Homework 3: Written Proofs

CS 81: Computability and Logic

Due: 11:59pm, Tuesday, September 19, 2023

As always, answers should be typed. *After first attempting these problems on your own,* you may discuss the problems with other students in the class this semester as long that discussion has educational value and no one is "giving away" answers. Answers must be written up individually in your own words; any insights that arose from discussions with other students must be reconstructed from memory.

1 Proof By Contraposition [6 points]

Assume n is an integer. Prove that if n^2 is not divisible by 4, then n is odd.

Hint: Sometimes when we are asked to prove $A \to B$, it is easier to give a proof for the logically-equivalent contrapositive. This strategy is called *Proof by Contrapositive* or *Proof by Contraposition*; you politely warn the reader by starting the proof with a statement like "We prove the contrapositive" or "Proof (by contraposition):" and then just prove that $\neg B \to \neg A$.

2 Proof by Contradiction [20 points]

In this class we'll use *Proof by Contradiction* to refer both to reasoning with $\neg E$ (suppose something is true; reach a contradiction, therefore it's false) and to reasoning with IP (suppose something is false; reach a contradiction; therefore it's true). We'll specifically mention $\neg E$ or IP if we need to be more specific about the method of reasoning.

Some people try to use Proof by Contradiction for all their proofs. That isn't inherently wrong, but whenever you finish a proof by contradiction, you should check to see if you've written a true proof by contradiction, or if there's a simpler proof hiding inside!

The following four proofs are technically correct and appeal to proof by contradiction. Identify the three proofs that use proof by contradiction in an unnecessary way, and for each of these, briefly explain how to simplify the proof. (We don't want you to come up with completely different proofs or to significantly rewrite these proofs! Rather, explain in a sentence or two what you could remove and/or tweak to get a shorter yet still correct proof without Proof by Contradiction.)

1. **Theorem:** Let a and b be positive real numbers. Then $\frac{a+b}{2} \geq \sqrt{ab}$ (that is, the *arithmetic mean* of a and b is at least as big as their *geometric mean*).

   Proof: By way of contradiction, suppose $\frac{a+b}{2} < \sqrt{ab}$. Now $(a-b)^2 \geq 0$ because squares aren't negative. Then $a^2 - 2ab + b^2 \geq 0$, so $a^2 + 2ab + b^2 \geq 4ab$ and $\left(\frac{a+b}{2}\right)^2 \geq ab$. Since a and b are positive, we can take square roots to get $\frac{a+b}{2} \geq \sqrt{ab}$. This is a contradiction; our supposition that $\frac{a+b}{2} < \sqrt{ab}$ must have been wrong and so $\frac{a+b}{2} \geq \sqrt{ab}$.

2. **Theorem:** Every undirected graph has an even number of vertices with odd degree.

   Proof: Let G be an arbitrary graph. Suppose by way of contradiction that G has an odd number of vertices with odd degree. Now every edge in G contributes one towards the degrees of its two endpoints, so if we add the degrees of all the vertices we get twice the number of edges, an even number. That is, (the sum of the degrees of the even-degree vertices of the graph) + (the sum of the degrees of the odd-degree vertices of the graph) is an even number. It follows that the sum of the degrees of the odd-degree vertices is even, requiring there be an even number of them. This contradicts our supposition, so the number of odd-degree vertices in G is even.

3. **Theorem:** If i and j are integers, then $i^2 - 4j - 2 \neq 0$.

   Proof: Let i and j be arbitrary integers. Suppose by way of contradiction that $i^2 - 4j - 2 = 0$. Then $i^2 = 4j + 2$, so i^2 is even. But that means that i is even, i.e., that $i = 2n$ for some natural number n. Then $4n^2 = (2n)^2 = i^2 = 4j + 2$, a contradiction because $4n^2$ is a multiple of 4 while $4j + 2$ is not. Thus, $i^2 - 4j - 2 \neq 0$.

4. **Theorem:** Let m be a natural number. If m^2 is even then m is even.

   Proof: Assume m^2 is even. By way of contradiction, suppose m is odd. Then $m = 2k + 1$ for some integer k, whence $m^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, and so m^2 is odd. This is a contradiction, so m must be even.

We would like to thank the League of Moose and Aardvark Owners (LMAO) for their generous sponsorship of the next two questions.

3 Logic to English [20 points]

Assume our domain of individuals is people. Let L denote a binary relation representing the "likes" relation (so that $L(x, y)$ means that x likes y). Let A be a unary predicate denoting whether its argument owns an aardvark, and let M be a unary predicate indicating whether its argument owns a moose.

Translate each of the following predicate calculus formulas into English. Keep your English statements as simple and concise as possible, and avoid referring to logic variables like x or y in your answer.

1. $\forall x \; (\; M(x) \rightarrow A(x) \;)$
2. $\exists x \; (\; M(x) \wedge A(x) \;)$
3. $\forall x \; \exists y \; (\, L(x, y) \wedge \neg L(y, x) \,)$
4. $\exists x \; \forall y \; (\, L(x, y) \wedge \neg L(y, x) \,)$
5. $\exists x \; (\, M(x) \wedge \forall y \; (A(y) \rightarrow \neg L(x, y)) \,)$

4 English to Logic [20 points]

Express each of the following English statements using these the same predicates L, A, and M as in the previous problem, along with the operators of first-order predicate logic. Keep your expressions as simple as possible.

In these statements, when we talk about a "pair of people" we permit the possibility that it's really the same person being mentioned twice; similarly "three moose owners" includes the possibility of 1 or 2 or 3 distinct individuals.

1. Everyone likes some person who owns an aardvark and a moose.
2. There is someone who owns a moose who likes every aardvark owner.
3. For every pair of people who don't own aardvarks, if the first likes the second then the second likes the first.
4. For every pair of people who own a moose and an aardvark respectively, those people either both like one another or both dislike one another.
5. For every three moose owners, if the first likes the second and the second likes the third then the first likes the third. (Transitive liking of moose owners!)

5 Models [32 points]

In each part (except as noted below), describe *two* models: one in which the formula is true and one in which the formula is false. For each of your models,

- State the domain set (the nonempty universe of elements that $\forall$ and $\exists$ quantify over).
- For each relevant predicate, precisely which elements of the domain make it true.
- Explain in 1-3 sentences why this model makes the formula true or makes it false

For your domain and predicates, you can either give a very abstract specification like

> "the domain is the set $\{a, b, c\}$, where $C(a)$ is true and $C(b)$ and $C(c)$ are false, and $P(x)$ is true for all three elements"

or you can give a real-world scenario like

> "the domain consists of three cats and three dogs (a Labrador and two pugs); $C(x)$ is true when x is a cat, $P(x)$ is true when x is a pug."

Be careful, though; real-world scenarios must be described precisely enough that a reader can calculate the truth of formulas. For example, if someone said

> "the domain is the set of animals in Claremont; $C(x)$ is true when x is cuddly, and $P(x)$ is true when x is a porcupine."

then $\exists x\, P(x)$ ("there's a porcupine [in Claremont]") is true or false, but you can't expect the reader to do a full field investigation to find out; the answer might even change over time, making it not a well-defined model. Similarly, $\forall x\, (\, P(x) \lor C(x)\,)$ ("all animals [in Claremont] are either porcupines or cuddly") cannot be given a truth value until we agree on exact criteria for being cuddly. So this would not be an acceptable model.

Warning: This is a trick question! One of the formulas is a *tautology*, true in every model. For that formula, you should give one model where the formula is true and explain convincingly (in 1–3 sentences) why it is true in all other models too.

1. $\forall x\, P(x) \;\lor\; \neg\exists x\, Q(x)$
2. $(\exists x\, D(x)) \;\rightarrow\; (\forall y\, D(y))$
3. $\exists x\; (\, D(x) \rightarrow \forall y\, D(y)\,)$
4. $(\, \forall x\, P(x) \;\rightarrow\; \forall x\, Q(x)\,) \;\rightarrow\; \forall x\, (\, P(x) \rightarrow Q(x)\,)$

6 Survey [2 points]

Please wait until you're done with the rest of the assignment to answer this quick survey:

1. How long (in hours) did you spend working on this assignment?
2. What was the most interesting thing you learned while doing this assignment? (We're sure there was something you learned!)