

Indirect equality enriched (and a proof by Netty)

Proofs known as "proofs by indirect equality" traditionally exploit

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

for some reflexive, antisymmetric \in : 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 \in and predicate P such that $P.x \wedge P.y$, we have

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

Proof

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

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

$$\begin{aligned} & \langle \forall u: P.u: u \in x \equiv u \in y \rangle \\ \Rightarrow & \quad \{ \text{instantiate } u := x \text{ and } u := y \} \\ & (P.x \Rightarrow (x \in x \equiv x \in y)) \wedge (P.y \Rightarrow (y \in x \equiv y \in y)) \\ \equiv & \quad \{ P.x \wedge P.y \} \\ & (x \in x \equiv x \in y) \wedge (y \in x \equiv y \in y) \\ \equiv & \quad \{ \in \text{ is reflexive} \} \end{aligned}$$

$$\Rightarrow \begin{array}{l} x \varepsilon y \wedge y \varepsilon x \\ \{ \varepsilon \text{ is antisymmetric} \} \\ x = y \end{array}$$

(End of Proof.)

* * *

An application

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

$$(2) \quad u \varepsilon x \downarrow y \equiv u \varepsilon x \wedge u \varepsilon y$$

Fairly directly follow the general lattice properties

(3) \downarrow is idempotent, symmetric, associative

$$(4) \quad x \downarrow y \varepsilon x \quad \text{and} \quad x \downarrow y \varepsilon y$$

$$(5) \quad x \varepsilon y \equiv x = x \downarrow y$$

We now specialize by making the variables x, y, u etc. of type natural and identifying ε 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

$$(7) m \sqsubseteq m * x \quad \text{and} \quad m = m \downarrow m * x$$

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 -tuples[‡] is an m -tuple[‡], in formula

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

Proof We observe

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

(End of Proof)

‡ An "m-tuple" 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 -tuple, on account of (8), the RHS is an m -tuple. Lemma (1) can thus be applied with $m \subseteq u$ for P.u. Accordingly we observe for $1 \leq m$ - the case $m=0$ is obvious -

$$\begin{aligned}
 & (9) \\
 \equiv & \{ (1) \} \\
 & \langle \forall u: m \subseteq u: u \subseteq m * (x \downarrow y) \equiv u \subseteq m * x \downarrow m * y \rangle \\
 \equiv & \{ \text{transforming the dummy: } u = m * w \} \\
 & \langle \forall w: m * w \subseteq m * (x \downarrow y) \equiv m * w \subseteq m * x \downarrow m * y \rangle \\
 \equiv & \{ (2) \} \\
 & \langle \forall w: m * w \subseteq m * (x \downarrow y) \equiv \\
 & \quad m * w \subseteq m * x \wedge m * w \subseteq m * y \rangle \\
 \equiv & \{ \Gamma \subseteq S \equiv m * \Gamma \subseteq m * S \text{ for } 1 \leq m \} \\
 & \langle \forall w: w \subseteq x \downarrow y \equiv w \subseteq x \wedge w \subseteq y \rangle \\
 \equiv & \{ (2) \} \\
 & \text{true}
 \end{aligned}$$

(End of Proof.)

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

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

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

(End of Addendum)

* * *

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

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

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

Nuenen, 14 December 2001

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