ and the latter happens independently with probability $\frac{3}{4}$.

(ii) What is the probability that James wins *in the first round*?

Answer: $\frac{1}{8}$. Similar to the last part, we know that in order for James to win in the first round, we need James to score and Vishnu to miss. These events happen independently with probabilities $\frac{1}{4}$ and $\frac{1}{2}$, respectively.

(iii) What distribution does the number of rounds in the game follow? Give a name and list any parameter(s). *(No formulas necessary.)*

Answer: Geometric with parameter $\frac{1}{2}$. In the first round, there is a $\frac{3}{8}+\frac{1}{8}=\frac{1}{2}$ chance that one of the two players wins. If neither player wins, we play another round that has exactly the same probabilities of each outcome. Hence, at each round there is a $\frac{1}{2}$ chance that the game immediately ends and a $\frac{1}{2}$ chance that the game continues to another round, which will exactly define a Geometric$(\frac{1}{2})$ distribution.

(iv) What is the probability that Vishnu wins *given that* the game ends in exactly one round? You may leave your answer in terms of (i) and (ii), the answers to the corresponding two parts.

Answer: $\frac{(i)}{(i)+(ii)}=\frac{3}{4}$. By the definition of conditional probability, this is just the probability that Vishnu wins in exactly one round divided by the probability that the game ends in exactly one

round. By the total probability rule, the latter is just the probability that Vishnu wins in one round plus the probability that James does.

(v) What is the probability that Vishnu eventually wins the game? You may leave your answer in terms of (i), (ii), and (iv), the answers to those parts.

Answer: $(iv) = \frac{(i)}{(i)+(ii)} = \frac{3}{4}$. Let p be the probability that Vishnu wins. If the game ends after exactly one round, we know that Vishnu wins with probability (iv). If the game does not end in the first round, the game starting from the second round has exactly the same distribution as the original game, since the rounds are all independent of one another. Thus, given that the game does not finish after one round, Vishnu will have a probability p of winning! Putting this all together, we have

$$\mathbb{P}(\text{Vishnu wins}) = \mathbb{P}(\text{Vishnu wins}|1\text{ round})\mathbb{P}(1\text{ round}) + \mathbb{P}(\text{Vishnu wins}|>1\text{ round})\mathbb{P}(>1\text{ round})$$
$$p = (iv)\cdot\frac{1}{2} + p\cdot\frac{1}{2}$$

Solving for p gives us (iv).

(vi) To level the playing field, we require Vishnu to take two shots each round; he must score both of them in order for it to count. Now what is the probability that Vishnu eventually wins?

Answer: $\frac{1}{2}$. The probability that Vishnu scores on both shots in a round is $\frac{1}{2}\cdot\frac{1}{2} = \frac{1}{4}$, as the shots are independent from each other. Hence, both Vishnu and James have a $\frac{1}{4}$ chance of "succeeding" in any given round, so by symmetry they each have a $\frac{1}{2}$ chance of eventually winning.

One could also repeat the calculations from the previous parts, which would yield the same answer.

(b) Now suppose that Vishnu and James are playing a full game of basketball. In an attempt to avoid James' guarding, Vishnu takes his shot from a distance uniformly distributed in the real interval $[4,8]$; if he shoots from a distance of d, his probability of scoring is $p(d)$.

(i) Fill in the boxes such that the following integral calculates the probability of Vishnu scoring.

$$\int_{\square}^{\square} \square \, dx$$

Answer: $\int_4^8 \frac{1}{4} p(x)dx$

(ii) Describe in one sentence what the variable of integration x represents.

Answer: x represents the distance at which Vishnu takes his shot.

(c) Continuing from the last part, let $p(d) = \frac{12}{d^2}$. Do not include integrals in any of the following answers.

(i) What is the probability that Vishnu scores?

Answer: Plugging in to our integral from before, we get

$$\int_4^8 \frac{1}{4} \cdot \frac{12}{x^2} dx = 3\int_4^8 \frac{1}{x^2} dx = 3\left[-\frac{1}{x}\right]_4^8 = 3\left(\frac{1}{4} - \frac{1}{8}\right) = \frac{3}{8}$$

(ii) What is the probability that Vishnu scores if we know that he shot from a distance of 6 or less?

Answer: $\frac{1}{2}$. Since Vishnu shot from a distance of 6 or less, the distance he shot from is uniformly distributed in the range $[4,6]$. Hence, the probability that he scores is

$$\int_4^6 \frac{1}{2} \cdot \frac{12}{x^2} dx = 6\left[-\frac{1}{x}\right]_4^6 = 6\left(\frac{1}{4} - \frac{1}{6}\right) = \frac{3}{2} - 1 = \frac{1}{2}$$

(iii) What is the probability that Vishnu shot from a distance of 6 or less given that he scored? You may leave your answer in terms of (i) and (ii), the answers to the previous two parts.

Answer: $\frac{1/2 \cdot (ii)}{(i)} = \frac{2}{3}$. Letting Sc be the event that Vishnu scores and Si be the event that he shot from a distance of 6 or less, Bayes' Rule gives us

$$\mathbb{P}(Si|Sc) = \frac{\mathbb{P}(Sc|Si)\mathbb{P}(Si)}{\mathbb{P}(Sc)}$$

We already solved for $\mathbb{P}(Sc|Si)$ in part (ii) and $\mathbb{P}(Sc)$ in part (i). The only thing left to calculate, then, is the probability that Vishnu shoots from a distance of 6 or less. Since this distance is uniformly distributed in the range $[4,8]$, that probability is just $\frac{6-4}{8-4} = \frac{1}{2}$.

6 A Walk in the Arc [4/5/4/4/5/4 Points, 26 Total]

Note: Parts (d)-(f) do not depend on (a)-(c), and vice versa.

There are 5 points spaced evenly around a circle, labeled $\{1,2,\ldots,5\}$ in clockwise order. The **distance** between two points is the length of the shorter path (either clockwise or counter-clockwise) between them. For example, the distance between points 1 and 4 is 2, as we can move counterclockwise from 1 to 5 to 4.

Two flies on the circle start in positions S_1 and S_2. After every minute, each fly either goes one spot clockwise or one spot counterclockwise, each with probability $\frac{1}{2}$. The flies make their choices **independently**.

(a) Prove that no matter what S_1 and S_2 are, there is some sequence of moves they can make so that they get to the same point.

Answer: Since there are 5 points, for every configuration of the flies, one arc between them will have even length and one will have odd length. The flies will coincide if both move towards each other on the even arc side.

(b) Draw a 3-state Markov chain that models how the distance between the flies changes each minute. Define all states and label transition probabilities.

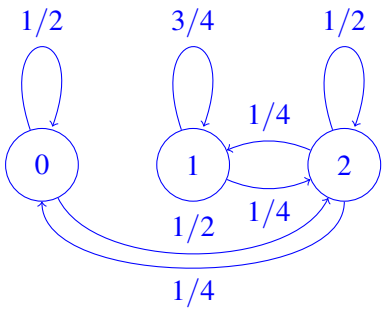
Answer: We'll describe the chain in words to explain where we got the probabilities. There are 3 states: 0, 1, and 2, corresponding to the three possible distances. The transition probabilities are:

- From state 0: $\frac{1}{2}$ self loop (from both flies going in the same direction), $\frac{1}{2}$ to 2 (from both flies going opposite directions)
- From 1: $\frac{3}{4}$ self loop (from both flies going in the same direction or from swapping spots), $\frac{1}{4}$ to 2 (from both flies going towards each other on the length 4 arc).
- From 2: $\frac{1}{2}$ self loop (from both flies going in the same direction), $\frac{1}{4}$ to 0 (from both flies going towards each other on the length 2 arc), and $\frac{1}{4}$ to 1 (from both flies going towards each other on the length 3 arc).

Put more succinctly, the transition matrix is:

$$\begin{bmatrix} \frac{1}{2} & 0 & \frac{1}{2} \\ 0 & \frac{3}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} & \frac{1}{2} \end{bmatrix}$$

As a picture:



(c) If the flies keep doing this for a very long time, what fraction of steps will they be on the same point?

Answer: We solve for $\pi P = \pi$. Let π_0, π_1, π_2 be the entries of the stationary distribution π:

$$\pi_0 = \frac{1}{2}\pi_0 + \frac{1}{4}\pi_2$$
$$\pi_1 = \frac{3}{4}\pi_1 + \frac{1}{4}\pi_2$$
$$\pi_2 = \frac{1}{2}\pi_0 + \frac{1}{4}\pi_1 + \frac{1}{2}\pi_2$$

We need this to be a distribution, so it sums to 1, so we have $\pi_0 + \pi_1 + \pi_2 = 1$. Solving, we have that: $\pi_0 = \frac{1}{5}, \pi_1 = \frac{2}{5}, \pi_2 = \frac{2}{5}$. Therefore, the answer we want is $\pi_0 = \frac{1}{5}$.

For the next parts, the flies have the same behavior. However, now there are instead 8 points spaced evenly around a circle, labeled $\{1, 2, \ldots, 8\}$ in clockwise order. We define distance as above.

(d) Prove that if the distance from S_1 to S_2 is odd, the flies will never end up at the same point.

Answer: If $|S_1 - S_2|$ is odd, both arcs between the flies have odd length. At each time step, each arc length either stays the same, or goes up / down by two, so at each step, both arcs between the flies still have odd length. If the flies coincide, both arcs need even length.

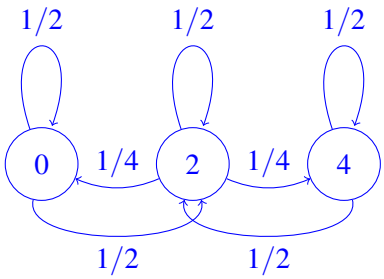
(e) Now, assume the distance from S_1 to S_2 is even. Draw a 3-state Markov chain to model how the distance between the flies changes each minute. Define all states and label all transition probabilities.

Answer: We'll describe the chain in words to explain where we got the probabilities. There are 3 states: 0, 2, and 4. The transition probabilities are:

- From state 0: $\frac{1}{2}$ self loop (from both flies going in the same direction), $\frac{1}{2}$ to 2 (from both flies going opposite directions)
- From 2: $\frac{1}{2}$ self loop (from both flies going in the same direction), $\frac{1}{4}$ to 0 (from both flies going towards each other on the length 2 arc), and $\frac{1}{4}$ to 4 (from both flies going towards each other on the length 6 arc).
- From 4: $\frac{1}{2}$ self loop (from both flies going in the same direction), $\frac{1}{2}$ to 2 (from both flies going opposite directions)

Put more succinctly as a transition matrix:

$$\begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ \frac{1}{4} & \frac{1}{2} & \frac{1}{4} \\ 0 & \frac{1}{2} & \frac{1}{2} \end{bmatrix}$$



As a picture:

(f) The flies start distance 2 apart. Find the expected number of minutes until they are at the same point for the first time. Partial credit will be awarded for setting up the correct first step analysis.

Answer: 6. We use first step analysis. Let $\tau(i)$ be the expected time to state 0. The goal is to find $\tau(2)$ The equations are:

$$\tau(4) = 1 + \frac{1}{2}\tau(4) + \frac{1}{2}\tau(2)$$
$$\tau(2) = 1 + \frac{1}{4}\tau(4) + \frac{1}{2}\tau(2) + \frac{1}{4}\tau(0)$$
$$\tau(0) = 0$$

Solving this system, we have $\tau(2) = 6$.

7 All Things Come to Path [5/4/4 Points, 13 Total]

A graph is k-**vertex-connected** if it has more than k vertices, and removing any set of **fewer** than k vertices keeps the graph connected.

A set of paths is **internally vertex-disjoint (IVD)** if they all have the same start and end vertices, but don't share any others.

(a) Let G be a graph with the property that for any u, v, there is a set of at least k IVD paths between them. Prove that G is k-vertex-connected.

Answer: Let S be a subset of fewer than k vertices. Delete S from G to obtain the graph G'. Let u, v be any pair of vertices in G'. It suffices to show that there is a path from u to v in G'. In G, there were at least k IVD paths between them. Removing S disconnected at most $(k-1)$ paths, which still leaves at least one path between u and v.

For the rest of the question, let $G = K_{n,n}$, a complete bipartite graph with n vertices on each side. If we prove the following two facts, then by part (a), we conclude that $K_{n,n}$ is n-vertex-connected.

(b) Prove that if u and v are both on the left side, there exist n IVD paths between them.

Answer: Let $l_1, l_2, \ldots, l_n$ be the left side vertices, and $r_1, r_2, \ldots, r_n$ be the right side vertices. WLOG we may assume $u = l_1$ and $v = l_2$, otherwise we can reorder the vertices. The n paths between u and v are of the form $u - r_i - v$, where i ranges from $1, \ldots, n$.

(c) Prove that for u on the left and v on the right, there exist n IVD paths between them.

Answer: Let $l_1, l_2, \ldots, l_n$ be the left side vertices, and $r_1, r_2, \ldots, r_n$ be the right side vertices. WLOG we may assume $u = l_1$ and $v = r_1$, otherwise we can reorder the vertices. The n paths between l_1 and r_1 are the edge $l_1 - r_1$, and length 3 paths of the form $u - r_i - l_i - v$, where i ranges from $2, \ldots, n$.

8 Moment (Generating Function) of Truth [4/5/4/5 Points, 18 Total]

We define the moment generating function (MGF), $M_X(t)$, of a random variable X, as follows:

$$M_X(t) = \mathbb{E}[e^{tX}]$$

(a) Determine the moment generating function of $X \sim \text{Bernoulli}(p)$.

Answer: Recall, since X follows the Bernoulli distribution, $\mathbb{P}[X=1] = p$ and $\mathbb{P}[X=0] = 1-p$. Then,

$$\begin{aligned} M_X(t) = \mathbb{E}[e^{tX}] &= \sum_x e^{tx} \cdot \mathbb{P}[X=x] \\ &= e^{t\cdot 1} \cdot p + e^{t\cdot 0} \cdot (1-p) \\ &= 1 - p + pe^t \end{aligned}$$

(b) Prove that if X and Y are independent, then $M_{X+Y}(t) = M_X(t)M_Y(t)$. *(Hint: You can use the fact that if X and Y are independent, then $f(X)$ and $g(Y)$ are also independent, for any two functions f, g.)*

Answer: As stated in the hint, we'll assume the fact that if two random variables are independent, then functions of the random variables are also independent. We see that since X and Y are independent, then the random variables $f(X) = e^{tX}$ and $g(Y) = e^{tY}$ are also independent. Therefore, if $f(X)$ and $g(Y)$ are independent, then $\mathbb{E}[f(X)g(Y)] = \mathbb{E}[f(X)]\mathbb{E}[g(Y)]$.

Thus, we have:

$$\begin{aligned} M_{X+Y}(t) &= \mathbb{E}[e^{t(X+Y)}] \\ &= \mathbb{E}[e^{tX}e^{tY}] \\ &= \mathbb{E}[e^{tX}]\mathbb{E}[e^{tY}] \\ &= M_X(t)M_Y(t) \end{aligned}$$

(c) Determine the moment generating function of $X \sim \text{Bin}(n, p)$. You may leave your answer in terms of a, the answer to Part (a), even if you do not get it correct.

Answer:

Solution 1: The first solution is to calculate it directly. Recall, $\mathbb{P}[X = x] = \binom{n}{x} p^x (1-p)^{n-x}$.

$$\begin{aligned} M_X(t) = \mathbb{E}[e^{tX}] &= \sum_x e^{tx} \cdot \mathbb{P}[X = x] \\ &= \sum_{x=0}^{n} e^{tx} \binom{n}{x} p^x (1-p)^{n-x} \\ &= \sum_{x=0}^{n} \binom{n}{x} (pe^t)^x (1-p)^{n-x} \\ &= (pe^t + 1 - p)^n \end{aligned}$$

In the last step, we used the binomial theorem.

Solution 2: Alternatively, we could use the fact that the binomial distribution is the sum of n independent Bernoulli trials, each with probability p — in other words, $X = \sum_{i=1}^{n} X_i$, where each $X_i \sim \text{Bern}(p)$. We can also use our result from part b.

Then,

$$\begin{aligned} M_X(t) &= \mathbb{E}[e^{tX}] \\ &= \mathbb{E}[e^{t(X_1+X_2+\ldots+X_n)}] \\ &= \mathbb{E}[e^{tX_1} \cdot e^{tX_2} \cdot \ldots \cdot e^{tX_n}] \\ &= \mathbb{E}[e^{tX_1}] \cdot \mathbb{E}[e^{tX_2}] \cdot \ldots \cdot \mathbb{E}[e^{tX_n}] \text{ (since each } X_i \text{ is independent)} \\ &= (1-p+pe^t) \cdot (1-p+pe^t) \cdot \ldots \cdot (1-p+pe^t) \text{ (from the MGF of a Bernoulli)} \\ &= (1-p+pe^t)^n \end{aligned}$$

(d) The moment generating function of a Gaussian random variable with mean μ and variance σ^2 is $M_X(t) = \exp(\mu t + \frac{\sigma^2 t^2}{2})$. Suppose X, Y are independent random variables such that $X \sim \mathcal{N}(\mu_1, \sigma_1^2)$ and $Y \sim \mathcal{N}(\mu_2, \sigma_2^2)$. Using moment generating functions, prove that $X + Y \sim \mathcal{N}(\mu_1 + \mu_2, \sigma_1^2 + \sigma_2^2)$.

Notes:

- $\exp(x)$ *is just another way to write* e^x.
- *Two random variables are identically distributed iff they have the same MGF.*
- *You may use the result in part (b), even if you do not correctly answer part (b).*

Answer:

Now, we will proceed with the MGFs of our particular X and Y.

$$\begin{aligned} M_{X+Y}(t) &= M_X(t)M_Y(t) \\ &= \exp(\mu_1 t + \frac{\sigma_1^2 t^2}{2}) \cdot \exp(\mu_2 t + \frac{\sigma_2^2 t^2}{2}) \\ &= \exp(\mu_1 t + \mu_2 t + \frac{\sigma_1 t^2}{2} + \frac{\sigma_2^2 t^2}{2}) \\ &= \exp\left((\mu_1 + \mu_2)t + \frac{(\sigma_1^2 + \sigma_2^2)t^2}{2}\right) \end{aligned}$$

This is the moment generating function of a Gaussian random variable with mean $\mu_1 + \mu_2$ and variance $\sigma_1^2 + \sigma_2^2$.

9 Relax, It's Not RE [5 Points Each, 10 Total]

(a) Suppose we wish to write a program `FindHalt` that takes in a program P and

(1) Returns an x from $\{1, 2, ..., 70\}$ such that $P(x)$ halts if such an x exists

(2) Returns "None" if no such x exists

Prove that no such program `FindHalt` can exist.

Answer: We can reduce the Halting Problem to finding such a program. In particular, assuming we have access to an implementation of `FindHalt`, we can write `TestHalt` as follows:

```
TestHalt(P, x):
    def P'(y):
        P(x)
    if FindHalt(P') = "None":  return False
    else:  return True
```

If P(x) does not halt, won't halt on any input, and hence `FindHalt(P')` will return "None". If P(x) halts, P'(y) will halt for all $y \in \{1, ..., 70\}$, meaning that `FindHalt(P')` will return one of those values — and so in particular will not return "None". Hence, if P(x) loops, `TestHalt(P, x)` will return false; if P(x) halts, `TestHalt(P, x)` will return true. Thus, we have a valid implementation of `TestHalt`, which is impossible, so we can conclude that `FindHalt` cannot exist.

(b) Suppose that we relax requirement (2), and only want a program `RelaxedFindHalt` that

(1) Returns an x from $\{1, 2, ..., 70\}$ such that $P(x)$ halts if such an x exists

(2) Loops forever if no such x exists

Describe, in pseudocode or English, how to implement `RelaxedFindHalt`.

Answer: We run P(1), P(2), ..., P(70) all in parallel, and wait for any one of them to finish. If one of them eventually does halt, we return its input. (If none ever do, we will just end up waiting forever.).

10 So Long, and Thanks for All the Poisson [3/3/5 Points, 11 Total]

Any correct answer will receive full credit. Partial credit may be awarded if work is shown.

A new GSI, Eel-izabeth, starts teaching CS 70 next fall. Each discussion, she keeps track of the number of mistakes she makes. The number of mistakes she makes per discussion follows a Poisson(1.5) distribution. Each discussion is independent of all others.

She promises that if she makes m mistakes over the semester, she will bring Swedish Fish for her section.

(a) Eel-izabeth gives 30 discussions over the fall. Let M be the number of mistakes she makes over the entire semester. What is $\mathbb{E}[M]$?

Answer: Let M_i be the number of mistakes in the i-th discussion. Then, the number of mistakes she makes over the semester is $M_1 + M_2 + \ldots + M_{30}$. Using linearity of expectation, and the fact that $\mathbb{E}[M_i] = 1.5$, we obtain $30 \cdot 1.5 = 45$.

(b) What is $\text{Var}(M)$?

Answer: Define M_i as above. We want $\text{Var}(M_1 + M_2 + \ldots + M_n)$. As the M_i are independent, this quantity becomes $n\,\text{Var}(M_1) = 30 \cdot 1.5 = 45$.

(c) Eel-izabeth doesn't actually want to buy Swedish Fish for her section. How large should she set m, so that with at least 90% probability, she doesn't have to buy the Swedish Fish? Use Chebyshev's inequality. *(You may leave your answer as a numerical expression rather than an integer.)*

Answer: We can translate the goal of this as $\mathbb{P}[M \geq m] \leq 0.1$. The event $M \geq m$ is equivalent to $M - 45 \geq m - 45$, and this event is a subset of the event $|M - 45| \geq m - 45$. Using Chebyshev:

$$\mathbb{P}[|M - 45| \geq m - 45] \leq \frac{\text{Var}(M)}{(m-45)^2} \leq 0.1$$

Solving for m, we obtain $m = \sqrt{450} + 45 = 15\sqrt{2} + 45$.

11 The End

Congrats, you finished the class! Here is a cute dog to celebrate:

Or, for those of you who like cats more, here is a kitten: