Three very little problems from Eindhoven

In my correspondence with Wim Feijen, he mentioned in the last months three little problems, which are nice enough not to be forgotten. Hence this note, which is purely for the record, and possibly for the instruction of my students. All in this note has been thought of by others before.

* * *

An "endofunction" is, by definition, a function whose value and whose argument are of the same type. Let f be an endofunction that is idempotent and surjective, i.e.

(0) $f.(f.x) = f.x$ for all x , and

(1) $\langle \exists y :: f.y = x \rangle$ for all x .

Show that f is the identity function, i.e.

(2) $f.x = x$ for all x .

To prove this, we observe for any x

$f.x = x$

= { (1), i.e. let y satisfy $f.y = x$ }

$f.(f.y) = f.y$

= { (0) with $x := y$ }

true .

The proof is not difficult to design after noticing that

- given (0), like demonstrandum (2), equates two expressions that only differ by 1 in their number of f-applications,
- (1) is the only given that equates something to the right-hand side of (2).

Finally, note that we did not build the proof on the terms "idempotent", "surjective" and "identity function", but on the formal definitions of these concepts.

*   *
*

Let N be a natural number such that $N \geq 1$, and let f be an endofunction such that f^N has exactly 1 fixpoint; show, that f has exactly 1 fixpoint.

In the problem statement, two "new" elements entered the picture: the notation "f^N" and the notion "fixpoint"; we deal with the first one first.

For endofunction f and natural n, f^n is an endofunction defined by

(3) $f^0.x = x$ for all x

(4) $f^{n+1}.x = f^n.(f.x)$ for all x, n .

The function f^n is sometimes called a "functional iteration" of f. About functional iteration we shall need the following lemma

(5) $\quad f^n.(f.x) = f.(f^n.x) \qquad$ for all x, n .

Proof of (5). The recursive definition (3), (4) of f^n and the fact that (5) is a proof obligation "for all n", make a proof by mathematical induction all but mandatory. Here we go.

For the base we have to demonstrate (5) with $n := 0$:

$$\begin{array}{ll} & f^0.(f.x) = f.(f^0.x) \\ = & \quad \{ (3),\ \text{twice} \} \\ & (f.x) = f.(x) \\ = & \quad \{ \text{redundancy of parentheses} \} \\ & \textit{true} \end{array}$$

For the step, we have to imply (5) with $n := N+1$ by (5) with $n \le N$. It is customary not to introduce the extra identifier N and to use n instead, and to label the appeals to (5) with $n \le N$ by the magic clause "ex hypothese". We shall follow the custom, and observe for any x, n

$$
\begin{array}{ll}
 & f^{n+1}.(f.x) \\
= & \quad \{ (4) \text{ with } x := (f.x) \} \\
 & f^{n}.(f.(f.x)) \\
= & \quad \{ \text{ex hypothese , i.e. } (5) \text{ with } x := (f.x) \} \\
 & f.(f^{n}.(f.x)) \\
= & \quad \{ (4) \} \\
 & f.(f^{n+1}.x)
\end{array}
$$

. (End of Proof of (5).)

Note. The proof of (5) has been included for purely educational reasons: it is one of a class of thousands and thousands, and, "if you have seen one of them, you have seen them all". The structure of the above proof is traditionally captured by the expression "mathematical induction over n". (End of note.)

Aside With functional composition $\circ$ defined by

$$(f \circ g).x = f.(g.x) \quad ,$$

(5) can be formulated as

$$f^{n} \circ f = f \circ f^{n} \quad .$$

Above, the step has been proved with two different instantiations for x in (4). Formulate (4) and the proof of the step in terms of the functional composition operator $\circ$, and you will discover to need that the latter is associative, i.e.

$$(f\circ g)\circ h \; = \; f\circ(g\circ h) \qquad \text{for all } f,g,h \; .$$

(End of Aside.)

Let us now deal with the notion of a "fixpoint": "x is a fixpoint of f" means $f.x = x$. A very simple lemma connects fixpoints and functional iteration: any fixpoint of f is also a fixpoint of any functional iteration of f:

(6) $\quad f.q = q \;\Rightarrow\; f^n.q = q \qquad$ for all f,q,n .

The proof is by mathematical induction over n , and —after the above elaboration about mathematical induction— is left, in confidence, to the reader.

After these preliminaries we return to our theorem to be proved. We capture the situation that f^N has exactly 1 fixpoint by naming it, p say:

(7) $\quad f^N.p = p$

(8) $\quad f^N.q = q \;\Rightarrow\; q = p \qquad$ for all q

Here (7) expresses that p is a fixpoint of f^N , and (8) that it is the only one.

On account of (6), the only acceptable candidate for the only fixpoint of f is p, i.e. we propose to demonstrate "f has exactly 1 fixpoint" by showing

$$(9) \qquad f.p = p$$

$$(10) \qquad f.q = q \;\Rightarrow\; q = p \qquad \text{for all } q .$$

To show (9), we observe

$$\begin{array}{ll}
 & f.p = p \\
\Leftarrow & \quad \{ (8) \text{ with } q := f.p \} \\
 & f^N.(f.p) = f.p \\
= & \quad \{ (5) \text{ with } n,x := N,p \} \\
 & f.(f^N.p) = f.p \\
\Leftarrow & \quad \{ \text{Leibniz's Principle} \} \\
 & f^N.p = p \\
= & \quad \{ (7) \} \\
 & \text{true}
\end{array}$$

To show (10) we observe for any q

$$\begin{array}{ll}
 & q = p \\
\Leftarrow & \quad \{ (8) \} \\
 & f^N.q = q \\
\Leftarrow & \quad \{ (6) \text{ with } n := N \} \\
 & f.q = q
\end{array}$$

Quod erat demonstrandum.

This problem was communicated (and perhaps designed) by M.L. Hautus.

* * *

We consider a set on which is defined a relation $\leq$ which is a "partial order", i.e. $\leq$ is

(11) reflexive: $x \leq x$
(12 antisymmetric: $x \leq y \ \wedge\ y \leq x \ \Rightarrow\ x = y$
(13) transitive: $x \leq y \ \wedge\ y \leq z \ \Rightarrow\ x \leq z$.

All three properties will be used below. Furthermore, our set is postulated to be such that for any two elements x, y the "infimum", denoted by $x{\downarrow}y$, exists; it has the defining property that for all w

(14) $w \leq x{\downarrow}y \ \equiv\ w \leq x \ \wedge\ w \leq y$

Instantiating (14) with $w := x{\downarrow}y$ and using (11), viz. that $\leq$ is reflexive, we directly derive

(15) $x{\downarrow}y \leq x \ \wedge\ x{\downarrow}y \leq y$,

a property that will be used below.

Endofunction f is "monotonic" means that for all x, y

(16) $x \leq y \ \Rightarrow\ f.x \leq f.y$

and "p is a least prefixpoint of f" means

(17) $f.p \leq p$

(18) $f.x \leq x \Rightarrow p \leq x$ for all x

<u>Remark</u> Let p and q each be a least prefixpoint of f. Instantiating (18) with $x := q$ and using $f.q \leq q$, we derive $p \leq q$; similarly we derive $q \leq p$ and on account of (12), viz. that $\leq$ is antisymmetric, we conclude that $p = q$. In other words, a function has at most 1 least prefixpoint (it could have none at all). (End of Remark.)

For a partial order with infimum and a monotonic endofunction f with least prefixpoint p -i.e. under validity of (11) through (18) - we are requested to show that f^2 has a least prefixpoint, i.e. we have to show the existence of a q such that

(19) $f.(f.q) \leq q$ and

(20) $f.(f.x) \leq x \Rightarrow q \leq x$ for all x.

It is sweetly reasonable to expect a constructive existence proof, i.e. a specific choice for q so that we can prove

(19) and (20). Let us first look at our obligation to prove (19), since that is the simplest of the two.

Since we have not yet used that $\le$ is transitive, we can decide to conclude (19) for suitably chosen z from

$$f.(f.q) \le z \;\wedge\; z \le q \qquad .$$

Remark Because $\le$ is reflexive, we never need to regret that decision: the choices $z := f.(f.q)$ and $z := q$ convert the above back into the original (19). (End of Remark.)

Because the structural novelty of (19) is 2 f-applications more to the left of $\le$ than to its right, we choose, to bridge that gap, $z := f.r$, with r to be suitably chosen later. We now observe for any q, r

$$\begin{array}{ll}
 & f.(f.q) \le q \\
\Leftarrow & \quad \{ \le \text{ is transitive} \} \\
 & f.(f.q) \le f.r \;\wedge\; f.r \le q \\
\Leftarrow & \quad \{ f \text{ is monotonic: (16) with } x,y := (f.q), r \} \\
 & f.q \le r \;\wedge\; f.r \le q \qquad ,
\end{array}$$

a proof-obligation that we can halve

by choosing r and q equal to each other. With $r := q$ we are left with the obligation to demonstrate $f.q \leq q$ for suitably chosen q. There are now two reasons for chosing $q := p$:

(i) given (17) then completes the proof of (19)

(ii) the consequent of (20) –still to be proved– then becomes the same as the consequent of given (18).

Having established

(19') $\quad f.(f.p) \leq p$,

our final proof obligation is

(20') $\quad f.(f.x) \leq x \quad \Rightarrow \quad p \leq x \quad$ for all x.

(20') would be established by a calculation of the form

$$\begin{array}{ll} & p \leq x \\ \Leftarrow & \quad \{(18)\} \\ & f.x \leq x \\ \Leftarrow & \quad \{???\} \\ & f(f.x) \leq x \end{array}$$,

but there is no way in which the hint {???} can justify the last step. (There exist counterexamples.) This is the moment to exploit a very special structural property of (18): while its consequent is strengthened when x is replaced by a "smaller" y (i.e. satisfying $y \leq x$), its antecedent is not necessarily strengthened by that replacement (and might become provable).

Remark The phenomenon usually occurs when a quantity -like p in this example- has been given as the extreme solution of an equation. We encounter the same situation when an induction hypothesis is strengthened in order to make the induction step provable. This third problem is included because it presents such a nice example of the phenomenon. (End of Remark.)

We use the existence of the infimum, in particular (15) to construct an expression that is "smaller" than x. After the introduction of $\downarrow$, it has to be eliminated again; to the right of $\leq$ we do this via (14) -what else?- and to the left of $\leq$ via (15) -what else?- .

We observe for any x

$$
\begin{array}{ll}
 & p \leq x \\
\Leftarrow & \quad \{ (15) \text{ with } y := f.x \text{ ; transitivity of } \leq \} \\
 & p \leq x \downarrow f.x \\
\Leftarrow & \quad \{ (18) \text{ with } x := x \downarrow f.x \} \\
 & f.(x \downarrow f.x) \leq x \downarrow f.x \\
= & \quad \{ (14) \text{ with } w, y := f.(x \downarrow f.x) , f.x \\
 & f.(x \downarrow f.x) \leq x \;\wedge\; f.(x \downarrow f.x) \leq f.x \\
\Leftarrow & \quad \{ (15) \text{ with } y := f.x \text{ -both conjuncts!-,} \\
 & \quad\;\; \text{monotonicity of } f \text{, transitivity of } \leq \} \\
 & f.(f.x) \leq x \;\wedge\; f.x \leq f.x \\
= & \quad \{ \leq \text{ is reflexive} \} \\
 & f.(f.x)
\end{array}
$$

Quod erat demonstrandum.

Remark The choice $y := f.x$ for (15) in the first step is not surprising. The purpose of appealing to (18) is to eliminate p from the intermediate result, so we should not instantiate y with an expression containing p; $f.x$ is the simplest combination of the two identifiers left. (End of Remark.)

In the above proof development I essentially followed Wim H.J. Feijen, the problem was communicated (and possibly designed) by Henk Doornbos and Jaap C.S.P. van der Woude; the latter also constructed a counterexample demonstrating that no {???} could exist.

I thank the students that attend my current undergraduate course for the incentive to write this down (and Mont Blanc USA, which repaired my pen and made it again a pleasure to handle.)

Austin, 4 February 1996

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