An example of how to lengthen formal proofs

For invertible \( t \) of the proper type

\[
[(\forall x:: f(x)) \equiv (\forall x:: f((t \cdot x)))]
\]

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

(0) \( [(\forall x:: f(x)) \Rightarrow (\exists x:: f((t \cdot x)))] \)

(1) \( [(\forall x:: f(x)) \Leftarrow (\forall x:: f((t \cdot x)))] \)

The proof of (0) is

(0)
\[
\Rightarrow \text{ distributes over } \land
\]
\[
[(\forall x:: (\forall x:: f(x)) \Rightarrow f((t \cdot x)))]
\]
\[
\Rightarrow \text{ instantiation: } x := t \cdot x
\]
\[
[(\exists x:: \text{ true}]
\]
\[
\Rightarrow \text{ pred. calc.}
\]
\[
\text{true}
\]

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

\[
(\forall x:: f((t \cdot x))
\]
\[
\Rightarrow \text{ definition of functional composition}
\]
\[
(\forall x:: (f \circ t) \cdot x)
\]
\[
\Rightarrow \text{ (0) with } f, t := (f \circ t), t^{-1}
\]
\[
(\forall x:: (f \circ t) \cdot (t^{-1} \cdot x))
\]
\begin{itemize}
\item \{ definition of functional composition \}
\hspace{1cm} (\forall x :: ((f \circ t) \circ t^{-1}) \cdot x )
\item \{ \circ is associative \}
\hspace{1cm} (\forall x :: ((f \circ (t \circ t^{-1})) \cdot x )
\item \{ \circ t^{-1} \ is \ the \ identity \ function \}
\hspace{1cm} (\forall x :: f \cdot x )
\end{itemize}

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

\begin{itemize}
\item (\forall x :: f \cdot (t \cdot x ) )
\item \Rightarrow \{ (0) \ with \ t := t^{-1} \}
\hspace{1cm} (\forall x :: f \cdot (t \cdot (t^{-1} \cdot x )))
\item = \{ t \cdot (t^{-1} \cdot x ) = x \}
\hspace{1cm} (\forall x :: f \cdot x )
\end{itemize}

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 \((t \circ t^{-1}) \cdot x = x \) - \( t \circ t^{-1} \) 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 \( f := (\forall x : f \cdot (t \cdot x )) \), 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 applying this to \((\forall x:\; f(t.x))\) the dummy is well-identified \(-\text{viz.} x-\), and so is the term \(-\text{viz.} f(t.x)\). 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
\[
(\forall x:\; f(t.(t^{-1} x)))
\]

\[
= \{ \text{def. of functional composition} \}
(\forall x:\; f((t\circ t^{-1}). x))
= \{ t\circ t^{-1} \text{ is the identity function} \}
(\forall x:\; f.x)
\]

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