HW5 Proofs and Induction

CSE20F21

Due: Tuesday, November 16, 2021 at 11:00PM on Gradescope

In this assignment,

You will work with recursively defined sets and functions and prove properties about them, practicing induction and other proof strategies.

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 "hw5-proofs-and-induction".

Resources: To review the topics you are working with for this assignment, see the class material from Weeks 5 through 7. 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.

- **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.

Assigned questions

1. Recall the definitions from class about factoring and divisibility: when a and b are integers and a is nonzero, a **divides** b means there is an integer c such that $b = ac$. In this case, we say a is a **factor** of b, a is a **divisor** of b, b is a **multiple** of a, $a|b$. We define the function $PosFactors : \mathbb{Z}^+ \to \mathcal{P}(\mathbb{Z}^+)$ by

$$PosFactors(n) = \{x \in \mathbb{Z}^+ \mid x \text{ is a factor of } n\}$$

Sample calculation that can be used as reference for the detail expected in your answer when working with this function:

The function application $PosFactors(4)$ evaluates to

$$PosFactors(4) = \{1, 2, 4\}$$

because the only possible positive factors of 4 are $1, 2, 3, 4$ (the positive integers less than or equal to 4) and when we divide we get:

$$\begin{aligned} 4 &= 4 \cdot 1 + 0 && \text{so 4 is a factor of 4} \\ 4 &= 3 \cdot 1 + 1 && \text{so 3 is not a factor of 4} \\ 4 &= 2 \cdot 2 + 0 && \text{so 2 is a factor of 4} \\ 4 &= 1 \cdot 4 + 0 && \text{so 1 is a factor of 4} \end{aligned}$$

(a) (*Graded for correctness*[1]) Give a witness that proves the statement

$$\exists x \in \mathbb{Z}^+ \; \forall y \in \mathbb{Z}^+ \; (\; x \in PosFactors(y) \;)$$

Justify your choice of witness by explanations that include references to the relevant definitions.

(b) (*Graded for correctness*) Give a counterexample that disproves the statement

$$\forall n \in \mathbb{Z}^+ \; (\; PosFactors(n) \subseteq PosFactors(n+1) \;)$$

Justify your choice of counterexample by explanations that include references to the relevant definitions.

[1] 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.

(c) (*Graded for fair effort completeness*) Consider the following attempted proof.

> **Attempted proof**: For arbitrary integers a, b, c, assume towards a direct proof that $(a+b)|c$. We need to show that $a|c$ and $b|c$. Let n be the integer c **div** $(a+b)$. Since $(a+b)|c$, by definition of divides, $n|c$ and n is an integer. Since $c = 1 \cdot n \cdot (a+b)$, $(n \cdot (a+b))|c$. Rewriting by distributing multiplication over addition, we have $na|c$ and $nb|c$. Since $a|na$ and $na|c$, we have $a|c$. Similarly, since $b|nb$ and $nb|c$, we have $b|c$. Thus, we have proved both conjuncts and the proof is complete.

Select the statement below that the attempted proof is trying to prove.

(i) $\forall a \in \mathbb{Z}^+ \, \forall b \in \mathbb{Z}^+ \, \forall c \in \mathbb{Z} \, (\, (\, a|c \, \vee \, b|c \,) \, \rightarrow \, (a+b)|c \,)$

(ii) $\forall a \in \mathbb{Z}^+ \, \forall b \in \mathbb{Z}^+ \, \forall c \in \mathbb{Z} \, (\, (\, a|b \, \wedge \, a|c \,) \, \rightarrow \, a|(b+c) \,)$

(iii) $\forall a \in \mathbb{Z}^+ \, \forall b \in \mathbb{Z}^+ \, \forall c \in \mathbb{Z} \, (\, (a+b)|c \, \rightarrow \, (\, a|c \, \wedge \, b|c \,) \,)$

Identify the first major error in the attempted proof and explain why it is incorrect.

Next, disprove the statement the attempted proof was attempting to prove.

Extra practice; not for credit: prove or disprove the other two statements.

2. In this question, we'll consider the function which calculates the sum of the first n positive integers.

(a) (*Graded for fair effort completeness*[2])

Give a recursive definition of this function, including domain, codomain and both the basis step and recursive step of the rule. That is, fill in the blanks

$$sumOfFirst : \underline{\quad domain \quad} \rightarrow \underline{\quad codomain}$$

given by

Basis step : fill in basis step

Recursive step : fill in recursive step

Notation: Using summation, this function can be written $sumOfFirst(n) = \sum_{i=1}^{n} i$.

(b) (*Graded for fair effort completeness*) It turns out that the value of this function can also be calculated explicitly (without recursion)[3]. You will prove this by completing the proof of the identity

$$\forall n \in \mathbb{Z}^+ \, \left(\, sumOfFirst(n) = \frac{n(n+1)}{2} \right)$$

[2]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.

[3]When the value of a function that is recursively defined can also be calculated without recursion, we call the formula that we can use to calculate the value without recursion the "closed form formula" for the function.

Fill in the missing parts of the proof of this statement:

Proof: We proceed by mathematical induction on the set of positive integers.
Basis Step: Choose $n = 1$ as the basis step. Using the Basis Step in the recursive definiton of $sumOfFirst$, $sumOfFirst(1) = 1$. Plugging n into the RHS of the desired formula, $\frac{1(1+1)}{2} = \frac{2}{2} = 1$. Since LHS=RHS, the Basis step is complete.
Recursive Step: Consider an arbitrary $k \geq 1$. We assume (as the induction hypothesis) that fill in the blank here.
We want to show that $sumOfFirst(k+1) = \frac{(k+1)\cdot((k+1)+1)}{2}$.
Fill in the rest of the proof here.

(c) (*Graded for fair effort completeness*) When calculating the runtime of an algorithm, nested for loops sometimes lead to program runtimes that involve the sum of the first n positive integers. To estimate the rate of growth of this runtime, it is useful to find an upper bound for this function in terms of a simpler function. Use the explicit formula from the earlier parts of this question and mathematical induction to prove

$$\forall n \in \mathbb{Z}^+ \ \left(\ sumOfFirst(n) \leq n^2 \right)$$

3. Recall the definition of linked lists that we discussed in class.

Define the function *count* which returns the number of occurrences of a datum in the list. Formally, $count : L \times \mathbb{N} \to \mathbb{N}$, where

Basis Step: If $m \in \mathbb{N}$, $count(\ ([], m)\ ) = 0$

Recursive Step: If $l \in L$ and $n \in \mathbb{N}$ and $m \in \mathbb{N}$, then

$$count(\ (\ (n, l), m\ )\ ) = \begin{cases} 1 + count(\ (l, m)\ ) & \text{if } n = m \\ count(\ (l, m)\ ) & \text{otherwise} \end{cases}$$

A mystery function is defined by $mystery : L \times \mathbb{N} \to L$, where

Basis Step: If $m \in \mathbb{N}$, $mystery(\ ([], m)\ ) = []$

Recursive Step: If $l \in L$ and $n \in \mathbb{N}$ and $m \in \mathbb{N}$, then

$$mystery(\ (\ (n, l), m\ )\ ) = \begin{cases} l & \text{if } n = m \\ mystery(\ (l, m)\ ) & \text{otherwise} \end{cases}$$

(a) (*Graded for correctness*) Prove that

$$\forall m \in \mathbb{N}\ \exists l \in L\ \ (count(\ (l, 20)\ ) = m\ )$$

(b) (*Graded for correctness*) Give an example input x to the function such that

$$mystery(\ (\ x\ ,\ 2\ )\ ) = []$$

For full credit, include all intermediate steps of the function application that justifies your choice of x, with brief justifications for each.

(c) (*Graded for correctness*) Evaluate the function application

$$mystery(\ (\ (2, (0, (2, [])))\ ,\ 2\ )\ )$$

For full credit, include all intermediate steps of the function application, with brief justifications for each.

(d) (*Graded for fair effort completeness for English statements and correctness in use of syntax for symbolic statements*) Describe the rule of the function *mystery* in English. Then, write a true statement that describes an invariant using both the functions *mystery* and *count*. Express this invariant both symbolically and in English.