From Mathematics to Generic Programming

Brooks Mershon

March 2017

9.3

Solution.

Distributivity of Multiplication over Addition

The exercise happens to ask us to prove (1) associativity and commutativity of multiplication as well as (2) distributivity of multiplication over addition. It just so happens that it may be easier to go ahead and prove the latter first.

We will first prove that:

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

As a basis we will let our induction variable c be the special value of 1:

$$\begin{aligned} a \cdot (b + 1) = a \cdot (b') &= a \cdot b + a \\ &= a \cdot b + a \cdot 1 \end{aligned}$$

Now for the inductive step, we will assume that $a \cdot (b + c) = a \cdot b + a \cdot c$ and attempt to show that if this is true, the same statement holds when we use the successor function on our inductive variable c.

$$\begin{aligned} a \cdot (b + c') &= a \cdot (b + c)' && \text{definition of addition} \\ &= a \cdot (b + c) + a && \text{definition of multiplication, expansion} \\ &= a \cdot b + a \cdot c) + a && \text{inductive hypothesis} \\ &= a \cdot b + a \cdot c' && \text{definition of multiplication, contraction} \end{aligned}$$

Thus, if distributivity of multiplication over addition holds for some value of c, it holds for all values of c. Our base case ensures that it holds for at least one value. We have proved that distributivity of multiplication over addition holds based purely off of logic performed on Peano's set of axioms published in 1889.

Commutativity of Multiplication

We started with distributivity of multiplication over addition because that law is in a way more basic than the one we will now prove. Some intuition for why this is true comes from the fact that a *ring* exhibits distributivity and many of the properties of groups (and additive and multiplicative monoids) without requiring that commutativity hold for the ring's binary operation.

Let us start with the basis (proven in the text):

$$a \cdot 0 = 0 \cdot a$$

For our inductive hypothesis we will assume that $a \cdot b = b \cdot a$.

$$\begin{aligned} a \cdot b' &= a \cdot b + a && \text{definition of multiplication} \\ &= b \cdot a + a && \text{inductive hypothesis} \\ &= && \text{we'll come back to this} \end{aligned}$$

We have a problem. We might intuitively wish to simply finish the above statement by writing that the RHS is equal to $b' \cdot a$. But alas we have not directly proved that we may do this. So we will return to this statement after proving that $x' \cdot y = x \cdot y + y$. This is the "mirror" of the definition given in the textbook for multiplication.

We will use an inductive proof. The basis is:

$$\begin{aligned} x' \cdot 0 &= 0 = 0 + 0 \\ &= x \cdot 0 + 0 && \text{proved earlier in the text (pattern matching)} \end{aligned}$$

We assume the inductive hypothesis that $x' \cdot y = x \cdot y + y$ and induct on y (using the successor function):

$$\begin{aligned} x' \cdot y' &= x' \cdot y + x' \\ &= x \cdot y + y + x' && \text{inductive hypothesis} \\ &= x \cdot y + (y + x') && \text{associativity of addition} \\ &= x \cdot y + (y + x)' && \text{definition of addition} \\ &= x \cdot y + (x + y)' && \text{commutativity of addition} \\ &= x \cdot y + (x + y') && \text{definition of addition} \\ &= (x \cdot y + x) + y' && \text{associativity of addition} \\ &= x \cdot y' + y' && \text{"original" definition of multiplication} \end{aligned}$$

This proves the statement we need in order to return to (☺).

$$
\begin{aligned}
a \cdot b' &= a \cdot b + a && \text{definition of multiplication} \\
&= b \cdot a + a && \text{inductive hypothesis} \\
&= b' \cdot a && \text{now using: } x' \cdot y = x \cdot y + y
\end{aligned}
$$

So we have that commutativity of multiplication is able to be proved with a bit more machinery than what was required to show that distributivity of multiplication over addition holds.

Associativity of Multiplication

We want to show that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. For our base case, we will show that this holds when $c = 0$.

$$
\begin{aligned}
(a \cdot b) \cdot 0 &= 0 \\
&= a \cdot 0 \\
&= a \cdot (b \cdot 0)
\end{aligned}
$$

And now we will induct on c, taking as our inductive hypothesis the statement:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

We have:

$$
\begin{aligned}
(a \cdot b) \cdot c' &= (a \cdot b) \cdot c + (a \cdot b) && \text{definition of multiplication} \\
&= a \cdot (b \cdot c) + (a \cdot b) && \text{induction hypothesis} \\
&= a \cdot ((b \cdot c) + b) && \text{distributivity of multiplication over addition} \\
&= a \cdot (b \cdot c') && \text{definition of multiplication}
\end{aligned}
$$

So we have proved that associativity of multiplication can be proved with the previously proven law stating that distributivity of multiplication over addition holds.