integer divisibility relation

Johan G. F. Belinfante
2006 October 21

summary

The integer divisibility relation $\text{INTDIV}$ has been introduced into the $\text{GOEDEL}$ program by means of a $\text{class}$-wrapped membership rule:

$\text{In}[2] := \text{Begin["Goedel`Private`"]};$

$\text{In}[3] := \text{?INTDIV}$

INTDIV is the integer divisibility relation

$\text{In}[4] := \text{FirstMatch}\left\{ \text{class}\left[x\_, \text{member}\left[y\_, \text{HoldPattern}\left[\text{INTDIV}\right]\right]\right]\right\}$

$\text{Out}[4] = \text{class}[x\_, \text{member}[y\_, \text{INTDIV}]] := \text{ReleaseHold}[\text{Module}\left\{ \text{z = Unique[]} \right\}, \text{class}\left[ x, \text{exists}[z, \text{and}[\text{member}[z, \text{binhom}[\text{INTADD}, \text{INTADD}]], \text{member}[y, z]]]]\right\}]$

A novel feature of this definition is that it does not involve explicit mention of integer multiplication. Indeed, at this stage of development, integer multiplication has not yet been defined in the $\text{GOEDEL}$ program. The definition of $\text{INTDIV}$ was inspired by a formula derived for the natural number divisibility relation $\text{DIV}$. (A technical comment: The expression $\text{binhom}[\text{INTADD}, \text{INTADD}]$ in this definition has been wrapped with $\text{HoldPattern}$ to prevent the $\text{class}$ rules from expanding this expression any further.)

\text{U[binhom[NATADD,NATADD]]}

The divisibility relation for natural numbers is the union of all $\text{times}[x]$ functions, a fact which can be succinctly stated as follows:
The function \( \text{times}[x] = \text{composite}[\text{NATMUL, LEFT}[x]] \) is the operation of multiplication of natural numbers by \( x \). These functions are precisely the binary homomorphisms for natural addition. Using the function \( \text{TIMES} = \text{lambda}[x, \text{times}[x]] \), one can write this fact as

\[
\text{In}[6] := \text{range[TIMES]}
\]

\[
\text{Out}[6] = \text{binom[NATADD, NATADD]}
\]

**Lemma.** (Comment. The orientation of this as a rewrite rule is based on an analogy with an existing rule in which the function \( \text{TIMES} \) is replaced by \( \text{PLUS} \).)

\[
\text{In}[7] := \text{Assoc[SWAP, inverse[E], composite[VERTSECT[inverse[rotate[\text{NATMUL}]]], id[omega]]]} // \text{Reverse}
\]

\[
\text{Out}[7] = \text{composite[inverse[E], TIMES] = composite[SWAP, inverse[rotate[\text{NATMUL}]]]}
\]

\[
\text{In}[8] := \text{composite[inverse[E], TIMES] := composite[SWAP, inverse[rotate[\text{NATMUL}]]]}
\]

An immediate corollary is that the divisibility relation is the union of all \( \text{times}[x] \) functions.

\[
\text{In}[9] := \text{ImageComp[inverse[E], TIMES, V]} // \text{Reverse}
\]

\[
\text{Out}[9] = U[\text{binom[NATADD, NATADD]]} = \text{DIV}
\]

\[
\text{In}[10] := U[\text{binom[NATADD, NATADD]]} := \text{DIV}
\]

**Theorem.** One can recover \( \text{NATMUL} \) from \( \text{TIMES} \).

\[
\text{In}[11] := \text{rotate[composite[inverse[\text{TIMES}], E]]} // \text{VSTriNormality}
\]

\[
\text{Out}[11] = \text{rotate[composite[inverse[\text{TIMES}], E]]} = \text{NATMUL}
\]

\[
\text{In}[12] := \text{rotate[composite[inverse[\text{TIMES}], E]]} := \text{NATMUL}
\]

---

**integer divisibility**

Although integer multiplication has yet to be defined, the above results for natural numbers suggests a definition of integer divisibility by simply replacing \( \text{NATADD} \) with \( \text{INTADD} \). The class-wrapped membership rule for \( \text{INTDIV} \) implies the following normalization rule:

\[
\text{In}[13] := \text{INTDIV} // \text{Normality} // \text{Reverse}
\]

\[
\text{Out}[13] = U[\text{binom[INTADD, INTADD]]} = \text{INTDIV}
\]

\[
\text{In}[14] := U[\text{binom[INTADD, INTADD]]} := \text{INTDIV}
\]
**INTDIV is a relation**

Upper bound.

\[
\text{In [15]} := \text{SubstTest[implies, subclass[u, v],}
\text{ subclass[U[u], U[v]], \{u \rightarrow \text{binhom[INTADD, INTADD]}, v \rightarrow \text{map}[Z, Z]\}]}
\]

\[
\text{Out[15]} = \text{subclass[INTDIV, cart[Z, Z]] = True}
\]

\[
\text{In [16]} := \text{subclass[INTDIV, cart[Z, Z]] := True}
\]

Corollary.

\[
\text{In [17]} := \text{SubstTest[implies, subclass[u, cart[Z, Z]], subclass[u, cart[V, V]], u \rightarrow \text{INTDIV}]}
\]

\[
\text{Out[17]} = \text{subclass[INTDIV, cart[V, V]] = True}
\]

\[
\text{In [18]} := \text{subclass[INTDIV, cart[V, V]] := True}
\]

Corollary.

\[
\text{In [19]} := \text{equal[composite[Id, INTDIV], INTDIV]}
\]

\[
\text{Out[19]} = \text{True}
\]

\[
\text{In [20]} := \text{composite[Id, INTDIV] := INTDIV}
\]

---

**sethood**

The relation INTDIV is a set:

\[
\text{In [21]} := \text{SubstTest[implies, and[subclass[x, y], member[y, V]],}
\text{ member[x, V], \{x \rightarrow \text{INTDIV}, y \rightarrow \text{cart[Z, Z]}\}]}
\]

\[
\text{Out[21]} = \text{member[INTDIV, V] = True}
\]

\[
\text{In [22]} := \text{member[INTDIV, V] := True}
\]

---

**a general theorem**

If a class is closed under composition then the relational part of its union is transitive.

\[
\text{In [23]} := \text{SubstTest[implies, subclass[u, v], subclass[\text{image}[w, u], \text{image}[w, v]],}
\text{ \{u \rightarrow \text{image[COMPOSE, cart[x, x]], v \rightarrow x, w \rightarrow \text{inverse}[E]}\}]
\]

\[
\text{Out[23]} = \text{or[not[subclass[\text{image[COMPOSE, cart[x, x]], x]]], TRANSITIVE[\text{composite[Id, U[x]]}]] = True}
\]
A variable-free corollary can be derived which captures this result for the special case of sets. Technical comment: The `setpart` wrapper helps in eliminating the variable `x`.

The reverse inclusion also holds:

These inclusions can be combined into an equation:

---

**TRANSITIVE**

**REFLEXIVE**

Lemma.
Substituting member[x, y], subclass[x, U[y]], {x \to \text{id}[Z], y \to \text{binom}[\text{INTADD}, \text{INTADD}]}

\text{Out}[33] = \text{subclass}[Z, \text{fix}[\text{INTDIV}]] = \text{True}

Substituting subclass[u, v], subclass[fix[u], fix[v]], {u \to \text{INTDIV}, v \to \text{cart}[Z, Z]}

\text{Out}[35] = \text{subclass}[\text{fix}[\text{INTDIV}], Z] = \text{True}

Theorem.

Substituting and, subclass[u, v], subclass[v, u], {u \to \text{fix}[\text{INTDIV}], v \to Z}

\text{Out}[37] = \text{True} = \text{equal}[Z, \text{fix}[\text{INTDIV}]]

\text{In}[38]:= \text{fix}[\text{INTDIV}] := Z

Corollary.

Substituting subclass, x, cart[fix[x], fix[x]], x \to \text{INTDIV} // Reverse

\text{Out}[39] = \text{REFLEXIVE}[\text{INTDIV}] = \text{True}

\text{In}[40]:= \text{REFLEXIVE}[\text{INTDIV}] := \text{True}

Corollary.

Substituting domain, rfx[x], x \to \text{INTDIV}

\text{Out}[41] = \text{domain}[\text{INTDIV}] = Z

\text{In}[42]:= \text{domain}[\text{INTDIV}] := Z

Corollary.

Substituting range, rfx[x], x \to \text{INTDIV}

\text{Out}[43] = \text{range}[\text{INTDIV}] = Z

\text{In}[44]:= \text{range}[\text{INTDIV}] := Z

Corollary.

Substituting idempotent, rfx[trv[x]], x \to \text{INTDIV}

\text{Out}[45] = \text{equal}[\text{INTDIV}, \text{composite}[\text{INTDIV}, \text{INTDIV}]] = \text{True}

\text{In}[46]:= \text{composite}[\text{INTDIV}, \text{INTDIV}] := \text{INTDIV}
The natural number divisibility relation is a partial order. Integer divisibility is not a partial order because any integer divides its negative.

Corollary.

Lemma.

Theorem.

A similar result holds in the reverse order.
Some additional facts discovered in the course of this work are recorded here. First, a general result:

```plaintext
In[65]:= member[x, image[逆函数[funpart[y]], z]] // AssertTest
Out[65]= member[x, image[逆函数[funpart[y]], z]] = member[APPLY[funpart[y], x], z]
In[66]:= member[x_, image[逆函数[funpart[y_]], z_]] := member[APPLY[funpart[y], x], z]
```

Corollary A general inverse-image rule for TIMES.

```plaintext
In[67]:= SubstTest[member, x, image[逆函数[funpart[z]], y], z -> TIMES]
Out[67]= member[x, image[逆函数[TIMES], y]] = and[member[x, omega], member[times[x], y]]
In[68]:= member[x_, image[逆函数[TIMES], y_]] := and[member[x, omega], member[times[x], y]]
```