Indirect equality enriched (and a proof by Netty)

Proofs known as "proofs by indirect equality" traditionally exploit

(0) $\quad x = y \;\equiv\; \langle \forall u : \text{true} : u \sqsubseteq x \equiv u \sqsubseteq y \rangle$

for some reflexive, antisymmetric $\sqsubseteq$: they establish equality by establishing the right-hand side of (0). The following lemma shows that we may be able to get away with a proof obligation that is formally weaker.

Lemma For reflexive, antisymmetric $\sqsubseteq$ and predicate P such that $P.x \wedge P.y$, we have

(1) $\quad x = y \;\equiv\; \langle \forall u : P.u : u \sqsubseteq x \equiv u \sqsubseteq y \rangle$.

Proof

LHS $\Rightarrow$ RHS This follows from Leibniz's Principle.

LHS $\Leftarrow$ RHS We observe for any x, y, P such that $P.x \wedge P.y$

$\quad \langle \forall u : P.u : u \sqsubseteq x \equiv u \sqsubseteq y \rangle$

$\Rightarrow$ $\quad$ {instantiate $u := x$ and $u := y$}

$\quad (P.x \Rightarrow (x \sqsubseteq x \equiv x \sqsubseteq y)) \;\wedge\; (P.y \Rightarrow (y \sqsubseteq x \equiv y \sqsubseteq y))$

$\equiv$ $\quad$ {$P.x \wedge P.y$}

$\quad (x \sqsubseteq x \equiv x \sqsubseteq y) \;\wedge\; (y \sqsubseteq x \equiv y \sqsubseteq y)$

$\equiv$ $\quad$ {$\sqsubseteq$ is reflexive}

$$
\begin{array}{ll}
 & x \sqsubseteq y \;\wedge\; y \sqsubseteq x \\
\Rightarrow & \quad \{\ \sqsubseteq \text{ is antisymmetric}\ \} \\
 & x = y
\end{array}
$$

(End of Proof.)

* * *

An application

Let the above $\sqsubseteq$ be the partial order of a lattice for which the infimum $\downarrow$ is defined by the usual

(2) $\quad u \sqsubseteq x \downarrow y \;\equiv\; u \sqsubseteq x \;\wedge\; u \sqsubseteq y$.

Fairly directly follow the general lattice properties

(3) $\downarrow$ is idempotent, symmetric, associative

(4) $x \downarrow y \sqsubseteq x$ and $x \downarrow y \sqsubseteq y$

(5) $x \sqsubseteq y \;\equiv\; x = x \downarrow y$.

We now specialize by making the variables x, y, u etc. of type natural and identifying $\sqsubseteq$ with "divides" - or "is a divisor of" -, which is a partial order on the naturals for which the infimum exists: $x \downarrow y$ is in fact the Greatest Common Divisor of x and y .

The formal link between our lattice and arithmetic on the naturals - multiplication in

in particular - is given by providing $\langle \exists q :: q * x = y \rangle$ as third expression for "x divides y", i.e. we add to our laws

(6) $\langle \exists q :: q * x = y \rangle \equiv x \sqsubseteq y$

from which the mutually equivalent

(7) $m \sqsubseteq m * x$ and $m = m \downarrow m * x$

immediately follow. (Please note that we have given * a stronger binding power than $\downarrow$.)

We are now ready to prove that the GCD of two m-tiples[‡] is an m-tiple[‡], in formula

(8) $m \sqsubseteq m * x \downarrow m * y$

Proof We observe

$$
\begin{array}{ll}
 & m \sqsubseteq m * x \downarrow m * y \\
\equiv & \quad \{ (5) \text{ and associativity of } \downarrow \ (3) \} \\
 & m = m \downarrow m * x \downarrow m * y \\
\equiv & \quad \{ (7) \} \\
 & m = m \downarrow m * y \\
\equiv & \quad \{ (7) \text{ with } x := y \} \\
 & \text{true}
\end{array}
$$

(End of Proof)

---

‡ An "m-tiple" is a multiple of m.

And now we are ready for an application of the Lemma with which this note started:

we shall show that multiplication distributes over the GCD, in formula

(9) $\quad m * (x \downarrow y) = m*x \downarrow m*y$.

Proof On account of (7), the LHS of (9) is an m-tiple, on account of (8), the RHS is an m-tiple. Lemma (1) can thus be applied with $m \sqsubseteq u$ for $P.u$. Accordingly we observe for $1 \leq m$ - the case $m=0$ is obvious -

$$
\begin{array}{ll}
 & (9) \\
\equiv & \quad \{(1)\} \\
 & \langle \forall u:\ m \sqsubseteq u:\ u \sqsubseteq m * (x \downarrow y) \equiv u \sqsubseteq m*x \downarrow m*y \rangle \\
\equiv & \quad \{\text{transforming the dummy: } u = m * w\} \\
 & \langle \forall w ::\ m*w \sqsubseteq m * (x \downarrow y) \equiv m*w \sqsubseteq m*x \downarrow m*y \rangle \\
\equiv & \quad \{(2)\} \\
 & \langle \forall w ::\ m*w \sqsubseteq m * (x \downarrow y) \equiv \\
 & \qquad m*w \sqsubseteq m*x \ \wedge\ m*w \sqsubseteq m*y \rangle \\
\equiv & \quad \{\ r \sqsubseteq s \equiv m*r \sqsubseteq m*s \text{ for } 1 \leq m\} \\
 & \langle \forall w ::\ w \sqsubseteq x \downarrow y \equiv w \sqsubseteq x \ \wedge\ w \sqsubseteq y \rangle \\
\equiv & \quad \{(2)\} \\
 & \text{true}
\end{array}
$$

(End of Proof.)

Addendum For those who are not comfortable with the dummy transformation, here is its pattern in a bit more detail

$$
\begin{array}{ll}
 & \langle \forall u:\ m \sqsubseteq u:\ Q.u \rangle \\
\equiv & \quad \{\text{for non-empty range } \langle \forall w ::\ C \rangle \equiv C\ \}
\end{array}
$$

$$
\begin{array}{ll}
 & \langle \forall u:\ m \sqsubseteq u:\ \langle \forall w:\ u = m * w:\ Q.u \rangle \rangle \\
\equiv & \quad \{ \text{ interchange of quantifications} \} \\
 & \langle \forall w ::\ \langle \forall u:\ u = m * w \ \wedge\ m \sqsubseteq u:\ Q.u \rangle \rangle \\
\equiv & \quad \{\ u = m * w \ \Rightarrow\ m \sqsubseteq u \} \\
 & \langle \forall w ::\ \langle \forall u:\ u = m * w:\ Q.u \rangle \rangle \\
\geq & \quad \{ \text{ one-point rule} \} \\
 & \langle \forall w ::\ \ Q.(m * w) \rangle
\end{array}
$$

(End of Addendum)

* * *

All the above was triggered by Netty van Gasteren's use of (9) in her ingenious proof of

(10) $\quad x \downarrow y = 1 \ \Rightarrow\ x \downarrow y * z = x \downarrow z$:

$$
\begin{array}{ll}
 & x \downarrow z \\
= & \quad \{ \text{antecedent of (10)} \} \\
 & x \downarrow (x \downarrow y) * z \\
= & \quad \{ \text{(9) and associativity of } \downarrow \} \\
 & x \downarrow x * z \downarrow y * z \\
= & \quad \{ \text{(7) with } m, x := x, z \} \\
 & x \downarrow y * z
\end{array}
$$

Nuenen, 14 December 2001

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