More equality proofs with instantiated definitions

We quote from the chapter "The design of a proof of equality" the following about the maximum operator ↑ and the minimum operator ↓ . For all real w, x, y

(0) $\quad x\uparrow y \leq w \quad\equiv\quad x\leq w \;\wedge\; y\leq w$

(1) $\quad w\leq x\uparrow y \quad\equiv\quad w\leq x \;\vee\; w\leq y$

(2) $\quad w\leq x\downarrow y \quad\equiv\quad w\leq x \;\wedge\; w\leq y$

(3) $\quad x\downarrow y\leq w \quad\equiv\quad x\leq w \;\vee\; y\leq w \quad ,$

and in the proof of the above, essential use was made of the antisymmetry of $\leq$, i.e

(4) $\quad p=q \;\Leftarrow\; p\leq q \wedge q\leq p \quad$ for all p, q .

Remark In predicate calculus, the antisymmetry of the implication, i.e.

$$[X\equiv Y] \;\Leftarrow\; [X\Rightarrow Y] \wedge [Y\Rightarrow X]$$

is often used similarly; it is there known as "a proof by mutual implication". Also the somewhat more general term "ping-pong argument" is in use: an appeal to (4) leads to a ping-pong argument but not to a proof by mutual implication. (End of Remark.)

Mathematical Methodology

Sometimes the ping-pong argument is entirely appropriate, for instance, when the ping part is totally independent of the pong part: in such a case, the ping-pong argument embodies a laudable disentanglement of the proof. The avoidable ping-pong argument, however, has a bad name because of its (avoidable) case analysis.

At first sight, one might expect equality proofs based on (0) through (3) to take the form of ping-pong arguments, but fortunately there is an alternative: for all real p, q ,

(5) $\quad p = q \;\Leftarrow\; (\underline{A}w :: p \leq w \equiv q \leq w)$ $\quad$ and

(6) $\quad p = q \;\Leftarrow\; (\underline{A}w :: w \leq p \equiv w \leq q)$

<u>Proof of (5)</u>

$$
\begin{array}{ll}
 & (\underline{A}w :: p \leq w \equiv q \leq w) \\
\Leftarrow & \quad \{ \text{with } w := q \text{ ; with } w := p \} \\
 & (p \leq q \equiv q \leq q) \wedge (p \leq p \equiv q \leq p) \\
= & \quad \{ \leq \text{ reflexive , } true \text{ is identity element of } \equiv \} \\
 & p \leq q \;\wedge\; q \leq p \\
\Leftarrow & \quad \{ (4) \} \\
 & p = q
\end{array}
$$

(End of Proof of (5).)

Mathematical Methodology

On account of the above proof of (5), one might be lead to believe that an appeal to (5) for proving $p=q$ is extremely wasteful: why establishing $p \le w \equiv q \le w$ for *any* w, whereas the equivalence is *only* needed for the two special cases $w=p$ and $w=q$? The first remark is that, instead of (5), we could have written

$$p=q \equiv (\underline{A}w:: p \le w \equiv q \le w)$$

– since, on account of Leibniz's Principle, the left-hand side implies the right-hand side –, so proving the equivalence for *any* w is, logically at least, no extra burden. The second remark is that proving $p \le w \equiv q \le w$ for *any* w absorbs the case analysis of proving it for $w=p$ and $w=q$ separately. The third remark is that proving the equivalence for *any* w is easier than proving it for special values, because in the proof for arbitrary w we are forced to ignore what makes those special values special.

By way of illustration we shall prove a number of little theorems

Theorem 0: Operator ↑ is idempotent, i.e. for any x

(7) $\quad x \uparrow x = x \quad .$

<u>Proof</u> On account of (5), it suffices to observe for any x, w

$$\begin{aligned}
& x\uparrow x \leq w \\
= \quad & \{ (0) \text{ with } y := x \} \\
& x \leq w \ \wedge \ x \leq w \\
= \quad & \{ \text{pred. calc., in particular idempotence of } \wedge \} \\
& x \leq w \quad .
\end{aligned}$$

(End of Proof)

<u>Theorem 1</u> Operator ↑ is symmetric, i.e. for any x, y

(8) $\qquad x\uparrow y = y\uparrow x \quad .$

<u>Proof</u> On account of (5), it suffices to observe for any x, y, w

$$\begin{aligned}
& x\uparrow y \leq w \\
= \quad & \{ (0) \} \\
& x \leq w \ \wedge \ y \leq w \\
= \quad & \{ \text{pred. calc., in particular symmetry of } \wedge \} \\
& y \leq w \ \wedge \ x \leq w \\
= \quad & \{ (0) \text{ with } x, y := y, x \} \\
& y\uparrow x \leq w \quad .
\end{aligned}$$

(End of Proof)

<u>Theorem 2</u> Operator ↑ is associative, i.e. for any x, y, z

(9) $\qquad (x\uparrow y)\uparrow z = x\uparrow(y\uparrow z) \quad .$

<u>Proof</u> On account of (5), it suffices to observe for any x, y, z, w

$$
\begin{array}{ll}
 & (x\uparrow y)\uparrow z \leqslant w \\
= & \quad \{(0) \text{ with } x,y := (x\uparrow y), z\} \\
 & (x\uparrow y) \leqslant w \;\wedge\; z \leqslant w \\
= & \quad \{(0)\} \\
 & (x \leqslant w \;\wedge\; y \leqslant w) \;\wedge\; z \leqslant w \\
= & \quad \{\text{pred. calc., in particular associativity of } \wedge\} \\
 & x \leqslant w \;\wedge\; (y \leqslant w \;\wedge\; z \leqslant w) \\
= & \quad \{(0) \text{ with } x,y := y,z\} \\
 & x \leqslant w \;\wedge\; (y\uparrow z) \leqslant w \\
= & \quad \{(0) \text{ with } y := (y\uparrow z)\} \\
 & x\uparrow(y\uparrow z) \quad .
\end{array}
$$

Theorem3 Operator ↓ distributes over ↑, i.e for any x, y, z

(10) $\quad (x\uparrow y)\downarrow z \;=\; (x\downarrow z)\uparrow(y\downarrow z) \quad .$

Proof In view of (5), it suffices to observe for any x, y, z, w

$$
\begin{array}{ll}
 & (x\uparrow y)\downarrow z \leqslant w \\
= & \quad \{(3) \text{ with } x,y := (x\uparrow y), z\} \\
 & (x\uparrow y) \leqslant w \;\vee\; z \leqslant w \\
= & \quad \{(0)\} \\
 & (x \leqslant w \;\wedge\; y \leqslant w) \;\vee\; z \leqslant w \\
= & \quad \{\text{pred. calc., in particular } \vee \text{ distributes over } \wedge\} \\
 & (x \leqslant w \;\vee\; z \leqslant w) \;\wedge\; (y \leqslant w \;\vee\; z \leqslant w) \\
= & \quad \{(3) \text{ with } y := z \;;\; (3) \text{ with } x,y := y,z\} \\
 & (x\downarrow z) \leqslant w \;\wedge\; (y\downarrow z) \leqslant w
\end{array}
$$

Mathematical Methodology

$$= \quad \{(0) \text{ with } x,y := (x{\downarrow}z), (y{\downarrow}z)\}$$
$$(x{\downarrow}z) \uparrow (y{\downarrow}z)$$

(End of Proof.)

The reader who has followed the above proofs in detail must have become highly suspicious: for the real numbers, the operator pair $(\uparrow, \downarrow)$ —or the other way round $(\downarrow, \uparrow)$— is very much like the operator pair $(\vee, \wedge)$ for the boolean domain. The pursuit of such analogies is a valid mathematical exercise. In fact, every equality between boolean expressions in $\vee$ and $\wedge$ only, can be translated into the equality between real expression in $\uparrow$ and $\downarrow$ only. For instance, the Law of Absorption

$$X \vee (X \wedge Y) \equiv X$$

yields $\quad x \uparrow (x \downarrow y) = x \quad ,$

and $\quad (X \vee Y) \wedge (Y \vee Z) \wedge (Z \vee X) \equiv$
$\quad (X \wedge Y) \vee (Y \wedge Z) \vee (Z \wedge X)$

yields $\quad (x \uparrow y) \downarrow (y \uparrow z) \downarrow (z \uparrow x) =$
$\quad (x \downarrow y) \uparrow (y \downarrow z) \uparrow (z \downarrow x)$

or: for any three real numbers the minimum of the pairwise maxima equals the maximum of the pairwise minima. The matter will not be pursued here, we prove another theorem

Mathematical Methodology

instead.

Theorem 4 Addition distributes over ↑, i.e. for any x, y, z

(11) $(x \uparrow y) + z \;=\; (x+z) \uparrow (y+z)$

Proof In view of (5), it suffices to observe for any x, y, z, w

$$\begin{array}{ll}
 & (x \uparrow y) + z \leq w \\
= & \quad \{\text{arithmetic}\} \\
 & (x \uparrow y) \leq w - z \\
= & \quad \{(0) \text{ with } w := w - z\} \\
 & x \leq w-z \;\wedge\; y \leq w-z \\
= & \quad \{\text{arithmetic, twice}\} \\
 & x+z \leq w \;\wedge\; y+z \leq w \\
= & \quad \{(0) \text{ with } x,y := x+z, y+z\} \\
 & (x+z) \uparrow (y+z) \leq w
\end{array}$$

(End of Proof)

Finally we show

Theorem 5 $x \uparrow y \leq x+y \;\equiv\; 0 \leq x \;\wedge\; 0 \leq y$

Proof We observe for any x, y

$$\begin{array}{ll}
 & x \uparrow y \leq x+y \\
= & \quad \{(0) \text{ with } w := x+y\} \\
 & x \leq x+y \;\wedge\; y \leq x+y \\
= & \quad \{\text{arith metic, twice}\} \\
 & 0 \leq y \;\wedge\; 0 \leq x \;.
\end{array}$$

(End of Proof)

Mathematical Methodology

All the above proofs owe their brevity to our freedom to instantiate (0) through (3) with special values for w – be it directly or through (5) or (6) – . Had we taken for the maximum a definition like

$\underline{\text{if}}\ x \geq y \rightarrow x\ [\!]\ y \geq x \rightarrow y\ \underline{\text{fi}}$,

proofs with case analyses would have been unavoidable.

* * *

We conclude this chapter with two proofs of the associativity of functional composition, i.e. for functions f, g, h (of the appropriate types) we have to show

(12) $\quad f\circ(g\circ h) = (f\circ g)\circ h$.

The first proof is based on a definition of functional composition expressed in terms of the formalism of the λ-calculus. For functions p, q , the function $p\circ q$ is defined by

(13) $\quad p\circ q = (\lambda z: p.(q.z))$;

at the right-hand side, the dummy z is a fresh variable (i.e. z does *not* occur as free variable in p or in q); consequently, the <u>only</u> occurrence of the free variable z in $p.(q.z)$ is the one shown as the argument to which q is applied.

From the λ-calculus we use

(14) $\quad (\lambda x\!: E).y =$ "E with y substituted for x".

We observe for any f, g, h

$f\circ(g\circ h)$
$=\quad \{$ (13) with $p,q := f, (g\circ h)\ \}$
$(\lambda z\!: f.((g\circ h).z))$
$=\quad \{$ (13) with $p,q,z := g,h,x\ \}$
$(\lambda z\!: f.((\lambda x\!: g.(h.x)).z))$
$=\quad \{$ (14) with $E,y := g.(h.x), z\ \}$
$(\lambda z\!: f.(g.(h.z)))$
$=\quad \{$ (14) with $E,y := f.(g.x), h.z\ \}$
$(\lambda z\!: (\lambda x\!: f.(g.x)).(h.z))$
$=\quad \{$ (13) with $p,q,z := f,g,x$
$(\lambda z\!: (f\circ g).(h.z))$
$=\quad \{$ (13) with $p,q := (f\circ g), h\ \}$
$(f\circ g)\circ h$,

thus having proved (12). The use of the λ-calculus enabled us to carry out this proof in terms of equality of functions. Let us now pursue what happens when we

Mathematical Methodology

avoid the λ-calculus and carry the argument out in terms of equality of function applications. Expressed in function applications, our demonstrandum (12) becomes

$$(15)\qquad (f\circ(g\circ h)).z = ((f\circ g)\circ h).z \quad \text{for all } z$$

and the definition of functional composition

$$(16)\qquad (p\circ q).z = p.(q.z) \quad \text{for all } z.$$

In order to demonstrate (15), we observe for any f, g, h, z

$$\begin{array}{ll}
 & (f\circ(g\circ h)).z \\
= & \quad \{(16) \text{ with } p,q := f,(g\circ h)\} \\
 & f.((g\circ h).z) \\
= & \quad \{(16) \text{ with } p,q := g,h\} \\
 & f.(g.(h.z)) \\
= & \quad \{(16) \text{ with } p,q,z := f,g,(h.z)\} \\
 & (f\circ g).(h.z) \\
= & \quad \{(16) \text{ with } p,q := (f\circ g),h\} \\
 & ((f\circ g)\circ h).z \quad .
\end{array}$$

As the instantiations of p,q show, this proof of (15) and the preceding proof of (12) are in a sense different renderings of the "same" proof, but in another sense they are very different.

Mathematical Methodology

There are striking quantitative differences. The former proof requires 6 steps, the latter one only 4 . In the latter proof the depth of parenthesis nesting is homogeneously 2, in the former proof it begins and ends at 1, but reaches 4 in between (which seems excessive). Symbol counts for the equated expressions in the former yield 7, 16, 23, 16, 23, 16, 7 (sum 108), in the latter 11, 11, 11, 11, 11 (sum 55); sum and maximum differ both by a factor of 2 . More important than these differences themselves is understanding their origin.

The theorem is about equality of functions, the former proof manipulates function expressions. Equality of functions, however, is defined in terms of there application

(17) $\varphi = \psi \;\equiv\; (\underline{A} z :: \; \varphi.z = \psi.z)$

and instead of transforming φ into ψ , as the former proof does, the latter one transforms $\varphi.z$ into $\psi.z$ for arbitrary z . We could change the former proof into one transforming $\varphi.z$ into $\psi.z$ by postfixing each of its equated expressions by ".z" —actually prefixing by "(" and postfixing by ").z"— but our latter proof is very different: *none* of the three intermediate results has the form of a function applied to z . In other words, the extra manipulative freedom provided by the initial and final ".z" is used all through the calculation (and evidently at good advantage).

A second source of brevity is that definition (16) of functional composition really combines what we need from (13) and (14). To deduce (16) from the latter two we observe for any p, q, z

$$\begin{array}{ll} & (p\circ q).\,z \\ = & \quad \{(13)\} \\ & (\lambda z{:}\ p.(q.\,z)).\,z \\ = & \quad \{(14) \text{ with } x, E, y := z,\ p.(q.\,z),\ z\} \\ & p.(q.z) \end{array}$$

and, since, thanks to (17), (16) captures all there is to be said about functional composition, we don't need lambdas at all.

The advantage of (16) over (13) as definition of functional composition is that it contains a variable more that can be instantiated; it is that additional freedom that allows us to eliminate in the latter proof the two middle steps of the former proof.

In comparison to (13), definition (16) of functional composition also limits our manipulative freedom: using it, we can only manipulate a functional composition that is applied to an argument. In the latter proof we are forced to eliminate the outer $\circ$ first, whereas in the former proof the first two steps could have been interchanged; but the outcome is the same and the freedom is irrelevant. The reader is invited to verify that the proof using (16) can be constructed on the very simple principle: "There is only one thing you can do.".

Acknowledgement I owe the examples with the maximum to W.H.J. Feijen. (End of Acknowledgement.)

Austin, 11 February 1991

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

Mathematical Methodology