
Johan G. F. Belinfante
2006 December 21

summary

In this notebook, the binary operation INTMUL for multiplication of integers is introduced, and some of its basic properties are derived. Integer multiplication is here defined by its properties, rather than by a particular construction. Specifically, an integer \( z \) is defined to be the product of an integer \( x \) and an integer \( y \) if there exists an addition-preserving operation \( w \) on the set \( Z \) of integers which takes the integer \( +1 = \text{plus}[0] \) to the integer \( x \) and takes the integer \( y \) to the integer \( z \). One might paraphrase this definition of multiplication loosely as follows: \( x \cdot y = z \iff x : 1 = z : y \). A class-wrapped membership rule for this function has been introduced:

This approach to integer multiplication is patterned closely on the previously developed theory of mixed multiplication of integers by natural numbers. The strategy is to construct the theory of the binary operation INTMUL using previously derived facts about the function INTTIMES. These two functions are related to each other via currying and uncurrying. The definition of the binary operation INTMUL is quite similar to the definition of the curried multiplication function INTTIMES, but that of INTTIMES involves fewer variable than that of INTMUL. This is why INTTIMES has been introduced before INTMUL.

normalization for INTMUL

The function INTMUL can be related to INTTIMES as follows:
Corollary.

\[
\text{In [6]} := \text{Assoc}[\text{Id}, \text{composite}[\text{inverse[SINGLETON]}, \text{IMG}, \text{cross[INTTIMES, SINGLETON]]}] = \text{INTMUL}
\]

Corollary.

\[
\text{In [8]} := \text{Assoc}[\text{composite[inverse[SINGLETON]}, \text{IMG}, \text{cross[INTTIMES, SINGLETON]}], \text{id[cart[V, V]]} \text{ // Reverse}]
\]

rotation theorems

Theorem. (A variant of the formula connecting INTMUL with INTTIMES.)

\[
\text{In [10]} := \text{Assoc}[\text{rotate[E], cross[FUNPART, Id], cross[INTTIMES, Id]}]
\]

Theorem. (Yet another variant.)

\[
\text{In [12]} := (\text{composite[rotate[E], cross[x, Id]]} \text{ // TripleRotate // Reverse}) \cdot x \rightarrow \text{INTTIMES}
\]

domain of INTMUL

Theorem.

\[
\text{In [14]} := \text{ImComp[composite[inverse[SINGLETON], IMG], cross[INTTIMES, SINGLETON], V]}
\]
**INTMUL is a function**

The fact that \texttt{INTTIMES} is a function implies that \texttt{INTMUL} is also a function.

\begin{verbatim}
In[16]:= SubstTest[FUNCTION, composite[funpart[x], funpart[y]],
  {x -> composite[inverse[SINGLETON], IMG], y -> cross[INTTIMES, SINGLETON]}] // Reverse
Out[16]= FUNCTION[INTMUL] = True
In[17]:= FUNCTION[INTMUL] := True
\end{verbatim}

Corollary. (A function is a set if and only if its domain is a set.)

\begin{verbatim}
In[18]:= member[INTMUL, V] // AssertTest
Out[18]= member[INTMUL, V] = True
In[19]:= member[INTMUL, V] := True
\end{verbatim}

**range formula**

\begin{verbatim}
In[20]:= ImageComp[rotate[E], cross[INTTIMES, Id], V]
In[21]:= range[INTMUL] := Z
\end{verbatim}

Corollary. (Mapping property of \texttt{INTMUL}.)

\begin{verbatim}
In[22]:= member[INTMUL, map[cart[Z, Z], Z]] // AssertTest
Out[22]= member[INTMUL, map[cart[Z, Z], Z]] = True
In[23]:= member[INTMUL, map[cart[Z, Z], Z]] := True
\end{verbatim}

**curry results relating INTMUL and INTTIMES**

Theorem.

\begin{verbatim}
In[24]:= ApComp[composite[IMAGE[inverse[ASSOC]], IMAGE[cross[Id, inverse[E]]]],
  id[range[CURRY]], INTTIMES] // Reverse
Out[24]= APPLY[inverse[CURRY], INTTIMES] = INTMUL
In[25]:= APPLY[inverse[CURRY], INTTIMES] := INTMUL
\end{verbatim}

Theorem.
The integer divisibility relation \texttt{INTDIV} was early on defined directly in terms of binary homomorphisms. Traditionally, divisibility is defined in terms of multiplication. This connection between multiplication and divisibility is now a theorem, which can be derived quickly as follows:

\begin{verbatim}
In[30]:= U[binhom[INTADD, INTADD]]
Out[30]= INTDIV
\end{verbatim}

Comment. The properties of the integer divisibility relation \texttt{INTDIV} were derived before the introduction of either of the functions \texttt{INTTIMES} or \texttt{INTMUL}. This non-traditional order of introducing the main concepts of integer arithmetic has been done to facilitate the derivations of the theorems.