NAME: _____

COMPSCI 250
Introduction to Computation
SOLUTIONS to First Midterm Spring 2023

D. A. M. Barrington and G. Parvini 23 March 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	/15
2	/30
3	/15
4	/20+5
5	/20
Total	/100+5

Questions 1, 2, and 3 involve a set of four dogs $D = \{b, p, r, s\}$, named Blaze, Pushkin, Rhonda, and Scout, who one day all met at the park. Some of these dogs growled at some of the others.

We define a binary relation G on D, so that $G(x, y)$ means "dog x growled at dog y". (Pronoun note: All four of these dogs are female.)

Question 1 (15): Translate each statement as according to the directions:

- (a, 2) (to English) (Statement I) $G(p, s) \to G(b, p)$
  If Pushkin growled at Scout, then Blaze growled at Pushkin.
- (b, 2) (to symbols) (Statement II) If Pushkin did not growl at Scout, then Pushkin growled at Rhonda but Blaze did not growl at Rhonda.
  $\neg G(p, s) \to (G(p, r) \wedge \neg G(b, r))$
- (c, 2) (to English) (Statement III) $G(b, p) \to \neg G(b, p)$
  If Blaze growled at Pushkin, then she did not growl at Pushkin. (Equivalently, Blaze did not growl at Pushkin.)
- (d, 3) (to symbols) (Statement IV) It is not the case that some dog growled at herself.
  $\forall z : \neg G(z, z)$**, or equivalently** $\neg \exists z : G(z, z)$
  The most common error here was putting the $\neg$ between the $\exists$ and the $G(x, x)$.
- (e, 3) (to English) (Statement V) $\forall y : G(y, b) \to G(b, y)$
  Blaze growled at any dog that growled at her.
  One common error here was "splitting the quantifier" by saying "If Blaze growled at all dogs, then all dogs growled at her."
- (f, 3) (to symbols) (Statement VI) There is some dog that growled at every dog except herself.
  $\exists x : \forall y : (x \neq y) \to G(x, y)$
  Most people got the $\exists x : \forall y :$ correct, but there were a lot of incorrect answers inside the quantifiers. If you say "$G(x, y) \wedge (x \neq y)$", for example, you are saying that inside the $\forall$, so you are saying that dog x growled at every dog and that every dog is not equal to x. Others got the implication backward.

Question 2 (30): These questions use the definitions, predicates, and premises on the supplementary sheet.

- (a, 10) Assuming *only* that Statements I, II and III are true, determine the truth values of the four propositions $q_1 = G(b, p)$, $q_2 = G(b, r)$, $q_3 = G(p, r)$, and $q_4 = G(p, s)$. You may use a truth table or a deductive sequence proof. Make sure that there is exactly one solution.

  The three statements translate to $q_4 \to q_1$, $\neg q_4 \to (q_3 \wedge q_2)$, and $q_1 \to \neg q_1$.

  We know that q_1 is false from Statement III. We know that q_4 is false by converting Statement II to its contrapositive $\neg q_1 \to \neg q_4$, and then using Modus Ponens. Finally, by Modus Ponens on Statement II we know that q_3 is true and q_2 is false.

  We have to make sure that these four values satisfy the three statements. Statement I is vacuously true because q_4 is false, Statement II is trivially true because $q_3 \wedge \neg q_2$ is true, and Statement III is true both vacuously and trivially.

  I'll leave off the truth table.

  Most of these were good, with most but not all using propositional rules. (I (Dave) picked statements where the propositional proof was easy, but if you wanted to do the truth table, that was fine. Some, usually correctly, left off the parts of the truth table that were irrelevant.) One error I saw a lot was to break into cases based on q_4, showing that q_4 being true was a contradiction, but never reasoning in the other case that q_1 has to be false.

- (b, 20) Now assume that all of Statements I-VI are true. Using propositional and quantifier rules, prove that Blaze growled at some dog, that is, $\exists x : G(b, x)$ is true. You may use either English or symbols, but make it clear each time you use a quantifier proof rule.

  By Instantiation, let a be the dog from Statement VI, so we know that $\forall y : (a \neq y) \to G(a, y)$.

  Case I: $a \neq b$. Specify the statement we just derived to $y = b$, so that we get $(a \neq b) \to G(a, b)$, and then by Modus Ponens on the assumption for this case, $G(a, b)$. We then use Specification on Statement V with $y = a$ to get $G(a, b) \to G(b, a)$, and use Modus Ponens to get $G(b, a)$. Finally the rule of Existence tells us $\exists x : G(b, x)$.

  Case 2: $a = b$. Statement III tells us $\neg G(b, p)$. But since $b \neq p$, and $a = b$, we know $a \neq p$, and we can specify our result $\forall y : (a \neq y) \to G(a, y)$ to $y = p$, telling us $(a \neq p) \to G(a, p)$, and thus $G(a, p)$ by Modus Ponens. Since $a = b$ and we know $\neg G(b, p)$, this is a contradiction.

  We took off five points for ignoring the case where Blaze was the dog from Statement VI, and took off four points for inadequately dealing with that case. There are at least two ways to deal with it. As above, you can prove that Blaze cannot be that dog. Or you could note that if Blaze were that dog, she would growl at all the other dogs and thus we could choose any one of them and prove our goal by Existence. (You could even use both of these solutions even though they are mutually exclusive – look up either "Argument in the Alternative" or "Kettle Logic" on Wikipedia.) We took off some points if you made essential use of an incorrect symbolic version of Statement VI in your proof, but most people worked with the English version.

A lot of the regrade requests were based on a claim that 4/20 or even 10/20 is too harsh if you had some valid work there. I'm very generous with the first 20% of the credit, but this is a hard problem in part because a fair number of things have to come together to get close to a valid solution. Forgetting that Blaze might be the dog from VI is a significant penalty in an otherwise good proof. An incorrect proof costs you more than that.

Question 3 (15): Now using the same set of dogs D, and the relation G from Questions 1 and 2, we define a function $f : D \to \mathbf{N}$, where $\mathbf{N}$ is the set of all naturals $\{0, 1, 2, 3, \ldots\}$. For any dog x in D, we define $f(x)$ to be the number of dogs that x growled at, that is, $f(x) = |\{y : G(x, y)\}|$.

Let Statement VII be: "$\forall n : \exists x : f(x) = n$".

Let Statement VIII be "$\forall x : \forall y : (f(x) = f(y)) \to (x = y)$."

Here are your questions:

- (a, 2) What property of f is defined by Statement VII?
  It says "f is onto" or "f is a surjection".
- (b, 3) Is Statement VII true of our function f defined above? Justify your answer.
  It is false, because if n is any natural greater than 4, $f(x)$ cannot be equal to n for any dog since there are only four possible dogs to growl at.
- (c, 2) What property of f is defined by Statement VIII?
  It says "f is one-to-one" or "f is an injection".
- (d, 8) Is Statement VIII true of our function f defined above? Justify your answer.
  It is not true. From part (a) of Question 2, we know that Blaze did not growl at either Pushkin or Rhonda, Pushkin growled at Rhonda, and Pushkin did not growl at Scout. Statement IV says that no dog growled at herself. Statement VI says that some dog a growled at every dog except herself, and this cannot be Blaze since she does not growl at Pushkin. Thus by Statement V, Blaze growls at dog a, who is also not Pushkin. Neither Pushkin nor Rhonda could have growled at Blaze, since otherwise one of them would have growled back. So we know that Pushkin growled at only Rhonda, and thus $f(p) = 1$. Since each of the other three dogs are known have failed to growl at some other dog, dog a must be Scout, she growled at Blaze, and thus by Statement V Blaze growled at Scout. This makes Scout the only dog that Blaze growled at, so $f(b) = 1$. Since $f(p) = f(b)$, the statement is false. In particular it fails if we Specify x to p and y to b.
  It wasn't possible to answer the question without the statements I-VI from Questions 1 and 2. If you showed understood what you needed, but didn't use the statements to find it out, this was typically 4/8 on part (d).

Question 4 (20+5): Here are a variety of number theory questions.

- (a, 5) Let $S = \{30, 31, 32, 33, 34, 35\}$ be a set of naturals. Which of these naturals have inverses modulo 42 and which do not? Justify your answers.

  We want to know which numbers have GCD's of 1 **with** 42**, which we could do by running the EA on each number with** 42**:**

  $42\%30 = 12$**,** $30\%12 = 6$**,** $12\%6 = 0$**, GCD is** 6**.**

  $42\%31 = 11$**,** $31\%11 = 9$**,** $11\%9 = 2$**, and** $9\%4 = 1$**, GCD is** 1**,** 42 **and** 31 **have inverses.**

  $42\%32 = 10$**,** $32\%10 = 2$**,** $10\%2 = 0$**, GCD is** 2**.**

  $42\%33 = 9$**,** $33\%9 = 6$**,** $9\%6 = 3$**,** $6\%3 = 0$**, GCD is** 3**.**

  $42\%34 = 8$**,** $32\%8 = 2$**,** $8\%2 = 0$**, GCD is** 2**.**

  $42\%35 = 7$**,** $35\%7 = 0$**, GCD is** 7**.**

  Or we could eliminate 30**,** 32**, and** 34 **because of its common factor of** 2 **with** 42**,** 33 **because of its common factor of** 3**, and** 35 **with its common factor of** 5**, leaving** 31 **as the only possibility. Then we can run** $EA(42, 31)$**, as above, to see that they are relatively prime, and thus that** 31 **does have an inverse modulo** 42**.**

  Some only did the EA and didn't say why you knew that 31 *and* 42 *are prime – that was a one-point penalty.*

- (b, 10) Find inverses modulo 42 for every element of S that has one.

  We run the Extended Euclidean Algorithm:

  $42 = 1 \cdot 42 + 0 \cdot 31$

  $31 = 0 \cdot 42 + 1 \cdot 31$

  $11 = 1 \cdot 42 - 1 \cdot 31$

  $9 = -2 \cdot 42 + 3 \cdot 31$

  $2 = 3 \cdot 42 - 4 \cdot 31$

  $1 = -14 \cdot 42 + 19 \cdot 31$ **(check,** $-14 \cdot 42 + 19 \cdot 31 = -588 + 589 = 1$**)**

  So 19 **is an inverse of** 31**, modulo** 42**.**

- (c, 5) **Cicadas** are large insects with unusual life cycles. When a cicada is born, it burrows underground for either 13 or 17 years (depending on the type of cicada) and emerges after that time as an adult. A given adult cicada is normally part of a **brood**, all of whom emerged in the same year. Suppose that a given area there are both a single 13-year brood and a single 17-year brood of cicadas. What does the Chinese Remainder Theorem tell us about when the two broods will emerge in the same year?

  Since 13 and 17 are prime numbers, we know that they are also relatively prime to one another. If in a given year, it has been a years since the 13-year cicadas emerged and b years since the 17-year cicadas did so, the CRT tells us that the two cycles coincide every $13 \cdot 17 = 221$ years, and that there is some number c, which we can calculate from a, b, 13, and 17, such that both broods last emerged c years ago.

  To get full credit here, you needed to talk about the fact that 13 and 17 are coprime, the number 221, and existence of some c that depends on 13 and 17 and their inverses, and the year that each brood starts.

- (d, 5XC) If our 13-year cicadas emerged in 2020, and our 17-year cicadas in 2023, and their cycles both persist through the entire coming millenium, what will be the first year after 3000 when both broods will emerge in the same year?

  Let x be the number of years since 2020. We know that the 13-year cicadas emerge whenever $x \equiv 0 \pmod{13}$ and that the 17-year cicadas emerge whenever $x \equiv 3 \pmod{17}$. Using the notation from lecture, we have $a = 0$, $m = 13$, $b = 3$, and $n = 17$. We need to calculate integers y and z so that $xm + bn = 1$. We can form the linear combinations $17 = 0 \cdot 13 + 1 \cdot 17$, $13 = 1 \cdot +0 \cdot 17$, $4 = -1 \cdot 13 + 1 \cdot 17$, and $1 = 4 \cdot 13 - 3 \cdot 17$, so $y = 4$ and $z = -3$. We compute c to be $bym + azn = 3 \cdot 4 \cdot \cdot 13 + 0 = 156$, so that both broods emerge whenever $x \equiv 156 \pmod{221}$. The last time this happened was in $2020 - 221 + 156 = 1955$, and it will happen again in 2176, 2397, 2618, 2839, and 3060.

  On the first pass, we gave only 3/5 for people who found the correct answer by brute force. On reflection, we noted that the question does not tell you how to do it, though it's implicit that you have to justify your number. We'll make a pass through the submissions and correct this on the regrade process, even if you didn't request a regrade.

Question 5 (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. Some of them use the sets, relations, and functions defined on the supplemental sheet, but you should assume the truth of Statements I-VII only if explicitly told to.

- (a) If X is the set $\{a, b, c\}$, then there are exactly three subsets of X that have exactly two elements.
  TRUE – they are $\{a, b\}$, $\{a, c\}$, and $\{b, c\}$.
- (b) $\emptyset^*$ is a non-empty language.
  TRUE – it is $\{\lambda\}$ which is not empty.
  A lot of people missed this.
- (c) Statement IV in Questions 1-3 is equivalent to the statement "the relation G is not reflexive". **FALSE – it means "G is antireflexive", which is not the same thing.**
- (d) If a binary relation T, on the set A, is both an equivalence relation and a partial order, then A must be the empty set.
  FALSE – The equality relation on any set is both a partial order and an equivalence relation.
  A lot of people missed this – some thought that symmetric and antisymmetric are negations of one another, which they are not.
- (e) If two distinct positive naturals x and y are relatively prime, then at least one of them must be prime.
  FALSE – for example 1 and 4 are relatively prime.
- (f) Let R be a binary relation on strings over the alphabet $\{a, b\}$, such that $R(u, v)$ is true if and only if the number of a's in u equals the number of b's in v. Then R is not reflexive, not symmetric, and not transitive.
  TRUE – $R(a, a)$ is false, $R(a, b)$ is true but $R(b, a)$ is false, and $R(a, b)$ and $R(b, c)$ are both true but $R(a, c)$ is false.
- (g) Let S be a binary relation on the set $\{1, 2, 3, 4\}$ such that $S(x, y)$ is true if and only if $x \leq y$. Then S is a partial order, and its Hasse diagram has exactly four edges.
  FALSE – there are only three edges, which are $(1, 2)$, $(2, 3)$, and $(3, 4)$.
- (h) In a truth table with four boolean variables, for the compound proposition $C = p \wedge (q \vee r \vee s)$, there are exactly seven lines of the table in which C is true. **TRUE – All the eight with p true, except for the one where the other three are all false.**
- (i) The statement $A \cup (B \cap C) = (A \cup B) \cap C$ is a set identity.
  FALSE – For example, elements in $A \setminus (B \cup C)$ are in the LHS but not the RHS.
- (j) If n is an odd natural, and $n > 1$, then there exists an odd prime number p such that n is a multiple of p. **TRUE – n must have a prime factor (possibly itself) and this cannot be 2, so it is odd.**