the third clause of Quaife's Theorem (GCD1)

Johan G. F. Belinfante
2009 March 23

```
In[1]:=  SetDirectory["l:"]; << goedel.09mar20a; << tools.m

         :Package Title: goedel.09mar20a            2009 March 20 at 4:25 p.m.

         It is now:  2009 Mar 23 at 11:40

         Loading Simplification Rules

         TOOLS.M                                    Revised 2009 February 18

         weightlimit = 40
```

summary

Several of Art Quaife's theorems about greatest common divisors were added to the **GOEDEL** program in the Spring of 2007 in collaboration with Ming Li, but this work was not completed. The third clause of Art Quaife's Theorem **(GCD1)** is derived in this notebook, along with some immediate corollaries.

```
In[2]:=    "Art Quaife, Automated Development of Fundamental Mathematical
           Theories, Appendix 3. Theorems Proved in Peano's Arithmetic,
           Kluwer Academic Publishers, Dordrecht, 1992. Cf. pp. 202-206";
```

review

The theory of greatest common divisors presented by Art Quaife depends on results about linear differences of natural numbers. The definition of **ld[x, y]** in the **GOEDEL** program is given by:

```
In[8]:=  image[rotate[NATADD], cart[image[DIV, set[x]], image[DIV, set[y]]]]

Out[8]=  ld[x, y]
```

Quaife's predicate **LD(x, y, z)** can be translated as **z ∈ ld[x, y]**. Because the development of linear differences in the **GOEDEL** program is done within the framework of set theory, one can often reformulate Quaife's statements using fewer variables. For example:

Theorem. If **w** is a linear difference of **x** and **y**, then so is every multiple of **w**.   This can be considered as a reformulation of Quaife's theorem **(LD10)**.

```
In[6]:=  SubstTest[implies, and[member[u, ld[x, y]], member[v, ld[x, y]]],
           subclass[ld[u, v], ld[x, y]], {u → w, v → w}] // Reverse

Out[6]=  or[not[member[w, ld[x, y]]], subclass[image[DIV, set[w]], ld[x, y]]] == True
```

```
In[7]:=  or[not[member[w_, ld[x_, y_]]], subclass[image[DIV, set[w_]], ld[x_, y_]]] := True
```

One can even eliminate the variable w here, yielding an even more compact statement:

```
In[9]:=  image[DIV, ld[x, y]]

Out[9]=  ld[x, y]
```

In the **GOEDEL** program, the development of greatest common divisors for natural numbers incorporates some of Quaife's results about linear differences, but also draws on the theory of complete lattices, as well as an analog for natural numbers of the fact that the integers form a principal ideal domain. The natural numbers form a complete lattice with respect to divisibility. While Quaife only considers greatest common divisors for pairsets, in fact every set of natural numbers has a gcd. Although the natural numbers obviously do not form an integral domain, there is nevertheless an analog for **omega** of the fact that **Z** is a **pid**. The role of principal ideal is replaced for natural numbers by the sets **image[DIV, set[nat[x]]]** of multiples of a natural number **nat[x]**. The class of all such sets is **image[VERTSECT[DIV], omega]**. Each member **t** of this class of subset of omega is a vertical section of the divisibility relation at some natural number, and moreover that natural number can even be identified: it is the gcd of the set **t**. The replacement for the statement that **Z** is pid is the statement that any set of natural numbers which is closed under both addition and subtraction is a vertical section of **DIV**. Every vertical section of **DIV** is closed under addition and subtraction, and conversely:

```
In[10]:=  intersection[P[omega], binclosed[NATADD], binclosed[rotate[NATADD]]]

Out[10]=  range[VERTSECT[DIV]]
```

In particular the set of linear differences **z = ld[nat[x], nat[y]]** is a vertical section of **DIV** at the natural number **APPLY[-GLB[DIV], z]**. The **GOEDEL** program automatically recognizes this fact, which will now be made into a rewrite rule.

Theorem. The set of linear differences of two natural numbers is the set of all multiples of its gcd.

```
In[11]:=  equal[image[DIV, set[APPLY[GLB[DIV], ld[nat[x], nat[y]]]]], ld[nat[x], nat[y]]]

Out[11]=  True
```

```
In[12]:=  image[DIV, set[APPLY[GLB[DIV], ld[nat[x_], nat[y_]]]]] := ld[nat[x], nat[y]]
```

Theorem. A number **w** is a linear difference of two natural numbers **x** and **y** if and only if the gcd of the set of linear differences of **x** and **y** is a divisor of **w**.

```
In[13]:=  SubstTest[member, w, image[DIV, set[t]], t -> APPLY[GLB[DIV], ld[nat[x], nat[y]]]]

Out[13]=  member[pair[APPLY[GLB[DIV], ld[nat[x], nat[y]]], w], DIV] ==
            member[w, ld[nat[x], nat[y]]]
```

```
In[14]:=  member[pair[APPLY[GLB[DIV], ld[nat[x_], nat[y_]]], w_], DIV] :=
            member[w, ld[nat[x], nat[y]]]
```

The third clause of Quaife's Theorem **(GCD1)** follows as a corollary:

Theorem. If **x** and **y** are natural numbers, then either **x** is zero or their gcd is a linear difference of **x** and **y**.

```
In[15]:= SubstTest[implies, and[member[pair[w, nat[x]], DIV], member[pair[w, nat[y]], DIV]],
            member[pair[w, APPLY[GLB[DIV], set[nat[x], nat[y]]]], DIV],
            w → APPLY[GLB[DIV], ld[nat[x], nat[y]]]] // Reverse // MapNotNot

Out[15]= or[equal[0, nat[x]],
           member[APPLY[GLB[DIV], set[nat[x], nat[y]]], ld[nat[x], nat[y]]]] == True

In[16]:= or[equal[0, nat[x_]],
           member[APPLY[GLB[DIV], set[nat[x_], nat[y_]]], ld[nat[x_], nat[y_]]]] := True
```

Corollary. If **x** and **y** are natural numbers, and if **x** is bot zero, then any multiple of the gcd is a linear difference.

```
In[17]:= Map[or[empty[nat[x]], #] &, SubstTest[subclass, image[DIV, set[t]],
            image[DIV, set[w]], {t -> APPLY[GLB[DIV], set[nat[x], nat[y]]],
             w -> APPLY[GLB[DIV], ld[nat[x], nat[y]]]}]] // Reverse

Out[17]= or[equal[0, nat[x]], subclass[
            image[DIV, set[APPLY[GLB[DIV], set[nat[x], nat[y]]]]], ld[nat[x], nat[y]]]] == True

In[18]:= or[equal[0, nat[x_]], subclass[image[DIV, set[APPLY[GLB[DIV], set[nat[x_], nat[y_]]]]],
            ld[nat[x_], nat[y_]]]] := True
```

Converse Theorem. Every linear difference of two natural numbers is a multiple of their gcd.

```
In[25]:= SubstTest[implies, and[member[pair[w, nat[x]], DIV], member[pair[w, nat[y]], DIV]],
           subclass[ld[nat[x], nat[y]], image[DIV, set[w]]],
           w → APPLY[GLB[DIV], set[nat[x], nat[y]]]] // Reverse

Out[25]= subclass[ld[nat[x], nat[y]],
           image[DIV, set[APPLY[GLB[DIV], set[nat[x], nat[y]]]]]] == True

In[26]:= subclass[ld[nat[x_], nat[y_]],
           image[DIV, set[APPLY[GLB[DIV], set[nat[x_], nat[y_]]]]]] := True
```

Theorem. If **x** and **y** are natural numbers, and **x** is not zero, then the set of their linear differences is equal to the set of multiples of their gcd.

```
In[27]:= SubstTest[and, implies[p, subclass[u, v]], subclass[v, u], {p → not[empty[nat[x]]],
           u -> image[DIV, set[APPLY[GLB[DIV], set[nat[x], nat[y]]]]], v -> ld[nat[x], nat[y]]}]

Out[27]= or[equal[0, nat[x]], equal[
            image[DIV, set[APPLY[GLB[DIV], set[nat[x], nat[y]]]]], ld[nat[x], nat[y]]]] == True

In[28]:= or[equal[0, nat[x_]], equal[image[DIV, set[APPLY[GLB[DIV], set[nat[x_], nat[y_]]]]],
            ld[nat[x_], nat[y_]]]] := True
```

Lemma. Any pairset of two natural numbers is equal to the pairset of the lesser and the greater of the two.

```
In[30]:= equal[set[intersection[nat[x], nat[y]], union[nat[x], nat[y]]], set[nat[x], nat[y]]]

Out[30]= True
```

```
In[32]:= set[intersection[nat[x_], nat[y_]], union[nat[x_], nat[y_]]] := set[nat[x], nat[y]]
```

Corollary. The set of multiples of two natural numbers is equal to the set of linear differences of the greater and lesser of the two numbers. This fact is made into a rewrite rule that could be used to eliminate linear differences in favor of gcd's.

```
In[34]:= SubstTest[or, equal[0, nat[u]],
            equal[image[DIV, set[APPLY[GLB[DIV], set[nat[u], nat[v]]]]], ld[nat[u], nat[v]]],
            {u → union[nat[x], nat[y]], v → intersection[nat[x], nat[y]]}] // Reverse // MapNotNot

Out[34]= equal[image[DIV, set[APPLY[GLB[DIV], set[nat[x], nat[y]]]]],
           ld[union[nat[x], nat[y]], intersection[nat[x], nat[y]]]] == True
```

```
In[36]:= ld[union[nat[x_], nat[y_]], intersection[nat[x_], nat[y_]]] :=
          image[DIV, set[APPLY[GLB[DIV], set[nat[x], nat[y]]]]]
```