The GCD and the minimum

It all began with a friend who was preparing his undergraduate lectures asking me whether I had a nice calculational proof of

(0) $\quad x \downarrow y = 1 \;\Rightarrow\; x \downarrow (y*z) = x \downarrow z$

(All variables are of type natural and $\downarrow$ stands for the greatest common divisor.) I did not have nice proof of (0), so I started to think about it, and then the fun started. Hence this little note.

* * *

Having learned to like Lattice Theory and the Galois Connection, I immediately decided to regard $\downarrow$ as the infimum with respect to the partial order $\sqsubseteq$, read as "divides". The greatest common divisor $\downarrow$ is then defined by

(1) $\quad u \sqsubseteq x \downarrow y \;\equiv\; u \sqsubseteq x \wedge u \sqsubseteq y \quad$ for all x, y, u.

From the above definition, many nice properties of $\downarrow$ elegantly follow, such as

(2) $\downarrow$ is associative, symmetric and idempotent

(3) $x \downarrow y \sqsubseteq x \quad$ and $\quad x = x \downarrow y \;\equiv\; x \sqsubseteq y$.

As the above are general results from elementary lattice theory and have nothing to do with integer arithmetic, I decided to use them freely as the need would arise. [It turned out that, to begin with, that need would only arise for (2).]

Besides $\downarrow$, (0) contains the special constants 1 and $*$, and the next question was how to capture their relevant properties. For 1 I could come up with two relations, connecting 1 to $*$ and to $\downarrow$ respectively;

(4) $1 * u = u$ for all u, and

(5) $1 \downarrow u = 1$ for all u,

and I postponed the choice.

Note At the time I did not realize that (4) is the more promising candidate. By presenting 1 as a unit element (of $*$), it offers a way of eliminating 1, while (5), which presents 1 as a zero element (of $\downarrow$), does not offer that service. (End of Note.)

(4) connects $*$ with 1 but I assumed that this was not enough to capture the "relevant properties" of $*$. To connect $*$ with $\downarrow$, I came up with

(6) $x \downarrow (y * z) = x \downarrow (x \downarrow y * x \downarrow z)$.

Now the proof of (0) was straightforward: we observe for any x, y, z (satisfying (6) and (0)'s antecedent)

$$
\begin{array}{ll}
 & x \downarrow (y * z) \\
= & \quad \{(6)\} \\
 & x \downarrow (x \downarrow y * x \downarrow z) \\
= & \quad \{\text{antecedent of (0)}\} \\
 & x \downarrow (1 * x \downarrow z) \\
= & \quad \{(4) \text{ with } u := x \downarrow z\} \\
 & x \downarrow (x \downarrow z) \\
= & \quad \{\downarrow \text{ associative and idempotent}\} \\
 & x \downarrow z \quad ,
\end{array}
$$

which completes the proof of (0).

* * *

The above proof is nice, but one can object that it does not prove very much, as (6), which we use, is hardly simpler than the demonstrandum (0). [It is, for (6) does not contain 1 .] So I started to think about proving (6), but in order to simplify matters, I switched to the additive version

(7) $x \downarrow (y + z) = x \downarrow (x \downarrow y + x \downarrow z)$,

where x, y, z are of type real and $\downarrow$ denotes

the minimum. For this proof I used - besides (1) with $\sqsubseteq$ specialized as $\leq$ -

$$(8)\quad x \downarrow y \leq u \;\equiv\; x \leq u \;\vee\; y \leq u \qquad \text{for all } x,y,u$$

which holds because $\leq$ is a total order - i.e $x \leq y \;\vee\; y \leq x$ - and

$$(9)\quad u + x \downarrow y \;=\; (u+x) \downarrow (u+y) \qquad \text{for all } x,y,u$$

- i.e. $+$ distributes over $\downarrow$ -, which follows from (1).

In order to prove (7) we observe

$$\begin{array}{ll}
 & x \downarrow (y+z) \;=\; x \downarrow (x \downarrow y \;+\; x \downarrow z) \\
\equiv & \quad \{ + \text{ over } \downarrow, \text{ i.e. (9) thrice} \} \\
 & x \downarrow (y+z) \;=\; x \downarrow (y+z) \downarrow (x+x) \downarrow (x+y) \downarrow (x+z) \\
\equiv & \quad \{ (3) \} \\
 & x \downarrow (y+z) \leq (x+x) \downarrow (x+y) \downarrow (x+z) \qquad (*) \\
\equiv & \quad \{(8)\} \\
 & x \leq (x+x) \downarrow (x+y) \downarrow (x+z) \;\vee \\
 & (y+z) \leq (x+x) \downarrow (x+y) \downarrow (x+z) \\
\equiv & \quad \{ (1),\ 2 \text{ times twice} \} \\
 & (x \leq x+x \;\wedge\; x \leq x+y \;\wedge\; x \leq x+z) \;\vee \\
 & (y+z \leq x+x \;\wedge\; y+z \leq x+y \;\wedge\; y+z \leq x+z) \\
\equiv & \quad \{ \text{simplifications} \} \\
 & (0 \leq x \;\wedge\; 0 \leq y \;\wedge\; 0 \leq z) \;\vee \\
 & (z \leq x \;\wedge\; y \leq x)
\end{array}$$

We failed to prove (7) because it is <u>not</u> a

theorem: it only holds for nonnegative x,y,z or when x is the largest of the three.

* * *

From (*) we first eliminated $\downarrow$ at the left-hand side, using (8), and than we used (1) to eliminate the $\downarrow$s at the right. We could have done it in the other order. We illustrate the consequences with a simpler example. Consider the calculations

$$
\begin{array}{ll}
 & x \downarrow y \leq a \downarrow b \\
\equiv & \quad \{(8)\} \\
 & x \leq a \downarrow b \;\vee\; y \leq a \downarrow b \\
\equiv & \quad \{(1)\} \\
 & (x \leq a \wedge x \leq b) \;\vee\; (y \leq a \wedge y \leq b)
\end{array}
$$

and

$$
\begin{array}{ll}
 & x \downarrow y \leq a \downarrow b \\
\equiv & \quad \{(7)\} \\
 & x \downarrow y \leq a \;\wedge\; x \downarrow y \leq b \\
\equiv & \quad \{(8)\} \\
 & (x \leq a \vee y \leq a) \wedge (x \leq b \vee y \leq b) \;.
\end{array}
$$

from which we conclude

$$
(x \leq a \wedge x \leq b) \vee (y \leq a \wedge y \leq b) \equiv (x \leq a \vee y \leq a) \wedge (x \leq b \vee y \leq b)
$$

a beautiful formula that I did not know, but don't try to prove it by predicate calculus alone, for you need that $\leq$ is a total order.

Because, in contrast to $\leq$, $\subseteq$ in the meaning of "divides" is not a total order we can expect (6) to be essentially harder to prove than its additive version (7). I would not be amazed if the uniqueness of the prime factorization were needed.

Acknowledgement I thank Hamilton Richards for starting me on these investigations and Jayadev Misra for his interest shown.

Austin, 27 November 2001

Prof. Dr. Edsger W. Dijkstra
Department of Computer Sciences
The University of Texas at Austin
Austin, TX 78712-1188
USA