greatest common divisors of pairsets

Johan G. F. Belinfante
2007 April 20

In[1]:= **SetDirectory["l:"]; << goedel92.17a; << tools.m**

```
:Package Title: goedel92.17a        2007 April 17 at 1:45 p.m.

It is now:  2007 Apr 20 at 5:9

Loading Simplification Rules

TOOLS.M                        Revised 2007 March 25

weightlimit = 40
```

summary

In the **GOEDEL** program, the theory of greatest common divisors is a special case of the general theory of greatest lower bounds. The function **GLB[DIV]** assigns to every subset **x** of **omega** its greatest common divisor, **APPLY[GLB[DIV], x]**. With respect to divisibility, the natural numbers form a complete lattice:

In[2]:= **member[DIV, CL]**

Out[2]= True

In this notebook various general facts about greatest common divisors are derived by specializing results for complete lattices. In addition, rewrite rules for the important special case of greatest common divisors for unordered pairs of natural numbers are obtained.

a simplification rule

In[3]:= **SubstTest[subclass, x, intersection[u, v], {u → omega, v → image[DIV, y]}]**

Out[3]= and[subclass[x, omega], subclass[x, image[DIV, y]]] == subclass[x, image[DIV, y]]

In[4]:= **and[subclass[x_, omega], subclass[x_, image[DIV, y_]]] := subclass[x, image[DIV, y]]**

characterizing greatest common divisors

A number **w** is a common divisor of a subset **x** of **omega** if every element of **x** is a multiple of **w**.

```
In[5]:= member[w, lb[DIV, x]]

Out[5]= and[member[w, V], subclass[x, image[DIV, set[w]]]]
```

In particular, the greatest common divisor (gcd) is a common divisor:

```
In[6]:= SubstTest[implies, and[member[y, CL], subclass[x, fix[y]]],
          subclass[x, image[y, set[APPLY[GLB[y], x]]]], y → DIV] // Reverse

Out[6]= or[not[subclass[x, omega]], subclass[x, image[DIV, set[APPLY[GLB[DIV], x]]]]] == True

In[7]:= (% /. x → x_) /. Equal → SetDelayed
```

Corollary.

```
In[8]:= equiv[subclass[x, image[DIV, set[APPLY[GLB[DIV], x]]]], subclass[x, omega]]

Out[8]= True

In[9]:= subclass[x_, image[DIV, set[APPLY[GLB[DIV], x_]]]] := subclass[x, omega]
```

The greatest common divisor is greatest in the sense that every other common divisor is a divisor of the greatest common divisor:

```
In[10]:= SubstTest[implies, and[member[y, CL], subclass[x, fix[y]], not[empty[x]]],
           subclass[lb[y, x], image[inverse[y], set[APPLY[GLB[y], x]]]], y → DIV] // Reverse

Out[10]= or[equal[0, x], not[subclass[x, omega]],
           subclass[lb[DIV, x], image[inverse[DIV], set[APPLY[GLB[DIV], x]]]]] == True

In[11]:= or[equal[0, x_], not[subclass[x_, omega]],
           subclass[lb[DIV, x_], image[inverse[DIV], set[APPLY[GLB[DIV], x_]]]]] := True
```

reformulation

The two-part characterization of the greatest common divisor a set of numbers given in the previous section can be reformulated by introducing another variable. The statement that the gcd is a common divisor is:

```
In[12]:= implies[and[member[y, x], subclass[x, omega]], member[pair[APPLY[GLB[DIV], x], y], DIV]]

Out[12]= True
```

The statement that the gcd is divisible by every other common divisor can be reformulated as follows:

```
In[13]:= SubstTest[implies, and[member[v, CL],
            subclass[x, fix[v]], not[empty[x]], subclass[x, image[v, set[y]]]],
           member[pair[y, APPLY[GLB[v], x]], v], v → DIV] // Reverse // MapNotNot

Out[13]= or[equal[0, x], member[pair[y, APPLY[GLB[DIV], x]], DIV],
           not[subclass[x, image[DIV, set[y]]]]] == True
```

```
In[14]:= or[equal[0, x_], member[pair[y_, APPLY[GLB[DIV], x_]], DIV],
           not[subclass[x_, image[DIV, set[y_]]]]] := True
```

gcd of a pairset

For the case of a pairset of natural numbers **set[nat[x],nat[y]]**, the statement that the gcd is a common divisor is:

```
In[15]:= SubstTest[implies, and[member[w, t], subclass[t, omega]],
           member[pair[APPLY[GLB[DIV], t], w], DIV],
           {t → set[nat[x], nat[y]], w → nat[x]}] // Reverse

Out[15]= member[pair[APPLY[GLB[DIV], set[nat[x], nat[y]]], nat[x]], DIV] == True

In[16]:= member[pair[APPLY[GLB[DIV], set[nat[x_], nat[y_]]], nat[x_]], DIV] := True
```

Since **set[x, y]** is symmetric in **x** and **y**, one does not need a separate rule for the case that **x** and **y** are interchanged. One does need a special rewrite rule for the case that **x = y**, but for that case one can derive a better rule:

```
In[17]:= Map[A, ImageComp[GLB[DIV], SINGLETON, set[nat[x]]]] // Reverse

Out[17]= APPLY[GLB[DIV], set[nat[x]]] == nat[x]

In[18]:= APPLY[GLB[DIV], set[nat[x_]]] := nat[x]
```

For the case of pairsets of natural numbers, the statement that the greatest common divisor is divisible by every other common divisor becomes:

```
In[21]:= SubstTest[or, equal[0, t], member[pair[w, APPLY[GLB[DIV], t]], DIV],
            not[subclass[t, image[DIV, set[w]]]], t → set[nat[x], nat[y]]] // Reverse // MapNotNot

Out[21]= or[member[pair[w, APPLY[GLB[DIV], set[nat[x], nat[y]]]], DIV],
           not[member[pair[w, nat[x]], DIV]], not[member[pair[w, nat[y]], DIV]]] == True

In[22]:= (% /. {w → w_, x → x_, y → y_}) /. Equal → SetDelayed
```

One can remove the **nat** wrappers:

```
In[23]:= SubstTest[implies, and[equal[x, nat[u]], equal[y, nat[v]]],
            or[member[pair[w, APPLY[GLB[DIV], set[x, y]]], DIV], not[member[pair[w, x], DIV]],
             not[member[pair[w, y], DIV]]], {u → x, v → y}] // Reverse // MapNotNot

Out[23]= or[member[pair[w, APPLY[GLB[DIV], set[x, y]]], DIV],
           not[member[pair[w, x], DIV]], not[member[pair[w, y], DIV]]] == True

In[24]:= or[member[pair[w_, APPLY[GLB[DIV], set[x_, y_]]], DIV],
           not[member[pair[w_, x_], DIV]], not[member[pair[w_, y_], DIV]]] := True
```