CS70 Discrete Mathematics and Probability Theory, Spring 2024

Midterm

7:00-9:00pm, 6 March 2024

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 13 pages (2-sided) on the exam. Notify a proctor immediately if a page 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 you are strongly advised to leave it and return to it later. In particular, you may find some of the later questions easier than some of the earlier ones.** *There is no penalty for incorrect answers.*

(e) *In the interests of fairness, proctors will* **not** *answer clarifying questions during the exam. If you believe there is an ambiguity or error in a problem, write down what you think is the most appropriate response and move on. Any legitimate such issues will be handled during grading.*

(f) *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.*

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

(h) *You have 120 minutes: there are 10 questions on this exam worth a total of 105 points.*

[exam starts on next page]

1. Warm-Up Multiple Choice [2 points].

Bob is in court being tried for stealing a bag of diamonds. The judge says: "If Bob stole the diamonds, then he didn't do it alone." Bob's attorney says: "That is not true!" Assuming that the attorney is telling the truth, which of the following statements must be true? [*Shade one bubble; no justification; no penalty for incorrect answers.*] *2pts*

◯ Bob did not steal the diamonds.

◯ Bob stole the diamonds, and did so alone.

◯ Bob stole the diamonds with someone else.

◯ Bob may have stolen the diamonds, but we don't know for sure.

◯ None of the above.

2. True/False [12 points].

Answer by shading the correct bubble; no justification; no penalty for incorrect answers.

TRUE	FALSE		
◯	◯	If the halting problem is computable, then pigs can fly.	*2pts*
◯	◯	$\forall x(P(x) \Rightarrow Q(x))$ is logically equivalent to $\neg\exists x\big(\neg P(x) \wedge Q(x)\big)$.	*2pts*
◯	◯	$Q(0) \wedge (\forall n \in \mathbb{N})\big([P(n) \Rightarrow Q(n+1)] \wedge [Q(n) \Rightarrow P(n)]\big) \Rightarrow (\forall n \in \mathbb{N})P(n)$.	*2pts*
◯	◯	$Q(0) \wedge (\forall n \in \mathbb{N})\big([P(n) \Rightarrow Q(n+1)] \wedge [Q(n) \Rightarrow P(n+1)]\big) \Rightarrow (\forall n \in \mathbb{N})P(n)$.	*2pts*
◯	◯	The following problem is computable: Given as input a decimal number x with a finite number n of digits, is x the first n digits of the decimal expansion of π?	*2pts*
◯	◯	The following problem is computable: Given as input a program P and two strings x, y, does P output y on input x?	*2pts*

[exam continues on next page]

3. Stable Matching T/F [10 points].

Answer by shading the correct bubble; no justification; no penalty for incorrect answers.

TRUE FALSE

◯ ◯ In a stable matching instance, if we run the propose-and-reject algorithm twice, once with jobs proposing and once with candidates proposing, and candidate C is matched with job J in both cases, then C must be matched with J in every stable pairing. *2pts*

◯ ◯ In a stable matching instance with n jobs and n candidates, for any n, the job-optimal pairing may contain a pair (J, C) where J is C's least favorite job and C is J's least favorite candidate. *2pts*

The next three questions use the following terminology. In a stable matching instance, we call a job J and a candidate C an *ideal pair* if C is J's top-ranked candidate and J is C's top-ranked job. We call J, C a *hell pair* if C is J's bottom-ranked candidate and J is C's bottom-ranked job. And we call J, C *outcasts* if both J and C are ranked last by all other candidates and jobs, respectively.

TRUE FALSE

◯ ◯ If J, C are an ideal pair, then they must be matched with each other in any stable pairing. *2pts*

◯ ◯ If J, C are a hell pair, and J', C' are another hell pair, then it is not possible for J to be matched with C and J' with C' in the same stable pairing. *2pts*

◯ ◯ If J, C are outcasts, then they must be matched with each other in any stable pairing. *2pts*

[exam continues on next page]

4. Logical Robot [10 points].

You've just unboxed your brand new personal assistance robot! As you flip through its user manual, you encounter the following propositional variables defining its behavior at a particular moment:

P: the robot is powered on
R: the robot is rerouting
M: the robot is in motion
S: the robot senses an obstacle in its path
A: the robot's alarm system is activated

(a) Express in logic: "The robot is not in motion unless it is powered on." *2pts*

(b) Express in logic the *contrapositive* of the following statement: "If the robot is powered on, then it is either in motion or its alarm system is activated." *2pts*

(c) Now assume the following propositional forms are true (and ignore any statements in parts (a)–(b)): *4pts*

- $M \Rightarrow P$
- $(S \wedge A) \Rightarrow (\neg R \vee \neg P)$
- $(P \wedge M \wedge R) \Rightarrow S$
- $(P \wedge S) \Rightarrow (A \vee \neg M)$

If you also assume that the robot is in motion (M is true), what can you deduce about the values of R and S? [*Shade one bubble; no justification; no penalty for incorrect answers.*]

◯ R is true & S is true
◯ R is false & S is true
◯ R is true & S is false
◯ R is false & S is false
◯ R is true & S could be either true or false
◯ R is false & S could be either true or false

(d) Later in the manual, you see the following predicates defining the robot's behavior at any given time $t \geq 0$: *2pts*

$L(t)$: the robot battery is low at time t $C(t)$: the robot is charging at time t

Express in logic: "At all times t, if the robot battery is low at t, then there is some future time strictly later than t when it is charging."

[exam continues on next page]

5. Spot the Errors [6 points].

Each of the induction proofs below contains a single fatal error. Shade the **single bubble** corresponding to the step in the proof that contains the error, and also explain the error **clearly and concisely** in the box provided. Do not attempt to write a lot of text—one sentence is typically enough! Points will be deducted for long-winded or imprecise answers.

(a) **Claim:** For all integers $n \geq 0$, we have $2^n = 1$. *3pts*

Proof:

◯ The base case $n = 0$ holds because $2^0 = 1$.

◯ For the inductive step, we write $n + 1 = i + j$ for two non-negative integers i, j with $i, j \leq n$.

◯ By strong induction, we may assume that the claim holds for i and j.

◯ Therefore, we have: $2^{n+1} = 2^i 2^j = 1 \times 1 = 1$.

◯ Hence the claim holds for $n + 1$.

(b) **Claim:** The sum of the interior angles of any polygon with $n \geq 3$ vertices is $180(n - 2)$ degrees. *3pts*

Proof:

◯ The base case $n = 3$ claims that the sum of the interior angles of a triangle is 180 degrees, which we know is true.

◯ For the inductive step, assume the claim holds for a polygon with n vertices.

◯ Now extend this polygon to one with $n + 1$ vertices by "adding a triangle", i.e., by replacing one of its edges by two new edges and a vertex.

◯ The increase in the sum of interior angles is exactly the angles of the added triangle, which is 180 degrees.

◯ Thus the new angle sum is $180(n - 2) + 180 = 180((n + 1) - 2)$, so the claim holds also for a polygon with $n + 1$ vertices.

[exam continues on next page]

6. Induction [10 points].

Prove parts (a) and (b) below by induction on n. Clearly label your base case and induction step for each part.

(a) Recall the Fibonacci numbers, defined by $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. Prove that $F_0^2 + F_1^2 + \ldots + F_n^2 = F_n F_{n+1}$ for all $n \geq 0$. *5pts*

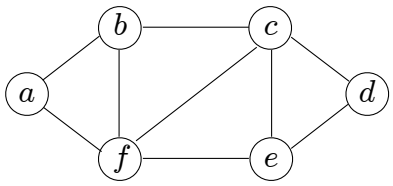
(b) Prove that $\sum_{i=1}^{n} i^3 = \left(\sum_{i=1}^{n} i\right)^2$ for all $n \geq 1$. $\left[\text{HINT: You may use the fact that } \sum_{i=1}^{n} i = \frac{n(n+1)}{2}.\right]$ *5pts*

[exam continues on next page]

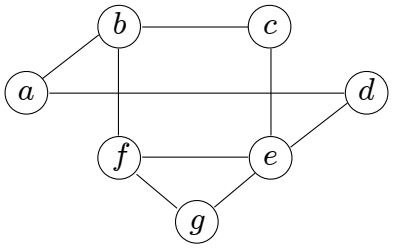
7. Graphs [14 points].

For parts (a) and (b), write your answer only in the box provided (no justification).

(a) Which one edge must be added to the following graph so that it contains an Eulerian tour? *2pts*



(b) Which one vertex must be removed from the following graph so that it contains a Hamiltonian cycle? *2pts*
[Recall that a Hamiltonian cycle is a cycle that visits every vertex of a graph exactly once.]



(c) Let T be a tree with n vertices. Suppose T has a vertex of degree k. Prove that T has at least k leaves. *4pts*

[Q7 continued]

(d) The *girth* of a graph G is the number of edges in a shortest cycle in G. (If G has no cycles then its girth is ∞.) Suppose that G is connected, has $n = 80$ vertices, $e = 135$ edges, and girth 5. Is G planar? Explain your answer carefully and show all your work. You may use Euler's theorem relating the numbers of vertices, edges and faces of planar graphs, provided you state it clearly. *6pts*

[exam continues on next page]

8. Modular Arithmetic and RSA [17 points].

(a) **Short answers.** Write your answer only in the box provided (no justification).

(i) Calculate $1! + 3! + 5! + \ldots + 99! \pmod{24}$. *2pts*

(ii) Solve the equation $5x \equiv 7 \pmod{11}$. *2pts*

(iii) What is the units digit of 7^{96} ? *2pts*

(iv) Suppose Bob implements RSA using the primes $p = 7$, $q = 11$ and $e = 11$. What is Bob's public key? *2pts*

(v) In the same scenario as part (iv), suppose Carol wants to send Bob the message $x = 3$. What encrypted value should Carol send to Bob? *2pts*

(vi) Again in the same scenario as part (iv), suppose Bob receives from Carol the encrypted message $y = 47$. What was Carol's original message? *2pts*

[exam continues on next page]

[Q8 continued]

(b) Nathan wants to prepare his favorite dish, the Tropical Trio Fruit Salad, a delicious mix of *lychee* (L), *mango* (M), and *passion fruit* (P). However, the local supermarket rarely stocks these exotic fruits. Based on Nathan's observations: *5pts*

- Lychees (L) are available every 5 days and were last seen in store 3 days ago;
- Mangoes (M) appear every 3 days and were last seen yesterday (1 day ago);
- Passion fruits (P) show up every 11 days and were last seen 2 days ago.

But there's a catch! The salad needs to be made the very day these fruits are purchased, in case they spoil. In how many days at the soonest will Nathan be able to buy on the same day all three fruits he needs? [HINT: One approach is to use the Chinese Remainder Theorem.]

9. Polynomials, Secret Sharing, and ECCs [16 points].

A group of students are participating in a treasure hunt on an island. Here is what they are told:

- The treasure is hidden at coordinates (x, y), where $x, y \in \{0, 1, \ldots, p-1\}$ for a large prime number $p > 20$.
- There is a polynomial P of degree $d = 2$ such that $x = P(10) \pmod{p}$ and $y = P(20) \pmod{p}$.
- Several hints are spread across the island. On each hint is written an integer $2 \leq k \leq p-1$ and the corresponding value $0 \leq P(k) \leq p-1$ of the polynomial. No two hints contain the same integer k, and there are no hints with $k = 10$ or $k = 20$.

Without any hints, the treasure could be in any of p^2 locations (x, y) (since there are p choices for x, and p choices for y).
For parts (a)-(c), write your answer only in the box provided (no justification).

(a) How many hints do the students need to find in order to determine the exact location of the treasure? *2pts*

(b) The students have now found one hint. Given this information, in how many different locations (x, y) could the treasure still be? *2pts*

(c) The students have now found two hints in total. In how many different locations (x, y) could the treasure still be? *2pts*

(d) The students have found the following three hints: $P(0) = 5$, $P(1) = 5$, $P(3) = 11$. Find $P(x)$. *4pts*
[HINT: You do not know p, except for the fact that it is a large prime. In this example, you can deduce the coefficients of P without knowing p. Rather than using Lagrange interpolation, write $P(x) = ax^2 + bx + c$ and solve equations for a, b, c.]

Write the polynomial P in the box below, and show your working in the space provided here.

[exam continues on next page]

[Q9 continued]

(e) You are now given that $p = 89$. Use the polynomial P from part (d) to determine the location of the treasure. *2pts*

Write your final answer in the box below, and show your working in the space provided here.

For parts (f)-(g), write your answer only in the box provided (no justification).

(f) Now suppose that one of the hints may be incorrect. How many hints in total do the students need to determine whether one of their hints is incorrect? *2pts*

(g) How many hints in total do the students need to find the correct polynomial, given that they have one incorrect hint (but don't know which one it is)? *2pts*

10. Countability [8 points].

Consider an infinite grid city, represented by $\mathbb{Z} \times \mathbb{Z}$, where the roads form a perfect grid pattern and each pair of integers (x, y) represents an intersection. A vehicle starts at the origin $(0, 0)$, pointing upwards. Then at each intersection, the vehicle can choose to drive straight, turn left or turn right. For example, it can first drive to either one of the $(-1, 0)$, $(0, 1)$ or $(1, 0)$ intersections. For each of the following sets, *determine whether the set is countable or uncountable, and give a one-sentence justification* by relating the set to specific examples or theorems covered in class.

(a) The set of all intersections $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ such that x and y are co-prime. *2pts*

(b) The set of all possible finite routes the vehicle can take. *2pts*

(c) The set of all possible infinite routes the vehicle can take. *2pts*

(d) At each intersection $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, there is a parking lot with $|x| + |y|$ parking spots. For example, at intersection $(-3, 7)$, there are $| - 3| + |7| = 10$ parking spots. Is the set of all parking spots in the city countable? *2pts*

[End of exam!]