COMPSCI/SFWRENG 2FA3

Discrete Mathematics with Applications II

Winter 2020

Assignment 2 with Solutions

Dr. William M. Farmer

McMaster University

Revised: February 1, 2020

Assignment 2 consists of two problems. You must write your solutions to the problems using LaTeX.

Please submit Assignment 2 as two files, `Assignment_2_`*`YourMacID`*`.tex` and `Assignment_2_`*`YourMacID`*`.pdf`, to the Assignment 2 folder on Avenue under Assessments/Assignments. *`YourMacID`* must be your personal MacID (written without capitalization). The `Assignment_2_`*`YourMacID`*`.tex` file is a copy of the LaTeX source file for this assignment (`Assignment_2.tex` found on Avenue under Contents/Assignments) with your solution entered after each problem. The `Assignment_2_`*`YourMacID`*`.pdf` is the PDF output produced by executing

```
pdflatex Assignment_2_YourMacID
```

This assignment is due **Sunday, February 2, 2020 before midnight.** You are allow to submit the assignment multiple times, but only the last submission will be marked. **Late submissions and files that are not named exactly as specified above will not be accepted!** It is suggested that you submit your preliminary `Assignment_2_`*`YourMacID`*`.tex` and `Assignment_2_`*`YourMacID`*`.pdf` files well before the deadline so that your mark is not zero if, e.g., your computer fails at 11:50 PM on February 2.

Although you are allowed to receive help from the instructional staff and other students, your submission must be your own work. Copying will be treated as academic dishonesty! If any of the ideas used in your submission were obtained from other students or sources outside of the lectures and tutorials, you must acknowledge where or from whom these ideas were obtained.

Problems

1. **[10 points]** Let C be a set of *coefficients* closed under addition and multiplication such as the integers $\mathbb{Z}$, the rational numbers $\mathbb{Q}$, or the real numbers $\mathbb{R}$. A *polynomial over* C is a mathematical expression that is constructed from an *indeterminant* x and members of C by applying addition $(+)$ and multiplication $(*)$ operators. For example, $x*((2*x)+3)$ is a polynomial over $\mathbb{Z}$. Let P be the set of polynomials over some C. The *value of a polynomial* $p \in P$ *at* $c \in C$ is the result of replacing the indeterminant x with c. For example, the value of $x*((2*x)+3)$ at 5 is $5*((2*5)+3) = 65$.

   Let Poly be the inductive type defined by the following constructors:

   $\mathsf{X} : \mathsf{Poly}.$

   $\mathsf{Coeff} : \mathbb{Q} \to \mathsf{Poly}.$

   $\mathsf{Sum} : \mathsf{Poly} \times \mathsf{Poly} \to \mathsf{Poly}.$

   $\mathsf{Prod} : \mathsf{Poly} \times \mathsf{Poly} \to \mathsf{Poly}.$

   The members of Poly represent the polynomials over $\mathbb{Q}$. Define

   $\mathsf{val} : \mathsf{Poly} \times \mathbb{Q} \to \mathbb{Q}$

   by structural recursion using pattern matching so that, for all $p \in \mathsf{Poly}$ and $q \in \mathbb{Q}$, $\mathsf{val}(p, q)$ is the value of p at q.

   Put your name, MacID, and date here.

   Solution: val is defined by structural recursion using pattern matching as:

   $\mathsf{val}(\mathsf{X}, q) = q.$

   $\mathsf{val}(\mathsf{Coeff}(q'), q) = q'.$

   $\mathsf{val}(\mathsf{Sum}(p_1, p_2), q) = \mathsf{val}(p_1, q) + \mathsf{val}(p_2, q).$

   $\mathsf{val}(\mathsf{Prod}(p_1, p_2), q) = \mathsf{val}(p_1, q) * \mathsf{val}(p_2, q).$

2. **[10 points]** Let Bit be the inductive set defined by the following constructors:

   $\mathsf{Zero} : \mathsf{Bit}.$

   $\mathsf{One} : \mathsf{Bit}.$

   The members of Bit represent 0 and 1.

   Let BinNum be the inductive set defined by the following constructors:

$\mathsf{Nil} : \mathsf{BinNum}.$

$\mathsf{Join} : \mathsf{BinNum} \times \mathsf{Bit} \to \mathsf{BinNum}.$

The members of BinNum not equal to Nil represent binary numerals; Nil represents an empty numeral. For example,

$$\mathsf{Join}(\mathsf{Join}(\mathsf{Join}(\mathsf{Nil}, \mathsf{One}), \mathsf{Zero}), \mathsf{One}),$$

represents the binary number 101.

The function

$$\mathsf{len} : \mathsf{BinNum} \to \mathbb{N}$$

maps a member of BinNum to its length. len is defined by the following equations using recursion and pattern matching:

$\mathsf{len}(\mathsf{Nil}) = 0.$

$\mathsf{len}(\mathsf{Join}(u, b)) = \mathsf{len}(u) + 1.$

The function

$$\mathsf{val} : \mathsf{BinNum} \to \mathbb{N}$$

maps a member of BinNum to the value of the binary numeral it represents. For example,

$$\mathsf{val}(\mathsf{Join}(\mathsf{Join}(\mathsf{Join}(\mathsf{Nil}, \mathsf{One}), \mathsf{Zero}), \mathsf{One})) = (101)_2 = 5.$$

val is defined by the following equations using recursion and pattern matching:

$\mathsf{val}(\mathsf{Nil}) = 0.$

$\mathsf{val}(\mathsf{Join}(u, \mathsf{Zero})) = 2 * \mathsf{val}(u).$

$\mathsf{val}(\mathsf{Join}(u, \mathsf{One})) = (2 * \mathsf{val}(u)) + 1.$

The function

$$\mathsf{add} : \mathsf{BinNum} \times \mathsf{BinNum} \to \mathsf{BinNum}$$

is intended to implement addition on members of BinNum. It is defined by the following equations using recursion and pattern matching:

$\mathsf{add}(u, \mathsf{Nil}) = u.$

$\mathsf{add}(\mathsf{Nil}, u) = u.$

$\mathsf{add}(\mathsf{Join}(u, \mathsf{Zero}), \mathsf{Join}(v, \mathsf{Zero})) = \mathsf{Join}(\mathsf{add}(u, v), \mathsf{Zero}).$

$\mathsf{add}(\mathsf{Join}(u, \mathsf{One}), \mathsf{Join}(v, \mathsf{Zero})) = \mathsf{Join}(\mathsf{add}(u, v), \mathsf{One}).$

$\mathsf{add}(\mathsf{Join}(u, \mathsf{Zero}), \mathsf{Join}(v, \mathsf{One})) = \mathsf{Join}(\mathsf{add}(u, v), \mathsf{One}).$

$$\begin{aligned}&\mathsf{add}(\mathsf{Join}(u, \mathsf{One}), \mathsf{Join}(v, \mathsf{One})) = \\ &\quad \mathsf{Join}(\mathsf{add}(\mathsf{add}(u, v), \mathsf{Join}(\mathsf{Nil}, \mathsf{One})), \mathsf{Zero}).\end{aligned}$$

Notice that the algorithm behind the definition is essentially the same algorithm that children learn to add numbers represented as decimal numerals. The last equation is a bit complicated because it involves a carry of 1.

Lemma 1. For all $u, v \in \mathsf{BinNum}$,

$$\mathsf{len}(\mathsf{add}(u, v)) \leq \mathsf{len}(u) + \mathsf{len}(v).$$

Theorem 1. For all $u, v \in \mathsf{BinNum}$,

$$\mathsf{val}(\mathsf{add}(u, v)) = \mathsf{val}(u) + \mathsf{val}(v).$$

Theorem 1 states that add correctly implements addition on the members of BinNum.

Prove Theorem 1 assuming Lemma 1. (You are not required to prove Lemma 1.) Hint: Use strong induction with $P(n) \equiv \mathsf{val}(\mathsf{add}(u, v)) = \mathsf{val}(u) + \mathsf{val}(v)$ for all $u, v \in \mathsf{BinNum}$ such that $n = \mathsf{len}(u) + \mathsf{len}(v)$.

Put your name, MacID, and date here.

Solution:

We will first prove the following simple lemma:

Lemma 2. Let $b, c \in \mathsf{Bit}$ and $u, v \in \mathsf{BinNum}$.

a. $\mathsf{len}(u) + \mathsf{len}(v) < \mathsf{len}(\mathsf{Join}(u, b)) + \mathsf{len}(\mathsf{Join}(v, c))$.

b. $\mathsf{len}(\mathsf{add}(u, v)) + \mathsf{len}(\mathsf{Join}(\mathsf{Nil}, \mathsf{One})) < \mathsf{len}(\mathsf{Join}(u, b)) + \mathsf{len}(\mathsf{Join}(v, c))$.

Proof.

Part a. This inequality obviously holds since $\mathsf{len}(\mathsf{Join}(u, b)) = \mathsf{len}(u)+1$ by the definition of len.

Part b.

$$\begin{aligned}
&\mathsf{len}(\mathsf{add}(u, v)) + \mathsf{len}(\mathsf{Join}(\mathsf{Nil}, \mathsf{One})) && \langle \text{LHS} \rangle \\
&\leq \mathsf{len}(u) + \mathsf{len}(v) + \mathsf{len}(\mathsf{Join}(\mathsf{Nil}, \mathsf{One})) && \langle \text{Lemma 1} \rangle \\
&= \mathsf{len}(u) + \mathsf{len}(v) + 1 && \langle \text{def. of } \mathsf{len} \rangle \\
&< (\mathsf{len}(u) + 1) + (\mathsf{len}(v) + 1) && \langle \text{arithmetic} \rangle \\
&= \mathsf{len}(\mathsf{Join}(u, b)) + \mathsf{len}(\mathsf{Join}(u, c)) && \langle \text{def. of } \mathsf{len}; \text{ RHS} \rangle
\end{aligned}$$

□

We will now prove

for all $n \in \mathbb{N}, P(n)$,

which clearly implies Theorem 1.

Proof. Our proof will be by strong induction. Let $n \in \mathbb{N}$. Assume $P(0), P(1), P(2), \ldots, P(n-1)$ hold. We must show $P(n)$. Let $u, v \in \mathsf{BinNum}$ with $\mathsf{len}(u) + \mathsf{len}(v) = n$.

Case 1: $v = \mathsf{Nil}$.

$$\begin{aligned}
&\mathsf{val}(\mathsf{add}(u, \mathsf{Nil})) && \langle\text{LHS}\rangle \\
&= \mathsf{val}(u) && \langle\text{def. of } \mathsf{add}\rangle \\
&= \mathsf{val}(u) + 0 && \langle\text{arithmetic}\rangle \\
&= \mathsf{val}(u) + \mathsf{val}(\mathsf{Nil}) && \langle\text{def. of } \mathsf{val}\rangle
\end{aligned}$$

So $\mathsf{val}(\mathsf{add}(u, v)) = \mathsf{val}(u) + \mathsf{val}(v)$ and thus $P(n)$ holds in this case.

Case 2: $u = \mathsf{Nil}$. Similar to Case 1.

Case 3: $u = \mathsf{Join}(u', \mathsf{Zero})$ and $v = \mathsf{Join}(v', \mathsf{Zero}))$.

$$\begin{aligned}
&\mathsf{val}(\mathsf{add}(\mathsf{Join}(u', \mathsf{Zero}), \mathsf{Join}(v', \mathsf{Zero}))) && \langle\text{LHS}\rangle \\
&= \mathsf{val}(\mathsf{Join}(\mathsf{add}(u, v), \mathsf{Zero})) && \langle\text{def. of } \mathsf{add}\rangle \\
&= 2 * \mathsf{val}(\mathsf{add}(u', v')) && \langle\text{def. of } \mathsf{val}\rangle \\
&= 2 * (\mathsf{val}(u') + \mathsf{val}(v')) && \langle\text{ind. hyp.; Lem. 2(a)}\rangle \\
&= (2 * \mathsf{val}(u')) + (2 * \mathsf{val}(v')) && \langle\text{arithmetic}\rangle \\
&= \mathsf{val}(\mathsf{Join}(u', \mathsf{Zero})) + \mathsf{val}(\mathsf{Join}(v', \mathsf{Zero})) && \langle\text{def. of } \mathsf{val}\text{; RHS}\rangle
\end{aligned}$$

So $\mathsf{val}(\mathsf{add}(u, v)) = \mathsf{val}(u) + \mathsf{val}(v)$ and thus $P(n)$ holds in this case.

Case 4: $u = \mathsf{Join}(u', \mathsf{One})$ and $v = \mathsf{Join}(v', \mathsf{Zero}))$. Similar to Case 3.

Case 5: $u = \mathsf{Join}(u', \mathsf{Zero})$ and $v = \mathsf{Join}(v', \mathsf{One}))$. Similar to Case 3.

Case 6: $u = \mathsf{Join}(u', \mathsf{One})$ and $v = \mathsf{Join}(v', \mathsf{One})$).

$$
\begin{aligned}
& \mathsf{val}(\mathsf{add}(\mathsf{Join}(u', \mathsf{One}), \mathsf{Join}(v', \mathsf{One}))) \\
& \qquad\qquad \langle \text{LHS} \rangle \\
=\ & \mathsf{val}(\mathsf{Join}(\mathsf{add}(\mathsf{add}(u', v'), \mathsf{Join}(\mathsf{Nil}, \mathsf{One})), \mathsf{Zero})) \\
& \qquad\qquad \langle \text{definition of } \mathsf{add} \rangle \\
=\ & 2 * \mathsf{val}(\mathsf{add}(\mathsf{add}(u', v'), \mathsf{Join}(\mathsf{Nil}, \mathsf{One}))) \\
& \qquad\qquad \langle \text{definition of } \mathsf{val} \rangle \\
=\ & 2 * (\mathsf{val}(\mathsf{add}(u', v')) + \mathsf{val}(\mathsf{Join}(\mathsf{Nil}, \mathsf{One}))) \\
& \qquad\qquad \langle \text{induction hypothesis; Lemma 2(b)} \rangle \\
=\ & 2 * (\mathsf{val}(u') + \mathsf{val}(v') + \mathsf{val}(\mathsf{Join}(\mathsf{Nil}, \mathsf{One}))) \\
& \qquad\qquad \langle \text{induction hypothesis; Lemma 2(a)} \rangle \\
=\ & 2 * (\mathsf{val}(u') + \mathsf{val}(v') + 1) \\
& \qquad\qquad \langle \text{definition of } \mathsf{val} \rangle \\
=\ & ((2 * \mathsf{val}(u') + 1) + ((2 * \mathsf{val}(v') + 1) \\
& \qquad\qquad \langle \text{arithmetic} \rangle \\
=\ & \mathsf{val}(\mathsf{Join}(u', \mathsf{One})) + \mathsf{val}(\mathsf{Join}(v', \mathsf{One})) \\
& \qquad\qquad \langle \text{definition of } \mathsf{val}; \text{ RHS} \rangle
\end{aligned}
$$

So $\mathsf{val}(\mathsf{add}(u, v)) = \mathsf{val}(u) + \mathsf{val}(v)$ and thus $P(n)$ holds in this case.

These six case cover all possibilities. Therefore, $P(n)$ holds. □