On extreme solutions

Introductory Remark Following J. Misra, I shall use the dedicated parenthesis pair ⟨ ⟩ to delineate the scope of dummies. Following J.L.A. van de Snepscheut, I shall write the quantifier to the left of the opening parenthesis. Finally, I shall use $\forall$ and $\exists$, but not for very good reason: it can be argued that $\underline{\wedge}$ and $\underline{\vee}$ are to be preferred. (End of Introductory Remark.)

Let $\sqsubseteq$ – read "below" – be a punctual relation on structures of some type, i.e.

$$[u=v \wedge x=y \Rightarrow (u \sqsubseteq x \equiv v \sqsubseteq y)] \quad \text{for all } u,v,x,y \ .$$

In EWD1102, we have shown that for $\sqsubseteq$ a preorder – i.e. a reflexive and transitive relation –

(0) $[x \sqsubseteq y \equiv \forall\langle z :: z \sqsubseteq x \Rightarrow z \sqsubseteq y\rangle]$ and

(1) $[x \sqsubseteq y \equiv \forall\langle z :: x \sqsubseteq z \Leftarrow y \sqsubseteq z\rangle]$.

Furthermore, for a preorder $\sqsubseteq$, a value k satisfying

(2) $\forall\langle x :: [x \sqsubseteq k \equiv \forall\langle y : y \in W : x \sqsubseteq f.y\rangle]\rangle$

is called a highest lower bound for the set $\{z \mid \exists\langle y : y \in W : [z = f.y]\rangle\}$. (Note that, for f equal

to the identity function, i.e. $\langle\forall y :: [f.y = y]\rangle$, the k satisfying (2) is a highest lower bound of the set W.) A lowest higher bound of that set is, similarly, a value h satisfying

(3) $\quad \langle\forall x :: [h \sqsubseteq x \equiv \langle\forall y : y \in W : f.y \sqsubseteq x\rangle]\rangle$.

We remind the reader that the names "highest lower bound" and "lowest higher bound" only make sense because we have chosen to pronounce the character $\sqsubseteq$ as "below".

* * *

Let us now investigate, how we can ensure that (2), viewed as equation in k, does not have more than 1 solution. Let k' satisfy

(2') $\quad \langle\forall x :: [x \sqsubseteq k' \equiv \langle\forall y : y \in W : x \sqsubseteq f.y\rangle]\rangle$;

demonstrating uniqueness of the highest lower bound then amounts to demonstrating $[k = k']$. We observe

$$
\begin{array}{ll}
 & \text{true} \\
= & \quad \{(2) \text{ with } x := k\} \\
 & [k \sqsubseteq k \equiv \langle\forall y : y \in W : k \sqsubseteq f.y\rangle] \\
= & \quad \{\sqsubseteq \text{ is reflexive}\} \\
 & [\langle\forall y : y \in W : k \sqsubseteq f.y\rangle] \\
= & \quad \{(2') \text{ with } x := k\} \\
 & [k \sqsubseteq k'] \quad .
\end{array}
$$

The transpose $[k' \sqsubseteq k]$ can be derived similarly.

In order to conclude now $[k = k']$, we assume $\sqsubseteq$ to be antisymmetric as well, i.e.

$$[x \sqsubseteq y \wedge y \sqsubseteq x \Rightarrow x = y] \quad .$$

A relation that is reflexive, transitive, & antisymmetric is called a <u>partial order</u>. For the rest of this note, $\sqsubseteq$ denotes a partial order.

By restricting ourselves for $\sqsubseteq$ to a partial order, we ensure that at most 1 value k satisfies (2) and at most 1 value h satisfies (3). But there may be none! From now onwards we restrict ourselves for $\sqsubseteq$ to such partial orders that a k and h, satisfying (2) and (3) respectively, always exist, i.e. for the rest of this note, each set has a unique lowest higher bound and a unique highest lower bound.

* * *

The lowest higher bound of the universe — i.e. $y \in W \equiv$ true and $[f.y = y]$ — is traditionally called "top" and denoted by "T"; it is also the highest lower bound of the empty set — i.e. $y \in W \equiv$ false —. In order to demonstrate this dual rôle of T we observe

(T is the lowest higher bound of the universe)
= { (3) with $h := T$, $y \in W \equiv$ true, $f.y = y$ }

$$\langle\forall x :: [T \sqsubseteq x \equiv \langle\forall y :: y \sqsubseteq x\rangle]\rangle$$

$\Rightarrow$ { instantiate with $x := T$ }

$$[T \sqsubseteq T \equiv \langle\forall y :: y \sqsubseteq T\rangle]$$

$=$ { $\sqsubseteq$ is reflexive; renaming dummy }

$$[\langle\forall x :: x \sqsubseteq T\rangle]$$

$=$ { predicate calculus }

$$\langle\forall x :: [x \sqsubseteq T \equiv \langle\forall y : \text{false} : x \sqsubseteq y\rangle]\rangle$$

$=$ { (2) with $k := T$, $y \in W \equiv \text{false}$, $f.y = y$ }

(T is the highest lower bound of the empty set).

Since (2) and (3) determine the bounds uniquely, we don't need to demonstrate the inverse implication (which is much harder).

Similarly, the highest lower bound of the universe is also the lowest higher bound of the empty set; it is traditionally called "bottom" and denoted by "$\bot$".

* * *

The extreme bounds now being unique, we are going to experiment with a functional notation. We denote the value k satisfying (2) by $\Pi\langle y : y \in W : f.y\rangle$, and the value h satisfying (3) by $\sqcup\langle y : y \in W : f.y\rangle$, i.e.

the highest lower bound Π is defined by

(4) $$\langle\forall x :: [x \sqsubseteq \Pi\langle y : y \in W : f.y\rangle \equiv \langle\forall y : y \in W : x \sqsubseteq f.y\rangle]\rangle$$

and the lowest higher bound is defined by

(5) $\quad \langle\forall x :: [\, \langle\sqcup y : y \in W : f.y\rangle \sqsubseteq x \;\equiv\; \langle\forall y : y \in W : f.y \sqsubseteq x\rangle \,]\rangle$.

The equivalent expressions are in both formulae so similar that doubts about the usefulness of $\sqcap$ and $\sqcup$ could be voiced.

The extreme bounds are monotonic in the following sense – we formulate and prove for $\sqcap$ –

$$[\langle\forall y : y \in W : f.y \sqsubseteq g.y\rangle \;\Rightarrow\; \langle\sqcap y : y \in W : f.y\rangle \sqsubseteq \langle\sqcap y : y \in W : g.y\rangle\,]$$

Proof We observe

$$\begin{aligned}
&\langle\sqcap y : y \in W : f.y\rangle \sqsubseteq \langle\sqcap y : y \in W : g.y\rangle \\
=\quad &\{(0)\} \\
&\langle\forall z :: z \sqsubseteq \langle\sqcap y : y \in W : f.y\rangle \Rightarrow z \sqsubseteq \langle\sqcap y : y \in W : g.y\rangle\rangle \\
=\quad &\{(4) \text{ twice}\} \\
&\langle\forall z :: \langle\forall y : y \in W : z \sqsubseteq f.y\rangle \Rightarrow \langle\forall y : y \in W : z \sqsubseteq g.y\rangle\rangle \\
\Leftarrow\quad &\{\text{monotonicity of } \forall\} \\
&\langle\forall z :: \langle\forall y : y \in W : z \sqsubseteq f.y \Rightarrow z \sqsubseteq g.y\rangle\rangle \\
=\quad &\{\text{interchange of universal quantifications}\} \\
&\langle\forall y : y \in W : \langle\forall z :: z \sqsubseteq f.y \Rightarrow z \sqsubseteq g.y\rangle\rangle \\
=\quad &\{(0)\} \\
&\langle\forall y : y \in W : f.y \sqsubseteq g.y\rangle
\end{aligned}$$

Note how (0) is used "in both directions": to introduce and to eliminate again the universal quantification over z. (End of Proof?)

In the above the symbol Π is primarily used to formulate the theorem; in the proof, the symbol Π is eliminated as soon as possible.

We leave to the reader the proofs of

$$V \subseteq W \Rightarrow [\Pi\langle y: y \in W: f.y\rangle \subseteq \Pi\langle y: y \in V: f.y\rangle] \wedge [\sqcup\langle y: y \in V: f.y\rangle \subseteq \sqcup\langle y: y \in W: f.y\rangle] \ .$$

The proofs are very similar to what we just saw.

* * *

Function f is monotonic means here

$$(6) \qquad [x \subseteq y] \Rightarrow [f.x \subseteq f.y] \ .$$

For monotonic f we can prove (7) & (8)

$$(7) \qquad [f.\Pi\langle y: y \in W: y\rangle \subseteq \Pi\langle y: y \in W: f.y\rangle]$$

$$(8) \qquad [\sqcup\langle y: y \in W: f.y\rangle \subseteq f.\sqcup\langle y: y \in W: y\rangle] \ ;$$

we shall prove (7).

Proof In the following we leave the range "$y \in W$" understood and observe for any monotonic f

$$\begin{aligned} & [f.\Pi\langle y :: y\rangle \subseteq \Pi\langle y :: f.y\rangle] \\ = & \quad \{(4) \text{ with } x := f.\Pi\langle y :: y\rangle\} \\ & [\forall\langle y :: f.\Pi\langle y :: y\rangle \subseteq f.y\rangle] \\ = & \quad \{\text{interchange}\} \\ & \forall\langle y :: [f.\Pi\langle y :: y\rangle \subseteq f.y]\rangle \\ \Leftarrow & \quad \{f \text{ monotonic}\} \end{aligned}$$

$$
\begin{array}{ll}
 & \langle \forall y :: [\langle \sqcap y :: y \rangle \sqsubseteq y] \rangle \\
= & \{(0), \text{see Note below}\} \\
 & \langle \forall y :: [\langle \forall z :: z \sqsubseteq \langle \sqcap y :: y \rangle \Rightarrow z \sqsubseteq y \rangle] \rangle \\
= & \{(4) \text{ with } x, f := z, \text{identity}\} \\
 & \langle \forall y :: [\langle \forall z :: \langle \forall y :: z \sqsubseteq y \rangle \Rightarrow z \sqsubseteq y \rangle] \rangle \\
= & \{\text{predicate calculus}\} \\
 & \text{true}
\end{array}
$$

(End of Proof.)

Note The appeal to (0), rather than to (1), is to get $\langle \sqcap y :: y \rangle$ as right-hand operand of $\sqsubseteq$, as - see (4) - we need $\sqcap$ there in order to be able to eliminate it. (End of Note.)

* * *

Now we are ready for the theorem of Knaster-Tarski:

For monotonic f, the equations

(9) $\quad x : [f.x \sqsubseteq x]$ and

(10) $\quad x : [f.x = x]$

both have a lowest solution, and the two lowest solutions are the same.

Proof We define q by

$$[q = \langle \sqcap y : [f.y \sqsubseteq y] : y \rangle]$$

and observe, in order to prove that q solves (9):

$$
\begin{array}{ll}
 & f.q \\
= & \quad \{\text{def. of } q\} \\
 & f.\langle\sqcap y : [f.y \sqsubseteq y] : y\rangle \\
\sqsubseteq & \quad \{f \text{ is monotonic, } (7)\} \\
 & \langle\sqcap y : [f.y \sqsubseteq y] : f.y\rangle \\
\sqsubseteq & \quad \{\sqcap \text{ is monotonic}\} \\
 & \langle\sqcap y : [f.y \sqsubseteq y] : y\rangle \\
= & \quad \{\text{def. of } q\} \\
 & q \quad ,
\end{array}
$$

which observation establishes $[f.q \sqsubseteq q]$ thanks to the transitivity of $\sqsubseteq$; so q is a solution of (9), and it is its lowest solution, for we observe

$$
\begin{array}{ll}
(11) & \langle\forall y : [f.y \sqsubseteq y] : q \sqsubseteq y\rangle \\
= & \quad \{\text{def. of } \sqcap\} \\
 & q \sqsubseteq \langle\sqcap y : [f.y \sqsubseteq y] : y\rangle \\
= & \quad \{\text{def. of } q, \sqsubseteq \text{ is reflexive}\} \\
 & \text{true} .
\end{array}
$$

Next we observe

$$
\begin{array}{ll}
 & [f.q = q] \\
\Leftarrow & \quad \{\sqsubseteq \text{ is antisymmetric}\} \\
 & [f.q \sqsubseteq q] \wedge [q \sqsubseteq f.q] \\
\Leftarrow & \quad \{(11) \text{ with } y := f.q\} \\
 & [f.q \sqsubseteq q] \wedge [f.(f.q) \sqsubseteq f.q] \\
\Leftarrow & \quad \{f \text{ is monotonic}\} \\
 & [f.q \sqsubseteq q] \wedge [f.q \sqsubseteq q] \\
= & \quad \{q \text{ solves } (9)\}
\end{array}
$$

true ,

so q solves (10) as well. Moreover, q is the lowest solution of (10), as follows from the observation

$$\begin{array}{ll} & \langle \forall y : [f.y = y] : q \sqsubseteq y \rangle \\ \Leftarrow & \quad \{ [f.y = y] \Rightarrow [f.y \sqsubseteq y], \text{ as } \sqsubseteq \text{ reflexive} \} \\ & \langle \forall y : [f.y \sqsubseteq y] : q \sqsubseteq y \rangle \\ = & \quad \{ 11 \} \\ & \text{true.} \end{array}$$

* * *

We now consider the equation

(12) $$x : [f.x.y \sqsubseteq x] \quad .$$

We assume $f.x.y$ to be a monotonic function of both arguments. We have just seen that f's monotonicity in its 1st argument guarantees the existence of a lowest solution of (12). We denote it by $g.y$, its being a solution expressed by

(13) $$[f.(g.y).y \sqsubseteq g.y] \quad \text{for all } y$$

and its being as low as any solution expressed by

(14) $$[f.x.y \sqsubseteq x] \Rightarrow [g.y \sqsubseteq x] \quad \text{for all } x,y \ .$$

(Here we mention (13) and (14) as properties of g; they do, in fact, determine g.)

It is well-known that g is monotonic if f is monotonic in its 2nd argument. I used to demonstrate that by observing

$$
\begin{array}{ll}
 & [\, g.p \sqsubseteq g.q \,] \\
\Leftarrow & \quad \{(14) \text{ with } x,y := g.q\,,\, p\} \\
 & [\, f.(g.q).p \sqsubseteq g.q \,] \\
\Leftarrow & \quad \{(13) \text{ with } y := q\,,\ \text{transitivity of } \sqsubseteq\} \\
 & [\, f.(g.q).p \sqsubseteq f.(g.q).q \,] \\
\Leftarrow & \quad \{f \text{ monotonic in 2nd argument}\} \\
 & [\, p \sqsubseteq q \,]
\end{array}
$$

QED.

But because

$$[\, g.y \equiv \sqcap\langle x : [\, f.x.y \sqsubseteq x \,] : x \rangle \,]$$

we can write alternatively

$$
\begin{array}{ll}
(*) & [\, \sqcap\langle x : [\, f.x.p \sqsubseteq x \,] : x \rangle \sqsubseteq \sqcap\langle x : [\, f.x.q \sqsubseteq x \,] : x \rangle \,] \\
\Leftarrow & \quad \{\text{"range monotonicity" of } \sqcap\text{, see EWD1107-5}\} \\
 & \forall\langle x :: [\, f.x.p \sqsubseteq x \,] \Leftarrow [\, f.x.q \sqsubseteq x \,] \rangle \\
\Leftarrow & \quad \{\text{transitivity of } \sqsubseteq\} \\
 & \forall\langle x :: [\, f.x.p \sqsubseteq f.x.q \,] \rangle \\
\Leftarrow & \quad \{f \text{ monotonic in 2nd argument}\} \\
 & [\, p \sqsubseteq q \,]
\end{array}
$$

Comparing the two proofs, we see that, in the latter proof, there was no need to formulate (13) and (14); we could even have done without the function name g, as we could have taken (*) as the consequent of our proof obligation. The latter proof has the

disadvantage -if it is one- of needing the theorem about the range monotonicity of Π, but the charm that after the first step, all traces of extreme solutions have disappeared. Notice, in contrast, that in the former proof the intermediate result after the second step

$$[f.(g.q).p \leq f.(g.q).q]$$

still mentions the no longer relevant function g.

* * *

In the writing of this note, there was a sizeable intermission, and in the mean time the quantifiers like $\forall$ and Π moved back inside the angular brackets. I owe to David A. Naumann the observation that

$$\langle \forall x: r.x: t.x \rangle$$

can be viewed as an abbreviation for

$$(\forall \langle x: r.x: t.x \rangle) \quad .$$

This abbreviation is most welcome because a parenthesis pair around the quantifier is needed as soon as a function is applied to a quantified expression.

* * *

I owe to J.R. Rao the theorem that for f monotonic in both arguments

$$[\langle \Pi x: [f.x.x \leq x]: x \rangle = \langle \Pi x: [\langle \Pi y: [f.x.y \leq y]: y \rangle \leq x]: x \rangle] \quad .$$

With a specific notation for the lowest fixpoint – applicable thanks to Knaster-Tarski – we can abbreviate the statement of the theorem to

$$[\langle \mu x :: f.x.x \rangle = \langle \mu x :: \langle \mu y :: f.x.y \rangle \rangle]$$

which looks a lot nicer, but is not nice enough. To show that the right-hand side is a fixpoint of $\langle \lambda x :: f.x.x \rangle$, one has to show

$$[f.\langle \mu x :: \langle \mu y :: f.x.y \rangle \rangle . \langle \mu x :: \langle \mu y :: f.x.y \rangle \rangle = \langle \mu x :: \langle \mu y :: f.x.y \rangle \rangle] ,$$

and these formulae become unwieldy. Naming functions and values solves the problem. Defining G and K by $[G.x = \langle \mu y :: f.x.y \rangle]$ and $[K = \langle \mu x :: G x \rangle]$, we are given about G and K

(a) $[f.x.(G.x) = G.x]$
(b) $[f.x.y \leq y] \Rightarrow [G.x \leq y]$

(c) $[G.K = K]$
(d) $[G.x \leq x] \Rightarrow [K \leq x]$,

and shall prove about them

(e) $[f.K.K = K]$
(f) $[f.x.x \leq x] \Rightarrow [K \leq x]$.

Note that in the above we have exploited Knaster-Tarski by choosing (a) through (d) formally as strong as possible; it turns out that for the demonstrandum we can do the same.

The appeal to Knaster-Tarski is our only use of the monotonicity of f. To fulfill our proof obligations, we observe for any x

to prove (e):

```
   [f.K.K = K]
=    {(c) twice}
   [f.K.(G.K) = G.K]
=    {(a) with x:=K}
   true
```

to prove (f):

```
   [K ⊑ x]
⇐    {(d)}
   [G.x ⊑ x]
⇐    {(b) with y:=x}
   [f.x.x ⊑ x]
```

Note that the left column is entirely formulated in terms of the "intolerant equations" whereas the right-hand column uses the "tolerant equations". The whole left-hand calculation is independent of the partial order ⊑, it only deals with the fixpoint issue. It is unclear to me to what extent the possibility of the above rigorous separation of concerns could have been predicted on general principles. (Such principles would be of great heuristic value.)

When comparing notational alternatives using Π or μ, lines (a) through (f) should be included in counting the number of lines of the above proof, for they record what otherwise would be standard properties of Π or μ. The reader is invited to reformulate the above, say, in terms of μ; it will make him appreciate the conciseness of the above.

* * *

We now consider a new type of equation, viz

$$x: [f.x \sqsubseteq y]$$

and define $h.y$ to be the lowest higher bound of its solution set, i.e.

(15) $$[h.y = \langle \sqcup x: [f.x \sqsubseteq y]: x \rangle] \quad ,$$

from which, using (5) and the reflexivity, one can derive in a few steps that for any x,y

(16) $$[f.x \sqsubseteq y] \Rightarrow [x \sqsubseteq h.y] \quad .$$

Our next theorem states now the equivalence of the following three assertions

(17) f distributes over $\sqcup$

(18) f is monotonic and $[f.(h.y) \sqsubseteq y]$

(19) there exists a function g, uniquely determined by

(20) $$[f.x \sqsubseteq y] \equiv [x \sqsubseteq g.y]$$

and it equals h, as defined by (15).

Before proceeding with the proof we first draw two general conclusions we should have drawn earlier. By instantiating (5) with $x := \langle \sqcup y: y \in W: f.y \rangle$ we derive, because $\sqsubseteq$ is reflexive

(21) $$\langle \forall y: y \in W: [f.y \sqsubseteq \langle \sqcup y: y \in W: f.y \rangle] \rangle \quad ,$$

i.e. $\sqcup$ is indeed a higher bound.

Investigating about the simplest example in which we can use this, we observe for any p,q,f :

$$
\begin{array}{ll}
 & \langle \sqcup z : z \in \{p,q\} : f.z \rangle = f.q \\
= & \quad \{ \sqsubseteq \text{ is antisymmetric} \} \\
 & \langle \sqcup z : z \in \{p,q\} : f.z \rangle \sqsubseteq f.q \;\wedge\; f.q \sqsubseteq \langle \sqcup z : z \in \{p,q\} : f.z \rangle \\
= & \quad \{ (21) \text{ with } y, W := q, \{p,q\} \} \\
 & \langle \sqcup z : z \in \{p,q\} : f.z \rangle \sqsubseteq f.q \\
= & \quad \{ (5) \text{ with } W, x := \{p,q\}, f.q \} \\
 & \langle \forall z : z \in \{p,q\} : f.z \sqsubseteq f.q \rangle \\
= & \quad \{ \text{range split and one-point rule} \} \\
 & f.p \sqsubseteq f.q \;\wedge\; f.q \sqsubseteq f.q \\
= & \quad \{ \sqsubseteq \text{ is reflexive} \} \\
 & f.p \sqsubseteq f.q \qquad , \quad \text{hence}
\end{array}
$$

$$
(22) \qquad [\langle \sqcup z : z \in \{p,q\} : f.z \rangle = f.q \;\equiv\; f.p \sqsubseteq f.q]
$$

And now we proceed with the proof of the equivalence of (17), (18), and (19).

Proof The proof is by cyclic implication.

(17) $\Rightarrow$ (18)

To demonstrate the monotonicity of f we observe for any p,q

$$
\begin{array}{ll}
 & [f.p \sqsubseteq f.q] \\
= & \quad \{(22)\} \\
 & [\langle \sqcup z : z \in \{p,q\} : f.z \rangle = f.q] \\
= & \quad \{ (17), \text{ i.e. } f \text{ distributes over } \sqcup \} \\
 & [\, f.\langle \sqcup z : z \in \{p,q\} : z \rangle = f.q] \\
\Leftarrow & \quad \{\text{Leibniz}\}
\end{array}
$$

$$
\begin{array}{ll}
 & [\langle \sqcup z : z \in \{p,q\} : z\rangle = q] \\
= & \quad \{(22) \text{ with } f \text{ the identity function}\} \\
 & [p \sqsubseteq q]
\end{array}
$$

and furthermore we observe

$$
\begin{array}{ll}
 & [f.(h.y) \sqsubseteq y] \\
= & \quad \{(15), \text{i.e. def. of } h.y\} \\
 & [f.\langle \sqcup x : [f.x \sqsubseteq y] : x\rangle \sqsubseteq y] \\
= & \quad \{(17): f \text{ distributes over } \sqcup\} \\
 & [\langle \sqcup x : [f.x \sqsubseteq y] : f.x\rangle \sqsubseteq y] \\
= & \quad \{(5), \text{i.e. def. of } \sqcup\} \\
 & [\langle \forall x : [f.x \sqsubseteq y] : f.x \sqsubseteq y\rangle] \\
= & \quad \{\text{pred. calc.}\} \\
 & \text{true}
\end{array}
$$

(End of Proof of (17) $\Rightarrow$ (18).)

(18) $\Rightarrow$ (19)

We show the existence of a g satisfying (20) by showing that h is a suitable witness. Without any assumptions about f, (16) gives LHS $\Rightarrow$ RHS. To show LHS $\Leftarrow$ RHS we observe for any x, y

$$
\begin{array}{ll}
 & [f.x \sqsubseteq y] \\
\Leftarrow & \quad \{\sqsubseteq \text{ is transitive}\} \\
 & [f.x \sqsubseteq f.(h.y)] \wedge [f.(h.y) \sqsubseteq y] \\
= & \quad \{(18)\} \\
 & [f.x \sqsubseteq f.(h.y)] \\
\Leftarrow & \quad \{(18), f \text{ is monotonic}\} \\
 & [x \sqsubseteq h.y]
\end{array}
$$

To show that (20) determines g uniquely,

we observe for any x, y

$$
\begin{array}{ll}
 & [x \sqsubseteq h.y] \\
= & \quad \{\text{previous result}\} \\
 & [f.x \sqsubseteq y] \\
= & \quad \{(20)\} \\
 & [x \sqsubseteq g.y]
\end{array}
$$

and now $\sqsubseteq$ being reflexive and antisymmetric does the rest; instantiating the above twice with $x := h.y$ and $x := g.y$ we observe for any y

$$
\begin{array}{ll}
 & \text{true} \\
= & \quad \{\text{above result}\} \\
 & ([h.y \sqsubseteq h.y] \equiv [h.y \sqsubseteq g.y]) \wedge ([g.y \sqsubseteq h.y] \equiv [g.y \sqsubseteq g.y]) \\
= & \quad \{\sqsubseteq \text{ is reflexive}\} \\
 & [h.y \sqsubseteq g.y] \wedge [g.y \sqsubseteq h.y] \\
= & \quad \{\sqsubseteq \text{ is antisymmetric}\} \\
 & [g.y = h.y]
\end{array}
$$

(End of Proof of (18) ⇒ (19).)

(19) ⇒ (17)

We observe for any y —leaving the x-range out—

$$
\begin{array}{ll}
 & [f.\langle \sqcup x :: x \rangle \sqsubseteq y] \\
= & \quad \{(20) \text{ with } x := \langle \sqcup x :: x \rangle\} \\
 & [\langle \sqcup x :: x \rangle \sqsubseteq g.y] \\
= & \quad \{\text{def. of } \sqcup\} \\
 & [\langle \forall x :: x \sqsubseteq g.y \rangle] \\
= & \quad \{\text{interchange: range of } x \text{ is scalar}\} \\
 & \langle \forall x :: [x \sqsubseteq g.y] \rangle \\
= & \quad \{(20)\}
\end{array}
$$

$$
\begin{array}{ll}
 & \langle \forall x :: [f.x \sqsubseteq y] \rangle \\
= & \quad \{\text{interchange}\} \\
 & [\langle \forall x :: f.x \sqsubseteq y \rangle] \\
= & \quad \{\text{def. of } \sqcup\} \\
 & [\langle \sqcup x :: f.x \rangle \sqsubseteq y] \quad ,
\end{array}
$$

and first and last terms being equivalent for any y, $[f.\langle \sqcup x :: x \rangle = \langle \sqcup x :: f.x \rangle]$ follows as before. Notice that the above proof establishes the stronger (20) $\Rightarrow$ (17).

(End of Proof of (19) $\Rightarrow$ (17).)
(End of Proof?)

* * *

The following section deals with (2). Mutatis mutandis, the same remark can be made about (3), (4), and (5).

Because of the Principle of Leibniz, $[A \equiv B] \Rightarrow ([A] \equiv [B])$, and therefore, a k satisfying (2) also satisfies the weaker

(23) $\langle \forall x :: [x \sqsubseteq k] \equiv \langle \forall y : y \in W : [x \sqsubseteq f.y] \rangle \rangle$

Though weaker, (23) still determines k uniquely.

Proof Let k' satisfy

(23') $\langle \forall x :: [x \sqsubseteq k'] \equiv \langle \forall y : y \in W : [x \sqsubseteq f.y] \rangle \rangle$

We now have to show $[k = k']$. We observe

$$
\begin{array}{ll}
 & \text{true} \\
= & \quad \{(23)\} \\
 & \langle \forall x :: [x \sqsubseteq k] \equiv \langle \forall y : y \in W : [x \sqsubseteq f.y] \rangle \rangle \\
= & \quad \{(23')\} \\
 & \langle \forall x :: [x \sqsubseteq k] \equiv [x \sqsubseteq k'] \rangle \\
\Rightarrow & \quad \{\text{instantiate with } x := k \text{ and } x := k'\} \\
 & ([k \sqsubseteq k] \equiv [k \sqsubseteq k']) \wedge ([k' \sqsubseteq k] \equiv [k' \sqsubseteq k']) \\
= & \quad \{\sqsubseteq \text{ reflexive}\} \\
 & [k \sqsubseteq k'] \wedge [k' \sqsubseteq k] \\
= & \quad \{[\,] \text{ is conjunctive}\} \\
 & [k \sqsubseteq k' \wedge k' \sqsubseteq k] \\
\Rightarrow & \quad \{\sqsubseteq \text{ is antisymmetric}\} \\
 & [k = k'] \quad .
\end{array}
$$

(End of Proof)

* * *

To gather an indication of how much we lost or gained by the introduction of $\sqcup$, we now reformulate (17) "f distributes over $\sqcup$", and then redo the proofs with (17) as antecedent or consequent.

Analogous to (3) and (5) we can reformulate "f distributes over $\sqcup$" by stating that for all h

$$
\begin{array}{ll}
(24) & \langle \forall y :: [h \sqsubseteq y \equiv \langle \forall x : x \in W : x \sqsubseteq y \rangle] \rangle \Rightarrow \\
 & \langle \forall y :: [f.h \sqsubseteq y \equiv \langle \forall x : x \in W : f.x \sqsubseteq y \rangle] \rangle
\end{array}
$$

or, in the style of (23)

(25) $\langle \forall y :: [h \sqsubseteq y] \equiv \langle \forall x : x \in W : [x \sqsubseteq y] \rangle \rangle \Rightarrow$
$\langle \forall y :: [f.h \sqsubseteq y] \equiv \langle \forall x : x \in W : [f.x \sqsubseteq y] \rangle \rangle$

We now show: (24) $\Rightarrow$ (f is monotonic). To this end we observe for any p,q

true
$=$ {(24) with $h, W := q, \{p,q\}$}
$\langle \forall y :: [q \sqsubseteq y \equiv \langle \forall x : x \in \{p,q\} : x \sqsubseteq y \rangle] \rangle \Rightarrow$
$\langle \forall y :: [f.q \sqsubseteq y \equiv \langle \forall x : x \in \{p,q\} : f.x \sqsubseteq y \rangle] \rangle$
$=$ {range-split and one-point rule}
$\langle \forall y :: [q \sqsubseteq y \equiv p \sqsubseteq y \wedge q \sqsubseteq y] \rangle \Rightarrow$
$\langle \forall y :: [f.q \sqsubseteq y \equiv f.p \sqsubseteq y \wedge f.q \sqsubseteq y] \rangle$
$=$ {pred. calculus}
$[\langle \forall y :: p \sqsubseteq y \Leftarrow q \sqsubseteq y \rangle] \Rightarrow$
$[\langle \forall y :: f.p \sqsubseteq y \Leftarrow f.q \sqsubseteq y \rangle]$
$=$ {(1)}
$[p \sqsubseteq q] \Rightarrow [f.p \sqsubseteq f.q]$

The above is mathematically the same as EWD1107-14, but it is notationally simpler. So much for the first part of the proof of (17) $\Rightarrow$ (18).

Our second obligation was to show $[f.(h.y) \sqsubseteq y]$, where h.y was given by (15). Eliminating $\sqcup$ from (15) gives

true
$=$ {def of h.y}
$\langle \forall z :: [h.y \sqsubseteq z] \equiv \langle \forall x : [f.x \sqsubseteq y] : [x \sqsubseteq z] \rangle \rangle$

$\Rightarrow$ { (25) }
$\langle \forall z :: [f.(h.y) \sqsubseteq z] \equiv \langle \forall x : [f.x \sqsubseteq y] : [f.x \sqsubseteq z] \rangle \rangle$
$\Rightarrow$ { instantiation, $z := y$; predicate calculus }
$[f.(h.y) \sqsubseteq y]$.

This proof is not shorter than the corresponding one on p. EWD1107-15; it is not much longer either; the individual lines are.

Now we shall prove (20) $\Rightarrow$ (25), to be compared with the proof of (19) $\Rightarrow$ (17) on p.p. EWD1107-16/17 .

We observe for any h

$\langle \forall y :: [h \sqsubseteq y] \equiv \langle \forall x : x \in W : [x \sqsubseteq y] \rangle \rangle$
$\Rightarrow$ { instantiation $y := g.y$ }
$\langle \forall y :: [h \sqsubseteq g.y] \equiv \langle \forall x : x \in W : [x \sqsubseteq g.y] \rangle \rangle$
$=$ { (20) twice }
$\langle \forall y :: [f.h \sqsubseteq y] \equiv \langle \forall x : x \in W : [f.x \sqsubseteq y] \rangle \rangle$

I think this proof at least as nice as the former proof.

* * *

Epilogue I apologize for my ill-considered choice of identifiers: I have used f, g, h, k, x, y, z over and over again in such a way that it sometimes almost confused myself. It is partly the consequence of the fact that when I started on this, I was not sure

where it would lead me. This is more a "working document" than most EWDs.

I started with a dual goal. Together with C.S. Scholten I had derived most of the above for the special case that the above $\sqsubseteq$ is the implication, and my first purpose was writing a summary of the theory for general $\sqsubseteq$. (After that summary had been written I found a lot of it -for those who can read enough Category Theory- in David A. Naumann's thesis.)

My second purpose was to investigate the utility of special purpose notations like $\sqcap$ and $\sqcup$ for tightest bounds and μ & ν for extreme fixpoints. I felt obliged to this investigation because I have seen these notations used but have never used them myself. I feel that this investigation has so far failed to establish their utility. If they can easily be eliminated, they are probably an example of how general mathematical reluctance to manipulate boolean expressions has led to spurious notational diversification.

Austin, 11 October 1991

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