NAME: ____________________________

SPIRE ID: ____________________________

COMPSCI 250
Introduction to Computation
First Midterm Fall 2025 – Version 1

D. A. M. Barrington and M. Golin 9 October 2025

DIRECTIONS:

- Answer the problems on the exam pages.
- There are 6 problems on pages 2-11, some with multiple parts, for 100 total points plus 5 extra credit. Final scale will be determined after the exam.
- Page 12 contains useful definitions and is given to you separately – do not put answers on it!
- But, if you do write on the back of a page, you must explicitly add a note on the front side stating that you are continuing on the back page. Otherwise, we might not see your solution on Gradescope.
- No books, notes, calculators, or collaboration.
- In case of a numerical answer, an arithmetic expression like "$2^{17} - 4$" need not be reduced to a single integer.
- Your answers must be LEGIBLE, and not cramped. Write only short paragraphs with space between paragraphs

1	/10
2	/10
3	/20
4	/20
5	/20+5
6	/20
Total	/100+5

Family Name: ____________________

Definitions for Questions 1-3: In this scenario, we have a set $D = \{b, c, i, k, r\}$ of exactly five dogs (Blaze, Clover, Indie, Kiké, and Rhonda), and a set $T = \{\text{Curly}, \text{Fluffy}, \text{None}, \text{Straight}\}$ of exactly four tail types.

The relation H from D to T, which is also a **function**, is defined by the predicate $H(d, t)$ meaning "dog d has tail type t". The binary relation Y on D is defined by the predicate $Y(d, e)$ meaning "dog d is younger than dog e". You are given that Y is a **strict partial order**, meaning that it is **antireflexive**, **antisymmetric**, and **transitive**.

Question 1 (10): (Translations)

- (a, to symbols, 2 points) **Statement I:** If Clover has a Fluffy tail, then either Indie has a Straight tail or Blaze has no tail, but not both.

- (b, to English, 2 points) **Statement II:** $H(c, F) \vee \neg(H(i, S) \rightarrow H(b, N))$

- (c, to symbols, 2 points) **Statement III:** If it is not the case that both Indie has a Straight tail and Clover has a Fluffy tail, then Clover has a Fluffy tail and it is not the case that Blaze has no tail.

- (d, to English, 2 points) **Statement IV:** $\forall d : ((d = r) \vee Y(r, d)) \wedge ((d = k) \vee Y(d, k))$

- (e, to symbols, 2 points) **Statement V:** Any dog has a Fluffy tail if and only if it is younger than Blaze, and any dog has a Straight tail if and only if Blaze is younger than it.

Question 2 (10): (Boolean Proof)

For this problem, please use the abbreviations $p = H(c, F)$, $q = H(i, S)$, and $r = H(b, N)$. Using **either** a truth table **or** a deductive sequence proof, **prove** that there is **exactly one setting** of these three variables that satisfies **Statements I, II, and III**.

Note that you must show both that your setting satisfies that statements, and that no other setting does so. If you construct a correct truth table, you will prove both. If you use a deductive sequence to that your setting is implied by the three statements, you must **also** verify that your setting in fact does satisfy the three statements.

So that you may have correct inputs to the following problem, we will tell you that the correct setting has p **true**, q **true**, and r **false**.

Family Name: ____________________

Question 3 (20) (Predicate Proof) :

For this proof, we ask you to determine two things:

- (a, 10) What is the age order of the five dogs?
- (b, 10) What is the tail type of each dog?

For part (a), number the dogs D_1, D_2, D_3, D_4, and D_5, with D_1 being the youngest dog and D_5 the oldest.

To show your results fill in the table below with, e.g., the entry below D_1 being the name of the youngest dog and the entry below D_5 the name of the oldest one.

D_1	D_2	D_3	D_4	D_5

Using quantifier rules on Statements I-V, and the **given properties** of H and Y, justify the claims that $Y(D_1, D_2)$, $Y(D_2, D_3)$, $Y(D_3, D_4)$, and $Y(D_4, D_5)$.

- Justify your claim that $Y(D_1, D_2)$:

- Justify your claim that $Y(D_2, D_3)$:

- Justify your claim that $Y(D_3, D_4)$:

- Justify your claim that $Y(D_4, D_5)$:

For part (b), find the tail type of each of the five dogs, justifying each choice by quantifier rules. Indicate where, if anywhere, you use the given properties of H and Y.

The tail types you find should be shown in the following table, with entry (d, t) being the value **1** if $H(d, t)$ is true and **0** if $H(d, t)$ is false. We start you off by filling in the three values you already know from Question 2.

$D \backslash T$	C	F	N	S
b			**0**	
c		**1**		
i				**1**
k				
r				

Question 4 (20): (Binary Relations on a Set) Parts (a) and (b) deal with two binary relations P and Q, each from a set to itself. Part (a) is on this page, part (b) on the next.

(a, 10) Let $A = \{a, b, c, d\}$. The relation $P \subseteq A \times A$ is a **partial order**. It is known that $(a, b) \in P$, $(a, d) \in P$, $(b, c) \in P$ and $(d, c) \notin P$.

(i) In the table given below, label all pairs that must be in P with a "✓" and all pairs that cannot be in P with a "×." For pairs that are neither, leave their entry blank. We start you off by labeling the four known pairs with the appropriate "✓" or ×.

Justify your answers. That is, you must provide a brief explanation as to why each of the pairs you marked "✓" are in P and those you marked "×" are not in P. Each pair that you justify must be explicitly named as being justified.

Your explanations must reference the properties of P that are being used. They must also be consistent. That is, if you somewhere use the fact that $(x, y) \notin P$ where $(x, y) \neq (d, c)$, then you must have already previously proven that $(x, y) \notin P$.

(ii) How many partial orders P' exist that satisfy $(a, b) \in P$, $(a, d) \in P$, $(b, c) \in P$ and $(d, c) \notin P$? Briefly explain how you know this. Draw a Hasse diagram illustrating each such P' that could exist.

(a,a)	(a,b)	(a,c)	(a,d)	(b,a)	(b,b)	(b,c)	(b,d)	(c,a)	(c,b)	(c,c)	(c,d)	(d,a)	(d,b)	(d,c)	(d,d)
	✓		✓			✓								×	

(b, 10) Let $B = \{a, b, c, d, e\}$. The relation $Q \subseteq B \times B$ is an **equivalence relation**. It is known that $(a, b) \in Q$, $(a, c) \in Q$, $(b, e) \notin Q$ and $(e, d) \notin Q$.

(i) In the table given below, label all pairs that must be in Q with a "✓" and all pairs that cannot be in Q with a "×." For pairs that are neither, leave their entry blank. We start you off by labeling the four known pairs with the appropriate "✓" or ×.

Justify your answers following the same rules that were given in part (a).

(ii) How many Equivalence Relations Q' exist that satisfy $(a, b) \in Q$, $(a, c) \in Q$, $(b, e) \notin Q$ and $(e, d) \notin Q$? Briefly explain how you know this. Write down the possible equivalence relation(s) in partition form, that is, as a set of sets of items in B.

(a,a)	(a,b)	(a,c)	(a,d)	(a,e)		(b,a)	(b,b)	(b,c)	(b,d)	(b,e)
	✓	✓								×
(c,a)	(c,b)	(c,c)	(c,d)	(c,e)		(d,a)	(d,b)	(d,c)	(d,d)	(d,e)
(e,a)	(e,b)	(e,c)	(e,d)	(e,e)						
			×							

Family Name: ____________________

Question 5 (20+5): (Number Theory)

- (a, 4) For each of (i) and (ii) below say whether m has a multiplicative inverse modulo n. In each one, if the inverse exists, write down what it is. You do not need to show your work. The number you write down should be between 0 and $n-1$. If the inverse does not exist, prove that it does not exist.

  (i) $m = 5$, $n = 34$.

  (ii) $m = 333$, $n = 336$

- (b, 8) The naturals 67 and 30 are relatively prime.
  Use the Extended GCD algorithm as taught in class to find integers a and b satisfying the equation $a \cdot 67 + b \cdot 30 = 1$. Show all of your work.

  After solving the problem, write your final solution here
  $a =$ _______. $b =$ _______.

- (c, 4) Using the results from the previous part, determine both an inverse of 30 modulo 67 and an inverse of 67 modulo 30.
  For full credit, your answers should each be the smallest natural numbers that are inverses.
  After solving the problem, write your final solutions here:
  _______ is an inverse of 67 modulo 30.
  _______ is an inverse of 30 modulo 67.

- (d, 4) You are now given that $2 \cdot 101 - 3 \cdot 67 = 1$.
  Using the technique taught in class, determine the smallest natural x that solves both the congruences
  $$x \equiv 3 \pmod{67} \quad \text{and} \quad x \equiv 2 \pmod{101}.$$
  Show all of your your work.
  After solving the problem, write your final solution below:

  The smallest natural satisfying both congruences is $x =$ ____.

- (e, 5 extra credit)

  There are a number of classic puzzles involving pirates on an island (usually also with a monkey) that need to divide a hoard of coconuts. In this case, three pirates A, B, and C, have n coconuts and have agreed to divide them equally in the morning. During the night, each pirate secretly takes away what they think to be their share. Specifically,

  - A first visits the hoard of n coconuts. She divides them into three equal piles of size a, except there is one left over which she gives to the monkey. She hides a coconuts, leaves $2a$ remaining, and gives one to the monkey, so $n = 3a + 1$.
  - B now visits, and divides the remaining $2a$ coconuts into three equal piles of size b, giving one left over to the monkey. He hides b coconuts, and leaves $2b$, so that $2a = 3b + 1$.
  - C finds the remaining $2b$ coconuts, divides them into three piles of size c, giving one to the monkey, and leaves $2c$, so that $2b = 3c + 1$.
  - In the morning, the remaining $2c$ coconuts are divided equally into three piles, *without* one for the monkey.

  In fact, there are an infinite number of possible sizes n that fit this scenario. Your job is to **find one** (write it below) and then **prove** that your solution for n is the smallest one possible. (**Hint:** Modular arithmetic definitely comes into play, but there is no obvious way to use the Chinese Remainder Theorem.)

  The smallest natural satisfying the conditions is $n =$ ____.

Family Name: ____________________

Question 6 (20): The following are ten true/false questions, with no explanation needed or wanted, no partial credit for wrong answers, and no penalty for guessing.

After reading the questions, write the correct answer, either T (for true) or F (for false), in the corresponding column.

(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)	(i)	(j)

- (a) Given the three premises $(p \wedge \neg x) \rightarrow c$, $(p \wedge \neg(x \rightarrow y)) \rightarrow c$, and $(p \wedge x \wedge y) \rightarrow c$, we can conclude that $p \rightarrow c$ is true.

- (b) Let u and v be two non-empty strings over the alphabet $\{a, b\}$. If u is both a prefix of v and a suffix of v, then u and v must be the same string, that is, $u = v$.

- (c) Let A, B, C, and D each be finite non-empty sets. Then the statement $A \times B \subseteq C \times D$ is logically equivalent to the statement $(A \subseteq C) \wedge (B \subseteq D)$.

- (d) Let $X = \{0, 1\}$ and $Y = \{a, b\}$. Then $\langle b, 0 \rangle \in X \times Y$.

- (e) Let P be a unary predicate on the set A, and assume the premise $\forall x : P(x)$. It may be possible that the statement $\exists y : P(y)$ is false.

- (f) Let R be a binary predicate on $\mathbb{N}$, defined as $\{\langle a, b \rangle : a^2 = b\}$. Then R is a function from $\mathbb{N}$ to $\mathbb{N}$, and is an injection (1-1 function), but it is not a surjection (onto function).

- (g) Let a, b, and c be distinct odd naturals, each greater than 1. Then the number $n = abc + 4$ is not divisible by a, not divisible by b, and not divisible by c.

- (h) A relation $R \subseteq A \times B$ is an injection (a one-to-one function) if and only if for every $x \in A$, there is exactly one element $y \in B$ such that $\langle x, y \rangle \in R$.

- (i) For all naturals x, y, and z, $x\%(y\%z) = (x\%y)\%z$, where "%" is the modular division operation, as in Java or Python.

- (j) Let $p_1, p_2, \ldots, p_k$ and $q_1, \ldots, q_m$ each be prime numbers, not necessarily distinct. If the two products $p_1 p_2 \ldots p_k$ and $q_1 \ldots q_m$ are equal, then we know both that $k = m$ and that for each i with $1 \leq i \leq k$, $p_i = q_1$.