An example of how to lengthen formal proofs

For invertible t of the proper type

$$[(\underline{A}x :: f.x) \equiv (\underline{A}x :: f.(t.x))] \quad .$$

The proof is by proving first (0), and then (1), with

(0) $\quad [(\underline{A}x :: f.x) \Rightarrow (\underline{A}x :: f.(t.x))]$

(1) $\quad [(\underline{A}x :: f.x) \Leftarrow (\underline{A}x :: f.(t.x))]$

The proof of (0) is

$$
\begin{array}{ll}
 & (0) \\
= & \{ Q\Rightarrow \text{ distributes over } \underline{A} \} \\
 & [(\underline{A}x :: (\underline{A}x :: f.x) \Rightarrow f.(t.x))] \\
= & \{ \text{instantiation: } x := t.x \} \\
 & [(\underline{A}x :: true] \\
= & \{ \text{pred. calc.} \} \\
 & true \qquad ,
\end{array}
$$

a proof with which I have no quarrel. Its independence of t's invertibility justifies a proof by mutual implication.

To prove now (1), one can proceed as follows

$$
\begin{array}{ll}
 & (\underline{A}x :: f.(t.x)) \\
= & \{ \text{definition of functional composition} \} \\
 & (\underline{A}x :: (f \circ t).x) \\
\Rightarrow & \{ (0) \text{ with } f, t := (f \circ t), t^{-1} \} \\
 & (\underline{A}x :: (f \circ t).(t^{-1}.x))
\end{array}
$$

$=\quad$ {definition of functional composition}

$(\underline{A}x:: ((f\circ t)\circ t^{-1}).x)$

$=\quad$ { $\circ$ is associative}

$(\underline{A}x:: (f\circ(t\circ t^{-1})).x)$

$=\quad$ { $t\circ t^{-1}$ is the identity function}

$(\underline{A}x:: f.x)$

The above is an exaggeration of a proof Carel S. Scholten and I included in our book. What about

$(\underline{A}x:: f.(t.x))$

$\Rightarrow\quad$ {(0) with $t:=t^{-1}$}

$(\underline{A}x:: f.(t.(t^{-1}.x)))$

$=\quad$ { $t.(t^{-1}.x) = x$ }

$(\underline{A}x:: f.x)$?

The first proof introduces $t\circ t^{-1}$ as the identity element of functional composition, whereas in the last hint of the second proof – which is equivalent with $(t\circ t^{-1}).x = x$ – $t\circ t^{-1}$ is not functionally composed but applied. Why did functional composition enter the first proof in the first place? Obviously, to be able to indicate explicitly in the instantiation of (0) $f:=(f\circ t)$. If we so desired, this could also be achieved by $f:=(\lambda x: f.(t.x))$, but this, too, now strikes me as unnecessarily pompous. You see, I am also willing to read (0) as: "A universal quantification is not strengthened by replacing in the term the dummy by a function of it." In applyin this to $(\underline{A}x{::}\ f.(t.x))$ the dummy is well-identified -viz. x- , and so is the term -viz. $f.(t.x)$. In order to perform the nonstrengthening transformation without look-ahead and pattern matching, we only need to know which function to apply to the dummy, and that is precisely the information the hint $t := t^{-1}$ supplies. So I think that the first hint of the last proof suffices.

We could have continued our second proof with

$$\begin{array}{ll} & (\underline{A}x{::}\ f.(t.(t^{-1}.x))) \\ = & \{\text{def. of functional composition}\} \\ & (\underline{A}x{::}\ f.((t \circ t^{-1}).x)) \\ = & \{t \circ t^{-1} \text{ is the identity function}\} \\ & (\underline{A}x{::}\ f.x) \end{array}$$

but, again, the explicit introduction of functional composition is no improvement.

Austin, 8 October 1989

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