Proving the equality of infinite sequences

In EWD827, I gave a very short proof of the equality of two infinite sequences by showing that the one sequence satisfied the defining equation of the other. I was annoyed by the destruction of the symmetry, the more so since I could not do it the other way round. I also pulled what at the time looked like a rabbit out of the hat, and the formalism used to conduct the proof in went beyond SASL, in which the sequences had been defined. Here is what could be a more systematic approach.

In order to prove $x=y$ for infinite sequences x, y, we show for suitable P

the base: $\quad P.(x,y)$

the step: $\quad P.(a{:}p\,,\,b{:}q) \Rightarrow a=b \wedge P.(p,q)$.

Here we apply this to the example of EWD827.

The function from is given by

(0) $\quad$ from. n = n : from. (n+1) $\quad$ for all n .

The sequence nat is given by

(1) $\quad$ nat = 0 : inc. nat

where inc is given by

(2) $\quad \text{inc.}(\text{head} : \text{tail}) = \text{head}+1 : \text{inc.tail}$.

We are requested to prove

(3) $\quad \text{from}.0 = \text{nat}$.

From (3) and the base we see that we have to choose a P such that

(4) $\quad P.(\text{from}.0 , \text{nat})$

is satisfied. To find a suitable P we observe

$$
\begin{array}{ll}
 & s = \text{from}.0 \ \wedge\ t = \text{nat} \\
\Rightarrow & \quad \{(1)\} \\
 & s = \text{from}.0 \ \wedge\ t = 0 : \text{inc}.t \\
\Rightarrow & \quad \{\text{ instantiation }\} \\
 & (\underline{E} n :: s = \text{from}.n \ \wedge\ t = n : \text{inc}.t)
\end{array}
$$

,

from which we see that (4) - the base - is satisfied if we choose

(5) $\quad P.(s,t) = (\underline{E} n :: s = \text{from}.n \ \wedge\ t = n : \text{inc}.t)$.

In order to prove the step we observe for any a, b, p, q

$$
\begin{array}{ll}
 & P.(a{:}p , b{:}q) \\
= & \quad \{(5) \text{ with } s,t := a{:}p , b{:}q\} \\
 & (\underline{E} n :: a{:}p = \text{from}.n \ \wedge\ b{:}q = n : \text{inc}.(b{:}q)) \\
= & \quad \{(0) ; (2) \text{ with head, tail} := b, q\} \\
 & (\underline{E} n :: a{:}p = n : \text{from}.(n+1) \ \wedge\ b{:}q = n : b+1 : \text{inc}.q) \\
= & \quad \{ \text{ head:tail} = \text{head}' : \text{tail}' \ \equiv \\
 & \quad\ \ \text{head} = \text{head}' \ \wedge\ \text{tail} = \text{tail}' ; \text{ Leibniz}\}
\end{array}
$$

$(\underline{E}n :: \ a = n \ \wedge \ p = from.(n+1) \ \wedge$
$\quad b = n \ \wedge \ q = n+1 : inc.q \ )$
$\Rightarrow$ {predicate calculus}
$a = b \ \wedge \ (\underline{E}n :: \ p = from.(n+1) \wedge q = n+1 : inc.q \ )$
$\Rightarrow$ {transforming the dummy and (5)}
$a = b \ \wedge \ P.(p, q)$.

The advantage of the above proof format is that it absorbs the fact that from and nat have been defined by rather different recursion patterns.

Finally we would like to point out that the introduction of the dummy n and the existential quantification in the design of P are not such rabbits. Though our demonstrandum (3) only contains from.0 , we have to use from (0) that the definition of from.n holds for all n . Hence the generalization s = from.n ; the "invariance requirement" of P makes the introduction of n in the other conjunct all but obligatory.

Austin 12 February 1991

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