NAME: ____________________________

COMPSCI 250
Introduction to Computation
SOLUTIONS to First Midterm Fall 2023

D. A. M. Barrington and G. Parvini

12 October 2023

DIRECTIONS:

- Answer the problems on the exam pages.
- There are four problems on pages 2-8, some with multiple parts, for 100 total points plus 5 extra credit. Final scale will be determined after the exam.
- Page 9 contains useful definitions and is given to you separately – do not put answers on it!
- If you need extra space use the back of a page.
- 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.

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

This problem deals with a set D of exactly eight distinct dogs named August (a), Blaze (b), Bliss (b'), Daisy (d), Ollie (o), Rhonda (r), Scout (s), and Tuesday (t). Note that Blaze and Bliss have similar names but have different abbreviations.

Each dog has one of the following jobs, from the set $J = \{FD, HP, SD\}$, as a Farm Dog, a House Pet, or a Service Dog. The function e from D to J is defined so that for any dog x in D, $e(x)$ is the job of x.

You are told some of the values of the function e. Blaze and Rhonda are Dave's dogs and are both House Pets. Ollie, who attends lecture -01 of COMPSCI 250 this term, is a Service Dog. And Scout, who has appeared in prior 250 exams, is a Farm Dog.

The binary relation P on the set D is defined so that for any dogs x and y, $P(x, y)$ is true if and only x's name *precedes* y's name in alphabetical order. So, for example, $P(b, b')$ is true and both $P(b, b)$ and $P(b', b)$ are false. You may assume that the relation P is antireflexive, antisymmetric, and transitive.

Question 1 (10): (Translations) Translate each statement as according to the directions:

- (a, 2) (to English) (Statement I) $(e(a) = SD) \rightarrow (e(b') = SD) \wedge (e(d) = SD))$
  If August is a Service Dog, then Bliss and Daisy are Service Dogs as well.

- (b, 2) (to symbols) (Statement II) If Bliss is a Service Dog, then so is either (or both) of August and Daisy.
  Solution: $(e(b') = SD) \rightarrow ((e(a) = SD) \vee (e(d) = SD))$

- (c, 2) (to English) (Statement III) $((\neg(e(a) = SD) \vee (e(b') = SD)) \rightarrow \neg(e(d) = SD))$
  If either August is not a Service Dog, or if Bliss is, then Daisy is not.

- (d, 2) (to symbols) (Statement IV) For every dog x, there is a dog different from x with the same job as x.
  Solution: $\forall x : \exists y : \neg(x = y) \wedge (e(x) = e(y))$
  A very common error was to replace the correct $\wedge$ with a $\rightarrow$. Another was to leave off the $\neg(x = y)$ required by the word "different".

- (e, 2) (to English) (Statement V) $\forall x : \forall y : ((e(x) = e(y)) \wedge P(x, y)) \rightarrow [\exists z : P(x, z) \wedge P(z, y)]$
  Given two dogs x and y, if those two dogs have the same job, and x precedes y, then there exists a dog z such that x precedes z and z precedes y. Equivalently, if any two different dogs have the same job, then there is a third dog between the two in the order.
  The most common error was to place the "if... then" construction in the wrong place.

Question 2 (10): (Boolean Proof) Questions 2 and 3 use the definitions, predicates, and statements above.

Using *only* Statements I, II, and III, determine the truth values of the three statements p defined as $e(a) = SD$, q defined as $e(b') = SD$, and r defined as $e(d) = SD$. It may be easier to refer to the three atomic propositions as p, q, and r. You may use a truth table or a deductive sequence proof.

Translating to p, q, and r as suggested, Statement I says $p \rightarrow (q \wedge r)$, Statement II says $q \rightarrow p \vee r$, and Statement III says $(\neg p \vee q) \rightarrow \neg r$.

A truth table shows that all three statements must be false – here is a deductive sequence proof by contradiction.

If p is true, all three must be true by Statement I, but r implies that q is false by Statement III. So then either q (by Statement II) or r (by the contrapositive $r \rightarrow (p \wedge \neg q)$ of Statement III) both imply p, which gives a contradiction. That is, any of the three being true gives a contradiction, so all three must be false.

This setting satisfies the three statements, the first two vacuously and the third trivially.

I'll leave off the truth table.

The most common error in the deductive sequence proofs was to omit the check that your derived conclusion is really a solution. If you don't verify that your solution satisfied all three statements, you have not ruled out the possibility that the three statements contradict one another.

Question 3 (20) (Predicate Proof) : This question also uses the definitions, predicates, and statements above. Now assume that all of Statements I-V are true, and assume the four values of the function e provided above. Using propositional and quantifier rules, determine the jobs of the four remaining dogs, that is, the function values $e(a)$, $e(b')$, $e(d)$, and $e(t)$.

If x and y are adjacent dogs in alphabetical order, they cannot have the same job because we would have a contradiction of Statement V. This tells us that neither August nor Bliss can be House Pets, since both are adjacent to Blaze. Statements I-III show that neither are Service Dogs, so they are Farm Dogs. Daisy is then adjacent to the Farm Dog Bliss, and cannot be a Service Dog both because she is adjacent to Ollie and because I-III says she isn't, so she is a House Pet. Tuesday must then be a Service Dog, since IV says that Ollie cannot be the only Service Dog and none of the others are.

These were generally good, though people who got Question 2 wrong gave themselves a different problem, some of which have no solutions, some have one, and some have more. If you solved the problem derived from your bad version of Q2, I gave up to full credit for it, unless the mistake caused your resulting problem to be much easier.

Question 4 (20): (Number Theory) This problem concerns the naturals 55 and 78.

Here are your questions:

- (a, 3) Write each of the naturals 55 and 78 as a product of prime numbers.

  Solution: $55 = 5 \cdot 11$ **and** $78 = 2 \cdot 3 \cdot 13$**.**

- (b, 3) Explain why the result of part (a) implies that the naturals 55 and 78 are relatively prime.

  The prime factors occurring in the two numbers are different, that is, no prime appears in both.

- (c, 4) Carry out the ordinary Euclidean Algorithm on 55 and 78, and explain why the result tells you that 55 and 78 are relatively prime.

  Solution: $78\%55 = 23$, $55\%23 = 9$, $23\%9 = 5$, $9\%5 = 4$, $5\%4 = 1$, $4\%1 = 0$**. The last positive number in the sequence is** 1**, which is the GCD of** 78 **and** 55**, so they are relatively prime.**

- (d, 10) Justifying your answers, find an inverse of 55, modulo 78, and an inverse of 78, modulo 55. Make sure that you indicate which is which.

  Solution: $78 = 0 \cdot 55 + 1 \cdot 78$, $55 = 1 \cdot 55 + 0 \cdot 78$, $23 = -1 \cdot 55 + 1 \cdot 78$, $9 = (55 - 2 \cdot 23) = 3 \cdot 55 - 2 \cdot 78$, $5 = 23 - 2 \cdot 9 = -7 \cdot 55 + 5 \cdot 78$, $4 = 9 - 5 = 10 \cdot 55 - 7 \cdot 78$, $1 = 5 - 4 = -17 \cdot 55 + 12 \cdot 78 = -935 + 936$**, so the inverse of** 55**, modulo** 78**, is** -17**, or** $78 - 17 = 61$**, and the inverse of** 78**, modulo** 55**, is** 12**.**

Question 5 (20+5): (Linear Functions) Let n be a positive natural, and let S be set of naturals $\{0, 1, \ldots, n-1\}$.

Given any two elements a and b of S, define a function f_{ab} from S to S such that $f_{ab}(x) = (ax+b)\%n$, using the Java or Python notation % for the remainder operator. (For any naturals x and y, $x\%y$ is defined to be the remainder when x is divided by y, so that for example $11\%3 = 2$.)

- (a, 5) Prove that if a, b, c, and d are any elements of S, the function composition $f_{cd} \circ f_{ab}$ is another function f_{pq}, for some two element p and q in S. What are the values p and q in this case? **Let x be an arbitrary element of S, Let $y = f_{ab}(x)$, which is**

  $(ax+b)\%n$. Then $(f_{cd} \circ f_{ab})(x) = f_{cd}(f_{ab}(x))$, which is $f_{cd}(y) = (cy+b)\%n$, which is $((c(ax+b)+d)\%n$ or $(cax+(cb+d))\%n$. So we may let p be ca and let q be $cb+d$.

- (b, 5) For a given n, for what values a and b is the function f_{ab} a bijection from S to S?

  The function f_{ab} has an inverse if and only if a and n are relatively prime. The value of b does not matter for this purpose. If we let c be the multiplicative inverse of a, modulo n, and let $d = -bc$, then by our computation above, $f_{cd} \circ f_{ab} = f_{10}$, as ca is congruent to 1 and $cb+d$ is congruent to 0. If a has no inverse modulo n, so that a and n have a common factor g greater than 1, the function f_{ab} cannot be onto, because for any x, $f_{ab}(x)$ is some multiple of g plus b, and not every number in S is of this form.

- (c, 5XC) Let n be a prime number. Let w, x, y, and z be elements of S, and assume $w \neq y$. Prove that there is exactly one pair (a, b) in $S \times S$ such that $f_{ab}(w) = x$ and $f_{ab}(y) = z$.

  Since $w \neq y$, $w - y$ is non zero, and since n is prime, $w - y$ is relatively prime to n and thus has an inverse u, modulo n. To get $aw + b = x$ and $ay + b = z$, we need to have $(aw + b) - (ay + b) = x - z$. Since $(aw + b) - (ay + z) = a(w - y)$, we can make this happen by letting $a = u(x - z)$, modulo n, because then $a(w - y) = u(w - y)(x - z)$ will be $x - z$, modulo n. Any other choice of a will not let $x - z$ have the required value. Once we have picked a, we have to pick b to be equal to $x - aw$ or $z - ay$, which are the same number because the difference between them is $(x - aw) - (z - ay) = (x - z) + a(y - w)$, which is zero by our choice of a.

- (d, 10) For $n = 78$, $a = 55$, and $b = 36$, compute the inverse of the function f_{ab}. That is, find elements c and d of S such that $f_{cd} \circ f_{ab}$ is the identity function on S. You may find some of the calculations from Question 4(d) to be useful.

  From part (a), we need $p = ca$ to be 1, and $q = cb + d$ to be 0, so that the composition function $f_{pq} = f_{cd} \circ f_{ab}$ is the identity function. We need c to be the multiplicative inverse of a, modulo n, which we computed in Question 4(d) to be -17 or 61. Then to make $q = 0$ true, we want d to be $-cb$ (modulo n) which is $(17)(36) = 612$. (Any number with the right remainder modulo 78 is correct, but 66 is the one in the range from 0 to 77.)

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.

- (a) Let $P(x)$ be a unary predicate on integers. If $\forall x : (x > 0) \rightarrow P(x)$ and $\forall x : (x < 0) \rightarrow P(x)$ are both true, then we may conclude $\forall x : P(x)$.

  FALSE. This omits the case $x = 0$ — for example we could have $P(x)$ mean $x \neq 0$, so that both premises were true but $P(0)$ is false.

- (b) Let A be any non-empty set. Then there exists a binary relation on A that is both an equivalence relation and a partial order.

  TRUE. The equality relation is both, whether the set A is empty or not.

- (c) Let all variables range over the type T. Then the statement "$\forall x : P(x)$" is equivalent to "$\forall x : (x \in T) \rightarrow P(x)$", and the statement "$\exists x : P(x)$" is equivalent to "$\exists x : (x \in T) \wedge P(x)$".

  TRUE. The first statements say "every element in T satisfies P", and the second statements say "there some element (which must be in T) satisfying P".

- (d) Let T be a type including several dogs, one of whom is Rhonda (r). If we are given the assumption $\exists x : P(x)$, where the variable x is over T, then we may conclude $P(r)$ by Instantiation.

  FALSE. This is a misuse of Instantiation – $P(a)$ is true for some dog a, but we don't know that this dog must equal Rhonda.

- (e) Let a, b, c, and d be any four *integers* (positive, negative, or zero). If $\exists c : ac = b$ and $\exists d : bd = a$ are both true, then $a = b$ must be true.

  FALSE. It's also possible that $a = -b$.

- (f) The Contrapositive Rule implies that the negation of the statement "$p \rightarrow q$" is equivalent to "$q \rightarrow p$".

  FALSE. This is the converse, which is different from the contrapositive and not equivalent to the negation of the original.

- (g) Let n be any positive natural and let A be a language. Then there exists a string in A^* with more than n letters if and only if there exists a non-empty string (a string other than λ) in A.

  TRUE. If there is such a string in A, then A^* contains arbitrarily long strings, and if not, $A^* = \{\lambda\}$.

- (h) Suppose we want to prove "All corgis are both lazy and silly". We could do this by making the assumption "There exists a corgi that is both lazy and silly", then deriving a contradiction from this assumption.

  FALSE. We would need the negation of the statement we want to prove, which would instead be "There exists a corgi that is either not lazy, or not silly, or both".

- (i) Let A be an non-empty set, let x be an element of A, and let R be a binary relation on A such that R is a subset of the relation $\{(x, y) : y \in A\}$, that is, R is a subset of the set of pairs whose first member is always x. Then R may fail to be a transitive relation.

  FALSE. The only way for there to be two pairs (a, b) and (b, c) in R would be if a and b are both x, in which case (a, c) would be in R, since is equal to (b, c).

- (j) There exists a set A of naturals such that A is the set of naturals that are both even and odd.

  TRUE. This set is empty, but the empty set exists.

COMPSCI 250 First Midterm Supplementary Handout: 12 October 2023

Here are definitions of sets, predicates, and statements used on the exam.

Remember that the scope of any quantifier is always to the end of the statement it is in.

In Question 4 we often use the Java operator % on naturals, so that $x\%y$ is the remainder when x is divided by y.

The five statements of Question 1 are:

- (a, 2) (to English) (Statement I) $(e(a) = SD) \rightarrow (e(b') = SD) \wedge (e(d) = SD))$

- (b, 2) (to symbols) (Statement II) If Bliss is a Service Dog, then so is either (or both) of August and Daisy.

- (c, 2) (to English) (Statement III) $((\neg(e(a) = SD) \vee (e(b') = SD)) \rightarrow \neg(e(d) = SD))$

- (d, 3) (to symbols) (Statement IV) For every dog x, there is a dog different from x with the same job as x.

- (e, 3) (to English) (Statement V) $\forall x : \forall y : ((e(x) = e(y)) \wedge P(x, y)) \rightarrow [\exists z : P(x, z) \wedge P(z, y)]$

You are also told (for Question 3) that Blaze and Rhonda are House Pets, Ollie is a Service Dog, and Scout is a Farm Dog. The entire set of dogs, in alphabetical order, are August, Blaze, Bliss, Daisy, Ollie, Rhonda, Scout, and Tuesday.