CS 70 Discrete Mathematics and Probability Theory
Spring 2022 Rao and Sen

Final

PRINT Your Name: _____, _____
(last) (first)

PRINT Your Student ID: _____

PRINT Your Exam Room: _____

SID of the person sitting to your left: _____

SID of the person sitting to your right: _____

SID of the person sitting in front of you: _____

SID of the person sitting behind you: _____

Advice.

- The questions vary in difficulty and are not in order of difficulty. All blanks are worth 3 points each unless otherwise specified. No negative points are given. **So do really scan over the exam a bit.**
- The question statement is your friend. Reading it carefully is a tool to get to your "rational place".
- You may consult *3 sheets of notes on both sides*. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronic devices are NOT permitted.
- **You may, without proof, use theorems and lemmas that were proven in the notes and/or in lecture, unless otherwise stated.**

Remote Proctoring Instructions.

- Gradescope assignment with the PDF **entire exam** will be available on the "Final" assignment (on either the regular or Alternate Gradescope).
- **Be sure** to **download** the PDF from the Final Gradescope assignment.
- There will be no clarifications made directly to individuals. We will listen to issues, we may choose to address some issues during or after the exam. Please keep moving through the exam.
- **Remote: You have 180 minutes to do the exam and then an extra 20 minutes to scan your answer sheet to the Final assignment.**
- **Remote: Clarification Request form:** https://forms.gle/N3eG9b3CvAfJybo57
- **Clarification Doc:** https://tinyurl.com/cs70-sp22-final-clarifications
- For emergencies, email sp22@eecs70.org or use the disruption form at: https://forms.gle/M2YKK9sQavFqyzYm6.
  Again, keep working as best as possible, as we cannot respond in real time.

Major Gradescope Issues. If there is a global issue and it is not affecting you, please continue. If you are experiencing difficulties with Gradescope or Zoom, you may check your email, and we will post a global message on Piazza and bypass email preferences to inform you of what to do.

1. Pledge.

Berkeley Honor Code: As a member of the UC Berkeley community, I act with honesty, integrity, and respect for others.

In particular, I acknowledge that:

- I alone am taking this exam. Other than with the instructor and GSIs, I will not have any verbal, written, or electronic communication about the exam with anyone else while I am taking the exam or while others are taking the exam.
- I will not have any other browsers open while taking the exam.
- I will not refer to any books, notes, or online sources of information while taking the exam, other than what the instructor has allowed.
- I will not take screenshots, photos, or otherwise make copies of exam questions to share with others.
- I won't work for people from Stanford. [This is optional.]

Signed:_____

2. Propositions. Other stuff.

1. $\forall x \exists y\ P(x,y) \equiv \neg \exists x \forall y$ _____

2. $P \implies Q \equiv \neg P \vee$ _____

3. Consider a non-empty set U, predicates $P(x)$ and $Q(x)$ for any $x \in U$, and predicates $R(x,y)$ and $S(x,y)$ for any $x,y \in U$. Which of the following statements are always true?

   (a) $(\forall x,y \in U, P(x) \implies Q(y)) \equiv (\exists x \in U, P(x)) \implies (\forall x \in U, Q(x))$

   ◯ True ◯ False

   (b) $(\exists x,y \in U, P(x) \implies Q(y)) \equiv (\exists x \in U, P(x)) \implies (\forall x \in U, Q(x))$

   ◯ True ◯ False

   (c) $(\exists x,y \in U, P(x) \implies Q(y)) \equiv (\exists x \in U, P(x)) \implies (\exists x \in U, Q(x))$

   ◯ True ◯ False

   (d) $(\forall x,y \in U, R(x,y) \equiv P(x) \wedge Q(y)) \implies (\forall x,y \in U, P(x) \implies R(x,y))$.

   ◯ True ◯ False

   (e) $(\forall x,y \in U, S(x,y) \implies R(x,y)) \implies (\forall x,y \in U, \neg S(x,y)) \vee (\exists x,y \in U, R(x,y))$.

   ◯ True ◯ False

4. For any natural numbers a and n both greater than 2, any solution to $x^n = a$ is either an integer or an irrational number.

   ◯ True ◯ False

5. In a stable matching instance where a candidate has the same partner in both the job-optimal matching and candidate-optimal matching, that candidate has only one possible partner in any stable matching.

   ◯ True ◯ False

6. In a stable matching instance that terminates in 5 days in the job-optimal stable matching algorithm, at most 5 jobs do not get the first partner in their preference list.

   ◯ True ◯ False

3. To Prove or Disprove, that is the question.

1. (8 points) Prove or disprove: If a positive integer is congruent to 2 mod 3, it is divisible by a prime that is congruent to 2 mod 3.

2. (10 points) Prove or disprove: For a three digit number n with digits a, b and c in the hundreds, tens and ones place, respectively, $7 \mid n$ if and only if $7 \mid (10a + b - 2c)$. (Hint: $7 \mid m$ if and only if $7 \mid 3m$.)

4. We are the mods! We are the mods! We are! We are! We are the mods!

1. For a prime p, if $a^4 \equiv 10 \pmod{p}$ and $a^6 \equiv 19 \pmod{p}$, what is $a^{10} \pmod{p}$?

2. For all integer x and y, $\gcd(x,y) = \gcd(x, x-5y)$.

   ◯ True ◯ False

3. If $\gcd(a,b) = 1$, then $a-b$ is not a multiple of a. (Assume a and b are integers such that $a,b \geq 2$.)

   ◯ True ◯ False

4. For a,b with $\gcd(a,b) = 1$, how many solutions are there to $za = b \pmod{ab}$? (A solution is a value for z that satisfies the equation.)

5. Let $x = pd$ and $y = qd$ where $d = \gcd(x,y)$ and p,q and d are prime, and $d = ax + by$. Answers below are possibly in terms of x, y, p, q, d, a, b and constants.
   (a) What is the multiplicative inverse of $q \pmod{p}$?

   (b) What is $a^x \pmod{p}$? (Simplify.)

   (c) What is $a^{(x-d)(y-d)} \pmod{pq}$? (Simplify.)

6. Let (N,e) and d be the public and private keys for an RSA scheme where $N = pq$ for primes p and q.
   (a) $x^{ed} = 1 \pmod{N}$ for all x.

   ◯ True ◯ False

   (b) $ed = 1 \pmod{N}$.

   ◯ True ◯ False

   (c) The encryption of x times the encryption of y is the encryption of xy.

   ◯ True ◯ False

   (d) The encryption of x plus the encryption of y is the encryption of $x+y$ for all x,y.

   ◯ True ◯ False

5. Polynomials: So much more than omials.

1. How many polynomials of degree 2 over arithmetic modulo 5 have exactly two, not necessarily distinct, roots? You may leave your answer as an expression.

2. Give a polynomial $\pmod 5$ of degree 2 that contains points $(1,0),(2,3),(3,0)$.

3. Any polynomial with d roots over arithmetic modulo a prime p has degree at most d.

   ◯ True ◯ False

4. Any polynomial of degree exactly 2 over arithmetic modulo a prime $p > 2$ has either 0 roots or 2 roots.

   ◯ True ◯ False

5. Given a Berlekamp–Welch scheme for a message of size 2 tolerating 1 error and a communication channel where there is at most 1 error.
   (a) What is the degree of the original polynomial, $P(x)$, encoding the message?

   (b) Suppose the received message is $R(0) = 0$, $R(1) = 0$, $R(2) = 0$ and $R(3) = 5$ over arithmetic modulo 5. Knowing that there is exactly one error, what is the original polynomial? (Hint: lots of zeros in received message.)

   (c) If the original polynomial is $P(x) = 2x+3 \pmod 5$, and the received message is $R(0) = 3$, $R(1) = 4$, $R(2) = 2$, and $R(3)$ is unknown, what is the error polynomial?

   (d) If the received message is $R(0) = 1$, $R(1) = 3$, and $R(2) = 5$, and $R(3)$ is unknown, what is the original polynomial?

   (e) Let $E(x) = x+e$, $Q(x) = ax^2+bx+c$, and $R(0) = 4$. Find the equation relating e,a,b,c for this received message.

6. Graphs

1. A cycle cover for a simple graph $G = (V, E)$ is a subset of edges $E' \subseteq E$ where every cycle in G uses an edge in E'. (A cycle must contain at least 3 edges.)

   (a) E is a cycle cover of G.

   ◯ True ◯ False

   (b) If G is a tree, the empty set is a cycle cover of G.

   ◯ True ◯ False

   (c) For a connected graph, what is the minimum size of a cycle cover? (Let $m = |E|$ and $n = |V|$.)

   (d) (5 points) Argue your answer above is sufficient. (Describe a cycle cover of this size.)

   (e) (5 points) Argue your answer above is necessary. (Say why fewer edges will not suffice.)

2. An edge coloring of a graph colors the edges so that any two edges incident to a vertex have different colors.

   (a) (6 points) Describe a method to edge color any graph with at most $2d - 1$ colors where d is the maximum degree of any vertex.

   (b) What is the minimum number of colors to edge color a hypercube of dimension n?

7. Some counting.

1. How many possible strings of red, blue, and purple beads are there of length n?

2. Given an unordered sample of size k out of n objects:
   (a) If the sample is chosen with repetition, how many different possible samples are there?

   (b) If the sample is chosen without repetition, how many different possible samples are there?

3. Consider the experiment of rolling a die until you see a 6 or until you have rolled 3 times. How many outcomes are there for this experiment? (Examples: (6), (5, 6) are possible outcomes, but (6, 6) is not as the first roll of 6 would have terminated the processes, nor is (5, 5, 5, 6) as it is longer than 3 rolls.)

4. (10 points) Prove the following identity using a combinatorial argument. **Correct answers that do not use a combinatorial argument will not receive credit.**

$$\sum_{n=k}^{m} \binom{n}{k} = \binom{m+1}{k+1}$$

8. Countability

In this problem, we consider that the natural numbers and the rational numbers have total orderings corresponding to their value; for example, $3 < 4$ and $1/3 < 1/2$.

1. For a set A and an ordering, $<$, on the set, let $S_{<x}(A)$ be the set of all subsets S of A, where $y \in S \implies y < x$. That is, $S_{<2}(\mathbb{N}) = \{\varnothing, \{0\}, \{1\}, \{0,1\}\}$, and has cardinality 4.

   (a) $S_{<n}(\mathbb{N})$ is countable for all $n \in \mathbb{N}$.

   ◯ True ◯ False

   (b) $\bigcup_{n\in\mathbb{N}} S_{<n}(\mathbb{N})$ is countable.

   ◯ True ◯ False

   (c) $\bigcup_{q\in\mathbb{Q}} S_{<q}(\mathbb{Q})$ is countable.

   ◯ True ◯ False

2. For a set A and an ordering, $<$, the set of ordered partitions of A are the partitions $(S,\ A \setminus S)$ where $\forall x \in S, \forall y \in A \setminus S,\ x < y$. For example, for $A = \{1,2,3\}$, the set of ordered partitions of A is

$$\Big\{(\varnothing,\ \{1,2,3\}),\ (\{1\},\{2,3\}),\ (\{1,2\},\{3\}),\ (\{1,2,3\},\varnothing)\Big\}.$$

   (a) The set of ordered partitions of $\mathbb{N}$ is countable.

   ◯ True ◯ False

   (b) The set of ordered partitions of $\mathbb{Q}$ is countable.

   ◯ True ◯ False

9. Computability

1. The problem of whether a computer program on input x uses more than M bits of memory is decidable.

   ◯ True ◯ False

2. The problem of whether a computer program on input x executes line n is decidable.

   ◯ True ◯ False

10. Probability: Mo' Better Venn.

Recall that a probability space has a sample space Ω and $\mathbb{P} : \Omega \to \mathbb{R}$, where $\mathbb{P}[\omega] \geq 0$ and $\sum_{\omega \in \Omega} \mathbb{P}[\omega] = 1$. For an event $A \subset \Omega$, $\overline{A} = \Omega \setminus A$. Consider events $A, B \subseteq \Omega$. In each box, write the expression that correctly completes the corresponding blank.

1. $\mathbb{P}[A \cap B] = 1 - \mathbb{P}[\overline{A} \cup \overline{B}] - \_\_?\_\_$.

2. For events $A, B \subset \Omega$ where A and B are independent, $\mathbb{P}[A \cap \overline{B}] = \mathbb{P}[A] \times \_\_?\_\_$.

3. For event B, and $\omega \in B$, $\mathbb{P}[\omega \mid B] = \mathbb{P}[\omega] \times \_\_?\_\_$

4. Given indicator random variables 1_A for event A, and 1_B for B, $\mathbb{E}[1_A \times 1_B] = \mathbb{P}[\_\_?\_\_]$. Note that $\mathbb{E}[1_A] = \mathbb{P}[A]$. (A set in terms of A and B possibly.)

5. $\mathrm{Cov}(1_A, 1_B) = \_\_?\_\_ - \mathbb{P}[A]\mathbb{P}[B]$

6. $\mathrm{Var}(1_A) = \_\_?\_\_$

7. $\mathbb{E}[1_A \mid 1_B = 0] = \mathbb{P}[A \cap B] \times \_\_?\_\_$

8. $\mathbb{E}[1_A + 1_B] = \mathbb{P}[A \cup B] + \_\_?\_\_$

11. Heads or Tails

1. Consider two coins, one that lands heads with probability 0.25 and another that lands heads with probability 0.75. We choose one of the two coins with equal probability and flip it twice. Let A be the event that the first toss is a heads, and let B be the event that the second toss is a heads.

   (a) What is $\mathbb{P}[A \mid B]$?

   (b) Let C be the event that the coin with heads probability 0.25 is chosen. What is $\mathbb{P}[C \mid A]$?

   (c) Let 1_A and 1_B be indicator random variables for events A and B, respectively. What is $\text{Corr}(1_A, 1_B)$? (Recall that $\text{Corr}(X,Y) = \text{Cov}(X,Y)/\sqrt{\text{Var}(X)\text{Var}(Y)}$ and $\text{Cov}(X,Y) = \mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y]$.)

2. Consider two independent Bernoulli random variables X and Y with $\mathbb{E}[X] = \mathbb{E}[Y] = 1/2$. What is $\mathbb{P}[X = Y]$?

3. Consider two Bernoulli random variables X and Y with $\mathbb{E}[X] = \mathbb{E}[Y] = 1/2$, such that $\text{Corr}(X,Y) = 0.5$.

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

   (b) What is $\mathbb{P}[X = Y]$?

12. Don't Deviate!

Consider $Y = X_1 + \ldots + X_n$, where X_i are independent and identically distributed as follows:

$$X_i = \begin{cases} -1 & \text{with probability } \frac{1}{2} \\ +1 & \text{with probability } \frac{1}{2} \end{cases}$$

1. What is $\mathbb{E}[Y]$?

2. What is $\text{Var}(Y)$?

3. Using Chebyshev's inequality, give a lower bound on ε such that $\mathbb{P}[|Y| > \varepsilon] \leq 0.05$.

13. Who doesn't like cake?

1. (10 points) Professor Rao is hosting a party for the CS 70 TAs, but since it is during dead week, not everyone can make it. The number of TAs that attend his party is distributed according to Poisson(λ). Professor Rao plans to split a cake evenly among himself and all of the TAs that arrive. What is the expected proportion of the cake that Professor Rao will receive? (Hint: Recall the Taylor series $e^x = \sum_{i=0}^{\infty} \frac{x^i}{i!}$.)

2. Qinhong is hosting an end-of-semester party, and needs to cut a cake into slices beforehand. Unfortunately, the more slices he cuts, the smaller each individual slice is, and the less likely it is for people to come to the party! Let X be a random variable representing the number of people who will show up to the party. If Qinhong cuts the cake into n slices, then $\mathbb{E}[X] = \frac{16}{n}$ and $\text{Var}(X) = \frac{256}{n^2}$.

   (a) Qinhong wants there to be enough cake for everyone, so he wants the expected number of people who will arrive to be no greater than the number of slices. Find the smallest value of n such that $\mathbb{E}[X] \leq n$.

   (b) Realizing that simply using expected value is not enough to ensure he doesn't run out of cake, Qinhong wants the probability of running out to be no greater than $\frac{1}{9}$. Use Markov's inequality to find the smallest value of n such that $\mathbb{P}[X \geq n] \leq \frac{1}{9}$.

   (c) Unsatisfied with this bound, Qinhong wonders if Chebyshev's inequality can give a better bound. Find the smallest value of n such that $\mathbb{P}[X \geq n] \leq \frac{1}{9}$ using Chebyshev's inequality.

   (d) Now, we will assume that the random variable X can be approximated by an exponential distribution, so $X \sim \text{Exp}(\frac{n}{16})$. Given this information, find the smallest value of n such that $\mathbb{P}[X \geq n] \leq \frac{1}{9}$.

14. Probability: small steps.

1. Consider a random variable X, with PDF $f(x)$ and CDF $F(x)$.
   (a) What is $\mathbb{P}[X \in [a,b]]$ in terms of $F(x)$?

   (b) What is $\mathbb{P}[X \in [a,b]]$ in terms of $f(x)$?

   (c) What is $\mathbb{P}[X \leq x \mid X > t]$ in terms of $F(x)$? (Look carefully at the event!)

2. Alice throws darts that land uniformly inside a circular dartboard of radius 1. Bob throws darts that land uniformly inside a circular dartboard of radius 2. Let A be the random variable representing the distance Alice's dart lands from the center of her dartboard, and B be the random variable representing the distance Bob's dart lands from the center of his dartboard. Assume A and B are independent.
   (a) What is $F_A(x)$, the CDF of A?

   (b) What is $f_B(x)$, the PDF of B?

   (c) What is the probability Bob beats Alice, $\mathbb{P}[B < A]$? (Hint: if $B < x$ and $A < x$, what is the probability that Bob beats Alice?)

(d) We wish to compute $\mathbb{P}[B < x \mid B < A]$.

i. What is $\mathbb{P}[B < x \cap A < x \cap B < A]$ as a function of x?

ii. What is $\mathbb{P}[B < x \cap A \geq x \cap B < A]$?

iii. What is $\mathbb{P}[B < x \mid B < A]$?

15. Estimating Wald(o).

Let $N \sim \text{Poisson}(\lambda)$ and $Y = X_1 + \cdots + X_N$ with i.i.d. $X_i \sim \text{Exp}(\lambda)$.

1. What is $\mathbb{E}[Y]$?

2. What is the MMSE of Y given N?

3. What is the LLSE of Y given N?

16. Chaining heads!

You have some biased coins with probability $p = \frac{3}{5}$ of heads.

1. You repeat pairs of coin tosses, until both flips in a pair are heads. How many coin tosses does this take in expectation?

2. You repeatedly flip the coin until two flips in a row are heads. How many coin tosses does this take in expectation?

17. Slip, slip, slip away!

(15 points) Leanne begins the following process: at time step 1, she chooses an integer uniformly at random from 0 to n, inclusive. For $t \geq 1$, at time step $t+1$, she chooses an integer uniformly at random from 0 to a_t, inclusive, where a_t is the integer chosen at time step t. Prove that the expected sum of all of the integers Leanne chooses is equal to n.

(Hint: You may find the variable S_m, the expected sum if Leanne starts choosing from 0 to m, useful in your proof. You may also find the following equation helpful: $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$. Finally, induction might be helpful.)

18. A single random variable in possession of a well-defined probability function must be in want of a joint distribution.

Elizabeth is visiting Pemberley and wants to explore the 10 rooms, numbered 1 through 10. However, she wants to avoid Mr. Darcy, who is also at Pemberley. Every minute, Elizabeth picks one of the 10 rooms uniformly at random to enter and Darcy, independently of Elizabeth, picks one of the 10 rooms uniformly at random to enter.

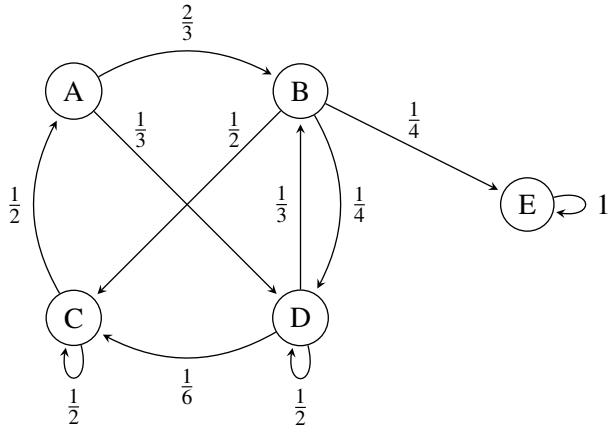
1. What is the expected number of minutes that will pass until Elizabeth and Darcy meet each other in the same room?

2. What is the probability that at least 10 minutes will pass before Elizabeth encounters Darcy in the same room as her?

3. Since Darcy owns Pemberley, he knows the estate very well and he has a rough idea of which room Elizabeth is going to. Anxious to redeem himself to her, Darcy changes his strategy: if Elizabeth goes to room number r at some minute, Darcy will choose to enter any room between 1 and r uniformly at random in that same minute. Let E_i be the random variable representing the room Elizabeth enters at the ith minute and D_i represent the room Darcy enters at the ith minute. Derive an expression, possibly involving cases, for the joint distribution $\mathbb{P}[E_i = r_e, D_i = r_d]$ for $r_e, r_d \in \{1, 2, 3, \ldots, 10\}$.

19. Heathcliff, it's me, Cathy!

Catherine and Ellen are locked inside of Wuthering Heights and are trying to escape! Their escape can be modeled as the Markov chain shown below, where at every time step, they transition from one place to another (or they hear servants around and choose to remain in place, represented with self-loops). They begin in Zillah's chamber, represented by **state A**, and if they reach the exit, represented by **state E**, they can successfully escape.



1. (5 points) Catherine and Ellen want to avoid Heathcliff's room, represented by **state C**, during their escape. Set up, **but do not solve**, first step equations for computing the probability that they reach the exit before they reach Heathcliff's room.

2. Catherine and Ellen reached the exit before they reached Heathcliff's room and were able to escape! Now, we wish to find the expected amount of time that their escape took. In the following parts, let X_t represent their state at time step t for $t \in \{0, 1, 2, \ldots\}$.

   (a)

   $$\mathbb{P}[X_{t+1} = D \mid X_t = B,\ X_{t+1} \neq C] =$$

   (b)

   $$\mathbb{P}[X_{t+1} = E \mid X_t = B,\ X_{t+1} \neq C] =$$

   (c) (8 points) Set up, **but do not solve**, hitting time equations for computing the expected amount of time Catherine and Ellen's escape took, given that they successfully avoided Heathcliff's room.