hw5-proofs-and-induction: Sample Solutions

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.

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.

Sample Solution: 3 points. Induction proof includes correctly executed base case **($n = 1$)** and connection demonstrated between induction hypothesis **(n^2 is the sum of the first n odd numbers)**, IH, and property being true for $n+1$, without clearly labelling the IH or where it's used, even thought it has relevant calculations and references to definitions such as **($2n+1$ is the next odd number in the sequence)** in both steps and (**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".)

[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.

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.

Sample Solution: 2 points. Induction proof with correctly executed base case **(**$n = 0$**)** and recursive step **(**$k+1$**)** that demonstrates connection (**rest of the proof**) between induction hypothesis and property being true for $n+1$, with significant errors (**It is not always possible to Write** $k+1 = m+n$**, where** m, n **are integers less than** $k+1$**. For example, you can't write 1 as the sum of two integers less than 1**).

(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).

Sample solution: The statement in (a) is True, and we can add some logical glue to complete the given proof.

Base Case ($n = 1$): First odd number is 1; We need to show $1^2 = 1$. $LHS = 1$, $RHS = 1$ so the equality holds.
Recursive step: Let n be an arbitrary integer greater than or equal to 1. Assume (as the IH) that n^2 is the sum of the first n odd integers, and we want to show that $(n+1)^2$ is the sum of the first $n+1$ odd integers. By multiplication: $(n+1)^2 = n^2 + 2n + 1$
In the RHS expression, by the IH, 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.

The statement in (b) is False. Consider the counterexample $n = 1$, which is a nonnegative integer so in the domain. $1 \textbf{ mod } 3 = 1 \neq 0$, so $3 \nmid 1$. Hence, the universal statement is false.

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).

Sample Solution:

Strategy for player 2: If player 1 chooses to removes k jelly beans from a pile, then we also remove k jelly beans from the opposite pile. If player 1 chooses to move jelly beans (e.g. if they move k jelly beans from pile A to pile B), then we remove $2k$ jelly beans from pile B.

Proof by strong induction: WTS: for all positive integers n, Player 2's strategy guarantees a win in the game that starts with n jellybeans in each pile.

Basis step: WTS Player 2's strategy guarantees a win when each pile starts with 1 jellybean. In this case, Player 1 has to remove the jellybean from one of the piles (because they can't take from both piles at once and they can't move jelly beans). Following the strategy, Player 2 removes the jellybean from the other pile, and wins because this is the last jellybean.

Recursive step: Let n be a positive integer. As the strong induction hypothesis, assume that Player 2's strategy guarantees a win in the games where there are $1, 2, \ldots, n$ many jellybeans in each pile at the start of the game.

WTS that Player 2's strategy guarantees a win in the game where there are $n + 1$ jellybeans in each pile at the start of the game.

In this game, the player 1's action can be categorized into these 3 cases: [moves k jelly beans from a pile to the other where $1 \leq k \leq n$; removes all $n + 1$ jelly beans from a pile; removes c jelly beans from a pile where $1 \leq c \leq n$].

Case 1: If player 1 moves k jelly beans from pile A to the other pile B where $1 \leq k \leq n$, then at this time, pile A has $n + 1 - k$ jelly beans and pile B has $n + 1 + k$ jelly beans. Based on our strategy, we will remove $2k$ jelly beans from pile B, which leaves it with $n+1+k-2k = n+1-k$ jelly beans. Since $1 \leq k \leq n$, this number $(n + 1) - k$ is also between 1 and n. Thus, at this stage of the game, the game appears identical to a new game where the two piles have an equal number of jellybeans between 1 and n. Thus, the strong induction hypothesis applies, and Player 2's strategy guarantees they win.

Case 2: If player 1 removes a whole pile of $n + 1$ jelly beans, then in their first move, Player 2 wins when following their strategy of removing the same number of jelly beans from the other pile because they remove all of the second pile, which includes the last jelly bean.

Case 3: If player 1 removes c jelly beans from a pile where $1 \leq c \leq n$, then after Player 2's first move following the strategy, the two piles have an equal number of $(n + 1) - c$ jelly beans. Since $1 \leq c \leq n$, this number $(n + 1) - c$ is also between 1 and n. Thus, at this stage of the game, the game appears identical to a new game where the two piles have an equal number of jellybeans between 1 and n. Thus, the strong induction hypothesis applies, and Player 2's strategy guarantees they win.

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

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

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

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

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

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	$append(\ (\ (n, l), m\ )\ )$	$= (n, append(\ (l, m)\ )\ )$

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:

$length(\ (4, (2, (7, [])))\ ) = 1 + length(\ (2, (7, []))\ )$
using recursive step of definition of $length$, with $n = 4, l = (2, (7, []))$
$= 1 + 1 + length(\ (7, [])\ )$
using recursive step of definition of $length$, with $n = 2, l = (7, [])$
$= 1 + 1 + 1 + length(\ []\ )$
using recursive step of definition of $length$, with $n = 7, l = []$
$= 1 + 1 + 1 + 0$
using basis step of definition of $length$, since input to $length$ is $[]$

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.

Solution: We first break down the nested functions into steps:

i. $a = (10,[])$
ii. $b = prepend\ (\ (a,5\ )\ )$
iii. $c = append(\ (b,20)\ )$
iv. $d = remove(c)$

Step 1: $b = prepend\ (\ (a,5\ )\ ) = prepend\ (\ ((10,[]),5\ )\ ) = (5,(10,[]))$

Step 2:

$$\begin{aligned} c = append(\ (b,20)\ ) &= append(\ ((5,(10,[])),20)\ ) \\ &= (5, append(\ ((10,[]),20)\ ) \\ &\text{using recursive step of definition of } append\text{, with } n=5, l=(10,[]), m=20 \\ &= (5,(10, append(\ ([],20)\ ))) \\ &\text{using recursive step of definition of } append\text{, with } n=10, l=[], m=20 \\ &= (5,(10,(20,[]))) \\ &\text{using basis step of definition of } append\text{, since input } m \text{ to } append \text{ is } 20 \end{aligned}$$

Step 3:

$$\begin{aligned} d = remove(c) &= remove((5,(10,(20,[])))) \\ &= (10,(20,[])) \\ &\text{using recursive step of definition of } remove\text{, with } l=(10,(20,[])), n=5 \end{aligned}$$

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

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

Sample Solution:

Proof by universal generalization: Let l be an arbitrary linked list $\in L$. By the definition of prepend, $prepend((l,0)) = (0,l)$. Since $(0,l) \neq []$, $remove((0,l))$ will fall into the recursive step and will result in l using recursive step of definition of remove, with $l = l, n = 0$. Now we have shown that for any arbitrary $l \in L$, $remove(prepend(\ (l,0)\ )) = l$. Hence, $\forall l \in L\ (\ remove(prepend(\ (l,0)\ )) = l\ )$.

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

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

Sample Solution:

Consider the counterexample $l = (1, [])$, which is in L by applying the recursive step in the definition of L once. Now we evaluate $append(\ (l, 0)\ ) = append(\ ((1, []), 0)\ ) = (1, append(\ ([], 0)\ )) = (1, (0, []))$ by applying the recursive step once (with $n = 1, l = [], m = 0$) and the basis step once in the definition of function append. Now we evaluate $remove(append(\ (l, 0)\ )) = remove((1, (0, []))) = (0, [])$ by applying the recursive step once (with $l = (0, []), n = 1$) in the definition of function remove. Since $remove(append(\ (l, 0)\ )) = (0, []) \neq (1, []) = l$, the universal statement is false.

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.

Solution:

The key word for the logical structure for this statement is "any", which means that it is an **universal** statement, as we can see by translating it to symbols:

$$\forall even\ e \quad \forall even\ f \neq 0\ (e\ \mathbf{div}\ f \text{ is even})$$

To prove an universal statement, the proof strategies we could use are universal generalization or structural induction (because the set of even numbers can be recursively defined by putting the element 0 in the set in the base case and then, in the recursive step, adding 2 or subtracting 2 to existing elements to get new elements) or proof by cases or proof by contradiction. Notice that proof by exhaustion is not possible because the domain is not finite.

To disprove an universal statement, main proof strategy we could use is to find a counterexample. We can also apply DeMorgan's Laws to write the negation as an existential statement and use strategies (like finding witness or prove by cases) to prove it.

The statement is false, as we can see from the counterexample $e = 2$, since it is even and when we evaluate

$$\forall even\ f \neq 0\ (2\ \textbf{div}\ f \text{ is even})$$

we can proceed again by counterexample $f = 2$, since it is even and nonzero and when we evaluate

$$e\ \textbf{div}\ f = 1 \textbf{ which is not even}$$

Hence, we used $f = 2$ to disprove $\forall even\ f \neq 0\ (2\ \textbf{div}\ f \text{ is even})$, and we used $e = 2$ to disprove $\forall even\ e \quad \forall even\ f \neq 0\ (e\ \textbf{div}\ f \text{ is even})$.

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

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

$$\exists odd\ x \quad \exists odd\ y\ (x + y \text{ is even})$$

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 the set of odd numbers can also be recursively defined) 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 $x = 1$, since it is an odd number and when we evaluate

$$\exists odd\ y\ (1 + y \text{ is even})$$

we can proceed by finding a witness for y. Take $y = 1$, since it is an odd number and when we evaluate

$$1 + 1 = 2 \text{ is even}$$

Hence, we used $y = 1$ to prove $\exists odd\ y\ (1 + y \text{ is even})$, and we used $x = 1$ to prove $\exists odd\ x \quad \exists odd\ y\ (x + y \text{ is even})$.

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

Solution: The main logical structure for this statement is "and", which means that it is a **conjunction**, as we can see by translating it to symbols:

$$(gcd((5, 23)) = 1) \wedge (gcd((7, 19)) = 1)$$

To prove a conjunction, the proof strategy we could use is to prove each of its components as a subgoal. To prove that $p \wedge q$ is true, have two subgoals: subgoal (1) prove p is true; and, subgoal (2) prove q is true. We could also use proof by cases or proof by contradiction.

To disprove a conjunction, main proof strategy is to disprove one of its components. 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.

The statement is **true**. We have two subgoals to prove:

(1) WTS: $(gcd((5, 23)) = 1)$. **Proof:** The positive factors of 5 are 1 and 5, and the positive factors of 23 are 1 and 23. Hence, the greatest common factor is 1.

(2) WTS: $(gcd((7, 19)) = 1)$. **Proof:** The positive factors of 7 are 1 and 7, and the positive factors of 19 are 1 and 19. Hence, the greatest common factor is 1.

Since we have proved both subgoals, the conjunction is true.

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

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

$$\exists x \in \mathbb{Z}^+ \quad \exists y \in \mathbb{Z}^+ \ (gcd((20, x)) = gcd((20, y)))$$

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 the set of odd numbers can also be recursively defined) 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**, and the theorem we can use is "For any positive integers a, b, if a divides b then $gcd((a, b)) = a$". If we choose witness $x = 40$, since it is a positive integer and when we evaluate

$$\exists y \in \mathbb{Z}^+ \ (gcd((20, 40)) = gcd((20, y)))$$

we can first evaluate $gcd((20,40))$, and it equals 20 as 20 divides 40. We can then proceed by finding a witness for y. Take $y = 60$, since it is a positive integer and when we evaluate

$$gcd((20,60))$$

it equals 20 as 20 divides 60. So $gcd((20,40)) = gcd((20,y)) = 20$.

Hence, we used $y = 60$ to prove $\exists y \in \mathbb{Z}^+ \ (gcd((20,40)) = gcd((20,y)))$, and we used $x = 40$ to prove $\exists x \in \mathbb{Z}^+ \quad \exists y \in \mathbb{Z}^+ \ (gcd((20,x)) = gcd((20,y)))$.