CS70 Discrete Mathematics and Probability Theory, Fall 2018

Midterm 2

8:00-10:00pm, 31 October

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 6 **double-sided** *sheets (11 numbered pages) on the exam. Notify a proctor immediately if a sheet is missing. Do* **not** *write any answers on page 12; it will not be scanned.*

(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 must 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.

(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, without proof, use theorems and lemmas that were proven in the notes and/or in lecture.

(i) You have 120 minutes: there are 6 questions on this exam worth a total of 128 points.

[exam starts on next page]

1. True/False [*No justification; answer by shading the correct bubble. 2 points per answer; total of 26 points. No penalty for incorrect answers.*]

(a) Are the following sets countable? Answer **YES** or **NO** for each set by shading the appropriate bubble.

YES	NO		
◯	◯	The set of all functions from $\mathbb{N}$ to $\{0,1\}$.	*2pts*
◯	◯	The set of all *finite* subsets of $\mathbb{N}$.	*2pts*
◯	◯	The set of all *irrational* numbers in the interval $[0,1]$.	*2pts*
◯	◯	The set of all possible Google search terms.	*2pts*
◯	◯	The set of all undirected graphs with a finite number of vertices.	*2pts*

(b) Answer each of the following questions **TRUE** or **FALSE** by shading the appropriate bubble.

TRUE	FALSE		
◯	◯	Any two distinct polynomials, each of degree at most d, can have at most d points in common.	*2pts*
◯	◯	Every function over $\mathrm{GF}(p)$ can be represented as a polynomial of degree at most $p-1$.	*2pts*
◯	◯	There exists a *fixed* computer program P such that no program can decide for any given input x whether P halts on x.	*2pts*
◯	◯	For any two sets A and B, if there exists an injection $f : A \to B$ and a surjection $g : B \to A$, then $\lvert A\rvert = \lvert B\rvert$.	*2pts*
◯	◯	For any two sets A and B, if there exists an injection $f : A \to B$ and an injection $g : B \to A$, then $\lvert A\rvert = \lvert B\rvert$.	*2pts*
◯	◯	For any two finite sets A and B, if there exists a surjection $f : A \to B$ such that $\lvert f^{-1}(x)\rvert = m$ for all $x \in B$, then $\lvert A\rvert = m\lvert B\rvert$. (Here $f^{-1}(x)$ denotes the preimage of x.)	*2pts*
◯	◯	Let A and B be events on the same probability space, and suppose $\mathbb{P}[A] = \frac{3}{4}$ and $\mathbb{P}[B] = \frac{1}{2}$. Then it must be the case that $\frac{1}{4} \le \mathbb{P}[A \cap B] \le \frac{1}{2}$.	*2pts*
◯	◯	Consider a fair coin and a biased coin. One of the two coins is chosen at random and tossed twice. The outcomes of the two tosses are independent.	*2pts*

2. Short Answers [*Answer is a single number or expression;* **write it in the box provided: anything outside the box will not be graded;** *no justification necessary. 3 points per answer; total of 45 points. No penalty for incorrect answers.*]

(a) Suppose that $P(x)$ is a real polynomial of degree 2 that has zeros at $x = 0$ and $x = 2$ and also passes through the point $(1, 1)$. What is the value of $P(3)$? *3pts*

(b) How many polynomials over $\mathrm{GF}(17)$ of degree at most 5 pass through the points $(0, 0)$, $(1, 3)$ and $(2, 5)$? (You may leave your answer as an unevaluated expression.) *3pts*

(c) A message consisting of $n = 3$ packets, each of which is an integer mod 11, is transmitted over an unreliable channel. We use the Berlekamp-Welch encoding scheme (over $\mathrm{GF}(11)$) to protect against $k = 1$ error. The $n + 2k = 5$ packets received are $(1, 1)$, $(2, 2)$, $(3, 0)$, $(4, 2)$, $(5, 8)$. After running the interpolation procedure, we recover the error polynomial $E(x) = x - 1$ and the product polynomial $Q(x) = P(x)E(x) = 2x^3 + 8x^2 + 8x + 4$. Answer the following two questions.

(i) Which one of the five received packets was (possibly) corrupted? *3pts*

(ii) What was the original value of the corrupted packet? *3pts*

(d) Alice and Bob are playing poker using a standard deck of cards. How many ways are there to deal 5 cards each to Alice and Bob (where the order of the cards does not matter)? *3pts*

(e) How many permutations of $\{1, \ldots, n\}$ are there with exactly k fixed points, where $1 \leq k < n$? Express your answer in terms of D_m, the number of derangements of $\{1, \ldots, m\}$. *3pts*

[Q2 continued on next page]

(f) Suppose a random number generator returns a number in $\{0, 1, \ldots, 9\}$ with uniform probability, and you run it 100 times to generate a 100-digit number (possibly with leading zeros).

(i) What is the probability that the 100-digit number contains the digit 7 more than 50 times? (You should leave your answer as a summation.) *3pts*

(ii) What is the probability that the 100-digit number contains either no 0-digits or no 1-digits? (You should leave your answer as an unevaluated expression.) *3pts*

(g) You have a fair 6-sided die, and also a loaded 6-sided die that shows 6 with probability $1/2$ and $1, 2, 3, 4, 5$ with probability $1/10$ each. One of the two dice is chosen uniformly at random and rolled once. Let A be the event that 6 is observed.

(i) What is $\mathbb{P}[A]$? *3pts*

(ii) What is $\mathbb{P}[\,\text{Loaded die was chosen} \mid A\,]$? *3pts*

(h) Let $X \sim \text{Bernoulli}(\frac{1}{2})$ and let Y be a random variable with probability distribution $\mathbb{P}[Y = 1] = \frac{1}{2}$ and $\mathbb{P}[Y = 2] = \frac{1}{2}$. Assuming that X, Y are independent, find $\mathbb{P}[X < Y]$. *3pts*

(i) Let X be a random variable with probability distribution $\mathbb{P}[X = -8] = \frac{1}{4}$, $\mathbb{P}[X = -4] = \frac{1}{2}$, $\mathbb{P}[X = 4] = \frac{1}{4}$. Find $\mathbb{E}[\,2X]$. *3pts*

[Q2 continued on next page]

(j) Suppose m balls are thrown uniformly at random into n bins (one ball at a time). What is the expected number of bins that have exactly one ball in them? *3pts*

(k) The problem *Finite* takes as input a program P and decides whether the set of inputs on which P loops forever is finite (or empty). The following pseudo-code gives a reduction from the Halting Problem, *Halt*, to *Finite*. Fill in the blanks to make the reduction behave correctly. *3pts*

```
Test-Halt(P,x)
      let P' be a program that, on every input, runs P on x
      if Test-Finite(P') then return [          ]
            else return [          ]
```

(l) We say that programs P_1, P_2 *differ* on input x if one of the programs halts and the other loops forever on x. The problem *InfDiff* takes as input two programs, P_1 and P_2, and decides whether there are infinitely many inputs x on which P_1, P_2 differ. The following pseudo-code gives a reduction from the Halting Problem, *Halt*, to *InfDiff*. Fill in the blank to make the reduction behave correctly. *3pts*

```
Test-Halt(P,x)
      let P1 be a program that, on every input, runs P on x
      let P2 be a program that, on every input, [                    ]
      if Test-InfDiff(P1,P2) then return "yes" else return "no"
```

3. Modifying Secrets [*All answers to be justified. Total of 12 points.*]

Alice sets up a secret sharing scheme with her n friends $\mathrm{Bob}_1, \ldots, \mathrm{Bob}_n$, in which each Bob_i gets a point (x_i, y_i) where $y_i = P(x_i)$ for a fixed polynomial P over a field $\mathrm{GF}(q)$, where $q > 2n$. The secret is kept at $P(0) = s$. When Alice is distributing these points to the Bobs, an adversary Eve can tamper with the points, and thus change the value of the secret that will be recovered. For each scenario in (a)–(c) below, give the value of the new secret that will be recovered; your answers may depend on s or on P. In each case, prove that your answer is correct.

(a) Eve replaces each point (x_i, y_i) with $(x_i, 2y_i + 1)$. *4pts*

(b) Eve replaces each point (x_i, y_i) with $(2x_i, y_i)$. *4pts*

(c) Eve replaces each point (x_i, y_i) with $(x_i - 1, y_i)$. [You may assume that $x_i \neq 1$ for all $i = 1, \ldots, n$.] *4pts*

4. Breaking RSA [*All parts to be briefly justified. Total of 16 points.*]

(a) Alice sends the same message, $m < N$, to two friends, Bob and Carol using the standard RSA protocol discussed in class. Bob's public key is (N, e_1) and Carol's is (N, e_2), where $\gcd(e_1, e_2) = 1$. Explain how an eavesdropper, Eve, can decrypt m by observing the encrypted messages that Alice sends to Bob and Carol. [Hint: Use the extended gcd algorithm.] *4pts*

(b) Dennis decides to simplify the RSA cryptosystem as follows. Instead of choosing the usual type of public key $(N = pq, e)$, he instead chooses a key (N, e) where N is a prime and e is an integer in $\{2, \ldots, N-1\}$ with $\gcd(N-1, e) = 1$. To send a message m to Dennis, Alice sends the encrypted message $m^e \pmod N$. Is Dennis' scheme secure? Explain your answer. *4pts*

[Q4 continued on next page]

(c) Frank has published his RSA public key $(N = pq, e)$. Gina wants to construct her own public key, and has found one large prime $p' \neq p$; being too lazy to find another one, she asks if she can use one of Frank's; since Frank trusts Gina, he gives her his prime q. Gina then publishes her key $(N' = p'q, e')$. Explain how Eve is able to break both Frank's and Gina's RSA schemes. *4pts*

(d) Harry, Imogen and Jasper have RSA public keys $(N_H, 3)$, $(N_I, 3)$ and $(N_J, 3)$ respectively, where N_H, N_I, N_J are all distinct. Alice sends the same message m (where m is less than all of N_H, N_I, N_J) to all three of them using their respective keys. Explain how Eve is able to decrypt this message by observing the three encrypted messages. [Hints: You may use without proof the Chinese Remainder Theorem, which says the following: *Let n be a natural number. Given the values $c_i = n \bmod r_i$, for $1 \leq i \leq k$, where the r_i are coprime, we can efficiently compute the value $c = n \bmod (r_1 r_2 \cdots r_k)$.* You may also use the fact that the cube root of an integer can be found efficiently.] *4pts*

5. Counting Team Compositions [*All parts to be briefly justified. Total of 16 points.*]

UC Berkeley has n students who are interested in participating in both the CS Programming and the Putnam Mathematical competitions. In parts (a) and (b), count the number of ways to choose a CS team with c members and a Putnam team with p members under the specified constraint, assuming that $n \geq c + p$.

Whenever possible, express your answers in terms of binomial coefficients and **clearly indicate how each coefficient arises.**

(a) No restriction; any student can be on both teams. *4pts*

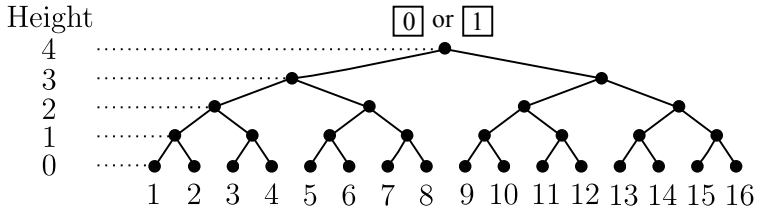
(b) No student can be on both teams. *4pts*

(c) Let $A_{n,c,p}$ denote the number of ways to choose the teams as in part (a), and let $B_{n,c,p}$ denote the number of ways to choose the teams as in part (b). Fill in the blank in the equation below to produce a valid combinatorial identity, **and briefly explain your reasoning**. *4pts*

$$A_{n,c,p} = \sum_{j=0}^{\min(c,p)} \boxed{} B_{n-j,c-j,p-j}$$

(d) The CS team wins an international programming contest and receives k gold coins as a prize. How many ways are there to divide up the coins among the c team members, under the condition that each student should receive at least three coins? (Assume that $k > 3c$.) *4pts*

6. Noisy Transmission on a Binary Tree [*All parts to be justified. Total of 13 points.*]



Consider a binary tree of depth D, which has 2^D leaves; in the example shown above, $D = 4$. At the root of the tree is a single bit (0 or 1). This bit is transmitted separately to each of the two children of the root, but in each case the value of the bit is *flipped* (i.e., $0 \to 1$ or $1 \to 0$) independently with probability p. This process continues, with each vertex of the tree transmitting its bit value (flipped with probability p, independently of all other transmissions) to its two children. The process stops at the leaves.

Suppose two distinct leaves a, b are chosen uniformly at random. Let T denote the height of the lowest common ancestor (LCA) of a and b; in the example above, $T = 1$ for $(a, b) = (1, 2)$, while $T = 3$ for $(a, b) = (1, 8)$.

(a) Find a formula for the probability $\mathbb{P}[T = t]$, where $t = 1, \ldots, D$, for a general binary tree of depth D. *5pts*

(b) Let M denote the total number of times the bit is flipped when traversing the tree from the LCA to leaf a **plus** the analogous number of bit flips from the LCA to b. Write down a formula for the conditional probability $\mathbb{P}[M = m \mid T = t]$. Be sure to specify what values of m are possible. *3pts*

[Q6 continued on next page]

(c) Now let the random variables B_a and B_b respectively denote the bits observed at the sampled leaves a and b. What condition on M guarantees that $B_a = B_b$? *2pts*

(d) Find a formula for $\mathbb{P}[B_a = B_b]$. You may leave your answer as an unevaluated expression. [Hints: Use parts (b) and (c) to compute $\mathbb{P}[B_a = B_b \mid T = t]$, then combine with part (a).] *3pts*

[End of Exam]

DO NOT WRITE ANY ANSWERS ON THIS PAGE!

THIS PAGE WILL NOT BE SCANNED