CS 70 Discrete Mathematics and Probability Theory
Spring 2017 Rao

Final

PRINT Your Name: ______________________________, ______________________________
(Last) (First)

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

PRINT Your Student ID: ______________________________

WRITE your exam room:

WRITE the name of the person sitting to your left: ______________________________

WRITE the name of the person sitting to your right: ______________________________

PLEASE READ THE FOLLOWING INSTRUCTIONS CAREFULLY

- After the exam starts, please *write your student ID on every page*. **You will not be allowed to write** *anything* **once the exam ends**.
- 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.
- The questions vary in difficulty. If you get stuck on any one, it helps to leave it and try another one.
- The questions vary in difficulty. If you get stuck on any one, it helps to leave it and try another one.
- We indicate where justification is needed and where it isn't. In general, no justification on short answer/true false questions unless otherwise indicated.
- Calculators are not allowed. **You do NOT need to simplify any probability related answers to a decimal fraction,** but your answer must be in the simplest form (no summations or integrals).
- You may consult only *3 sheets of notes*. Apart from that, you are not allowed to look at books, notes, etc. Any electronic devices such as phones and computers are NOT permitted.
- **You may not discuss any exam related content until Saturday night**. Final exam scores will be released around *Saturday*. Regrade requests will be due around *Sunday)*.
- There are **16** single sided pages on the exam. Notify a proctor immediately if a page is missing.
- You have **180** minutes: there are **8** questions on this exam worth a total of **192** points.

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

SID:

1. True/False/Short Answer: Discrete Math (mostly). 3 points by 10 parts.

Please write your answer in the provided box, or bubble in the corresponding option. **This is what is to be graded. No need to justify!**

1. (True/False) $A \implies B$ is logically equivalent to $\neg B \implies \neg A$.

   ◯ True

   ◯ False

2. (True/False) $P(0) \wedge (\forall n \in \mathbb{N}, P(n) \implies P(n+1))$ is logically equivalent to $\forall n \in \mathbb{N}, P(n)$.

   ◯ True

   ◯ False

3. (True/False) If $d = gcd(y,z)$ then $gcd(\frac{yz}{d^2}, d) = 1$.

   ◯ True

   ◯ False

4. Give an example of x and m where x has no multiplicative inverse $\pmod m$.

5. If there is at least one solution to the equation $ax = b \pmod m$ where $d = gcd(a,m)$, how many total solutions in $\{0, \dots, m-1\}$ are there?

6. What is the maximum number of solutions in $\{0, \dots, m-1\}$ for $ax = 1 \pmod m$ for any natural numbers a and m?

7. What is $\Delta_1(x)$ in Lagrange interpolation for the points $(1,3)$,$(2,3)$, $(3,4)$ modulo 5, for a degree 2 polynomial? (Factored form is fine.)

8. Polynomial Related Questions. In the following, recall that a polynomial, $P(x)$, contains a point (a,b) when $P(a) = b$. Two polynomials, $P(x)$ and $Q(x)$, intersect at a point (a,b) when $P(a) = Q(a) = b$.

   (a) Working modulo p where p is prime, what is the maximum number of times a polynomial $P(x)$ of degree exactly $d > 0$ and $d < p$ can take on a value v modulo p?

   (b) What is the smallest number of degree exactly $0 < d \leq p$ polynomials all modulo p for a prime p, whose product is the zero polynomial. (A product of polynomials $P(x)$, $Q(x)$, $R(x)$, is the function $F(x) = P(x)Q(x)R(x)$. A function is the zero function if $F(x) = 0$, for all x. Your answer may be in terms of p and d.)

9. What is $2^{27} \pmod{15}$?

10. The RSA scheme only has $m^{ed} = m \pmod{N}$ for messages m where $gcd(m,N) = 1$. (Recall (N,e) is the public, and d is the private key.) (True/False)

○ True

○ False

2. Short Arguments: Mostly Discrete Math. 10/12 points
Provide a clear and concise justification of your answer.

1. Stable Marriage/Simple Proof.

   Consider a stable room-mates problem on $2n$ people where all people have consistently ordered preference lists. That is, if $a > b$ in one list, this is true in every preference list that contains both a and b. Prove or disprove, that there is always a stable pairing. (Recall that a stable pairing of $2n$ people is a partition of the people into n pairs where there are no rogue couples. In this case, a rougue couple is two people not currently paired, who both prefer each other to their current partners).

2. Colorings/Graphs. Recall a vertex coloring of a graph is an assignement of colors to vertices where the endpoints of each edge are different colors.

   (a) Give an example of a graph with maximum degree 4 that requires 5 colors to be vertex-colored. (No or very brief justification.)

   (b) What is the least number of colors needed to color any n-vertex tree? (No or very brief justification.)

   (c) Prove that for any connected graph with all vertices having degree at most d, that all but one vertex can be colored using only d colors. (That is, the removal of a single vertex leaves a graph that can be colored with $d-1$ colors.)

3. **Counting outfits. (10/10) points**

   This problem should have brief justification.

   1. You have 5 shirts, 3 pairs of pants, 4 dresses, and 5 pairs of shoes. Every day you choose to wear either a dress and shoes, or a shirt, pants and shoes.

      (a) How many outfits do you have?

      (b) If on each day of a 100 day semester, you choose a possible outfit to wear uniformly at random and independently of all other days, what is the expected number of outfits that are worn more than once over the semester? (No need to simplify.)

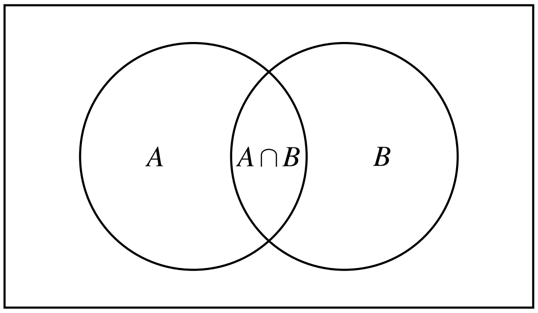
2. You have 5 pairs of socks. Each pair is a different color (and so is distinguishable), but the two socks within a pair are indistinguishable. (Note your left foot, right foot and nose are all distinguishable.)

   (a) How many ways are there for you to choose two socks to wear on your feet?

   (b) You want to be super cool, so you are also going to wear a third sock on your nose. Now how many ways are there for you to choose socks?

4. Probability Warmup: Zen with Venn. 7 parts. 3 points each.

Consider the diagram, not drawn to scale:



Let x be $Pr[A]$, y be $Pr[B]$ and $z = Pr[A \cap B]$.

In terms of x, y and z, what is

1. $Pr[A|B]$?

2. $Pr[B|A]$?

3. $Pr[B|\overline{A}]$?

4. $Pr[A \cup B]$?

5. If A and B are independent, what is z in terms of x and y? (Henceforth, the diagram may be misleading.)

6. If A and B are disjoint, what is z?

7. If A and $\overline{B}$ are disjoint, what is z in terms of x and y?

5. **Probability: Short Answers/True/False. 12 parts. 3 points each.**

Please write your answer in the provided box, or bubble in the corresponding option. **This is what is to be graded. No need to justify!**

1. Given a random variable, X, with expectation $\mu = E[X]$, what value a minimizes $E[(X-a)^2]$? (Answer is an expression.)

2. Given random variables, X and Y, with $E[X] = 1$ and $E[Y] = 2$, and $cov(X,Y) = 1$, and $var(X) = 2$, what is the LLSE prediction for Y if $X = 2$?

3. (True/False) The covariance of X and Y is always less than the variance of X.

○ True

○ False

4. For independent exponentially distributed random variables, X and Y, both with parameter λ, the covariance of $Z = \min(X,Y)$ and $W = \max(X,Y) - \min(X,Y)$ is positive, negative or zero?

5. For independent exponentially distributed random variables, X and Y, with different parameters λ_X and λ_Y, the covariance of $Z = \min(X,Y)$ and $W = \max(X,Y) - \min(X,Y)$ is positive, negative or zero?

6. (True/False:) Let X, Y, and Z be random variables. Then $\mathbf{E}[(Y - L[Y \mid X])L[Z \mid X]] = 0$.

○ True

○ False

7. (True/False) $\mathbf{E}[(Y - L[Y \mid X])^2] \geq \mathbf{E}[(Y - L[Z \mid X])^2]$.

   ◯ True

   ◯ False

8. (True/False:) If Z is a linear function of Y and Y is a linear function of X, then $L[Z \mid X] = L[Z \mid L[Y \mid X]]$.

   ◯ True

   ◯ False

9. What is the probability density function for a continuous random variable with $Pr[X \leq x] = 1 - 1/x$, for $x \geq 1$ and $Pr[X \leq x] = 0$, for $x < 1$?

10. What is the Covariance of X and X^3 where X is a uniformly distributed variable on the interval $[0,1]$. ($X \sim U[0,1]$)

11. (Conditional/Wald) In a certain casino game, you either gain one dollar or lose five dollars with equal probability. You roll a fair 6-sided die and play the game that number of times. What is the expected amount of money that you lose?

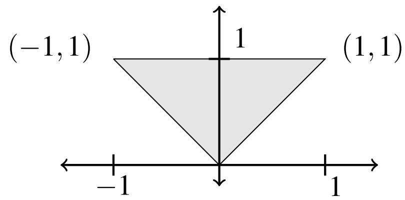
12. Let $\Phi(z)$ be the CDF of the standard normal distribution, i.e. $\Phi(z) = \int_{-\infty}^{z} (2\pi)^{-1/2} \exp(-x^2/2)\,\mathrm{d}x$. It is known that $\Phi(2) - \Phi(-2) \approx 0.95$. Moreover, the CLT states that when taking n samples from a distribution, that the average, A_n, shifted by its mean and scaled by the standard deviation converges to the standard normal. Assume the CLT holds for n, what is a good upper bound on the probability that A_n is *larger* than the mean of the distribution by 2 standard deviations?

6. Some confidence! 10 points.

You take n samples $X_1, \cdots, X_n$ from an exponentially distributed variable X with known parameter λ, and calculate the average $A_n = \frac{X_1 + \ldots + X_n}{n}$. What value of n do we need to ensure that A_n is within 0.1μ of $\mu = E[X]$ with 95% probability? (You may use Chebyshev or the CLT.)

7. Probability Again: continuous similar to discete. Breathe, just breathe. 12/12/12 points

1. (Continuous Joint distribution: conceptual.)
   Consider that a point is chosen uniformly in the area corresponding to the figure below.



Let X be the x-coordinate of the chosen point and Y be the y-coordinate.

(a) What is $Pr[Y > X]$?

(b) What is $E[X]$?

(c) What is $E[Y]$?

(d) What is $E[Y|X]$? (Describe a real valued function whose domain is $[-1,1]$.)

(e) What is $L[Y|X]$?

2. You pick a real number from the range $[0,1]$ using the uniform distribution. Then Alvin independently picks a real number uniformly at random from the range $[0,2]$.

   (a) What is the probability that your two numbers differ by no more than 1?

   (b) You pick a real number from the range $[0,1]$ this time with pdf $f(x) = 2x$. Then Alvin picks a real number uniformly at random from the range $[0,2]$. What is the probability that your two numbers differ by no more than 1?

3. Darts (again.) An ok player hits a circular dartboard of radius 1 centered at $(0,0)$, with uniform probability over the area of the dartboard, a good player has distance from the center that is uniform over $[0,1]$. Say we pick a player who is good with probability 1/2 and ok with probability 1/2 and she throws a dart.

   (a) What is the pdf for the random variable, X, corresponding to the distance from the center?

   (b) If the dart lands at the point $(\frac{1}{2\sqrt{2}}, \frac{1}{2\sqrt{2}})$, what is the probability that the player is good.

   (c) If that player from part (b) throws another dart, what is the expected distance from the center for this dart.

8. It's all about that Chain. True/False Part 1 is 15 points. Part 2 is 12 points.
No justification for True/False.

1. True/False.
   (a) (True/False:) A finite Markov chain with a transition matrix where every column sums to 1 is irreducible.

   ◯ True

   ◯ False

   (b) (True/False:) A finite Markov chain which is not irreducible does not converge in distribution.

   ◯ True

   ◯ False

   (c) (True/False:) If the fraction of time spent in state i is q, and $P(i, j) = 0.3$, then the fraction of time spent in state j is at least $0.3q$.

   ◯ True

   ◯ False

   (d) (True/False:) If the fraction of time spent in state i is q and $P(j,i) = 0.3$, then the fraction of time spent in state j is at most $q/0.3$.

   ◯ True

   ◯ False

   (e) (True/False:) A two-state aperiodic Markov chain has a self-loop.

   ◯ True

   ◯ False

2. Let n be a positive integer. Take $X_0 = n$, and for each $k \geq 0$, let X_{k+1} have the discrete uniform distribution from 0 to X_k, inclusive. If $X_k = 0$, then it follows that $X_{k+1} = 0$.

   (a) The sequence (X_k) is a Markov chain. Describe its state space and its transition probabilities (a diagram would suffice).

   (b) Compute the expected number of steps until the sequence (X_k) first reaches 0. Partial credit will be awarded for a correct linear system of equations. Solve the system for full credit.