Final Exam

7:00-10:00pm, 20 December

Your First Name: **Your Last Name:**

SIGN Your Name: **Your SID Number:**

Your Exam Room:

Name of Person Sitting on Your Left:

Name of Person Sitting on Your Right:

Name of Person Sitting in Front of You:

Name of Person Sitting Behind You:

Instructions:

(a) *As soon as the exam starts, please write your student ID in the space provided at the top of every page! (We will remove the staple when scanning your exam.)*

(b) *There are* **7 double-sided** *sheets (14 numbered pages) on the exam. Notify a proctor immediately if a sheet is missing.*

(c) *We will not grade anything outside of the space provided for a question (i.e., either a designated box if it is provided, or otherwise the white space immediately below the question).* **Be sure to write your full answer in the box or space provided!** *Scratch paper is provided on request; however, please bear in mind that nothing you write on scratch paper will be graded!*

(d) *The questions vary in difficulty, so if you get stuck on any question it may help to leave it and return to it later.*

(e) *On questions 1-2, you need only give the answer in the format requested (e.g., True/False, an expression, a statement.) An expression may simply be a number or an expression with a relevant variable in it. For short answer questions, correct, clearly identified answers will receive full credit with no justification. Incorrect answers may receive partial credit.*

(f) *On questions 3-8, you should give arguments, proofs or clear descriptions if requested. If there is a box you must use it for your answer: answers written outside the box may not be graded!*

(g) *You may consult three two-sided "cheat sheets" of notes. Apart from that, you may not look at any other materials. Calculators, phones, computers, and other electronic devices are NOT permitted.*

(h) *You may use, without proof, theorems and lemmas that were proved in the notes and/or in lecture.*

(i) *You have 3 hours: there are 8 questions on this exam worth a total of 185 points.*

[exam starts on next page]

1. **True/False** [*No justification; answer by shading the correct bubble. 2 points per answer unless otherwise stated; total of 39 points. No penalty for incorrect answers.*]

   (a) Let $P(x), Q(x), R(x)$ be propositions involving a variable x belonging to a universe $\mathcal{U}$. Suppose you are asked to prove the following statement: $(\forall x \in \mathcal{U})(P(x) \Rightarrow (\neg Q(x) \vee \neg R(x))$. Which of the following would constitute a valid proof strategy? Answer **YES** or **NO** for each by shading the appropriate bubble.

YES NO

○ ○ Find some $x \in \mathcal{U}$ for which $P(x)$ holds and $Q(x)$ does not hold. *2pts*

○ ○ Show that $P(x)$ is false for all $x \in \mathcal{U}$. *2pts*

○ ○ Show that, for all $x \in \mathcal{U}$ for which $P(x)$ and $Q(x)$ both hold, $R(x)$ does not hold. *2pts*

○ ○ Show that $R(x)$ is false for all $x \in \mathcal{U}$. *2pts*

○ ○ For all $x \in \mathcal{U}$, show that if $Q(x)$ and $R(x)$ both hold, then $P(x)$ does not hold. *2pts*

   (b) Classify each of the following functions $f : \mathbb{Z} \to \mathbb{Z}$ as (i) neither 1-1 nor onto; (ii) 1-1 but not onto; (iii) onto but not 1-1; (iv) both 1-1 and onto (a bijection).

(i) Neither	**(ii)** 1-1	**(iii)** Onto	**(iv)** Both		
○	○	○	○	$f(n) = 3n - 4$	*1pt*
○	○	○	○	$f(n) = -3n^2 + 7$	*1pt*
○	○	○	○	$f(n) = n + 17$	*1pt*
○	○	○	○	$f(n) = \lfloor \frac{n}{2} \rfloor$. [Note: for any rational number r, $\lfloor r \rfloor$ denotes the largest integer less than or equal to r.]	*1pt*
○	○	○	○	$f(n) = n \bmod 1000$	*1pt*

[Q1 continued on next page]

(c) Indicate which of the following statements is **TRUE** or **FALSE** by shading the appropriate bubble.

TRUE FALSE

○ ○ A stable marriage instance has a *unique* stable pairing if and only if the male-optimal pairing is the same as the female-optimal pairing. *2pts*

○ ○ In a stable marriage instance, if every man has a different favorite woman, and every woman has a different favorite man, then there is a *unique* stable pairing. *2pts*

○ ○ There exists a tree with 7 vertices whose degrees are respectively $(1, 1, 1, 2, 2, 3, 4)$. *2pts*

○ ○ In any simple, undirected graph G with at least two vertices, there must be at least two vertices with the same degree. *2pts*

○ ○ If (N, e) is a valid RSA public key with private key d, then (N, d) is also a valid public key with private key e. *2pts*

○ ○ Let A be an event with $\mathbb{P}[A] = 1$ and let B be any other event. Then, A and B are independent. *2pts*

○ ○ There exist random variables X, Y with $\text{Cov}(X, Y) > 0$ and $\text{Var}[X + Y] < \text{Var}[X] + \text{Var}[Y]$. *2pts*

○ ○ For some $0 < p < 1$, let W_1 and W_2 be independent Geometric(p) random variables. Then, $\mathbb{P}[W_1 + W_2 = n] = \binom{n}{2} p^2 (1-p)^{n-2}$ for all integers $n \geq 2$. *2pts*

○ ○ Suppose $X \sim \text{Exp}(\lambda)$ for arbitrary $\lambda > 0$. Then, for all $t \in \mathbb{R}^+$, $\mathbb{P}[X > t] > \mathbb{P}[X > 3t \mid X > t]$. *2pts*

○ ○ For a continuous random variable $X \sim \text{Uniform}(0, 1)$, $\mathbb{P}[X \in S] = 0$ for every countable subset S of the unit interval $(0, 1)$. *2pts*

○ ○ Let X be a continuous random variable with p.d.f. $f(x)$. Then, for all intervals $(a, b) \subseteq \mathbb{R}$, $\mathbb{P}[X \notin (a, b)] = \int_a^b [1 - f(x)] dx$. *2pts*

○ ○ For X a random variable with finite mean $\mathbb{E}[X]$, and for all constants a and $\varepsilon > 0$, the generalized Markov inequality implies $\mathbb{P}[|X - a| \geq \varepsilon] \leq \frac{\text{Var}[X] + (\mathbb{E}[X] - a)^2}{\varepsilon^2}$. *2pts*

[exam continued on next page]

2. Short Answers [*Answer is a single number or expression; write it in the box provided; no justification necessary. 3 points per answer unless otherwise stated; total of 53 points. No penalty for incorrect answers.*]

(a) **Note: The next four questions all concern the following equation in the integer variable n:**

$$133^5 + 110^5 + 84^5 + 27^5 = n^5.$$

(i) What is the value of n mod 2? *2pts*

(ii) What is the value of n mod 3? *2pts*

(iii) What is the value of n mod 5? [Hint: Use Fermat's Little Theorem.] *2pts*

(iv) Assuming that n exists and is less than 170, what is n? *2pts*

(b) What is the inverse of 7 mod 60? [Your answer should be an integer in $\{0, 1, \ldots, 59\}$.] *3pts*

(c) A dial on a piece of equipment has a circular scale with integer markings $\{0, 1, \ldots, 19\}$ arranged clockwise in increasing order. Whenever it detects an event, the dial jumps a distance of 7 clockwise on the scale. If it starts at position 0, after how many jumps will the dial first reach position 5 on the scale? *3pts*

(d) Polly has chosen a degree-13 polynomial $P(x)$ over $GF(19)$, but has forgotten one of its coefficients. Fortunately, however, she did write down the value of $P(x)$ at a few points $x > 0$. How many of these values does she need in order to reconstruct the missing coefficient? *3pts*

[Q2 continued on next page]

(e) Alice wants to send a message to Bob over an expensive, noisy channel, which may corrupt up to 10% of the packets sent. If Alice's budget allows her to send only 100 packets in total, and she uses the Berlekamp-Welch scheme, how many message packets can she send? *3pts*

(f) Consider a 9×9 regular grid consisting of the vertices (i, j), where $i, j \in \{0, 1, \ldots, 9\}$. Your goal is to move from the $(0, 0)$ corner of the grid to the $(9, 9)$ corner while obeying the following rule: from any given position (i, j), you are allowed to move to either $(i, j + 1)$ or $(i + 1, j)$, provided that you stay inside the grid. **For the following two questions, leave your answers in terms of binomial coefficients.**

(i) How many paths from $(0, 0)$ to $(4, 5)$ are there? [Hint: Note that all of these paths are of length 9.] *3pts*

(ii) How many paths from $(0, 0)$ to $(9, 9)$ pass through $(3, 3)$ or $(6, 6)$? *3pts*

(g) For $0 < p < 1$, let $W_1, W_2, \ldots, W_n$ be i.i.d. Geometric(p) random variables and define $S_n := W_1 + \cdots + W_n$.

(i) Let m be a positive integer $\geq n$. For how many different configurations $(a_1, a_2, \ldots, a_n)$ is the conditional probability $\mathbb{P}[W_1 = a_1, \ldots, W_n = a_n \mid S_n = m]$ non-zero? *3pts*

(ii) Find $\mathbb{P}[W_1 = a_1, W_2 = a_2 \mid S_2 = m]$ for (a_1, a_2) such that $a_1 + a_2 = m \geq 2$. *3pts*

(h) For a continuous random variable $X \sim$ Uniform(0,2), find $\mathbb{E}[X], \mathbb{E}[X^2]$, and $\mathrm{Var}[X]$. *3pts*

$\mathbb{E}[X] = \boxed{}$, $\mathbb{E}[X^2] = \boxed{}$, $\mathrm{Var}[X] = \boxed{}$.

[Q2 continued on next page]

(i) Suppose $X \sim \text{Normal}(2, 2)$ and $Y \sim \text{Normal}(0, 1)$ are independent random variables, and define $Z = X - 2Y - 3$. Find $\mathbb{E}[Z]$ and $\text{Var}[Z]$. *3pts*

$$\mathbb{E}[Z] = \boxed{\quad}, \qquad \text{Var}[Z] = \boxed{\quad}.$$

(j) Let X be a continuous random variable with the following probability density function (p.d.f.): *3pts*

$$f(x) = \begin{cases} 0, & x < 1, \\ e^{1-x}, & x \geq 1. \end{cases}$$

Find the cumulative distribution function (c.d.f.) F of X.

$$F(x) = \boxed{\qquad}$$

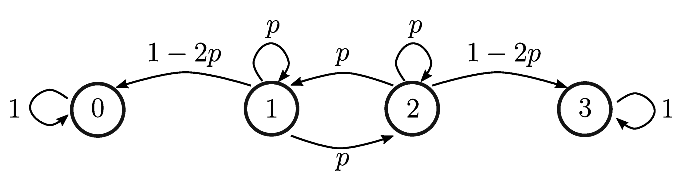
(k) Let $X_1, X_2, X_3, \ldots$ be a sequence of i.i.d. random variables and define $S_n = X_1 + \cdots + X_n$. If $\mathbb{P}[X_i = +1] = \frac{3}{4}$ and $\mathbb{P}[X_i = -1] = \frac{1}{4}$ for $\forall i \in \mathbb{Z}^+$, what is $\lim_{n\to\infty} \mathbb{P}[2S_n < (1 + 10^{-100})n]$? *3pts*

$\boxed{\quad}$

(l) Let $X_1, \ldots, X_n$ be i.i.d. random variables and let F denote their c.d.f. Find $\mathbb{P}[\min\{X_1, \ldots, X_n\} \leq a]$ in terms of F. *3pts*

$\boxed{\qquad}$

(m) Consider a 4-state Markov Chain $\{X_n, n \in \mathbb{N}\}$ with the following allowed transitions, where $0 < p < \frac{1}{2}$:



(i) Find $\mathbb{P}[X_3 = 1 \mid X_0 = 1]$. *3pts*

$\boxed{\quad}$

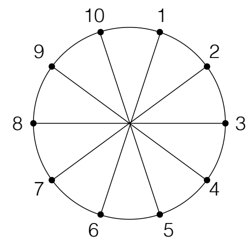
(ii) Find $\mathbb{E}[\text{Time to hit either state 0 or state 3} \mid X_0 = 1]$. *3pts*

$\boxed{\quad}$

[exam continued on next page]

3. Möbius Ladders [*Total of 15 points.*]

Consider the family of graphs G_n ($n \geq 2$) known as *Möbius ladders*. G_n has $2n$ vertices arranged in a single cycle, with an additional edge for each vertex connecting it to the "opposite" vertex on the cycle. The figure below shows the graph G_5. [Note: the point in the center where edges cross is *not* a vertex!]



In parts (a)–(c) below, indicate whether the claimed property holds for ALL values of n, for no (NONE) values of n, only for EVEN values of n, or only for ODD values of n, by shading the appropriate bubble.

	ALL	NONE	EVEN	ODD	
(a) For which values of n (if any) does G_n have an Eulerian tour?	◯	◯	◯	◯	*2pts*
(b) For which values of n (if any) does G_n have a Hamiltonian cycle?	◯	◯	◯	◯	*2pts*
(c) For which values of n (if any) is G_n bipartite?	◯	◯	◯	◯	*2pts*

In parts (d)–(f), you may use without proof results from class, provided you state them clearly.

(d) Is G_2 planar? Shade the correct bubble and **justify your answer.** ◯ Yes ◯ No *3pts*

(e) Is G_3 planar? Shade the correct bubble and **justify your answer.** ◯ Yes ◯ No *3pts*

(f) For all $n > 3$, show that G_n is non-planar. *3pts*

[exam continued on next page]

4. An Inductive Proof of Fermat's Little Theorem [*All parts to be justified. Total of 10 points.*]

Recall Fermat's Little Theorem (FLT): for any prime p, and all $a \in \{1, \dots, p-1\}$, we have $a^{p-1} \equiv 1 \pmod{p}$. In class we gave a proof of FLT using a bijection between integers mod p. In this problem we'll look at a different, inductive proof based on the binomial theorem, which says that

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1. \qquad (*)$$

(a) Fix an arbitrary prime p. We will actually prove the following statement by induction. *2pts*

Claim: *For all natural numbers a, $a^p \equiv a \pmod{p}$.*

Explain why this Claim implies FLT.

(b) For any prime p, prove that p divides every binomial coefficient $\binom{p}{k}$ for $1 \le k \le p-1$. *3pts*

(c) Prove the Claim in part (a) by induction on a, using the binomial theorem $(*)$ and part (b) for the inductive step. *5pts*

[exam continued on next page]

5. Testing Equality of Polynomials [*All parts to be justified unless stated otherwise. Total of 14 points.*]

Let $P(x), Q(x)$ be polynomials of degree at most d over $GF(q)$, where $d \leq q/2$. We do not know the coefficients of P or Q, but instead we are given a black box for each of them that, when given as input a point $x \in GF(q)$, outputs the value of $P(x)$ (respectively, $Q(x)$).

We want to use these black boxes to test whether $P = Q$ (i.e., whether they are the same polynomial).

(a) If $P \neq Q$, what is the maximum possible number of points $x \in GF(q)$ for which $P(x) = Q(x)$? *2pts*

Write your answer in the box; no justification required.

(b) Explain how you would use the black boxes to test whether $P = Q$, and specify how many evaluations of each black box you would need. **Justify your answer.** *4pts*

(c) Suppose now that you are given a random number generator that outputs independent uniform samples from $\{0, 1, \ldots, q-1\}$. Explain how to use the generator and just *one* evaluation of each black box to design a randomized test with the following behavior: *4pts*

(i) if $P = Q$ then the test always outputs "same";

(ii) if $P \neq Q$ then the test outputs "not the same" with probability at least $1/2$.

Justify your answer. [Hint: Use the fact that $d \leq q/2$.]

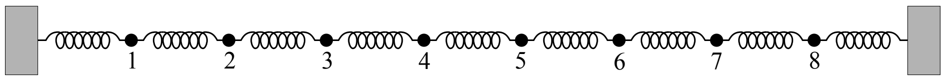
[Q5 continued on next page]

(d) How could you increase the success probability in case (ii) of part (c) to $1 - 2^{-t}$ for any desired positive integer t? **Justify your answer.** [Note: You may make additional uses of the generator and black boxes.] *4pts*

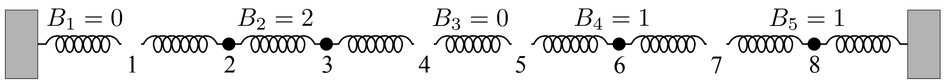
[exam continued on next page]

6. Sampling without Replacement [*Write your answer in the box provided. Total of 16 points.*]

Suppose the Physics 7A class is doing an experiment involving n beads connected by springs in a linear chain, as illustrated below ($n = 8$ in the example). The beads are labeled $1, \dots, n$.



The instructor brings a well-shuffled deck of n cards numbered $1, \dots, n$, and draws $k < n$ cards from the deck *without replacement*. She then removes the beads corresponding to the numbers drawn, thereby producing $k + 1$ connected components of bead-spring chains. Let B_i denote the number of beads in connected component i. For example, if $k = 4$ and the set of numbers drawn are $\{1, 4, 5, 7\}$, then the resulting configuration with 5 connected components is:



(**NOTE:** Whenever possible, express your answers in terms of binomial coefficients.)

(a) Are $B_1, \dots, B_{k+1}$ independent random variables? Shade the correct bubble. ◯ Yes ◯ No *2pts*

(b) How many distinct configurations $(B_1, \dots, B_{k+1})$ are possible? No justification required. *3pts*

(c) For $i \in \{1, \dots, k+1\}$, what is the range of B_i? No justification required. *2pts*

(d) For $i \in \{1, \dots, k+1\}$, find $\mathbb{P}[B_i = b]$, where b is in the range found in part (c). Write your final answer in the box below, **and justify your answer in the space provided**. *5pts*

(e) For $i \in \{1, \dots, k+1\}$, find $\mathbb{E}[B_i]$ in terms of n and k. Your answer should not involve any summation signs. No justification required. [Hint: Do not try to solve this problem using the formula for $\mathbb{P}[B_i = b]$ found in part (d). There is a way to find $\mathbb{E}[B_i]$ without explicitly using $\mathbb{P}[B_i = b]$.] *4pts*

[exam continued on next page]

7. Random Hash Function [*Write your answer in the box provided. Total of 18 points.*]

Suppose a hash function is defined by mapping m keys independently and uniformly at random to the n bins of a hash table. Two different keys may get mapped to the same bin, and when that happens we say that a "collision" has occurred in that bin.

(a) Let C_1 denote the event that there is at least one collision in bin 1. Find $\mathbb{P}[C_1]$. No justification required. *4pts*

(b) Let p denote the answer to part (a), and let N denote the number of bins with collisions. Use Markov's Inequality to obtain an upper bound on $\mathbb{P}[N \geq \frac{n}{2}]$ in terms of p. No justification required. *3pts*

(c) Let K_i denote the number of keys assigned to bin i, where $i = 1, \ldots, n$. Find $\mathrm{Var}[K_i]$. Your answer should not involve any summation sign. No justification required. *3pts*

(d) Let v denote the answer to part (c). Use Chebyshev's Inequality to obtain an upper bound on $\mathbb{P}[K_i \geq \frac{3m}{n}]$ in terms of m, n, and v. Write your final answer in the box below, **and justify your answer in the space provided**. *4pts*

(e) For $k \leq m, n$, find $\mathbb{P}$[Exactly k bins are non-empty] in terms of m, n, k, and $S(a, b)$ for suitable values of a, b, where $S(a, b)$ denotes the number of surjections from $\{1, \ldots, a\}$ to $\{1, \ldots, b\}$. No justification required. [Note: You found a formula for $S(a, b)$ in Homework 8, but you do not need it here.] *4pts*

[exam continued on next page]

8. Competing Poisson Arrival Processes [*Write your answer in the box provided. Total of 20 points.*]

Suppose spam calls arrive at a call center according to a Poisson Arrival Process at rate $\lambda > 0$ per minute, while non-spam calls arrive according to a Poisson Arrival Process at rate 1 per minute, independently of spam calls. In this problem, all times are measured in minutes.

(a) Suppose you reset your timer to 0 exactly at noon and let W denote the waiting time (starting at noon) until either a spam or a non-spam call arrives. What is $\mathbb{P}[W \leq t]$? No justification required. *3pts*

(b) Define W as in part (a) and let E denote the event that exactly 1 call arrives in the time interval $(0, s)$, for $s > t$. Find $\mathbb{P}[W \leq t \mid E]$. Write your final answer in the box below, **and justify your answer in the space provided**. *4pts*

(c) Given that a call arrives, what is the probability that it is a spam call? No justification required. *3pts*

(d) Let p denote the probability found in part (c). Let N denote the number of non-spam calls received before a spam call arrives. For $k \in \mathbb{N}$, find $\mathbb{P}[N = k]$ in terms of p and k. No justification required. *3pts*

[Q8 continued on next page]

(e) For $i \in \mathbb{Z}^+$, let X_i denote the number of non-spam calls received in the time interval $[i-1, i)$ and define $S_n = X_1 + X_2 + \cdots + X_n$. For $k \in \mathbb{N}$, find $\mathbb{P}[S_n = k]$. Your answer should not involve any summation signs. No justification required. *3pts*

(f) Let S_n be defined as in part (e), and let c and ε be some constants. For $\varepsilon < \frac{1}{2}$, what is $\lim_{n\to\infty} \mathbb{P}[S_n < c\,n^{\varepsilon} + n]$? Write your final answer in the box below, **and justify your answer in the space provided**. *4pts*

[End of Exam!]