CS70 Discrete Mathematics and Probability Theory, Fall 2019

Midterm 2

8:00-10:00pm, 14 November

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 **5 double-sided** *sheets (10 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 3-6, 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 one two-sided "cheat sheet" 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 120 minutes: there are 6 questions on this exam worth a total of 140 points.

[exam starts on next page]

1. True/False [*No justification; answer by shading the correct bubble. 2 points per answer; total of 28 points. No penalty for incorrect answers.*]

(a) For each of the following sets, indicate whether it is finite, countably infinite (CTBL INF) or uncountable (UNC) by shading by shading the appropriate bubble.

FINITE	CTBL INF	UNC		
◯	◯	◯	The set $\{\frac{2^i}{3^j} \mid i, j \in \mathbb{N}\}$.	*2pts*
◯	◯	◯	The set of all subsets of the prime numbers.	*2pts*
◯	◯	◯	The set of all finite sets of rational numbers.	*2pts*
◯	◯	◯	The set of real numbers in the interval $[0, 1]$ whose decimal expansion involves only the digits 3 and 5.	*2pts*
◯	◯	◯	The set of finite arithmetic expressions over the integers, using symbols $+, -, \times, \div, (,)$.	*2pts*
◯	◯	◯	The set of all movies with file size at most 4 GB.	*2pts*

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

TRUE	FALSE		
◯	◯	Every infinite set has a countably infinite subset.	*2pts*
◯	◯	There are uncountably many real polynomials of degree 2 that pass through the points $(0, 0)$ and $(1, 1)$.	*2pts*
◯	◯	Let A and B be finite sets. If $f : A \to B$ is a surjection such that $\lvert f^{-1}(\{b\})\rvert \leq m$ for all $b \in B$, where f^{-1} denotes the preimage of f, then $\lvert A\rvert \geq \lvert B\rvert \geq \lvert A\rvert/m$.	*2pts*
◯	◯	For events A and B on the same probability space such that $A \subseteq B$, it is possible to have $\mathbb{P}[A] > \mathbb{P}[B]$.	*2pts*
◯	◯	For any event B, $\mathbb{P}[B] = \sum_{k=1}^{n} \mathbb{P}[B \cap A_k]$ if $A_1, A_2, \ldots, A_n$ are any subsets of the same sample space Ω satisfying $A_1 \cup A_2 \cup \cdots \cup A_n = \Omega$.	*2pts*
◯	◯	For events A, B on the same probability space, if $A \cap B = \varnothing$, then A and B are independent.	*2pts*
◯	◯	Let X and Y be Bernoulli random variables. If $\mathbb{P}[X = 0, Y = 1] = \mathbb{P}[X = 0]\ \mathbb{P}[Y = 1]$, then X and Y are independent.	*2pts*
◯	◯	For all random variables X and Y defined on the same probability space, $\mathbb{E}[XY] \leq \frac{1}{2}(\mathbb{E}[X^2] + \mathbb{E}[Y^2])$.	*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; total of 54 points. No penalty for incorrect answers.*]

(a) Two real polynomials $P(x), Q(x)$ have degrees exactly 3 and 2 respectively. What is the maximum number of points x for which $P(x) = Q(x)$? *3pts*

(b) Two real polynomials $P(x), Q(x)$ have exactly 2 and 3 zeros respectively. What is the maximum possible number of zeros of $P(x)Q(x)$? *3pts*

(c) A polynomial $P(x)$ of degree 2 over $GF(11)$ has zeros at $x = 0$ and $x = 2$, and passes through the point $(1, 1)$. What is P? [All coefficients should be integers in $\{0, \ldots, 10\}$.] *3pts*

$$P(x) = \square\, x^2 + \square\, x + \square$$

(d) Alice uses the Berlekamp-Welch encoding scheme to send Bob a message consisting of three characters, each an integer mod 11, using a degree-2 polynomial $P(x)$ over $GF(11)$ where the message characters are encoded as $P(1), P(2), P(3)$. It is known that up to two characters may be corrupted during transmission. Answer the following questions.

(i) How many points of P in total must be sent to ensure that the message can be reconstructed? *3pts*

(ii) Following the Berlekamp-Welch scheme, Bob computes the error-locator polynomial as $E(x) = x^2 + 7x + 3$. Which of the characters, $P(1), P(2), P(3)$, were corrupted? *3pts*

(iii) Bob also computes the polynomial $Q(x) = x^4 + 7x^3 + 4x^2 + 7x + 3$ (with notation as in the class notes). What was the original message sent by Alice? *3pts*

[Q2 continued on next page]

PLEASE NOTE: In the remaining short problems, express your answers in terms of binomial coefficients and factorials whenever possible.

(e) How many distinct 6-digit numbers can you create by rearranging the numbers $\{1, 3, 5, 7, 7, 9\}$ such that no two consecutive numbers are identical? *3pts*

(f) Suppose you hold 100 stocks for each of five utility companies, including PG&E. You wish to sell a total of 100 stocks while ensuring you sell at least 50 PG&E stocks. In how many different ways can you do this? (Stocks in a given company are indistinguishable.) *3pts*

(g) For $k \leq n$, how many functions from $\{1, \ldots, k\}$ to $\{1, \ldots, n\}$ are **not** injective? *3pts*

(h) What should x be to make the following a valid combinatorial identity? $\sum_{m=k}^{n-k-1} \binom{m}{k}\binom{n-m-1}{k} = \binom{n}{x}$. *3pts*

(i) Consider a biased coin which shows heads with probability $2/3$. Suppose Alice tosses the coin n times and then Bob also tosses it n times. You may assume independence between trials.

(i) For $j, k \in \{0, 1, \ldots, n\}$, let A_j denote the event that Alice gets heads j times, and B_k the event that Bob gets heads k times. Find $\mathbb{P}[A_j \cap B_k]$. *3pts*

(ii) For $m \in \{0, \ldots, 2n\}$, let S_m denote the event of getting heads m times in total when Alice's and Bob's results are combined. Find $\mathbb{P}[S_m]$. (**NOTE**: Your answer should not involve any summation signs.) *3pts*

[Q2 continued on next page]

(j) In the U.S., suppose the proportion of people who have diabetes is $d > 0$, and a fraction $m > 0$ of those people have a particular risk mutation. Also, among those who do **not** have diabetes, a fraction $a > 0$ do **not** have the risk mutation. Suppose a person is selected uniformly at random from the population. Given that the person has the risk mutation, what is the probability that she/he has diabetes? Express your answer in terms of d, m, and a. *3pts*

(k) In a given day, a computer manufacturer produced L laptops each containing 4 memory chips. It turns out that, of the $4L$ chips inserted into the laptops, exactly d chips were defective. Assume that the memory chips were well-shuffled before they went into the laptops, and let X denote the number of defective memory chips in a randomly selected laptop. For $k \in \{0, 1, 2, 3, 4\}$, what is $\mathbb{P}[X = k]$? *3pts*

(l) Suppose a single card is dealt from a well-shuffled standard deck of 52 cards. What is the probability that the card is either a red suit or an ace? *3pts*

(m) Let X be a random variable with $\mathbb{P}[X = -4] = \frac{1}{4}, \mathbb{P}[X = 0] = \frac{1}{4}$, and $\mathbb{P}[X = 4] = \frac{1}{2}$. Find $\mathbb{E}[X]$, $\mathbb{E}[X^2]$ and $\mathrm{Var}[X]$. *3pts*

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

(n) Let X and Y be independent random variables with $\mathrm{Var}[X] = 2$ and $\mathrm{Var}[Y] = 3$. Find $\mathrm{Var}[3X - Y]$. *3pts*

(o) Consider two events A and B on the same probability space and suppose $A \subset B$. Let I_A and I_B denote indicator random variables for events A and B, respectively. Find $\mathrm{Cov}(I_A, I_B)$ in terms of $\mathbb{P}[A]$ and $\mathbb{P}[B]$. *3pts*

[exam continued on next page]

3. Homomorphic Secret Sharing [*Total of 13 points.*]

A group of n students in a charity fundraising group wish to compute the total amount of money they have raised without revealing how much each of them has individually raised. To do this, they enlist the help of $k \geq 2$ administrators at the charity. Under the assumption that individual amounts are natural numbers no larger than \$1,000, the students want to design a scheme with the following properties:

(i) The k administrators can work together to compute the sum of the raised amounts.

(ii) The administrators cannot discover anything about the individual amounts raised by the students (other than what can be deduced from the sum), unless all k of them conspire to do that.

Since the students have recently taken CS70, they come up with the following secret sharing scheme to solve this problem:

Each student i, for $1 \leq i \leq n$, constructs a polynomial p_i over $GF(q)$, for a suitable prime q, so that $p_i(0) = m_i$, the amount that i has raised. The student then sends the value $p_i(j) \pmod q$ to administrator j, for all $1 \leq j \leq k$.

Answer the following questions about this scheme.

(a) What should the degree of the polynomials p_i be? Write your answer in the box; no justification required. *2pts*

(b) How can the administrators compute the total amount of money raised, $\sum_{i=1}^{n} m_i$, without computing the individual amounts m_i? Be sure to specify clearly the computations that the administrators perform. *5pts*

[Q3 continued on next page]

(c) Give a lower bound on the field size q. Write your answer in the box; no justification required. *2pts*

(d) Explain briefly why this scheme is secure in the sense demanded by the students, i.e., why the administrators cannot learn anything about the individual amounts m_i unless all k of them conspire to do so (as specified in property (ii) above). *4pts*

[exam continued on next page]

4. Counting [*Total of 14 points.*]

Alice has n distinct items on her wish list $W = \{1, \ldots, n\}$ and, after getting her first paycheck, she decides to purchase $m \leq n$ items from the list. Suppose items $1, \ldots, k$, where $k < m$ and $k \leq n - m$, are of special interest to her. (**NOTE:** Whenever possible, express your answers in terms of binomial coefficients.)

(a) In how many ways can Alice choose m distinct items from her wish list W? Write your answer in the box; no justification required. *2pts*

(b) If all of items $1, \ldots, k$ must be included, in how many ways can Alice choose m distinct items from W? Write your answer in the box; no justification required. *3pts*

(c) If at least two of items $1, \ldots, k$ must be included, in how many ways can Alice choose m distinct items from W? Write your answer in the box; no justification required. *4pts*

(d) Let A and B denote the answers to parts (a) and (b), respectively. If we let I_i denote the event that item i is included when m distinct items are chosen from W, note that $B = |I_1 \cap \cdots \cap I_k|$. Fill in the blank in the following equation to produce a valid combinatorial identity, **and provide a brief justification below that equation**. Your justification should include a mathematical expression in terms of the I_i's for what the right hand side of the equation is counting. *5pts*

$$A - B = \sum_{j=1}^{k} \boxed{} \binom{n-j}{m}.$$

[exam continued on next page]

5. Balls and Bins [*Total of 14 points.*]

Suppose k balls are thrown one at a time and uniformly at random into n labeled bins. For $i = 1, \ldots, n$, let E_i denote the event that bin i is empty. (**NOTE:** Your answers should not involve any summation signs.)

(a) Find $\mathbb{P}[E_1]$. Write your answer in the box; no justification required. *3pts*

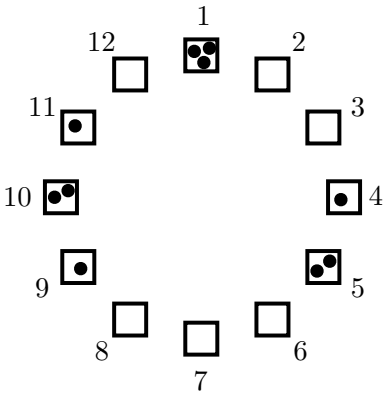
(b) Find $\mathbb{P}[E_1 \cap \overline{E_2}]$. Write your answer in the box; no justification required. *3pts*

NOTE: For the remaining parts, let p and q denote the probabilities found in parts (a) and (b), respectively. Express your answers to parts (c) and (d) in terms of some or all of $n, p,$ and q.

(c) For this part, assume $k \geq n$. Apply the union bound to $\mathbb{P}[\text{at least one bin is empty}]$ and use this result to find a lower bound on $\mathbb{P}[\text{no bin is empty}]$. Write your answer in the box; no justification required. (**Hint**: Express the event "at least one bin is empty" in terms of $E_1, \ldots, E_n$.) *4pts*

$\mathbb{P}[\text{no bin is empty}] \geq$

(d) Suppose the n bins are arranged in a circle. A contiguous set of empty bins flanked by non-empty bins is called a *gap*. Below is an example for $k = 10$ and $n = 12$ with $G = 3$ gaps: $\{2, 3\}$, $\{6, 7, 8\}$, and $\{12\}$. Find the expectation $\mathbb{E}[G]$, where G denotes the number of gaps. Write your final answer in the box provided, **and give a brief justification in the space to the right of the figure**. *4pts*



$\mathbb{E}[G] =$

[exam continued on next page]

6. Random Permutations [*Total of 17 points.*]

Suppose a permutation is sampled uniformly at random from the set of all permutations of $\{1, \ldots, n\}$. Let Ω denote the sample space, and for $i = 1, \ldots, n$, let X_i be random variables such that $X_i(\omega) \in \{1, \ldots, n\}$ denotes the number that i maps to under permutation $\omega \in \Omega$. (**NOTE:** Your answers should not involve any summation signs.)

(a) What is the cardinality of Ω? Write your answer in the box; no justification required. *2pts*

(b) Find $\mathbb{P}[X_1 = 2, X_2 = 1]$. Write your answer in the box; no justification required. *3pts*

(c) Find $\mathbb{P}[X_1 = 2, X_2 \neq 1]$. Write your answer in the box; no justification required. *3pts*

(d) Find $\mathbb{P}[X_1 < X_2 - 1]$. Write your final answer in the box below, **and show your work in the space provided**. (**Hint**: Use the Total Probability Rule. Also, recall from earlier in the course that $\sum_{i=1}^{m} i = \frac{m(m+1)}{2}$.) *5pts*

(e) Let p denote the probability found in part (c), and let D_n denote the number of derangements of $\{1, \ldots, n\}$. Consider the event Δ that the sampled permutation is a derangement. Find $\mathbb{P}[\Delta \mid X_1 = 2, X_2 \neq 1]$ in terms of p, n, and D_k for a suitable k. Write your final answer in the box below; no justification required. *4pts*

[End of Exam!]