HW6 Proofs, Numbers, and Cardinality

CSE20F21

Due: Tuesday, November 23, 2021 at 11:00PM on Gradescope

In this assignment,

You will practice determining and justifying whether statements are true in multiple contexts.

Instructions and academic integrity reminders for all homework assignments in CSE20 this quarter are on the class website and on the hw1-definitions-and-notations assignment.

You will submit this assignment via Gradescope (https://www.gradescope.com) in the assignment called "hw6-proofs-numbers-cardinality".

Resources: To review the topics you are working with for this assignment, see the class material from Weeks 6 through 8. We will post frequently asked questions and our answers to them in a pinned Piazza post.

In your proofs and disproofs of statements below, justify each step by reference to a component of the following proof strategies we have discussed so far, and/or to relevant definitions and calculations.

- A counterexample can be used to prove that $\forall x P(x)$ is **false**.
- A witness can be used to prove that $\exists x P(x)$ is **true**.
- **Proof of universal by exhaustion**: To prove that $\forall x\, P(x)$ is true when P has a finite domain, evaluate the predicate at **each** domain element to confirm that it is always T.
- **Proof by universal generalization**: To prove that $\forall x\, P(x)$ is true, we can take an arbitrary element e from the domain and show that $P(e)$ is true, without making any assumptions about e other than that it comes from the domain.
- To prove that $\exists x P(x)$ is **false**, write the universal statement that is logically equivalent to its negation and then prove it true using universal generalization.

Copyright Mia Minnes, 2021, Version November 18, 2021 (1)

- **Strategies for conjunction**: To prove that $p \wedge q$ is true, have two subgoals: subgoal (1) prove p is true; and, subgoal (2) prove q is true. To prove that $p \wedge q$ is false, it's enough to prove that p is false. To prove that $p \wedge q$ is false, it's enough to prove that q is false.

- **Proof of Conditional by Direct Proof**: To prove that the implication $p \rightarrow q$ is true, we can assume p is true and use that assumption to show q is true.

- **Proof of Conditional by Contrapositive Proof**: To prove that the implication $p \rightarrow q$ is true, we can assume $\neg q$ is true and use that assumption to show $\neg p$ is true.

- **Proof of disjuction using equivalent conditional**: To prove that the disjunction $p \vee q$ is true, we can rewrite it equivalently as $\neg p \rightarrow q$ and then use direct proof or contrapositive proof.

- **Proof by Cases**: To prove q when we know $p_1 \vee p_2$, show that $p_1 \rightarrow q$ and $p_2 \rightarrow q$.

- **Proof by Structural Induction**: To prove that $\forall x \in X\, P(x)$ where X is a recursively defined set, prove two cases:

  Basis Step: Show the statement holds for elements specified in the basis step of the definition.

  Recursive Step: Show that if the statement is true for each of the elements used to construct new elements in the recursive step of the definition, the result holds for these new elements.

- **Proof by Mathematical Induction**: To prove a universal quantification over the set of all integers greater than or equal to some base integer b:

  Basis Step: Show the statement holds for b.

  Recursive Step: Consider an arbitrary integer n greater than or equal to b, assume (as the **induction hypothesis**) that the property holds for n, and use this and other facts to prove that the property holds for $n + 1$.

- **Proof by Strong Induction** To prove that a universal quantification over the set of all integers greater than or equal to some base integer b holds, pick a fixed nonnegative integer j and then:

  Basis Step: Show the statement holds for b, $b + 1$, $\ldots$, $b + j$.

  Recursive Step: Consider an arbitrary integer n greater than or equal to $b + j$, assume (as the **strong induction hypothesis**) that the property holds for **each of** b, $b + 1$, $\ldots$, n, and use this and other facts to prove that the property holds for $n + 1$.

- **Proof by Contradiction**

  To prove that a statement p is true, pick another statement r and once we show that $\neg p \rightarrow (r \wedge \neg r)$ then we can conclude that p is true.

  Informally The statement we care about can't possibly be false, so it must be true.

Copyright Mia Minnes, 2021, Version November 18, 2021 (2)

Assigned questions

1. Recall the definition of the set of linked lists from class, and some associated functions.

   Basis Step: $[] \in L$
   Recursive Step: If $l \in L$ and $n \in \mathbb{N}$, then $(n, l) \in L$

   The length function $length : L \to \mathbb{N}$ is defined by

Basis Step:		$length(\ []\ )$	$= 0$
Recursive Step:	If $l \in L$ and $n \in \mathbb{N}$, then	$length(\ (n, l)\ )$	$= 1 + length(l)$

   The function $prepend : L \times \mathbb{N} \to L$ is defined by

   $$prepend(\ (l, n)\ ) = (n, l)$$

   The function $append : L \times \mathbb{N} \to L$ is defined by

Basis Step:	If $m \in \mathbb{N}$ then	$append(\ ([], m)\ )$	$= (m, [])$
Recursive Step:	If $l \in L$ and $n \in \mathbb{N}$ and $m \in \mathbb{N}$, then	$append(\ (\ (n, l), m\ )\ )$	$= (n, append(\ (l, m)\ )\ )$

   (a) (*Graded for fair effort completeness*[1]) Fill in the blanks in the following proof of the statement

   $$\forall l \in L\ \forall m \in \mathbb{N}\ (\ length(prepend(\ (l, m)\ )) = length(append(\ (l, m)\ ))\ )$$

   Proof: We proceed by structural induction on L.
   Basis step: We need to show that

   $$\forall m \in \mathbb{N}\ (\ length(prepend(\ ([], m)\ )) = length(append(\ ([], m)\ ))\ )$$

   Towards universal generalization, let m be an arbitrary natural number. Calculating:

   $$LHS = \underline{\text{BLANK 1}}$$

   $$RHS = \underline{\text{BLANK 2}}$$

   Since $LHS = RHS$, the basis step is complete.
   Recursive step: Consider an arbitrary: $l' \in L$, $n \in \mathbb{N}$, and we assume as the **induction hypothesis** that:

   $$\underline{\text{BLANK 3}}$$

   Our goal is to show that

   $$\forall m \in \mathbb{N}\ (\ length(prepend(\ (\ (n, l')\ , m)\ )) = length(append(\ (\ (n, l'), m)\ ))\ )$$

   is also true. Let m be an arbitrary natural number. Calculating:

   $$LHS = \underline{\text{BLANK 4}}$$

   $$RHS = \underline{\text{BLANK 5}}$$

   Since $LHS = RHS$, the recursive step is complete.

[1] Graded for fair effort completeness means you will get full credit so long as your submission demonstrates honest effort to answer the question. You will not be penalized for incorrect answers.

Copyright Mia Minnes, 2021, Version November 18, 2021 (3)

(b) (*Graded for correctness*[2]) Disprove the statement

$$\forall l \in L\ \forall m \in \mathbb{N}\ (\ prepend(\ (l, m)\ ) = append(\ (l, m)\ )\ )$$

(c) (*Graded for correctness*) Determine whether the statement

$$\exists l \in L\ \exists m \in \mathbb{N}\ (\ prepend(\ (l, m)\ ) = append(\ (l, m)\ )\ )$$

is true or false, and justify your conclusion using valid proof strategies.

2. Recall the definition of the set of rational numbers,

$$Q = \left\{ \frac{p}{q} \mid p \in \mathbb{Z} \text{ and } q \in \mathbb{Z} \text{ and } q \neq 0 \right\}$$

We define the set of **irrational** numbers $\overline{\mathbb{Q}} = \mathbb{R} - \mathbb{Q} = \{x \in \mathbb{R} \mid x \notin \mathbb{Q}\}$.

(a) (*Translation graded for fair effort completeness; Witness graded for correctness*) Translate the statement to English and then give a witness that could be used to prove the statement

$$\exists x \in \mathbb{Q}\ \forall y \in \overline{\mathbb{Q}}\ (x \cdot y \in \mathbb{Q})$$

You do not need to justify your answer. However, if you include clear explanations, we may be able to give partial credit for an answer with some imprecision.

(b) (*Translation graded for fair effort completeness; Witness graded for correctness*) Translate the statement to English and then give a counterexample that could be used to disprove the statement

$$\forall x \in \overline{\mathbb{Q}}\ \ (x > 0\ \rightarrow\ x \geq 1)$$

You do not need to justify your answer. However, if you include clear explanations, we may be able to give partial credit for an answer with some imprecision.

(c) (*Translation graded for fair effort completeness; Witness graded for correctness*) Translate the statement to English and then give a witness that could be used to prove the statement

$$\exists (x, y, z) \in \overline{\mathbb{Q}} \times \mathbb{Q} \times \mathbb{Q}\ (y \neq z \wedge x^y = z)$$

You do not need to justify your answer. However, if you include clear explanations, we may be able to give partial credit for an answer with some imprecision.

(d) (*Graded for fair effort completeness*[3]) Fill in the blanks in the following argument.
Claimed statement: $\exists x \in \overline{\mathbb{Q}}\ \exists y \in \overline{\mathbb{Q}}\ \exists z \in \mathbb{Q}\ (x^y = z)$.

[2]Graded for correctness means your solution will be evaluated not only on the correctness of your answers, but on your ability to present your ideas clearly and logically. You should explain how you arrived at your conclusions, using mathematically sound reasoning. Whether you use formal proof techniques or write a more informal argument for why something is true, your answers should always be well-supported. Your goal should be to convince the reader that your results and methods are sound.

[3]Fair effort completeness for this question means either attempting to correctly answer each part or to write a sentence or two on where you get stuck in your attempt to correctly answer the question.

Copyright Mia Minnes, 2021, Version November 18, 2021 (4)

Proof: We need to give a witness to prove this existential claim. We proceed in a proof by cases, since the disjunction **(i)**_____ is true.

- **Case 1**: We need to show that

$$(\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}) \to \exists x \in \overline{\mathbb{Q}}\ \exists y \in \overline{\mathbb{Q}}\ \exists z \in \mathbb{Q}\ (x^y = z)$$

  Assume towards a direct proof that **(ii)**_____. We choose the witnesses $x = \sqrt{2}$, $y = \sqrt{2}$, $z = \sqrt{2}^{\sqrt{2}}$. By the theorem we proved in class, $\sqrt{2} \notin \mathbb{Q}$. Since $x = y = \sqrt{2}$, $x \in \overline{\mathbb{Q}}$ and $y \in \overline{\mathbb{Q}}$. By the assumption of this direct proof, $z \in \mathbb{Q}$. Thus, the witnesses we picked are in the required domains. Moreover, by definition, $z = x^y$, as required. Thus, the existential claim is proved and we have completed the direct proof required for this case.

- **Case 2**: We need to show that

$$(\sqrt{2}^{\sqrt{2}} \in \overline{\mathbb{Q}}) \to \exists x \in \overline{\mathbb{Q}}\ \exists y \in \overline{\mathbb{Q}}\ \exists z \in \mathbb{Q}\ (x^y = z)$$

  Assume towards a direct proof that $(\sqrt{2}^{\sqrt{2}} \in \overline{\mathbb{Q}})$. We choose the witnesses

  $x =$ **(iii)**_____, $y =$ **(iv)**_____, $z =$ **(v)**_____

  By the assumption of this direct proof, $x \in \overline{\mathbb{Q}}$. As we mentioned above, $\sqrt{2} \notin \mathbb{Q}$ so $y \in \overline{\mathbb{Q}}$. Picking $p = 2, q = 1$, we observe that $z = \frac{2}{1}$ and since **(vi)**_____, $z \in \mathbb{Q}$. Thus, the three witnesses we picked are in the required domains. Calculating:

$$\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^{\sqrt{2}\cdot\sqrt{2}} = \left(\sqrt{2}\right)^2 = \sqrt{2}\cdot\sqrt{2} = 2$$

  which proves that **(vii)**_____, and hence x, y, z are the required witnesses. Thus, the existential claim is proved and we have completed the direct proof required for this case.

The proof by cases is now complete and the statement has been proved. QED

3. Recall that A **hex color** is a nonnegative integer, n, that has a base 16 fixed-width 6 expansion

$$n = (r_1 r_2 g_1 g_2 b_1 b_2)_{16,6}$$

where $(r_1 r_2)_{16,2}$ is the red component, $(g_1 g_2)_{16,2}$ is the green component, and $(b_1 b_2)_{16,2}$ is the blue component. For notational convenience, we define the set $C = \{x \in \mathbb{N} \mid x < 16^6\}$. This is the set of possible hex colors because these are all numbers that have hexadecimal fixed-width 6 expansions.

   (a) (*Graded for correctness*) Determine and briefly justify whether C is finite, countably infinite, or uncountable.

Copyright Mia Minnes, 2021, Version November 18, 2021 (5)

(b) Consider the function $red : C \to C$ given by $red(\ (r_1r_2g_1g_2b_1b_2)_{16,6}\ ) = (r_1r_20000)_{16,6}$.

i. (*Graded for correctness*) Determine whether red is one-to-one, and justify your conclusion using valid proof strategies.

ii. (*Graded for correctness*) Determine whether red is onto, and justify your conclusion using valid proof strategies.

4. Consider the set of ratings in a 3-movie database $R = \{-1, 0, 1\} \times \{-1, 0, 1\} \times \{-1, 0, 1\}$ and the set of bases of RNA strands $B = \{\mathtt{A}, \mathtt{C}, \mathtt{U}, \mathtt{G}\}$.

(a) (*Graded for fair effort completeness*) Give a (well-defined) one-to-one function with domain R and codomain B or explain why there is no such function.

(b) (*Graded for fair effort completeness*) Give a (well-defined) one-to-one function with domain B and codomain R or explain why there is no such function.

(c) (*Graded for fair effort completeness*) Give a (well-defined) onto function with domain R and codomain B or explain why there is no such function.

(d) (*Graded for fair effort completeness*) Give a (well-defined) onto function with domain R and codomain B or explain why there is no such function.

Sample calculation that can be used as reference for the detail expected in your answer when specifying functions and reasoning about their properties:

We give a (well-defined) function with domain R and codomain B that is neither one-to-one nor onto.

Define $g : R \to B$ by, for $(x_1, x_2, x_3) \in R$,

$$g(\ (x_1, x_2, x_3)\ ) = \begin{cases} \mathtt{A} & \text{if } x_1 = 1 \\ \mathtt{C} & \text{if } x_1 = 0 \\ \mathtt{G} & \text{if } x_1 = -1 \end{cases}$$

This function is well-defined because each ratings 3-tuples is mapped to a unique base. However, this function is not one-to-one, as we can see from the counterexample: $a = (1, 1, 1)$, $b = (1, 0, 0)$. These are ratings 3-tuples (in the domain) which are distinct (they disagree about the second and third movies) but

$$g(a) = g(\ (1, 1, 1)\ ) = \mathtt{A} = g(\ (1, 0, 0)\ ) = g(b)$$

because the two ratings agree on the first movie. Distinct domain elements getting mapped to the same codomain elements is a counterexample to injectivity.

The function g is also not onto, as we can see from the counterexample $\mathtt{U}$. This is an element of the codomain which is not $f(x)$ for any x in the domain, as we can see from the piecewise definition of g, where in no case do we have the output value $\mathtt{U}$.

Copyright Mia Minnes, 2021, Version November 18, 2021 (6)