CS 70 Discrete Mathematics and Probability Theory
Spring 2025 Rao

# 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: ______________________________

**Read This.**

- There will be no clarifications. We will correct any mistakes post-exam in as fair a manner as possible. Please just answer the question as best you can and move on even if you feel it is a mistake.
- Due to the above. Please move on. There are lots of problems to get points from. Do not get stuck. This is good advice anyway. In fact, we repeat it below.
- Anything written outside the boxes provided will not be graded.

**Advice.**

- The questions vary in difficulty. In particular, the exam is not in the order of difficulty and quite accessible short answer and proof questions are late in the exam. All blanks are worth 3 points each unless otherwise specified. No points will be given for a blank answer, and there will be no negative points on the exam. **So do really scan over the exam.**
- The question statement is your friend. Reading it carefully is a tool to get to your "rational place".
- You may consult only *two 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. That is, if we ask you to prove a statement, prove it from basic definitions, e.g., "$d \mid x$ means $x = kd$ for some integer $k$" is a definition.**
- There are a total of 348 points on this exam, with 21 total questions.

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 course staff, 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 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.

SIGN Your Name: ________________________________________

## 2. Warmup.

(1 point) May 16th is a special day: not only is it the day of the Spring 2025 CS70 final exam, but it is also which TA's birthday? (Hint: It may help to read through the entire exam!)

## 3. Propositional Logic

1. Let $P$, $Q$ and $R$ be propositions.
   (a) $(P \implies \neg Q) \equiv (\neg P \vee \_\_\_\_\_)$ (Fill in the blank to make the statement always true.)

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

   ○ True ○ False

   (c) $P \wedge (\neg P \vee Q) \wedge (\neg P \vee \neg Q)$

   ○ Always True ○ Always False ○ Either

2. Let $P(n)$ and $Q(n)$ are propositions over $n \in \mathbb{N}$.
   (a) Suppose the following is true:

   $$(\forall n \in \mathbb{N})(P(n) \implies Q(n+1)) \wedge (\forall n \in \mathbb{N})(Q(n) \implies P(n+1)) \wedge P(0)$$

   Determine whether the following statements are true or false.

   i. $(\forall n \in \mathbb{N})(2 \mid n \implies P(n))$

   ○ True ○ False

   ii. $(\forall n \in \mathbb{N})(\neg Q(n+1) \implies \neg P(n))$

   ○ True ○ False

   iii. $Q(0) \implies (\forall n \in \mathbb{N})(Q(n))$.

   ○ True ○ False

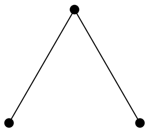
   (b) $\neg(\forall n \in \mathbb{N})(P(n) \vee Q(n)) \implies (\exists n \in \mathbb{N})(\neg P(n))$.

   ○ True ○ False

## 4. Proofs

1. (8 points) Suppose $p$ and $q$ are distinct primes larger than 2.
   Prove that if $e \equiv d^{-1} \pmod{(p-1)(q-1)}$, then $x^{ed} \equiv x \pmod{pq}$.
   (You are welcome to use the Chinese Remainder Theorem and/or Fermat's Little Theorem, but simply asserting this is true from the fact that RSA works properly will earn 0 points.)

2. A graph $H = (V_H, E_H)$ is a *subgraph* of another graph $G = (V_G, E_G)$ if there exists an injective function $h : V_H \to V_G$ mapping vertices in $H$ to vertices in $G$, such that each edge $(u, v) \in E_H$ corresponds to an edge $(h(u), h(v)) \in E_G$.
   There is only one tree on three vertices; the length two path:



   (a) (4 points) Draw all of the 4-vertex trees.

   (b) Every three vertex tree is a subgraph of $K_3$.

   ○ True ○ False

(c) (10 points) Prove by induction on $k$ that any simple graph $G$ with minimum degree $d$ contains every $k$-vertex tree as a subgraph, for each $1 \leq k \leq d$.

## 5. Stable Matching

1. In a stable matching instance with $n$ jobs and $n$ candidates, if all jobs have the same preference list, how many days does it take for the job propose and reject algorithm to terminate?

2. If all jobs have the same preference list, there is only one stable matching.

   ○ True ○ False

3. If all candidates have the same preference list, there is only one stable matching.

   ○ True ○ False

4. Consider a stable matching instance with $n$ jobs and $n$ candidates, where the job and candidate preference lists are uniformly random permutations.
   (a) What is the expected number of candidates who get exactly $i$ proposals on the first day? (Hint: the binomial distribution might be useful.)

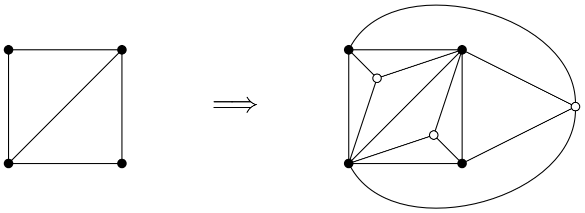
   (b) For $n = 2$, recall that there are only two possible matchings. What is the probability that both are stable?

## 6. Graphs

1. Given an $n$ vertex planar graph where every face has exactly four edges, then the graph has exactly _______ edges. (Your answer may possibly be in terms of $n$.)

2. Let $G$ be a simple planar graph; in the following, we will consider a planar drawing of $G$. We define the *face-vertex graph* $F = (V_F, E_F)$ of $G$ to be the graph that contains all vertices in $G$ alongside an additional vertex for each face in $G$. Every edge in $G$ also appears in $F$, but we additionally define edges incident to face vertices such that $(f, v) \in E_F$ if the face $f$ (which is a cycle in $G$) contains the vertex $v$.

   For example, we have the following drawing of a graph $G$ and its face-vertex graph $F$ (face vertices are in white).



   In the following, let $F$ be the face vertex graph for a planar drawing of a graph $G$ with $v$ vertices, $f$ faces, and $e$ edges. You may assume that $F$ is planar.

   (a) How many vertices are in the face-vertex graph of $G$?

(b) How many edges are in the face-vertex graph of $G$? (Hint: What is the length of each face?)

3. A tree has one connected component. Removing an edge results in a graph with ________ connected component(s).

4. To make $K_{2n}$ bipartite, one must remove at least ________ edges. (Give a tight bound; your answer may possibly be in terms of $n$.)

5. The least number of colors to *vertex color* a tree with max degree $d$ is ________. (Your answer may possibly be in terms of $d$.)

6. The least number of colors to *edge color* a degree $d$ tree is ________. (Your answer may possibly be in terms of $d$.)

7. The maximum number of edges in an $n$ vertex graph where every cycle has length at least $n$ is ________. (Your answer may possibly be in terms of $n$.)

8. The length of an Eulerian tour in an Eulerian graph with $n$ vertices and $m$ edges is ________. (Your answer may possibly be in terms of $n$ and/or $m$.)

9. Consider removing a simple cycle of length $k$ from a connected graph with $m$ edges and $n$ vertices. The resulting graph has $c$ connected components.

   (a) What is the minimum value of $c$? (Your answer may possibly be in terms of $k$ and/or $n$. Do not use $m$.)

   (b) What is the maximum value of $c$? (Your answer may possibly be in terms of $k$ and/or $n$. Do not use $m$.)

## 7. Modular Arithmetic

In the following parts, when working under arithmetic modulo $N$, your answers should be given in the range $\{0,1,\ldots,N-1\}$.

1. What is $2^{36} \pmod 7$?

2. What is $2^{36} \pmod{35}$?

3. If $x \equiv 0 \pmod d$, then $bx - kd \equiv 0 \pmod d$ for any values of $b$ and $k$.

   ○ True ○ False

4. If $x \equiv 1 \pmod d$, then $bx - kd \equiv 1 \pmod d$ for any values of $b$ and $k$.

   ○ True ○ False

5. Find $\gcd(385, 70)$.

6. Let $\gcd(a, m) = d$, and $2a \equiv b \pmod{m}$.

   (a) Then $(2 + \_\_\_\_)a \equiv b \pmod{m}$. (Your answer may possibly be in terms of $a$, $d$, and/or $m$, and must not be $0 \pmod{m}$.)

   (b) $2 \mid b$.

   ○ True ○ False

   (c) $d \mid b$.

   ○ True ○ False

   (d) The number of solutions to $ax \equiv b \pmod{m}$ is ________ if there is at least 1 solution.

7. A perfect square modulo $m$ is a value $x$ such that there exists an $a$ such that $a^2 \equiv x \pmod{m}$.

   (a) How many perfect squares are there under modulo 3?

   (b) If $p > 2$ is prime, how many perfect squares are there under modulo $p$?

   (c) How many perfect squares are there under modulo 15? (It might be easier to do the next problem.)

   (d) If $m = pq$ for distinct primes $p, q > 2$, how many perfect squares are there under modulo $m$? (Hint: CRT. You may also use the function $P(r)$ as the number of perfect squares under modulo $r$ for a prime $r$, with appropriate arguments in your solution.)

**8. Polynomials.**

1. (1 point each) Your friend Faith is performing Lagrange interpolation through three distinct points in the field GF(5). She has already found the interpolating polynomial $P(x) = x^2 + 4x + 1$ and you know that one of her *delta polynomials* is $\Delta(x) = x^2 + 3x + 2$.
   Determine the three original points she must have used, in the form $(x, y)$.

2. Any degree exactly 2 polynomial is a bijection under modulo $p$ for a prime $p$. (Hint: think about perfect squares.)

   ○ True ○ False

3. Any degree exactly 1 polynomial is a bijection under modulo $p$ for a prime $p$.

   ○ True ○ False

4. Recall that two polynomials $P(x)$ and $Q(x)$ intersect at $a$ if $P(a) = Q(a)$.
   (a) Find the $x$-value where $P(x) = 2x + 3 \pmod 5$ and $Q(x) = 3x + 2 \pmod 5$ intersect. (That is, find a value $a$ where $P(a) \equiv Q(a) \pmod 5$. )

   (b) If $P(x)$ and $Q(x)$ are distinct polynomials, with degrees $d_p$ and $d_q$ respectively, what is the maximum possible number of intersections under modulo $p$ for a prime $p > \max(d_p, d_q)$? (In other words, at most how many distinct values of $a$ are there such that $P(a) \equiv Q(a) \pmod p$? Give a tight bound.)

   (c) Working modulo a prime $p > 3$, suppose we fix a polynomial $P(x)$ of degree 3. How many degree 3 polynomials $Q(x)$ are there such that $Q(1) \equiv P(1) \pmod p$ and $Q(2) \equiv P(2) \pmod p$?

5. Recall that the Berlekamp–Welch algorithm encodes a message using a polynomial $P(x)$, and decodes using the error polynomial $E(x)$.
   (a) Suppose you want to send a message of length $n$, and would like to tolerate $k$ corruptions. What is the degree of $P(x)$?

(b) Suppose you want to send a message of length $n$, and would like to tolerate $k$ corruptions. How many points $(i, P(i))$ would you be sending?

(c) (5 points) Suppose you receive the packets $(i, r_i)$, with at most $k$ corruptions (i.e. $r_i \neq P(i)$ at most $k$ times.)
Argue that $E(i)(P(i) - r_i) = 0$ at all of the points that are sent. (You should use properties of the error polynomial $E(x)$ which corresponds to the errors in $r_i$.)

**9. Counting**

Throughout this question, you may leave your answers unsimplified (i.e. you can leave binomial coefficients, factorials, exponents, etc. as is), but you should not use any summation or product notation (i.e. you may not use $\sum$ or $\prod$).

1. How many ways can the letters in BAA be arranged?

2. How many ways can the digits in 126 be arranged?

3. Suppose there are $n$ teddy bears and $k$ children, for $n > k$. How many ways are there to assign teddy bears to the children, such that every child has a single distinct teddy bear? The bears and children are both distinguishable.

4. How many simple bipartite graphs $G = (L, R, E)$ are there with $m$ total edges, such that $|L| = |R| = n$ and $E \subseteq L \times R$? Here, assume that vertices are labeled.

5. How many functions are there under modulo $p$, for a prime $p$? (A function under modulo $p$ maps $f : \{0,\dots,p-1\} \to \{0,\dots,p-1\}$.)

6. How many bijective functions are there under modulo $p$, for a prime $p$?

7. How many ways are there to make 3 teams of 4 players out of 15 players in total? (The teams are distinguishable, i.e., assume the teams are named as Teams 1, 2 and 3.)

**10. Combinatorial Proof.**

1. (8 points) Give a combinatorial proof that $\sum_{i=0}^{n} \binom{n}{i}\binom{n}{n-i} = \binom{2n}{n}$.

2. (4 points) Argue the previous part implies that $\sum_{i=0}^{n} \binom{n}{i}^2 = \binom{2n}{n}$.

## 11. Countability

1. The cardinality of the set of all subsets of the natural numbers is the same as the cardinality of the set of real numbers in the interval $[0,1]$.

   ○ True ○ False

2. If $A_1, A_2, \ldots, A_n$ are countable sets, than the $\mathscr{A} = \{(a_1, \ldots, a_n) : a_i \in A_i\}$ is countable.

   ○ True ○ False

3. Let $A$, $B$, and $C$ be sets, with $A = \mathbb{Z} \times \mathbb{Z}$. Suppose there exists a surjective (onto) function $f : A \to C$, and an injective (one-to-one) function $g : C \to B$.

   (a) $A$ is countable.

   ○ True ○ False

   (b) The cardinality of $A$ is strictly smaller than the cardinality of $B$.

   ○ True ○ False

4. Give a bijection from the reals in $(0,1]$ to the reals in $[1,\infty)$.

   $f(x) =$

## 12. Computability

1. There exists a program which given another program $P$, an integer $k$, and an input $x$, determines whether the program $P(x)$ halts in at most $|x|^k$ steps.

   ○ True ○ False

2. Suppose you have a program `HaltsOnEmpty`, which given an program $P$, determines whether $P$ halts on the empty string.

   Fill in the following blanks to write a program `Halt` that takes a program $P$ and an input $x$ and determines whether $P$ halts on input $x$. You may only use variables defined in the template.

```
def Halt(P, x):
    def inner(y):
        _______(1)_______

    return HaltsOnEmpty(______(2)______)
```

(1)

(2)

## 13. Basic Probability.

Consider a sample space $\Omega$ with the probability function $\mathbb{P} : \Omega \to (0,1]$, and events $A, B, C \subseteq \Omega$ all with non-zero size.

All of your answers below may only be expressions involving $\mathbb{P}[A]$, $\mathbb{P}[B]$, $\mathbb{P}[C]$, and/or some real numbers.

1. Give the lowest upper bound on $\mathbb{P}[A \cup B]$.

2. Give the highest lower bound on $\mathbb{P}[A \cup B]$.

3. If $A \subseteq B$, give the highest lower bound on $\mathbb{P}[A \mid B]$.

4. If $A \subseteq B$, give the highest lower bound on $\mathbb{P}[B \mid A]$.

5. Suppose $\mathbb{P}[A \cap B] = \alpha$ and $\mathbb{P}[B \cap C] = \alpha$.
   Your answers below may now additionally involve $\alpha$. (Hint: Think about the sets for various $\alpha$'s.)
   (a) Give the lowest upper bound on $\mathbb{P}[A \cap C]$.

   (b) Give the highest lower bound on $\mathbb{P}[A \cap C]$.

   (c) (3 points) Justify your answer for the previous question.

### 14. Four or six?

Suppose you have a four sided die and a six sided die. You choose one die uniformly at random and roll it twice. Let $A$ be the event that the first roll is 1, and let $B$ be the event that the second roll is a 1.

1. What is $\mathbb{P}[A \mid B]$?

2. Let $C$ be the event that the four sided die is chosen. What is $\mathbb{P}[C \mid A]$?

### 15. Bernoulli Random Variables

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

2. 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 $\mathbb{P}[X = Y]$?

### 16. Confidence Interval.

Consider the process of sampling $n$ people who tested for flu last year to determine the fraction $p$ of the population that would test positive. To set this up, let $X_i$ be the indicator random variable that person $i$ in the sample tested positive for the flu for $i \in \{1, \ldots, n\}$.

1. What is $\mathbb{E}[X_i]$ in terms of $p$?

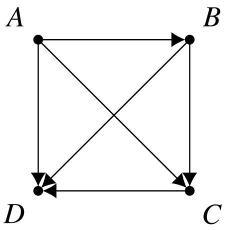
2. What is the tightest possible upper bound on $\text{Var}(X_i)$, independent of the value of $p$?

3. Using Chebyshev's inequality, give a 95% confidence interval for $p$, given that 50 people in your sample of 100 people tested positive for having the flu.

**17. Hamiltonian Paths.**

Consider a tournament, i.e. a complete directed graph on $n$ vertices. A Hamiltonian path on a tournament is a sequence of directed edges that visits every vertex exactly once, with each edge pointing from one vertex to the next in the sequence.

For example, the following tournament contains only 1 Hamiltonian path $A \to B \to C \to D$:



1. (8 points) Prove that every tournament contains a Hamiltonian path.

2. Consider the following way of choosing a random tournament $T$ on $n$ vertices: independently for each (unordered) pair of distinct vertices $i, j \in \{1, ..., n\}$, flip a coin and include the edge $i \to j$ in the graph if the outcome is heads, and the edge $j \to i$ if tails.

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

   (b) What is the expected number of Hamiltonian paths? (Hint: use indicator random variables that indicates whether a permutation forms a Hamiltonian path.)

## 18. Linear Regression.

1. For random variables $X$ and $Y$, the linear regression line of $Y$ given $X$ goes through the origin if and only if $\mathbb{E}[Y] =$ ________.

2. For a random variable $X$, $\mathbb{E}[X^2] =$ ________. (Give an answer in terms of $\text{Var}(X)$ and/or $\mathbb{E}[X]$.)

3. For random variables $X$ and $Y$, we have $\text{cov}(X,Y) = \mathbb{E}[XY]$ if $\mathbb{E}[X] = \mathbb{E}[Y] =$ ________.

4. For independent random variables $X$ and $Y$, what is the best linear estimator for $Y$ given $X$, i.e., $\hat{Y}(X)$? (Your answer should be fully simplified.)

## 19. Distributions

1. Given independent random variables $X,Y \sim \text{Bin}(n,p)$, what is the distribution of $X+Y$?

2. Given independent random variables $X,Y \sim \text{Geom}(p)$, what is the distribution of $\min(X,Y)$?

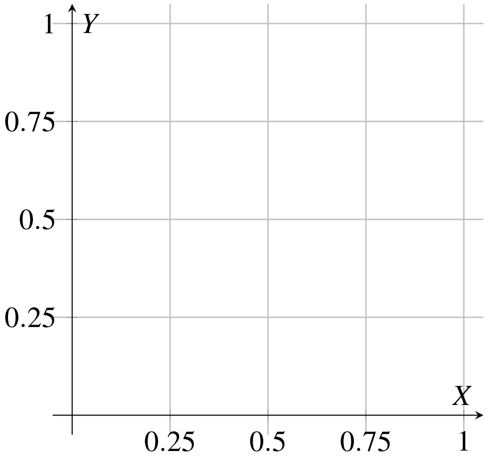
3. What is $\lim_{n\to\infty} \binom{n}{i} \left(\frac{\lambda}{n}\right)^i \left(1-\frac{\lambda}{n}\right)^{n-i}$?

4. Suppose $X \sim \text{Uniform}(0,1]$ and $Y \sim \text{Uniform}[0,X]$.

   (a) What is the marginal density function for $X$? (2 points for the expression, 1 point for bounds)

$$f_X(x) = \begin{cases} \boxed{\qquad\qquad\qquad} & \text{if } \boxed{\qquad\qquad\qquad} \\ 0 & \text{otherwise} \end{cases}$$

   (b) (3 points) Shade the region where the density is non-zero.



   (c) What is the conditional density function $f_{Y|X}(x,y)$ on the shaded region from (b)?

$$f_{Y|X}(x,y) = \boxed{\qquad\qquad\qquad}$$

   (d) What is the marginal density function for $f_Y(y)$? (2 points for the expression, 1 point for bounds)

$$f_Y(y) = \begin{cases} \boxed{\qquad\qquad\qquad} & \text{if } \boxed{\qquad\qquad\qquad} \\ 0 & \text{otherwise} \end{cases}$$

**20. Continuous Probability.**

1. Let $X$ be a continuous RV with cumulative distribution function (CDF) $F(x)$, and probability density function (PDF) $f(x)$.

   (a) Express $\mathbb{P}[X \in [a,b]]$ in terms of the CDF $F(x)$ for $X$.

   (b) Express $\mathbb{P}[X \in [a,b]]$ in terms of the PDF $f(x)$ for $X$.

   (c) What is $\mathbb{P}[X \leq b \mid X \geq a]$ in terms of the CDF $F(x)$ for $X$? (Think carefully about the events.)

2. For $X \sim \text{Uniform}[a,b]$.

   (a) What is $\mathbb{P}[X \leq t \mid X \geq s]$ for $a < s < t < b$?

   (b) $\text{Uniform}[a,b]$ is memoryless.

   ○ True ○ False

3. Suppose $m$ real numbers are chosen uniformly and independently at random from $[0,1]$. Let $X$ be the smallest one of these numbers.

   (a) What is the PDF of $X$? (2 points for expression, 1 point for bounds)

$$f_X(x) = \begin{cases} \boxed{\phantom{xxxxxxxxxx}} & \text{if } \boxed{\phantom{xxxxxxxxxx}} \\ 0 & \text{otherwise} \end{cases}$$

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

**21. Markov Chain.**

1. Consider the Markov Chain on the elements of $\{0,\ldots,29\} \pmod{30}$ where there are transitions with equal probability from state $i \pmod{30}$ to state $i+3 \pmod{30}$ and state $i+5 \pmod{30}$.

   (a) Is the chain irreducible?

   ○ Yes ○ No

   (b) What is the period of state $0 \pmod{30}$?

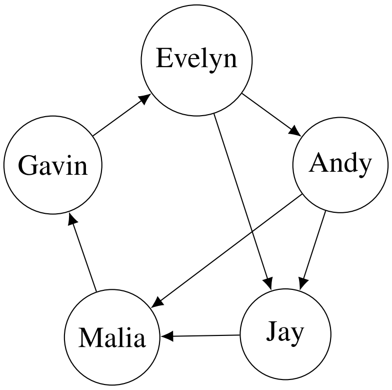
   (c) The uniform distribution is invariant.

   ○ True ○ False

2. There is an unexpected pepper shortage at La Val's Pizza! Five friends (Andy, Gavin, Evelyn, Jay, and Malia) must share a single pepper shaker. At time 0, the shaker is in Evelyn's hands, and its location is thereafter recorded at discrete one-minute intervals. During each minute, the current holder passes it to one of the other four friends, according to fixed transition probabilities. The shaker's movement is modeled as a Markov chain with state space

$$S = \{\text{Andy}, \text{Gavin}, \text{Evelyn}, \text{Jay}, \text{Malia}\}.$$

   The transitions are depicted below, where each person chooses uniformly over their outgoing arrows.



   (a) Compute the expected *hitting time* of Andy, i.e. the expected number of minutes until the shaker first reaches Andy.

   (b) It's Jay's birthday today (May 16), and he is worried that Gavin will use all the pepper. Find the probability that the shaker reaches Jay before it next reaches Gavin.