Two "equivalent" characterizations of suprema

(In EWD1090, Edsger W Dijkstra explores under what conditions he can prove $p = q$ for p and q satisfying

$$\langle \forall w :: p \le w \equiv x \le w \wedge y \le w \rangle \quad \text{and}$$

$$\langle \forall w :: w \le q \equiv w \le x \vee w \le y \rangle .$$

The main purpose of that note was to show systematic proof design, not chasing results. In this - our - note, we generalize Dijkstra's problem statement, and our main target is the result.)

In what follows relation $\le$ is a partial order: it is reflexive, transitive, and antisymmetric. Furthermore, for some fixed predicate R we deem to exist $\langle \uparrow x ; R.x : x \rangle$, commonly called the "supremum of R". We will abbreviate this expression to $\uparrow R$.

Now, we might postulate of $\uparrow R$

$$A: \quad \langle \forall y :: \uparrow R \le y \equiv \langle \forall x :: R.x : x \le y \rangle \rangle .$$

But someone else might postulate

$$E: \quad \langle \forall y :: y \le \uparrow R \equiv \langle \exists x : R.x : y \le x \rangle \rangle .$$

The question that arises is how A and E are connected. It turns out that they are connected via property

S: $\quad \mathcal{R}.(\uparrow\mathcal{R})$

by what is our main theorem in this note:

<u>Theorem</u> $\quad A \wedge S \equiv E$

(<u>End</u> of Theorem.)

<u>Remark</u> Property S states that $\uparrow$ is a "selector" on $\mathcal{R}$. The most well-known example of such a selector is the maximum operator for numbers. And in that case, A and E are equivalent characterizations for the maximum.
(<u>End</u> of Remark.)

* * *

Before we start proving the theorem we first give two immediate consequences of A and E, which come in handy. They arise from instantiating both A and E with $y := \uparrow\mathcal{R}$:

Cor A: $\quad \langle \forall x : \mathcal{R}.x : x \leq \uparrow\mathcal{R} \rangle$

Cor E: $\quad \langle \exists x : \mathcal{R}.x : \uparrow\mathcal{R} \leq x \rangle$.

Now we are ready for the

Proof We subsequently show

$A \wedge S \Rightarrow E$, $E \Rightarrow A$, and $E \Rightarrow S$.

The theorem then follows.

$A \wedge S \Rightarrow E$:

We prove the equivalence in E by mutual implication

ping for E :

$$
\begin{array}{ll}
 & \langle \exists x : R.x : y \leq x \rangle \\
\Leftarrow & \quad \{ x := \uparrow R \} \\
 & R.(\uparrow R) \ \wedge \ y \leq \uparrow R \\
\equiv & \quad \{ S \} \\
 & y \leq \uparrow R \quad .
\end{array}
$$

pong for E :

$$
\begin{array}{ll}
 & y \leq \uparrow R \\
\Leftarrow & \quad \{ \text{transitivity of } \leq \} \\
 & \langle \exists x :: y \leq x \wedge x \leq \uparrow R \rangle \\
\Leftarrow & \quad \{ \text{cor } A : \ x \leq \uparrow R \Leftarrow R.x \} \{ \text{trading} \} \\
 & \langle \exists x : R.x : y \leq x \rangle \quad .
\end{array}
$$

$E \Rightarrow A$:

We prove the equivalence in A by a series of equivalence preserving steps.

$$
\begin{array}{ll}
 & \uparrow R \leq y \\
\equiv & \quad \{ \text{indirect inequality (using} \\
 & \quad\quad \text{reflexivity and transitivity of } \leq \text{)} \} \\
 & \langle \forall z : z \leq \uparrow R : z \leq y \rangle
\end{array}
$$

$$
\begin{array}{ll}
\equiv & \quad \{ \text{E on the range} \} \\
& \langle \forall z : \langle \exists x : R.x : z \leq x \rangle : z \leq y \rangle \\
\equiv & \quad \{ \text{range disjunction} \} \\
& \langle \forall x : R.x : \langle \forall z : z \leq x : z \leq y \rangle \rangle \\
\equiv & \quad \{ \text{indirect inequality} \} \\
& \langle \forall x : R.x : x \leq y \rangle \; .
\end{array}
$$

<u>$E \Rightarrow S$</u> :

In view of the fact that $E \Rightarrow A$ —just shown— we might as well prove the formally weaker $E \wedge A \Rightarrow S$:

$$
\begin{array}{ll}
& S \\
\equiv & \quad \{ \text{definition of } S \} \\
& R.(\uparrow R) \\
\Leftarrow & \quad \{ \text{predicate calculus} \} \\
& \langle \exists x : R.x : x = \uparrow R \rangle \\
\Leftarrow & \quad \{ \leq \text{ is antisymmetric} \} \\
& \langle \exists x : R.x : x \leq \uparrow R \wedge \uparrow R \leq x \rangle \\
\equiv & \quad \{ \text{CorA} : R.x \Rightarrow x \leq \uparrow R \} \\
& \langle \exists x : R.x : \uparrow R \leq x \rangle \\
\equiv & \quad \{ \text{CorE verbatim} \} \\
& \text{true} \; .
\end{array}
$$

(<u>End</u> of Proof.)

Finally, two corollaries of our theorem are worth being mentioned. One is

$$S \Rightarrow (A \equiv E) \; ,$$

which is immediate from the theorem. The other is

$$A \wedge E \Rightarrow S \quad ,$$

which follows from

$$\begin{array}{ll} & A \wedge E \\ \equiv & \quad \{ \text{Theorem} \} \\ & A \wedge A \wedge S \\ \Rightarrow & \quad \{\} \\ & S \quad . \end{array}$$

WHJ Feijen and
A.J.M. van Gasteren,

Eindhoven,
14 November 1994

<u>Postscript</u> We now also understand why A is the usual definition for suprema. Of A and E the former is the least demanding.
(<u>End</u> of Postscript.)