Problem Set 13: Structural Induction

CS/MATH 113 Discrete Mathematics

Spring 2024

Each of the problems below is similar in some way to some worked example in the corresponding section of the book. You have already gone over them as part of the reading for the lectures. Revisiting them will help to clarify any issues.

1. For the set, S, defined below, provide a formula for its elements and then prove it using structural induction.

   - Basis: $0 \in S$
   - Induction: If $n \in S$, then $2n + 1 \in S$.

   Solution:

   Proof. We claim that $n \in S$ if and only if $n = 2^k - 1$ for some $k \in \mathbb{N}$. We will prove this claim by structural induction.

   Basis: $0 = 2^0 - 1$.

   Induction: Suppose $n = 2^k - 1$ for some $k \in \mathbb{N}$. Then $2n + 1 = 2(2^k - 1) + 1 = 2^{k+1} - 2 + 1 = 2^{k+1} - 1$. Thus, $2n + 1 = 2^{k+1} - 1$.

   By structural induction, we have shown that $n \in S$ if and only if $n = 2^k - 1$ for some $k \in \mathbb{N}$. □

2. Let λ denote the empty string. Let A be any finite nonempty set. A *palindrome* over A can be defined as a string that reads the same forward as backward. For example, "mom" and "dad" are palindromes over the English alphabet.

   Consider the set, S, defined as follows:

   - Basis: $\lambda \in S$ and $\forall a \in A(a \in S)$
   - Induction: $\forall a \in A \forall x \in S(axa \in S)$

   Prove, using structural induction where appropriate, that S equals the set of all palindromes over A.

   Recall that a set-equality proof requires to show that both sides are subsets of each other. That is, you will have to show that an element of S is a palindrome over A, and that any palindrome over A is present in S.

Solution:

Proof. We claim that S is the set of all palindromes over A. We will prove this claim by structural induction.

Basis: λ is a palindrome over A.

Induction: Suppose $a \in A$ and $x \in S$ is a palindrome over A. Then axa is a palindrome over A.

By structural induction, we have shown that S is the set of all palindromes over A. Now we will show that any palindrome over A is in S.

Basis: Any palindrome of length 0 is λ, which is in S.

Induction: Suppose p is a palindrome over A of length n. Then $p = axa$ for some $a \in A$ and x is a palindrome over A of length $n-2$. By the induction hypothesis, $x \in S$. By the induction step, $axa \in S$.

By structural induction, we have shown that any palindrome over A is in S. □

3. Let $a, b, c \in \mathbb{Z}$ such that $c \mid a$ and $c \mid b$. We recursively define G, which is a set of ordered pairs of integers, i.e., $G \subseteq \mathbb{Z}^2$, as follows.

   - Basis: $(a, b) \in G$.
   - Induction: If $(u, v) \in G$, then $(u, v-u) \in G$ and $(u-v, v) \in G$.

   Prove that for any $(x, y) \in G$, $c|x$ and $c|y$.

Solution:

Proof. We claim that for any $(x, y) \in G$, $c|x$ and $c|y$. We will prove this claim by structural induction.

Basis: $(a, b) \in G$, so $c|a$ and $c|b$.

Induction: Suppose $(u, v) \in G$ such that $c|u$ and $c|v$. Then $(u, v-u) \in G$ and $(u-v, v) \in G$. By the induction hypothesis, $c|u$ and $c|(v-u)$, so $c|v$. Similarly, $c|(u-v)$ and $c|v$, so $c|u$.

By structural induction, we have shown that for any $(x, y) \in G$, $c|x$ and $c|y$. □

4. Let set S be a set of strings over a's and b's defined recursively as follows:

   1. $a \in S$, $b \in S$.
   2. If $\mu \in S$ and $\nu \in S$, then $\mu\nu \in S$.

   We also recursively define the reverse operation, R, on S as:

   1. $R(a) = a$, and $R(b) = b$.
   2. If $\mu \in S$, then $R(a\mu) = R(\mu)a$, and $R(b\mu) = R(\mu)b$.

Prove by structural induction that for all $\mu, \nu \in S$,

$$R(\mu\nu) = R(\nu)R(\mu).$$

Solution:

Proof. We claim that for all $\mu, \nu \in S$, $R(\mu\nu) = R(\nu)R(\mu)$. We will prove this claim by structural induction.

Basis: If $\mu = a$ and $\nu = a$, then $R(\mu\nu) = R(aa) = a$ and $R(\nu)R(\mu) = aa = a$. If $\mu = a$ and $\nu = b$, then $R(\mu\nu) = R(ab) = ba$ and $R(\nu)R(\mu) = ba = ba$. If $\mu = b$ and $\nu = a$, then $R(\mu\nu) = R(ba) = ab$ and $R(\nu)R(\mu) = ab = ab$. If $\mu = b$ and $\nu = b$, then $R(\mu\nu) = R(bb) = b$ and $R(\nu)R(\mu) = bb = b$.

Induction: Suppose $\mu, \nu \in S$ such that $R(\mu\nu) = R(\nu)R(\mu)$. Then $R(\mu\nu a) = R(a\mu\nu) = R(\nu a)R(\mu) = R(\nu)R(a\mu) = R(\nu)R(\mu a) = R(\nu\mu a)$. Similarly, $R(\mu\nu b) = R(b\mu\nu) = R(\nu b)R(\mu) = R(\nu)R(b\mu) = R(\nu)R(\mu b) = R(\nu\mu b)$.

By structural induction, we have shown that for all $\mu, \nu \in S$, $R(\mu\nu) = R(\nu)R(\mu)$. □