Section 07: Solutions

1. Structural Induction

(a) Consider the following recursive definition of strings.

Basis Step: `""` is a string

Recursive Step: If X is a string and c is a character then $\mathsf{append}(c, X)$ is a string.

Recall the following recursive definition of the function len:

$$\begin{aligned} \mathsf{len}(\texttt{""}) &= 0 \\ \mathsf{len}(\mathsf{append}(c, X)) &= 1 + \mathsf{len}(X) \end{aligned}$$

Now, consider the following recursive definition:

$$\begin{aligned} \mathsf{double}(\texttt{""}) &= \texttt{""} \\ \mathsf{double}(\mathsf{append}(c, X)) &= \mathsf{append}(c, \mathsf{append}(c, \mathsf{double}(X))). \end{aligned}$$

Prove that for any string X, $\mathsf{len}(\mathsf{double}(X)) = 2\mathsf{len}(X)$.

Solution:

For a string X, let $\mathsf{P}(X)$ be "$\mathsf{len}(\mathsf{double}(X)) = 2\mathsf{len}(X)$". We prove $\mathsf{P}(X)$ for all strings X by structural induction on X.

Base Case (X = `""`): By definition, $\mathsf{len}(\mathsf{double}(\texttt{""})) = \mathsf{len}(\texttt{""}) = 0 = 2 \cdot 0 = 2\mathsf{len}(\texttt{""})$, so $\mathsf{P}(\texttt{""})$ holds

Inductive Hypothesis: Suppose $\mathsf{P}(X)$ holds for some arbitrary string X.

Inductive Step: $\boxed{\text{Goal: Show that } \mathsf{P}(\mathsf{append}(c, X)) \text{ holds for any character } c.}$

$$\begin{aligned} \mathsf{len}(\mathsf{double}(\mathsf{append}(c, X))) &= \mathsf{len}(\mathsf{append}(c, \mathsf{append}(c, \mathsf{double}(X)))) && \text{[By Definition of double]} \\ &= 1 + \mathsf{len}(\mathsf{append}(c, \mathsf{double}(X))) && \text{[By Definition of len]} \\ &= 1 + 1 + \mathsf{len}(\mathsf{double}(X)) && \text{[By Definition of len]} \\ &= 2 + 2\mathsf{len}(X) && \text{[By IH]} \\ &= 2(1 + \mathsf{len}(X)) && \text{[Algebra]} \\ &= 2(\mathsf{len}(\mathsf{append}(c, X))) && \text{[By Definition of len]} \end{aligned}$$

This proves $\mathsf{P}(\mathsf{append}(c, X))$.

Conclusion: $\mathsf{P}(X)$ holds for all strings X by structural induction.

(b) Consider the following definition of a (binary) **Tree**:

Basis Step: $\bullet$ is a **Tree**.

Recursive Step: If L is a **Tree** and R is a **Tree** then $\texttt{Tree}(\bullet, L, R)$ is a **Tree**.

The function leaves returns the number of leaves of a **Tree**. It is defined as follows:

$$\begin{aligned} \mathsf{leaves}(\bullet) &= 1 \\ \mathsf{leaves}(\texttt{Tree}(\bullet, L, R)) &= \mathsf{leaves}(L) + \mathsf{leaves}(R) \end{aligned}$$

Also, recall the definition of size on trees:

$$\begin{aligned} \mathsf{size}(\bullet) &= 1 \\ \mathsf{size}(\texttt{Tree}(\bullet, L, R)) &= 1 + \mathsf{size}(L) + \mathsf{size}(R) \end{aligned}$$

Prove that $\mathsf{leaves}(T) \geq \mathsf{size}(T)/2 + 1/2$ for all Trees T.

Solution:

For a tree T, let P be $\mathsf{leaves}(T) \geq \mathsf{size}(T)/2 + 1/2$. We prove P for all trees T by structural induction on T.

Base Case (T = •): By definition of $\mathsf{leaves}(\bullet)$, $\mathsf{leaves}(\bullet) = 1$ and $\mathsf{size}(\bullet) = 1$. So, $\mathsf{leaves}(\bullet) = 1 \geq 1/2 + 1/2 = \mathsf{size}(\bullet)/2 + 1/2$, so $\mathsf{P}(\bullet)$ holds.

Inductive Hypothesis: Suppose $\mathsf{P}(L)$ and $\mathsf{P}(R)$ hold for some arbitrary trees L, R.

Inductive Step: $\boxed{\text{Goal: Show that } \mathsf{P}(\texttt{Tree}(\bullet, L, R)) \text{ holds.}}$

$$\begin{aligned} \mathsf{leaves}(\texttt{Tree}(\bullet, L, R)) &= \mathsf{leaves}(L) + \mathsf{leaves}(R) && \text{[By Definition of leaves]} \\ &\geq (\mathsf{size}(L)/2 + 1/2) + (\mathsf{size}(R)/2 + 1/2) && \text{[By IH]} \\ &= (1/2 + \mathsf{size}(L)/2 + \mathsf{size}(R)/2) + 1/2 && \text{[By Algebra]} \\ &= \frac{1 + \mathsf{size}(L) + \mathsf{size}(R)}{2} + 1/2 && \text{[By Algebra]} \\ &= \mathsf{size}(T)/2 + 1/2 && \text{[By Definition of size]} \end{aligned}$$

This proves $\mathsf{P}(\texttt{Tree}(\bullet, L, R))$.

Conclusion: Thus, $\mathsf{P}(T)$ holds for all trees T by structural induction.

(c) Prove the previous claim using strong induction. Define $P(n)$ as "all trees T of size n satisfy $\mathsf{leaves}(T) \geq \mathsf{size}(T)/2 + 1/2$". You may use the following facts:

- For any tree T we have $\mathsf{size}(T) \geq 1$.
- For any tree T, $\mathsf{size}(T) = 1$ if and only if $T = \bullet$.

If we wanted to prove these claims, we could do so by structural induction.

Note, in the inductive step you should start by letting T be an arbitrary tree of size $k + 1$.

Solution:

Let $P(n)$ be "all trees T of size n satisfy $\mathsf{leaves}(T) \geq \mathsf{size}(T)/2 + 1/2$". We show $P(n)$ for all integers $n \geq 1$ by strong induction on n.

Base Case: Let T be an arbitrary tree of size 1. The only tree with size 1 is $\bullet$, so $T = \bullet$. By definition, $\mathsf{leaves}(T) = \mathsf{leaves}(\bullet) = 1$ and thus $\mathsf{size}(T) = 1 = 1/2 + 1/2 = \mathsf{size}(T)/2 + 1/2$. This shows the base case holds.

Inductive Hypothesis: Suppose that $P(j)$ holds for all integers $j = 1, 2, \ldots, k$ for some arbitrary integer $k \geq 1$.

Inductive Step: Let T be an arbitrary tree of size $k + 1$. Since $k + 1 > 1$, we must have $T \neq \bullet$. It follows from the definition of a tree that $T = \texttt{Tree}(\bullet, L, R)$ for some trees L and R. By definition, we have $\mathsf{size}(T) = 1 + \mathsf{size}(L) + \mathsf{size}(R)$. Since sizes are non-negative, this equation shows $\mathsf{size}(T) > \mathsf{size}(L)$ and $\mathsf{size}(T) > \mathsf{size}(R)$ meaning we can apply the inductive hypothesis. This says that $\mathsf{leaves}(L) \geq \mathsf{size}(L)/2 + 1/2$ and $\mathsf{leaves}(R) \geq \mathsf{size}(R)/2 + 1/2$.

We have,

$$\begin{aligned}
\mathsf{leaves}(T) &= \mathsf{leaves}(\texttt{Tree}(\bullet, L, R)) \\
&= \mathsf{leaves}(L) + \mathsf{leaves}(R) && \text{[By Definition of } \mathsf{leaves}\text{]} \\
&\geq (\mathsf{size}(L)/2 + 1/2) + (\mathsf{size}(R)/2 + 1/2) && \text{[By IH]} \\
&= (1/2 + \mathsf{size}(L)/2 + \mathsf{size}(R)/2) + 1/2 && \text{[By Algebra]} \\
&= \frac{1 + \mathsf{size}(L) + \mathsf{size}(R)}{2} + 1/2 && \text{[By Algebra]} \\
&= \mathsf{size}(T)/2 + 1/2 && \text{[By Definition of } \mathsf{size}\text{]}
\end{aligned}$$

This shows $P(k+1)$.

Conclusion: $P(n)$ holds for all integers $n \geq 1$ by the principle of strong induction.

Note, this proves the claim for all trees because every tree T has some size $s \geq 1$. Then $P(s)$ says that all trees of size s satisfy the claim, including T.

2. Midterm Review: Translation

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

- $\texttt{soy}(x)$ is true iff x contains soy milk.
- $\texttt{whole}(x)$ is true iff x contains whole milk.
- $\texttt{sugar}(x)$ is true iff x contains sugar
- $\texttt{decaf}(x)$ is true iff x is not caffeinated.
- $\texttt{vegan}(x)$ is true iff x is vegan.
- $\texttt{RobbieLikes}(x)$ is true iff Robbie 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:**

$\forall x(\texttt{whole}(x) \rightarrow \neg\,\texttt{vegan}(x))$.

(b) Robbie only likes one coffee drink, and that drink is not vegan. **Solution:**

$\exists x \forall y(\texttt{RobbieLikes}(x) \wedge \neg\,\texttt{Vegan}(x) \wedge [\texttt{RobbieLikes}(y) \rightarrow x = y])$

OR $\exists x(\texttt{RobbieLikes}(x) \wedge \neg\,\texttt{Vegan}(x) \wedge \forall y[\texttt{RobbieLikes}(y) \rightarrow x = y])$

(c) There is a drink that has both sugar and soy milk. **Solution:**

$\exists x(\texttt{sugar}(x) \wedge \texttt{soy}(x))$

Translate the following symbolic logic statement into a (natural) English sentence. Take advantage of domain restriction.

$$\forall x([\texttt{decaf}(x) \wedge \texttt{RobbieLikes}(x)] \rightarrow \texttt{sugar}(x))$$

Solution:

Every decaf drink that Robbie likes has sugar.

Statements like "For every decaf drink, if Robbie likes it then it has sugar" are equivalent, but only partially take advantage of domain restriction.

3. Midterm Review: Number Theory

Let p be a prime number at least 3, and let x be an integer such that $x^2\%p = 1$.

(a) Show that if an integer y satisfies $y \equiv 1 \pmod{p}$, then $y^2 \equiv 1 \pmod{p}$. (this proof will be short!) (Try to do this without using the theorem "Raising Congruences To A Power")

Solution:

Let y be an arbitrary integer and suppose $y \equiv 1 \pmod{p}$. We can multiply congruences, so multiplying this congruence by itself we get $y^2 \equiv 1^2 \pmod{p}$. Since y is arbitrary, the claim holds.

(b) Repeat part (a), but don't use any theorems from the Number Theory Reference Sheet. That is, show the claim directly from the definitions.

Solution:

Suppose $x \equiv 1 \pmod{p}$. By the definition of Congruences, $p \mid (x-1)$. 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

$$pk(x+1) = (x-1)(x+1)$$
$$p(k(x+1)) = (x-1)(x+1)$$

Since $(x-1)(x+1) = x^2-1$, by replacing $(x-1)(x+1)$ with x^2-1, we have

$$p(k(x+1)) = x^2 - 1$$

Note that 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 Congruences, $x^2 \equiv 1 \pmod{p}$.

(c) From part (a), we can see that $x\%p$ can equal 1. Show that for any integer x, if $x^2 \equiv 1 \pmod{p}$, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. That is, show that the only value $x\%p$ can take other than 1 is $p-1$.
Hint: Suppose you have an x such that $x^2 \equiv 1 \pmod{p}$ and use the fact that $x^2 - 1 = (x-1)(x+1)$
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:

Suppose $x^2 \equiv 1 \pmod{p}$. By the definition of Congruences,

$$p \mid x^2 - 1$$

Since $(x-1)(x+1) = x^2 - 1$, by replacing $x^2 - 1$ with $(x-1)(x+1)$, we have

$$p \mid (x-1)(x+1)$$

Note that for an integer p if p is a prime number and $p \mid (ab)$, then $p \mid a$ or $p \mid b$. In this case, since p is a prime number, by applying the rule, we have $p \mid (x-1)$ or $p \mid (x+1)$.
Therefore, by the definition of Congruences, we have $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

4. 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 $k \in \mathbb{N}$.

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