CS 70 Spring 2019 — Discrete Mathematics and Probability Theory — Ayazifar and Rao — Final Exam

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

SIGN Your Name: ________________________

PRINT Your Student ID: ________________________

PRINT Your Exam Room: ________________________

Name of the person sitting to your left: ________________________

Name of the person sitting to your right: ________________________

- After the exam starts, please *write your student ID (or name) on every odd page* (we will remove the staple when scanning your exam).
- We will not grade anything outside of the space provided for a problem.
- The questions **vary in difficulty**, so if you get stuck on any question, it might help to leave it and try another one.
- If there is a box provided, put your answer in it. If not, use the space provided for your proof or argument.
- You may consult only *three sides of notes*. Apart from that, you may not look at books, notes, etc. Calculators, phones, computers, and other electronic devices are NOT permitted.
- There are **21** single sided pages including the cover sheet on the exam. Notify a proctor immediately if a page is missing.
- **You may, without proof, use theorems and lemmas that were proven in the notes and/or in lecture.**
- **You have 170 minutes: there are 12 questions (with 66 parts) on this exam worth a total of 222 points.**
- Graphs are simple and undirected unless we say otherwise.

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

1. TRUE or FALSE? 2 points each part, 26 total.

For each of the questions below, answer TRUE or FALSE. No need to justify answer.

Please fill in the appropriate bubble!

1. $(P \implies (R \wedge \neg R)) \implies \neg P$

   ◯ True

   ◯ False

2. Let $\mathbb{Z}$ be the integers, and $P(i)$ be a predicate on integers, $(P(0) \wedge ((\exists i \in \mathbb{Z})\ P(i) \wedge P(i+1)) \implies (\forall i \in \mathbb{Z})\ ((i \geq 0) \implies P(i)))$

   ◯ True

   ◯ False

3. Let $\mathbb{R}$ be the real numbers, $(\forall x, y \in \mathbb{R})((x < y) \implies ((\exists z \in \mathbb{R})\ (x < z < y))))$

   ◯ True

   ◯ False

4. Let $\mathbb{Q}$ be the rational numbers, $(\forall x, y \in \mathbb{Q})((x < y) \implies ((\exists z \in \mathbb{Q})\ (x < z < y))))$

   ◯ True

   ◯ False

5. Any stable pairing that is optimal for one man is optimal for all men.

   ◯ True

   ◯ False

6. Any graph with no triangles is two colorable.

   ◯ True

   ◯ False

7. There is a graph with average degree 2 that does not have a cycle.

   ◯ True

   ◯ False

8. The length of any Eulerian tour of a graph is even.

   ◯ True

   ◯ False

9. There is a program that takes a program P and input x and number of steps, s and returns YES if and only if P run on x halts in s steps.

   ◯ True

   ◯ False

10. If one can write a program that solves a problem P using the halting problem as a subroutine then the problem P is undecidable.

◯ True

◯ False

11. There is a bijection between the powerset of rational numbers and the real numbers. (The powerset of set S is the set of all subsets of S.)

◯ True

◯ False

12. If $\Pr[A \cup B] = \Pr[A] + \Pr[B]$ then A and B are independent.

◯ True

◯ False

13. Given n balls being thrown into n bins, the event "the first bin is empty" and the event "the second bin is empty" are independent.

◯ True

◯ False

SID:

2. Quick proof. 7 points.

Prove that $\sum_{i=1}^{n} \frac{1}{i(i+1)} = \frac{n}{n+1}$.

3. Short Answer: Discrete Math. 3 points each part, 48 points total.

1. What is the number of faces in a planar drawing of a planar graph with n vertices where every vertex has degree 3?

2. Given a graph $G = (V, E)$ with k connected components, what is the minimum number of edges one needs to add to ensure that the resulting graph is connected?

3. The hypercube graph for dimension d has an Eulerian tour when $d =$ ____ $\pmod 2$.

4. For a dimension d hypercube with a Eulerian tour of length L and a Hamiltonian cycle of length ℓ, what is L/ℓ?

5. What is the minimum number of odd degree vertices in a connected acyclic graph?

6. What is $2^{10} \pmod{11}$?

7. For distinct primes p, q, r and $N = pqr$, how many elements of $\{0, 1, \ldots, N-1\}$ are relatively prime to N?

8. Consider N and the set $S = \{x \in \{0, \ldots N-1\} : gcd(x,N) = 1\}$ where $k = |S|$.
For $a \in S$, we define $T = \{ax \pmod N) : x \in S\}$. What is $|T|$? Answer may include N and k.

9. For a prime p, what is a positive integer x that guarantees $a^x = 1 \pmod{p^2}$ for all a relatively prime to p? Answer may include p.

10. For distinct primes p,q,r, what is $a^{(p-1)(q-1)(r-1)} \pmod{pqr}$, where a is relatively prime to pqr. Answer may include p,q,r.

11. Jonathan wants to tell Emaan how many chicken nuggets he ate today, which we will call c. He doesn't want the world to know, so he encrypts it with Emaan's public key (N,e), which yields the ciphertext x. Jerry intercepts the message, and wants to make it look like Jonathan actually ate 5 times as many chicken nuggets. What message should she send to Emaan? Answer may include x, N, and e. You may not include c.

For the following parts consider two non-zero polynomials $P(x)$ and $Q(x)$ of degree d over $GF(p)$ (modulo p), with r_p roots and r_q roots respectively.

12. What is the maximum number of roots for the polynomial $P(x)Q(x)$? Answer may include d, r_p, and r_q. (Your answer should be achievable for any valid d, r_p and r_q.)

13. What is the minimum number of roots for the polynomial $P(x)Q(x)$? Answer may include d, r_p, and r_q.

14. Let $S = \{(x_1, y_1), \ldots, (x_{n+2k}, y_{n+2k})\}$ be a set of $n+2k$ points where the x_i are distinct. If $P(x)$ and $Q(x)$ are polynomials where $P(x_i) = y_i$ for at least $n+k$ points in S and $Q(x_j) = y_j$ for at least $n+k$ points in S, what is the minimum number of points that $P(x)$ and $Q(x)$ must agree on in S? Answer may include n and k.

15. Working over $GF(5)$, describe a degree *exactly* 2 polynomial where $P(1) = 1$ and $P(2) = 2$.

16. Let $P(x)$ be a degree $d = n-1$ polynomial over $GF(p)$ (p is prime) that contains all but $\ell \leq k$ of $n+2k$ points which are given. In this situation, recall that the Berlekamp-Welsh procedure can reconstruct $P(x)$ by assuming the existence of an error polynomial $E(x)$ of degree exactly k and leading coefficient of 1, and a polynomial $Q(x) = P(x)E(x)$. How many possible pairs of $Q(x)$ and $E(x)$ are consistent with the Berlekamp-Welsh procedure? Answer may include ℓ, k, d, n, and p.

4. Short Answer: Counting. 3 points each. 12 points total.

1. What is the number of ways to place n distinguishable balls into k distinguishable bins?

2. What is the number of ways to place n distinguishable balls into k distinguishable bins where no two balls are placed in the same bin? You may assume that $n \leq k$.

3. What is the number of ways to divide d dollar bills among p people? Assume dollar bills are indistinguishable and people are distinguishable.

4. How many $(x_1, \ldots, x_k, y_1, y_2, \ldots, y_k)$ are there such that all x_i, y_i are non-negative integers, $\sum_{i=1}^{k} x_i = n$, and $y_i \leq x_i$ for $1 \leq i \leq k$? Answer may *not* include any summations.

SID:

5. Short Answer: Probability. 3 points each part, 18 points total.

1. Given two tosses of a fair coin, what is Pr[heads on the second coin|at least one heads in the two tosses].

2. Consider two events, A and B with $\Pr[A \cup B] = \frac{3}{4}$, and $\Pr[A] = \frac{1}{2}$, and $\Pr[B] = \frac{4}{5}$, what is $\Pr[A \cap B]$?

3. Alice and Bob both try to a climb a rope. Alice and Bob will get to the top of the rope with probability $1/3$ and $1/4$ respectively. Given that exactly one person got to the top, what is the probability that the person is Alice?

4. Given $X \sim \text{Geom}(p)$, what is $\Pr[X = i | X > j]$? Assume $i > j$.

5. Given independent $X, Y \sim \text{Bin}(n, p)$, what is $\Pr[X + Y = i]$?

6. Consider a random variable X where $E[X^4] = 5$, give as good upper bound on $\Pr[X \geq 5]$ as you can.

6. Concepts through balls in bins. 3 points each part, 18 points total.

Consider throwing n balls into n bins uniformly at random. Let X be the number of balls in the first bin.

1. What is the expected value of X?

2. Use Markov's inequality to give an upper bound on $\Pr[X \geq k]$.

3. What is the variance of X?

4. Use Chebyshev's inequality to give an upper bound on $\Pr[X \geq k]$.

5. Now let Y be the number of balls in the second bin. What the joint distribution of X, Y, i.e., what is $\Pr[X = i, Y = j]$?

6. What is $\Pr[X = i | Y = j]$?

7. Lots of chicken nuggets. 5 points each part, 15 points total.

We will model the number of customers going into Emaan's and Jonathan's favorite McDonalds within an hour as a random Poisson variable, i.e., $X \sim \text{Poisson}(\lambda)$.

1. Given that $\lambda = 5$, what is the probability that 5 people come in during the hour that Emaan and Jonathan are eating chicken nuggets?

2. If λ is unknown but is definitely at most 10, how many hours do Emaan and Jonathan need to be at McDonalds to be able to construct a 95% confidence interval for λ that is of width 2. (You should use Chebyshev's inequality here. Recall for $X \sim \text{Poisson}(\lambda)$ that $Var(X) = \lambda$)

3. Solve the previous problem but now assume you can use the Central Limit Theorem. (*Hint:* You may want to use the table in the back of the exam).

8. Not so dense density functions. 5 points each (sub)part, 15 points total.

1. Consider a continuous random variable whose probability density function is cx^{-3} for $x \geq 1$, and 0 outside this range. What is c?

2. Consider random variables X, Y with joint density function $f(x,y) = cxy$ for $x, y \in [0,1]$, and 0 outside that range.
   (a) What is c?

   (b) What is $\Pr[|X-Y| \leq 1/2]$?

9. This is Absolutely Not Normal! 6 points each part, 12 points total.

Consider a standard Gaussian random variable Z whose PDF is

$$\forall z \in \mathbb{R}, \quad f_Z(z) = \frac{1}{\sqrt{2\pi}} e^{-z^2/2}.$$

Define another random variable X such that $X = |Z|$.

(a) Determine a reasonably simple expression for $f_X(x)$, the PDF of X. It may be helpful to draw a plot. Place your final expression in the box below.

(b) Determine a reasonably simple expression for $E(X)$, the mean of X. Place your final answer in the box below.

10. Joint Distributions with Kyle and Lara. 6 points each part, 18 points total.

Kyle and Lara arrive in Saint Petersburg randomly and independently, on any one of the first five (5) days of May 2019. Let K be the day that Kyle arrives, and let L be the day that Lara arrives. (Note that K and L will both be in $\{1,2,3,4,5\}$).
Whoever arrives first must wait for the other to arrive before going on any kind of excursion in the city.

(a) Determine $E[|K-L|]$, the expected wait time in days.

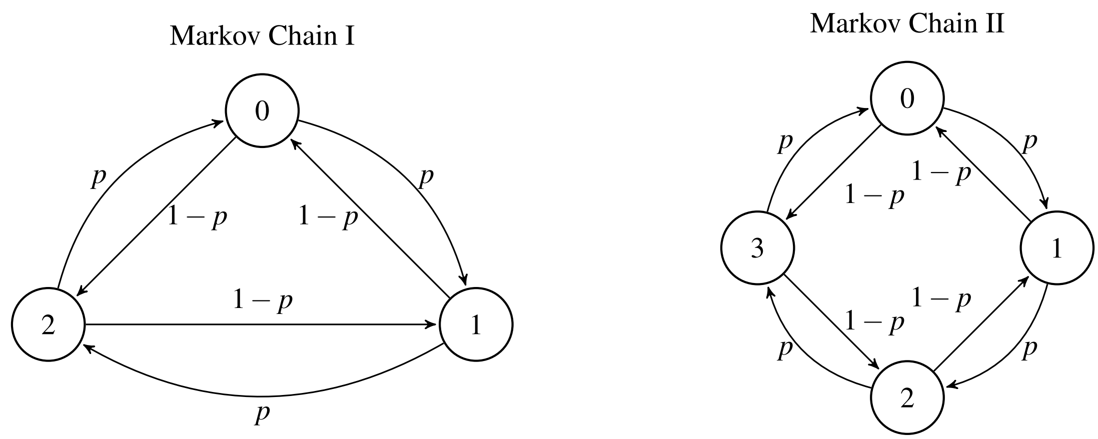
(b) Given that Kyle arrives *at least a day later* than Lara:

(i) Determine the conditional probability mass function for Kyle's arrival day, $p_{K|(K>L)}(k)$

(ii) Provide a well-labeled plot of $p_{K|(K>L)}(k)$.

11. Markov Chains 3 points for each part, 18 points total.

Consider the two Markov Chains represented by the following state transition diagrams.



(a) For Markov Chain I:

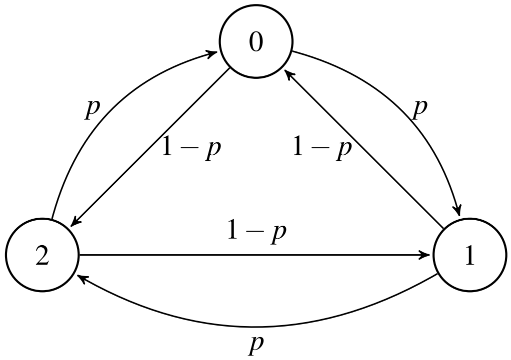
(i) Do the n-step transition probabilities—defined by $r_{ij}(n) = \Pr\left(X_n = j \middle| X_0 = i\right)$ —converge as $n \to \infty$?

○ Converges

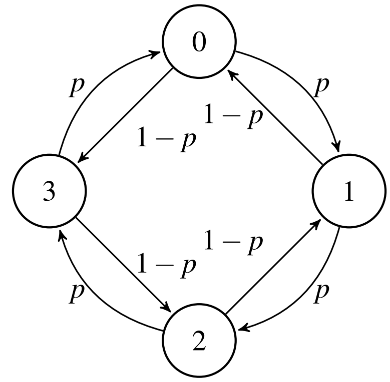
○ Does not converge

(ii) If so, determine the corresponding limit to which each transition probability converges, and explain whether and why the limit depends on the initial state (i.e., the state at which the walker was stationed initially). If you assert that the transitional probabilities do not converge, explain why no limit exists.

Markov Chain I



Markov Chain II



(b) For Markov Chain II:

(i) Do the n-step transition probabilities—defined by $r_{ij}(n) = \Pr\left(X_n = j \middle| X_0 = i\right)$ —converge as $n \to \infty$?

◯ Converges

◯ Does not converge

(ii) If so, determine the corresponding limit to which each transition probability converges, and explain whether and why the limit depends on the initial state (i.e., the state at which the walker was stationed initially). If you assert that the transitional probabilities do not converge, explain why no limit exists.

(c) (Points) Consider Markov Chain I above. Determine t_0^*, the *mean recurrence time* for State 0.

The mean recurrence time for a state s is the expected number of steps up to the first return to state s, starting from state s. In other words,

$$t_s^* = E\left[\min(n \geq 1 \text{ such that } X_n = s) \mid X_0 = s\right].$$

In particular,

$$t_s^* = 1 + \sum_i p_{si} t_i,$$

where t_i, which denotes the *mean first passage time* from State i to State s, is given by

$$t_i = E\left[\min(n \geq 0 \text{ such that } X_n = s) \mid X_0 = i\right].$$

(i) Write the system of equations that you would solve in the box below. Use t_0^*, t_1, t_2, and p.

(ii) Set p to $1/2$ and write your final answer for the value of t_0^* in the box below.

12. Derive Magic from a Uniform PDF. 5 points per part. 15 points.

A random-number generator produces sample values of a continuous random variable U that is uniformly distributed between 0 and 1.

In this problem you'll explore a method that uses the generated values of U to produce another random variable X that follows a desired probability law distinct from the uniform.

(a) Let $g : \mathbb{R} \to [0,1]$ be a function that satisfies all the properties of a CDF. Furthermore, assume that g is invertible, i.e. for every $y \in (0,1)$ there exists a unique $x \in \mathbb{R}$ such that $g(x) = y$.
Let random variable X be given by $X = g^{-1}(U)$, where g^{-1} denotes the inverse of g. Prove that the CDF of X is $F_X(x) = g(x)$.

(b) A random variable X follows a *double-exponential* PDF given by

$$\forall x \in \mathbb{R}, \qquad f_X(x) = \frac{\lambda}{2} e^{-\lambda|x|},$$

where $\lambda > 0$ is a fixed parameter.

Using the random-number generator described above (which samples U), we want to generate sample values of X. Derive the explicit function that expresses X in terms of U. In other words, determine the expression on the right-hand side of

$$X = g^{-1}(U).$$

To do this, you must first determine the function g. From part (a) you know that $g(x) = F_X(x)$, so you must first determine $F_X(x)$. It might help you to sketch the PDF of X first. Place your expression for g^{-1} in the box below.

Introduction to Probability, 2nd Ed, by D. Bertsekas and J. Tsitsiklis, Athena Scientific, 2008

	.00	.01	.02	.03	.04	.05	.06	.07	.08	.09
0.0	.5000	.5040	.5080	.5120	.5160	.5199	.5239	.5279	.5319	.5359
0.1	.5398	.5438	.5478	.5517	.5557	.5596	.5636	.5675	.5714	.5753
0.2	.5793	.5832	.5871	.5910	.5948	.5987	.6026	.6064	.6103	.6141
0.3	.6179	.6217	.6255	.6293	.6331	.6368	.6406	.6443	.6480	.6517
0.4	.6554	.6591	.6628	.6664	.6700	.6736	.6772	.6808	.6844	.6879
0.5	.6915	.6950	.6985	.7019	.7054	.7088	.7123	.7157	.7190	.7224
0.6	.7257	.7291	.7324	.7357	.7389	.7422	.7454	.7486	.7517	.7549
0.7	.7580	.7611	.7642	.7673	.7704	.7734	.7764	.7794	.7823	.7852
0.8	.7881	.7910	.7939	.7967	.7995	.8023	.8051	.8078	.8106	.8133
0.9	.8159	.8186	.8212	.8238	.8264	.8289	.8315	.8340	.8365	.8389
1.0	.8413	.8438	.8461	.8485	.8508	.8531	.8554	.8577	.8599	.8621
1.1	.8643	.8665	.8686	.8708	.8729	.8749	.8770	.8790	.8810	.8830
1.2	.8849	.8869	.8888	.8907	.8925	.8944	.8962	.8980	.8997	.9015
1.3	.9032	.9049	.9066	.9082	.9099	.9115	.9131	.9147	.9162	.9177
1.4	.9192	.9207	.9222	.9236	.9251	.9265	.9279	.9292	.9306	.9319
1.5	.9332	.9345	.9357	.9370	.9382	.9394	.9406	.9418	.9429	.9441
1.6	.9452	.9463	.9474	.9484	.9495	.9505	.9515	.9525	.9535	.9545
1.7	.9554	.9564	.9573	.9582	.9591	.9599	.9608	.9616	.9625	.9633
1.8	.9641	.9649	.9656	.9664	.9671	.9678	.9686	.9693	.9699	.9706
1.9	.9713	.9719	.9726	.9732	.9738	.9744	.9750	.9756	.9761	.9767
2.0	.9772	.9778	.9783	.9788	.9793	.9798	.9803	.9808	.9812	.9817
2.1	.9821	.9826	.9830	.9834	.9838	.9842	.9846	.9850	.9854	.9857
2.2	.9861	.9864	.9868	.9871	.9875	.9878	.9881	.9884	.9887	.9890
2.3	.9893	.9896	.9898	.9901	.9904	.9906	.9909	.9911	.9913	.9916
2.4	.9918	.9920	.9922	.9925	.9927	.9929	.9931	.9932	.9934	.9936
2.5	.9938	.9940	.9941	.9943	.9945	.9946	.9948	.9949	.9951	.9952
2.6	.9953	.9955	.9956	.9957	.9959	.9960	.9961	.9962	.9963	.9964
2.7	.9965	.9966	.9967	.9968	.9969	.9970	.9971	.9972	.9973	.9974
2.8	.9974	.9975	.9976	.9977	.9977	.9978	.9979	.9979	.9980	.9981
2.9	.9981	.9982	.9982	.9983	.9984	.9984	.9985	.9985	.9986	.9986
3.0	.9987	.9987	.9987	.9988	.9988	.9989	.9989	.9989	.9990	.9990
3.1	.9990	.9991	.9991	.9991	.9992	.9992	.9992	.9992	.9993	.9993
3.2	.9993	.9993	.9994	.9994	.9994	.9994	.9994	.9995	.9995	.9995
3.3	.9995	.9995	.9995	.9996	.9996	.9996	.9996	.9996	.9996	.9997
3.4	.9997	.9997	.9997	.9997	.9997	.9997	.9997	.9997	.9997	.9998

The standard normal table. The entries in this table provide the numerical values of $\Phi(y) = \mathbf{P}(Y \leq y)$, where Y is a standard normal random variable, for y between 0 and 3.49. For example, to find $\Phi(1.71)$, we look at the row corresponding to 1.7 and the column corresponding to 0.01, so that $\Phi(1.71) = .9564$. When y is negative, the value of $\Phi(y)$ can be found using the formula $\Phi(y) = 1 - \Phi(-y)$.