CS 70 Summer 2019 — Discrete Mathematics and Probability Theory — 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**

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

○ **True**

○ **False**

(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**

(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**

(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**

(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**

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

○ **True**

○ **False**

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

○ **True**

○ **False**

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

○ **True**

○ **False**

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

○ **True**

○ **False**

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

○ **True**

○ **False**

(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**

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 $\wedge$).

(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.

(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.

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.

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

(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 $d_P + d_Q$?

Graphs

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

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

Modular Arithmetic

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

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

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

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

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**

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

○ **1-1** ○ **Onto** ○ **Both** ○ **Neither**

(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**

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

○ **1-1** ○ **Onto** ○ **Both** ○ **Neither**

Counting

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

(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.

(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.*

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 $\mathbb{P}(X \geq 20)$.

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

Random Variables

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

(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.

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

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

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

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

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

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

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 $\mathbb{E}[X]$?

□

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

□

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

(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.)

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.)*

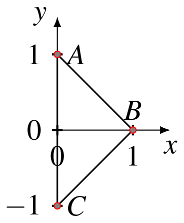
(f) What is $\mathbb{E}[N]$? You may leave your answer in terms of the variables q_i for $i = 1, \ldots, n$, where q_i is the answer to Part (e). *You may use a summation, but you may not use expectations in your answer.*

(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.*

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.

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

(c) Find the PDF of X.

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

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*?

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

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

(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.

(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.

(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?

(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.

$$\int_{\boxed{}}^{\boxed{}} \boxed{}\; dx$$

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

(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?

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

(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.

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.

(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.

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

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.

(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.

(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.

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.

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.

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

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 $X \sim \text{Bernoulli}(p)$.

(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.)*

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

(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).*

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.

(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`.

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 $\mathbb{E}[M]$?

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

(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.)*

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: