CS 70 Discrete Mathematics and Probability Theory
Fall 2024 Hug, 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 326 points on this exam, with 21 total questions.

SID: ______________________________

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. Propositions and Proofs

1. In the following parts, let P, Q and R be propositions. Determine the truth value of the following statements as always true, always false, or either true or false.

   (a) $P \vee Q \vee R \vee \neg R$

   ◯ Always True ◯ Always False ◯ Either

   (b) $(\neg P \implies (R \wedge \neg R)) \implies P$

   ◯ Always True ◯ Always False ◯ Either

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

   ◯ Always True ◯ Always False ◯ Either

2. Let $P(x)$, $Q(x)$, and $R(x,y)$ be predicates for $x, y \in U$, where U is a non-empty universe.
   Suppose we know the following is true:

   $$(\forall x \in U)\big(P(x) \implies [Q(x) \vee (\exists y \in U)(R(x,y))]\big)$$

   (a) Consider an element $x \in U$ such that $P(x)$ is True, and $(\forall y \in U)(\neg R(x,y))$ is True. What is $Q(x)$?

   ◯ Always True ◯ Always False ◯ Either

   (b) Consider an element $x \in U$ such that $Q(x)$ is False, and $(\forall y \in U)(\neg R(x,y))$ is True. What is $P(x)$?

   ◯ Always True ◯ Always False ◯ Either

   (c) Consider an element $x \in U$ such that $P(x)$ is True, and $(\exists y \in U)(R(x,y))$ is True. What is $Q(x)$?

   ◯ Always True ◯ Always False ◯ Either

3. Fill in the following blank using an expression involving *only* $\max(a,b)$ and $\min(a,b)$:

   $$|a-b| = \underline{\qquad\qquad}.$$

3. Induction

1. (0 points) Dogs know induction.

   ◯ True ◯ False

2. Consider a predicate $P(n)$ for $n \in \mathbb{N}$. Fill in the blank to make the following statement true.

$$(\forall n \in \mathbb{N})(P(n) \implies P(n+1)) \equiv \neg(\exists n \in \mathbb{N})(P(n) \wedge \_\_\_\_\_)$$

3. Recall the Fibonacci sequence is defined by $F_0 = 1$, $F_1 = 1$, and $\forall i \geq 2$, $F_i = F_{i-1} + F_{i-2}$.
   We would like to show that $F_i \geq c^{i-1}$ for some specific value of c and all $i \geq 1$.

   (a) What is the value of c? Your value of c should be as large as possible. (Note: $F_1 \geq c^0$ for any c.)

   (b) (8 points) Prove that your answer is correct.

4. Stable Matching

1. Consider the following preferences lists for a stable matching instance:

Jobs	Preferences
A	$1 > 2$
B	$2 > 1$

Candidates	Preferences
1	$B > A$
2	$A > B$

(a) Provide a job optimal stable pairing.

(b) Provide a candidate optimal stable pairing.

2. Consider the following preferences lists for a stable matching instance:

Jobs	Preferences
A	$1 > 2 > 3 > 4$
B	$2 > 1 > 4 > 3$
C	$3 > 4 > 1 > 2$
D	$4 > 3 > 2 > 1$

Candidates	Preferences
1	$B > A > C > D$
2	$A > B > D > C$
3	$D > C > A > B$
4	$C > D > B > A$

(a) How many stable matchings are there for these preference lists?

(b) Provide a stable matching that is neither candidate optimal nor job optimal.

5. Graphs

All graphs are simple and undirected unless otherwise specified.

1. Let $G = (V, E)$, with k **connected components**.
   (a) What is the sum of the degrees of all vertices in G? (Your answer should possibly be in terms of $|E|$, $|V|$ and/or k.)

   (b) What is the maximum possible number of edges in G? (Give a tight bound in terms $|V|$ and k. Your answer should not include $|E|$.)

   (c) What is the minimum possible number of edges in G? (Give a tight bound in terms of $|V|$ and k. Your answer should not include $|E|$.)

2. Consider a hypercube $G = (V, E)$.
   (a) Recall a vertex coloring is an assignment of colors to vertices such that the endpoints of every edge are colored differently. What is the minimum number of colors needed to vertex color G? (Possibly in terms of $|V|$ and $|E|$.)

   (b) Recall an edge coloring is an assignment of colors to edges such that any two edges incident to the same vertex are colored differently. What is the minimum number of colors needed to edge color G? (Possibly in terms of $|V|$ and $|E|$.)

3. Removing the edges in a cycle of length k from a connected graph produces a graph with at most _______ connected components. (Give a tight bound.)

6. 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 $2^{63} \pmod{77}$?

2. What is $1 \times 2 \times 3 \times 4 \times 5 \times 6 \pmod{7}$?

3. Compute the multiplicative inverse of $63 \pmod{71}$.

4. Consider equations of the form $ax \equiv b \pmod{pq}$, for distinct primes p and q. Note that there are $(pq)^2$ possible values of (a,b) pairs modulo pq.

   (a) How many values $a \in \{0,\ldots,pq-1\}$ are relatively prime to p?

   (b) How many values $a \in \{0,\ldots,pq-1\}$ are relatively prime to p and q?

   (c) For how many pairs (a,b) does $ax \equiv b \pmod{pq}$ have a unique solution?

   (d) Consider the equation $ax \equiv b \pmod{pq}$ where $\gcd(a,pq) = p$. If x is a solution to the equivalence, then $x +$ _____ is also a solution.

   ○ p　　○ q

(e) For how many pairs (a,b) does $ax \equiv b \pmod{pq}$ have exactly p solutions?

(f) (5 points) For how many pairs (a,b) does $ax \equiv b \pmod{pq}$ have 0 solutions?

5. For any natural number $N \geq 1$, if $(\forall a,b \in \{1,\ldots,N-1\})(ab \not\equiv$ _____ $\pmod{N})$, then N is prime. (Fill in the blank to make the statement true.)

6. (5 points) Recall the CRT implies that there is a unique $x \pmod{pq}$ where $x \equiv a \pmod{p}$ and $x \equiv b \pmod{q}$, for distinct primes p and q. Use this fact to prove that there are $(p-1)(q-1)$ values in $\{0,\ldots,pq-1\}$ that are relatively prime to pq.

7. Polynomials

1. What is $\Delta_0(x)$ for the points $(0,0)$, $(1,1)$, $(4,1)$ under arithmetic modulo 5?

2. Suppose we would like to perform the Berlekamp–Welch algorithm, where a degree 0 polynomial (for a message of size $n=1$) was sent and $k=1$ error is possible.
   Working in GF(5), the points $(0,1)$, $(2,1)$, $(3,4)$ are received.
   (a) What is the original polynomial?
   (b) Let $Q(x) = q_1x + q_0$ and $E(x) = x + b_0$. Write out the equation in the Berlekamp–Welch system for the point $(3,4)$.

3. Consider the $\Delta_i(x)$ polynomials for the points $(0,y_0),(1,y_1),\ldots,(n-1,y_{n-1})$, modulo a prime p.
   (a) What is the value of $\Delta_i(i)$? (Your answer should either be a numerical value or an expression possibly in terms of n and p.)
   (b) What is $\Delta_i(j)$ for $j \neq i$? (Your answer should either be a numerical value or an expression possibly in terms of n and p.)
   (c) Consider the points $(0,y_0),(1,y_1)$ and $(2,y_2)$. What is the corresponding degree 2 polynomial $P(x)$ in terms of the delta polynomials $\Delta_0(x)$, $\Delta_1(x)$, and $\Delta_2(x)$?

8. Counting Basics

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 distinct ways can you rearrange the letters in the word "BERKELEY"?

2. How many ways can you arrange n labeled balls into m labeled bins?

3. Recall that there are 52 cards in a deck, and there are 13 cards in each of four suits. Further, the order of cards in a poker hand does not matter.

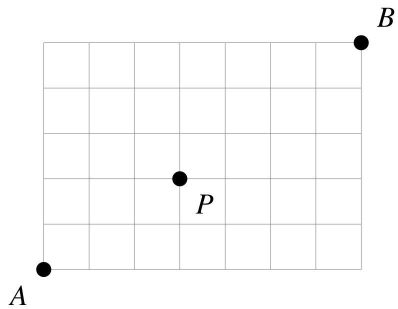
   (a) How many flushes (all cards of the same suit) are there in a 5 card poker hand?

   (b) Suppose you are playing Texas Hold'em, and you have two hearts, and five more cards from the remaining 50 will be flipped over. How many ways can at least 3 more hearts be present in the 5 new cards flipped over? (In other words, how many ways can the 7 total cards contain a flush?)

4. How many integer solutions are there for $x_1 + \cdots + x_k = n$, where $x_i \geq -1$ for all i?

9. Grids

Consider the following grid. A walk on this grid is only allowed to move right or up.



1. How many ways can you walk from A to B? (Note that it has width 7 and height 5.)

2. How many ways can you walk from A to B while passing through P?

3. (8 points) Show that $\binom{12}{7} = \sum_{i=0}^{5} \binom{3+i}{i}\binom{8-i}{5-i}$ using a combinatorial proof. (Proofs based on calculations and algebra alone will not receive any points.)

10. Counting Polynomials.

Recall that a polynomial is defined as $f(x) = \sum_{k=0}^{n} a_k x^k$, where a_k's are a finite list of coefficients. We will extend this definition to *infinite polynomials*, which take the form $f(x) = \sum_{k=0}^{\infty} a_k x^k$, where a_k's are an infinite list of coefficients.

Recall that two polynomials f and g are *equivalent* if for all x, $f(x) = g(x)$.

Classify the following sets as either finite, countably infinite, or uncountably infinite.

1. The set of all non-equivalent finite polynomials with integer coefficients.

   ◯ Finite ◯ Countably Infinite ◯ Uncountably Infinite

2. The set of all non-equivalent finite polynomials with real coefficients.

   ◯ Finite ◯ Countably Infinite ◯ Uncountably Infinite

3. For a fixed prime p, the set of all non-equivalent finite polynomials over modulo p.

   ◯ Finite ◯ Countably Infinite ◯ Uncountably Infinite

4. The set of all non-equivalent *infinite* polynomials with integer coefficients.

   ◯ Finite ◯ Countably Infinite ◯ Uncountably Infinite

5. The set of all non-equivalent *infinite* polynomials with real coefficients.

   ◯ Finite ◯ Countably Infinite ◯ Uncountably Infinite

6. For a fixed prime p, the set of all non-equivalent *infinite* polynomials over modulo p.

   ◯ Finite ◯ Countably Infinite ◯ Uncountably Infinite

11. Computability. (2 points each)

Given a program P and an input x, you want to determine whether $P(x)$ ever calls the subroutine Q. We'll show that this problem is uncomputable.

Let `TestCalls(P, Q, x)` be a program that determines if $P(x)$ ever calls the subroutine Q.

Fill in the blanks below to implement `TestHalt` using `TestCalls`, utilizing only variables defined in the template. You may assume that `dummy` is a unique subroutine that is not present in `F`.

```
def TestHalt(F, a):
    def dummy():
        pass  # do nothing

    def inner(b):
        _______(1)_______
        _______(2)_______

    return TestCalls(_____(3)_____, _____(4)_____, a)
```

(1)

(2)

(3)

(4)

12. Probability Theory.

1. Let A, B, and C be events, where $\mathbb{P}[A] = \frac{1}{2}$, $\mathbb{P}[B] = \frac{1}{3}$, and $\mathbb{P}[C] = \frac{1}{6}$.
   Suppose further that $\mathbb{P}[A \cup B] = \frac{2}{3}$ and $\mathbb{P}[A \mid C] = \frac{2}{3}$.
   (a) What is $\mathbb{P}[A \cap B]$?

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

   (c) What is $\mathbb{P}[C \cap A]$?

   (d) What is $\mathbb{P}[C \mid A]$?

2. Suppose I_D, and I_E are indicator random variables for the events D and E, where $\mathbb{P}[D] = 1/3$, $\mathbb{P}[E] = 1/2$, and $\mathbb{P}[D \cap E] = 1/5$.
   (a) What is $\text{cov}(I_D, I_E)$?

   (b) Recall $\text{LLSE}[I_D \mid I_E] = a(I_E - \mathbb{E}[I_E]) + b$ for constants a and b.
      i. Is the constant a positive or negative or zero?

      ○ Positive ○ Negative ○ Zero

      ii. What is the value of a?

      iii. What is the value of b?

3. Suppose X and Y are independent random variables, where $\mathbb{E}[X] = 2$, $\mathbb{E}[Y] = 3$, $\mathrm{Var}(X) = 1$, and $\mathrm{Var}(Y) = 2$. (The following answers should be numerical values.)

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

   (b) What is $\mathbb{E}[X^2]$?

   (c) What is $\mathrm{Var}(XY)$?

4. Let X be a random variable with PDF $f_X(x) = x$ for $x \in [0, c]$ and $f_X(x) = 0$ otherwise.

   (a) What is c?

   (b) What is the CDF $F_X(x)$ of X, for $x \in [0, c]$?

13. Distributions

1. Consider two independent binomial random variables $X \sim \text{Bin}(n, p)$ and $Y \sim \text{Bin}(n, q)$.
   (a) What is $\text{cov}(X,Y)$?

   (b) What is $\text{Var}(X+Y)$?

2. For a geometric random variable $X \sim \text{Geom}(p)$, what is $\mathbb{E}[X - x \mid X \geq x]$, for $x \geq 0$?

3. For a Poisson random variable $X \sim \text{Poisson}(\lambda)$, what is $\mathbb{P}[X > 0]$?

4. For independent Poisson random variables $X \sim \text{Poisson}(\lambda)$ and $Y \sim \text{Poisson}(\lambda')$, what is $\mathbb{P}[X+Y > 0]$?

5. For an exponential random variable $X \sim \text{Exp}(\lambda)$, what is its PDF $f_X(x)$ for $x \geq 0$?

6. For independent exponential random variables $X \sim \text{Exp}(\lambda)$ and $Y \sim \text{Exp}(\lambda)$, what is the PDF $f_Z(z)$ for $Z = \min(X,Y)$? (*Hint*: what is the probability that both X and Y are greater than z?)

7. Consider a dart hitting a dartboard of radius r, uniformly over its area. Let X be the distance from the dart to the center of the dartboard. What is the PDF $f_X(x)$ of X?

14. Uniform Distribution

Consider continuous uniform random variables X, Y that are independently distributed as $U[0, r]$.

1. Compute the CDF $F_Z(z)$ of $Z = \max(X, Y)$.

2. Compute the PDF $f_Z(z)$ of $Z = \max(X, Y)$.

3. Compute $\mathbb{E}[\max(X, Y)]$.

4. Compute $\mathbb{E}[\min(X, Y)]$. (*Hint*: you do not have to compute any integrals or find the distribution of $\min(X, Y)$.)

5. Compute $\mathbb{E}[|X - Y|]$. (*Hint*: you do not have to compute any integrals; try relying on linearity of expectation.)

15. Close to Home

Suppose we have balls numbered 1 through 100 in bins numbered 1 through 100. Suppose we then shuffle the balls by uniformly permuting them in the 100 bins, such that each bin has exactly one ball.

After shuffling, we say that a ball is "close to home" if it lands within 1 step of its original position. For example:

- Ball 4 is close to home if and only if it lands in bin 3, 4, or 5.
- Ball 100 is close to home if and only if it lands in bin 99 or 100.

1. Let X be the number of balls that are "close to home" after shuffling. What is $\mathbb{E}[X]$?

2. Let I_i be an indicator for whether the ith ball is close to home after shuffling.

   (a) What is $\mathbb{E}[I_2 I_5]$?

   (b) What is $\mathbb{E}[I_2 I_4]$?

   (c) Are I_i and I_j independent for any $i, j \in \{1, \dots, 100\}$?

   ◯ Yes ◯ No

16. Which deck?

A dealer picks one of two decks with equal probability. The loaded deck has 39 red cards and 13 black cards, the fair deck has 26 red cards and 26 black cards.

1. If the dealer deals a red card, what is the probability that the deck is fair?

2. Let p be the answer to the previous part. Still assuming that the dealer deals a red card, what is the probability that the next card will be red? (No need to simplify your answer. You may express your answer in terms of p.)

17. Union Bound, Markov, and Chebyshev

1. (4 points) Let $X = \sum_{j=1}^{n} I_j$, where each I_j is some indicator variable. Let p be the probability that at least one indicator is true. Prove that $p \leq \mathbb{E}[X]$.

2. (4 points) Let W be the number of successes in n independent Bernoulli trials, each with success probability p. Prove that $\mathbb{P}[W \geq k] \leq \frac{np}{k}$.

3. (5 points) Suppose $Y \sim \text{Poisson}(\lambda)$. Prove that $\mathbb{P}[Y \geq 10\lambda] \leq \frac{1}{81\lambda}$.

18. Conditional Probability. (2 + 7 points)

Consider this statement: For any events A, B, and C, we have $\mathbb{P}[C \mid A \cup B] = \mathbb{P}[C \mid A] + \mathbb{P}[C \mid B] - \mathbb{P}[C \mid A \cap B]$.

Is this true or false? If true, give a brief sketch of why this is true. If it is false, give a counterexample. In your counterexample, give the calculations for these four quantities.

○ True ○ False

19. Confidence

Consider independent $X_1, \dots, X_n$, where each $X_i \sim \text{Poisson}(\lambda)$. (Recall $\mathbb{E}[X_i] = \lambda$ and $\text{Var}(X_i) = \lambda$.) Your answers to the following parts should all be in terms of λ.

1. Suppose $A_n = \frac{1}{n} \sum_{i=1}^{n} X_i$. What is $\mathbb{E}[A_n]$?

2. Use Chebyshev's inequality to find the value of n that ensures that

$$\mathbb{P}\big[|A_n - \mathbb{E}[A_n]| \geq 0.1\mathbb{E}[A_n]\big] \leq 0.05.$$

3. Suppose A_n is normally distributed as $N(\mu, \sigma^2)$ for $\mu = \mathbb{E}[A_n]$ and $\sigma^2 = \text{Var}(A_n)$. Further, recall that for a standard normal Z, $\mathbb{P}[|Z| \geq 2] \leq 0.05$. Find n that ensures that

$$\mathbb{P}\big[|A_n - \mathbb{E}[A_n]| \geq 0.1\mathbb{E}[A_n]\big] \leq 0.05.$$

20. Markov Models

Suppose we repeatedly roll a four sided die and wish to track whether our last roll or last two rolls were ones. This process can be modeled by a Markov Chain with three states:

- State 0, where the previous roll was not a one.
- State 1, where the previous roll was a one, but the previous two rolls were not ones.
- State 2, where the previous two rolls were both ones.

1. (4 points) We wish to find the expected number of times we roll an even number before rolling two ones in a row. Write the first-step equations for this problem. (Do not solve the system of equations.)

2. Is there a unique stationary distribution $\pi = \begin{bmatrix}\pi(0) & \pi(1) & \pi(2)\end{bmatrix}$?

   ○ Yes ○ No

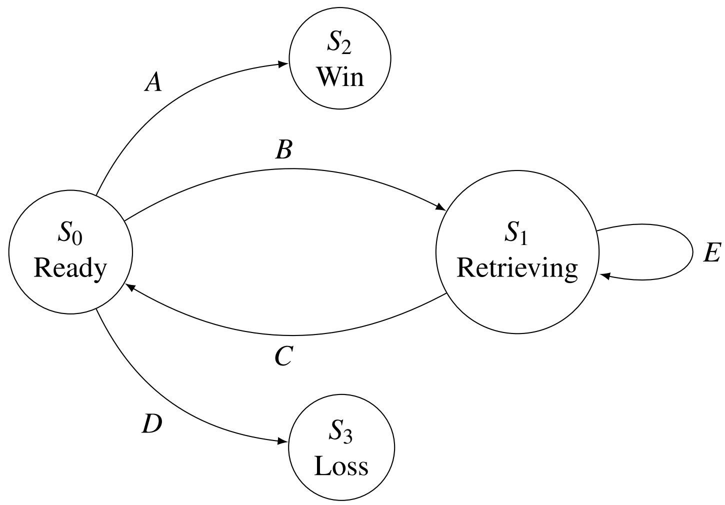
3. (4 points) Either argue that there is no unique stationary distribution, or set up a system of equations for finding $\pi = \begin{bmatrix}\pi(0) & \pi(1) & \pi(2)\end{bmatrix}$.

21. Collaborative Basketball.

Two friends are playing basketball, and they each have a separate basketball hoop. At each timestep, both attempt to shoot the basketball into their hoop, where each makes their shot with an independent probability of $\frac{2}{3}$.

However, if one friend misses, they spend that turn retrieving the basketball, and the other will take a shot that turn. Note that if the friend that shoots misses, they will take the next turn retrieving. If, at a given timestep, they both shoot and make their shots, then they win the game. However, if they both shoot and miss their shots, then they lose the game.

We can model this game as a Markov chain, shown below.



1. (1 point each) Fill in the transition probabilities A through E below.

$A =$ ☐ $B =$ ☐ $C =$ ☐ $D =$ ☐ $E =$ ☐

2. (4 points) What is the probability of winning?

3. (4 points) What is the expected number of timesteps it takes to terminate the game?