hw5-proofs-and-induction

CSE20S24

Due: 5/21/24 at 5pm (no penalty late submission until 8am next morning)

In this assignment, you will work with recursively defined sets and functions and prove properties about them, practicing induction and other proof strategies.

Relevant class material: Weeks 5,6,7.

You will submit this assignment via Gradescope (https://www.gradescope.com) in the assignment called "hw5-proofs-and-induction".

For all HW assignments: These homework assignments may be done individually or in groups of up to 3 students. Please ensure your name(s) and PID(s) are clearly visible on the first page of your homework submission, start each question on a new page, and upload the PDF to Gradescope. If you're working in a group, *submit only one submission per group*: one partner uploads the submission through their Gradescope account and then adds the other group member(s) to the Gradescope submission by selecting their name(s) in the "Add Group Members" dialog box. You will need to re-add your group member(s) every time you resubmit a new version of your assignment.

Each homework question will be graded either for **correctness** (including clear and precise explanations and justifications of all answers) or **fair effort completeness**. You may collaborate on "graded for correctness" questions only with CSE 20 students in your group; if your group has questions about a problem, you may ask in drop-in help hours or post a private post (visible only to the Instructors) on Piazza. For "graded for completeness" questions: collaboration is allowed with any CSE 20 students this quarter; if your group has questions about a problem, you may ask in drop-in help hours or post a public post on Piazza.

All submitted homework for this class must be typed. You can use a word processing editor if you like (Microsoft Word, Open Office, Notepad, Vim, Google Docs, etc.) but you might find it useful to take this opportunity to learn LaTeX. LaTeX is a markup language used widely in computer science and mathematics. The homework assignments are typed using LaTeX and you can use the source files as templates for typesetting your solutions.

Integrity reminders

Copyright Mia Minnes, 2024, Version May 20, 2024 (1)

- Problems should be solved together, not divided up between the partners. The homework is designed to give you practice with the main concepts and techniques of the course, while getting to know and learn from your classmates.
- You may not collaborate on homework questions graded for correctness with anyone other than your group members. You may ask questions about the homework in office hours (of the instructor, TAs, and/or tutors) and on Piazza (as private notes viewable only to the Instructors). You *cannot* use any online resources about the course content other than the class material from this quarter – this is primarily to ensure that we all use consistent notation and definitions (aligned with the textbook) and also to protect the learning experience you will have when the 'aha' moments of solving the problem authentically happen.
- Do not share written solutions or partial solutions for homework with other students in the class who are not in your group. Doing so would dilute their learning experience and detract from their success in the class.

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 $p \to q$ 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 $p \to q$ is true, we can assume $\neg q$ is true and use that assumption to show $\neg p$ is true.
- **Proof by Cases**: To prove q when we know $p_1 \vee p_2$, show that $p_1 \to q$ and $p_2 \to q$.

- **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 $\neg p \to (r \wedge \neg r)$ 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. Mathematical and strong induction for properties of numbers.

   (a) (*Graded for completeness*) [1] Consider each of the following statements and attempted proofs below. Pretend you are the TA/tutor for CSE 20 and grade each of these attempts. In particular, you should give each one a score out of 5 points and justify your decisions with

[1] This 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. To demonstrate your honest effort in answering the question, we expect you to include your attempt to answer *each* part of the question. If you get stuck with your attempt, you can still demonstrate your effort by explaining where you got stuck and what you did to try to get unstuck.

specific, **actionable**, and **justified** feedback; your explanations should be convincing but brief. Here is the rubric[2] you should use:

5 points Induction proof includes correctly executed base case and recursive step (with induction hypothesis, IH, clearly and correctly defined and used). Uses clear and correct calculations and references to definitions in both steps, including using the IH, to conclude both.

4 points Induction proof includes base case and recursive step (with induction hypothesis clearly and mostly correctly defined and used), where base case attempted but incomplete OR, incorrect base element chosen but valid proof made for chosen element, OR induction hypothesis incorrectly stated but correctly used.

3 points Any one of the following: (1) Induction proof with correctly executed base case and recursive step that demonstrates connection between induction hypothesis and property being true for $n+1$, some missing or incorrect logical glue; (2) Induction proof with missing base case and correctly executed recursive step.

2 points Any one of the following: (1) Induction proof includes attempts at correct steps of an induction proof (base case, recursive step), with significant logical gaps and/or errors; (2) correctly executed base case with missing / incorrect recursive step,

1 point Demonstrates knowledge of proof techniques (e.g. attempts some proof type other than induction, but uses some proof technique correctly) and/or structure of induction argument.

i. Statement: "the sum of the first n positive odd integers is n^2"
Attempted Proof:

Base Case: $n = 1$
First odd number is 1; $1^2 = 1$. True.
$(n+1)^2 = n^2 + 2n + 1$
n^2 is the sum of the first n odd numbers, and $2n+1$ is the next odd number in the sequence, therefore $(n+1)^2 =$ the sum of the first $n+1$ odd numbers.

ii. Statement: "For every nonnegative integer n, $3|n$." (Recall that the | symbol is used to mean "divides" or "is a factor of".)
Attempted Proof:

Attempted Proof: We proceed by strong mathematical induction.
Basis step: Indeed, $3|0$ because there is an integer, namely 0 such that $0 = 3 \cdot 0$.
Induction step: Let k be arbitrary. Assume, as the strong induction hypothesis, that for all nonnegative integers j with $0 \leq j \leq k$, that $3|j$. Write $k+1 = m+n$, where m, n are integers less than $k+1$. By the induction hypothesis, $3|m$ and $3|n$. That is, there are integers a, b such that $m = 3a$ and $n = 3b$. Therefore, $k+1 = (3a) + (3b) = 3(a+b)$. We can choose $a+b$, where we know $a+b \in \mathbb{Z}$, to show that $3|(k+1)$, as required.

[2] According to the Merriam Webster definition, a **rubric** is "a guide listing specific criteria for grading or scoring academic papers, projects, or tests". For CSE 20, you can see the rubrics we use to grade assignments and exams on Gradescope: next to your submission for each question you will find the rubric items and associated point values. The highlighted items are the ones we select to describe your work; these correspond to the score assigned for the question.

(b) (*Graded for completeness*) Decide whether each statement above is true or false, give correct and complete induction proofs for the true statement(s) and disprove by counterexample for the false statement(s).

2. (*Graded for correctness*) Games and induction. The game of Nim-Var is a two-player game (which is a variant of Nim). At the start of the game, there are two piles, each containing n jelly beans (n is a positive integer). On a player's turn, that player picks one of the two piles and does **one** of the following: either

   - removes some positive number of jelly beans from that pile, **or**
   - moves some positive number of jelly beans (that is less than the current total number of jelly beans in the pile) from that pile to the other. *Note: if there is only one jelly bean left in a pile, the player cannot move this jelly bean to the other pile.*

   The player to take the last jelly bean wins. Use strong induction to prove that the second player always has a winning strategy in Nim-Move. A complete and correct solution will first identify what the strategy is, and then prove that following this strategy will lead the second player to win the game (no matter what the first player chooses to do at each turn).

3. Linked Lists. Recall the recursive definition of the set of linked lists of natural numbers (from class)

$$\begin{array}{ll} \text{Basis Step:} & [] \in L \\ \text{Recursive Step:} & \text{If } l \in L \text{ and } n \in \mathbb{N}, \text{ then } (n, l) \in L \end{array}$$

   and the definitions of the function which gives the length of a linked list of natural numbers $length : L \to \mathbb{N}$

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

   the function $append : L \times \mathbb{N} \to L$ that adds an element at the end of a linked list

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

   and the function $prepend : L \times \mathbb{N} \to L$ that adds an element at the front of a linked list

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

Sample response that can be used as reference for the detail expected in your answer: To evaluate

the result of $length(\ (4,(2,(7,[])))\ )$ we calculate:

$$
\begin{aligned}
length(\ (4,(2,(7,[])))\ ) &= 1 + length(\ (2,(7,[]))\ ) \\
&\qquad \text{using recursive step of definition of } length\text{, with } n=4, l=(2,(7,[])) \\
&= 1+1+length(\ (7,[])\ ) \\
&\qquad \text{using recursive step of definition of } length\text{, with } n=2, l=(7,[]) \\
&= 1+1+1+length(\ []\ ) \\
&\qquad \text{using recursive step of definition of } length\text{, with } n=7, l=[] \\
&= 1+1+1+0 \\
&\qquad \text{using basis step of definition of } length\text{, since input to } length \text{ is } []
\end{aligned}
$$

In this question, we'll consider the combination of these functions with a new function, one that removes the element at the front of the list (if there is any). We define $remove : L \to L$ by

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

(a) (*Graded for correctness*) What is the result of $remove(\ append(\ (prepend\ (\ (\ (10,[]),5\ )\ ),20)\ )\ )$? For full credit, include all intermediate steps with brief justifications for each.

(b) (*Graded for correctness*) Prove the statement

$$\forall l \in L\ (\ remove(prepend(\ (l,0)\ )) = l\ )$$

(c) (*Graded for correctness*) Disprove the statement

$$\forall l \in L\ (\ remove(append(\ (l,0)\ )) = l\ )$$

4. Primes, divisors, and proof strategies. For each statement below, identify the **main logical structure or connective** of the statement, list the proof strategies that could be used to prove and to disprove a statement with that structure, then identify whether the statement is true or false and justify with a proof of the statement or its negation. (*Graded for correctness of identification of logical structure and proof strategies and evaluation of statement (is it true or false?) and fair effort completeness of the proof*)

Sample response that can be used as reference for the detail expected in your answer:

Consider the statement: There is a greatest negative integer.

The main logical structure for this statement is that it is an **existential** statement, as we can see by translating it to symbols:

$$\exists g \in \mathbb{Z}^- \forall x \in \mathbb{Z}^- (g \geq x)$$

To prove an existential statement, the main proof strategy we could use is to find a witness. Proof by cases and proof by contradiction could also be used, because both can be used to prove any statement (no matter its logical structure).

To disprove an existential statement, we would need to prove its negation, which (using DeMorgan's Laws) can be written as a universal statement. Therefore, to disprove this statement the strategies we could use are universal generalization or structural induction (because $\mathbb{Z}^-$ is a recursively defined set) or proof by cases or proof by contradiction. Notice that proof by exhaustion is not possible because the domain is not finite.

The statement is true, as we can see from the witness $g = -1$, since it is in the domain $\mathbb{Z}^-$ and when we evaluate

$$\forall x \in \mathbb{Z}^-(-1 \geq x)$$

we can proceed by universal generalization and take an arbitrary negative integer x, which by definition means $x < 0$, and since x is an integer, guarantees $x \leq -1 = g$, as required.

(a) The quotient of any even number with any nonzero even number is even.

(b) There are two odd numbers (not necessarily distinct) whose sum is even.

(c) The greatest common divisor of 5 and 23 is 1 and the greatest common divisior of 7 and 19 is 1.

(d) There are two positive integers greater than 20 that have the same greatest common division with 20.