CSE 311: Foundations of Computing I

Section 6: Induction, Midterm Review Solutions

1. Find the Bug!

Did you know that all dogs are named Dubs? Let's prove it by induction. The key is talking about groups of dogs, where every dog has the same name.

Let $P(i)$ mean "all groups of i dogs have the same name." We prove $\forall n\, P(n)$ by induction on n.

Base Case: $P(1)$ Take an arbitrary group of one dog, all dogs in that group all have the same name (there's only the one, so it has the same name as itself).

Inductive Hypothesis: Suppose $P(k)$ holds for some arbitrary k.

Inductive Step: Consider an arbitrary group of $k+1$ dogs. Arbitrarily select a dog, D, and remove it from the group. What remains is a group of k dogs. By inductive hypothesis, all k of those dogs have the same name. Add D back to the group, and remove some other dog D'. We have a (different) group of k dogs, so the inductive hypothesis applies again, and every dog in that group also shares the same name. All $k+1$ dogs appeared in at least one of the two groups, and our groups overlapped, so all of our $k+1$ dogs have the same name, as required.

Conclusion: We conclude $P(n)$ holds for all n by the principle of induction.

Recalling that Dubs is a dog, we have that every dog must have the same name as him, so every dog is named Dubs.

This proof cannot be correct (the proposed claim is false). Where is the bug?

Solution:

The bug is in the final sentence of the inductive step. We claimed that the groups overlapped, i.e. that some dog was in both of them. That's true for large k, but not when $k+1=2$. When $k=2$, D is in a group by itself, and D' was in a group by itself. The inductive hypothesis holds (D has the only name in its subgroup, and D' has the only name in its subgroup) but returning to the full group $\{D, D'\}$ we cannot conclude that they share a name.

From there everything unravels. $P(1) \not\to P(2)$, so we cannot use the principle of induction. It turns out this is the **only** bug in the proof. The argument in the inductive step is correct as long as $k+1>2$. But that implication is always vacuous, since $P(2)$ is false.

2. Cantelli's Rabbits

Xavier Cantelli owns some rabbits. The number of rabbits he has in any given year is described by the function f:

$$f(0) = 0$$
$$f(1) = 1$$
$$f(n) = 2f(n-1) - f(n-2) \text{ for } n \geq 2$$

Determine, with proof, the number, $f(n)$, of rabbits that Cantelli owns in year n. That is, construct a formula for $f(n)$ and prove its correctness.

Solution:

Let $P(n)$ be "$f(n) = n$". We prove that $P(n)$ is true for all $n \in \mathbb{N}$ by strong induction.

Base Cases $(n = 0, n = 1)$**:** $f(0) = 0$ and $f(1) = 1$ by definition.

Inductive Hypothesis: Assume that $P(0) \wedge P(1) \wedge \dots P(k)$ hold for some arbitrary $k \geq 1$.

Inductive Step: We show $P(k+1)$:

$$\begin{aligned} f(k+1) &= 2f(k) - f(k-1) && \text{[Definition of } f\text{]} \\ &= 2(k) - (k-1) && \text{[Inductive Hypothesis]} \\ &= k+1 && \text{[Algebra]} \end{aligned}$$

Conclusion: $P(n)$ is true for all $n \in \mathbb{N}$ by principle of strong induction.

3. Snack Induction

You want to buy snacks for a party you're throwing. However, the local grocery store only sells snacks in packs of 5 and packs of 7.

Prove that you can buy exactly n snacks for all integers $n \geq 24$.

Solution:

Let P(n) be the statement "You can buy n snacks with packs of 5 and packs of 7 snacks". We prove that P(n) holds for all $n \geq 24$ by strong induction.

Base Case:

n = 24: 24 snacks can be bought with 2 packs of 7 and 2 packs of 5 snacks.

n = 25: 25 snacks can be bought with 5 packs of 5 snacks.

n = 26: 26 snacks can be bought with 3 packs of 7 and 1 pack of 5 snacks.

n = 27: 27 snacks can be bought with 1 pack of 7 and 4 packs of 5 snacks.

n = 28: 28 snacks can be bought with 4 packs of 7 snacks.

Inductive Hypothesis: Suppose that P$(24) \wedge$ P$(25) \wedge \cdots \wedge$ P(k) is true for some arbitrary $k \geq 28$.

Inductive Step: We want to show that you can buy exactly $k+1$ snacks. By the inductive hypothesis, we know that you can buy exactly $k-4$ snacks, so you can buy another pack of 5 to get exactly $k+1$ snacks.

Conclusion: Therefore, P(n) holds for all integers $n \geq 24$ by the principle of strong induction.

4. Midterm Review: Translation

Let your domain of discourse be all coffee drinks. You should use the following predicates:

- Soy(x) is true iff x contains soy milk.
- Whole(x) is true iff x contains whole milk.
- Sugar(x) is true iff x contains sugar
- Decaf(x) is true iff x is not caffeinated.
- Vegan(x) is true iff x is vegan.
- CadeLikes(x) is true iff Cade likes the drink x.
- RobertLikes(x) is true iff Robert likes the drink x.

Translate each of the following statements into predicate logic. You may use quantifiers, the predicates above, and usual math connectors like $=$ and $\neq$.

(a) Coffee drinks with whole milk are not vegan.

Solution:

$\forall x(\text{Whole}(x) \to \neg\text{Vegan}(x))$.

(b) Robert only likes one coffee drink, and that drink is not vegan.

Solution:

$\exists x(\text{RobertLikes}(x) \wedge \neg\text{Vegan}(x) \wedge \forall y[\text{RobertLikes}(y) \to (x = y)])$

OR $\exists x(\text{RobertLikes}(x) \wedge \neg\text{Vegan}(x) \wedge \forall y[(x \neq y) \to \neg\text{RobertLikes}(y)])$

(c) Unless a drink has whole milk and sugar, Robert won't like it.

Solution:

$\forall x(\neg(\text{Whole}(x) \wedge \text{Sugar}(x)) \to \neg\text{RobertLikes}(x))$

(d) Every decaf drink that Cade likes has sugar.

Solution:

$\forall x([\text{Decaf}(x) \wedge \text{CadeLikes}(x)] \to \text{Sugar}(x))$

5. Midterm Review: Number Theory

(a) Prove that for all integers x and all integers $p > 1$, if $x \equiv_p 1$, then $x^2 \equiv_p 1$. Try to prove this directly by definitions, instead of using modular arithmetic properties!

Hint: Recall that $(x-1)(x+1) = x^2 - 1$.

Solution:

Let x and $p > 1$ be arbitrary integers. Suppose $x \equiv_p 1$. By the definition of congruence, $p \mid (x-1)$. Therefore, by the definition of divides, there exists an integer k such that

$$pk = (x-1)$$

By multiplying both sides of $pk = (x-1)$ by $(x+1)$ and re-arranging the equation, we have:

$$pk(x+1) = (x-1)(x+1)$$
$$pk(x+1) = x^2 - 1$$

Since k and x are integers, $k(x+1)$ is also an integer. Therefore, by the definition of divides $p \mid x^2 - 1$. Hence, by the definition of congruence, $x^2 \equiv_p 1$. Since x, p were arbitrary, the claim holds.

(b) Now prove that for all integers x and all **prime** integers p, if $x^2 \equiv_p 1$, then $x \equiv_p 1$ or $x \equiv_p -1$.

Hint: You may the following theorem without proof: if p is prime and $p \mid (ab)$ then $p \mid a$ or $p \mid b$.

Solution:

Let x and p be arbitrary integers. Suppose p is prime and $x^2 \equiv_p 1$. By the definition of congruence, $p \mid (x^2 - 1)$. Since $(x-1)(x+1) = x^2 - 1$, we have $p \mid (x-1)(x+1)$.

By the given fact above, that for a prime integer p such that $p \mid (ab)$, then $p \mid a$ or $p \mid b$. In this case, since p is prime, by applying the fact, we have $p \mid (x-1)$ or $p \mid (x+1)$. Then by the definition of congruence, we have $x \equiv_p 1$ or $x \equiv_p -1$.

(c) We showed in part (b) that if x, p are integers and p is prime, then $x^2 \equiv_p 1$, then $x \equiv_p 1$ or $x \equiv_p -1$. Prove that this claim does not always hold for integers $p > 1$ when p is **not prime**.

Solution:

Consider $p = 8$ and $x = 5$. Then $x^2 \equiv_8 25 \equiv_8 1$. However $x \equiv_8 5$, so $x \not\equiv_8 1$ and $x \not\equiv_8 -1$.

6. Midterm Review: Set Theory

(a) Prove or disprove: For all sets A, B, C if $A \cap C = B \cap C$ then $A = B$.

Solution:

This claim is false. Consider $A = \{1\}$, $B = \{2\}$, and $C = \varnothing$. Then $A \cap C = \varnothing = B \cap C$, but $A \neq B$.

(b) Prove or disprove: For all sets A, B, C if $A \cup C = B \cup C$ then $A = B$.

Solution:

This claim is false. Consider $A = \{1\}$, $B = \{2\}$, and $C = \{1, 2\}$. Then $A \cup C = \{1, 2\} = B \cup C$, but $A \neq B$.

(c) Prove or disprove: For all sets A, B, C if $A \cup C = B \cup C$ and $A \cap C = B \cap C$ then $A = B$.

Solution:

This claim is true. Let sets A, B, C be arbitrary, and suppose that $A \cup C = B \cup C$ and $A \cap C = B \cap C$. We prove by two subset proofs.

$\subseteq$: We aim to show that $A \subseteq B$. Let $x \in A$ be arbitrary.
Case 1: $x \in A$ and $x \in C$. Then by definition of intersection, $x \in A \cap C$. Since $A \cap C = B \cap C$, $x \in B \cap C$. Then by definition of intersection, $x \in B$ and $x \in C$. So $x \in B$. Since x was arbitrary, $A \subseteq B$.
Case 2: $x \in A$ and $x \notin C$. Since $x \in A$, by definition of union, $x \in A \cup C$. Since $A \cup C = B \cup C$, $x \in B \cup C$. Then by definition of union, $x \in B$ or $x \in C$. But since $x \notin C$, we have $x \in B$. Since x was arbitrary, $A \subseteq B$.
Thus in all cases $A \subseteq B$.

$\supseteq$: Now we aim to show that $B \subseteq A$. This argument follows similarly to the previous, since the setup is symmetric.

Thus we have shown that $A \subseteq B$ and $B \subseteq A$, so $A = B$, as desired. Since A, B, C were arbitrary, the claim holds.

7. Midterm Review: Induction

For any $n \in \mathbb{N}$, define S_n to be the sum of the squares of the first n positive integers, or

$$S_n = 1^2 + 2^2 + \cdots + n^2.$$

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Solution:

Let $\mathsf{P}(n)$ be the statement "$S_n = \frac{1}{6}n(n+1)(2n+1)$" defined for all $n \in \mathbb{N}$. We prove that $\mathsf{P}(n)$ is true for all $n \in \mathbb{N}$ by induction on n.

Base Case: When $n = 0$, we know the sum of the squares of the first n positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)((2)(0)+1) = 0$, we know that $\mathsf{P}(0)$ is true.

Inductive Hypothesis: Suppose that $\mathsf{P}(k)$ is true for some arbitrary $k \in \mathbb{N}$. That is, $S_k = \frac{1}{6}k(k+1)(2k+1)$.

Inductive Step: Examining S_{k+1}, we see that

$$S_{k+1} = 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = S_k + (k+1)^2.$$

By the inductive hypothesis, we know that $S_k = \frac{1}{6}k(k+1)(2k+1)$. Therefore, we can substitute and rewrite the expression as follows:

$$\begin{aligned}
S_{k+1} &= S_k + (k+1)^2 \\
&= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \\
&= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right) \\
&= \frac{1}{6}(k+1)\left(k(2k+1) + 6(k+1)\right) \\
&= \frac{1}{6}(k+1)\left(2k^2 + 7k + 6\right) \\
&= \frac{1}{6}(k+1)(k+2)(2k+3) \\
&= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}$$

Thus, we can conclude that $\mathsf{P}(k+1)$ is true.

Conclusion: $P(n)$ holds for all integers $n \geq 0$ by the principle of induction.