Knaster-Tarski in disguise

We consider predicates on a set V. For (fixed) predicate Q and (fixed) function $F: V \to V$, we are interested in the strongest solution of the equation

(0) $X: \ [X \Leftarrow Q] \wedge [X \circ F \Leftarrow X]$.

($[\cdots]$ denotes universal quantification over V and $\circ$ denotes function composition; note that for predicate X and function F, $X \circ F$ is a predicate too.)

Equation (0) may be considered as the prototype of a recursive datatype-definition.

We now calculate:

$$\begin{array}{ll}
 & [X \Leftarrow Q] \wedge [X \circ F \Leftarrow X] \\
= & \quad \{ \text{ lemma, see below (don't worry about @) } \} \\
 & [X \Leftarrow Q] \wedge [X \Leftarrow F@X] \\
= & \quad \{ \text{ predicate calculus } \} \\
 & [(X \Leftarrow Q) \wedge (X \Leftarrow F@X)] \\
= & \quad \{ \text{ idem } \} \\
 & [X \Leftarrow Q \vee F@X] \\
= & \quad \{ \text{ introduction of } \varphi \text{, see below } \} \\
 & [X \Leftarrow \varphi.X] \ .
\end{array}$$

So, equation (0) can be rewritten into the equivalent

(1) $X: \ [X \Leftarrow \varphi.X]$,

where function φ, which is a predicate transformer, is defined by

$$[\ \varphi.X \equiv Q \vee F@X\ ]\ .$$

Operator @ is such that (F@) is universally disjunctive, and so is φ. Hence, φ is monotonic and or-continuous, and we may apply Knaster-Tarski's theorem to obtain the strongest solution of (1) (and (0)). This solution is

$$(\exists i : 0 \leq i : \varphi^i.\text{false})\ .$$

<u>aside</u> : Because the range of dummy i in this formula is the natural numbers, the above immediately yields a mathematical-induction principle for proving theorems about recursively defined datatypes.

□

The lemma used in the above derivation reads as follows. A suitable definition of operator @ is obtained by proving the lemma.

<u>lemma</u>: for predicates X, Y and function F:

$$[\ X \circ F \Leftarrow Y\ ] \equiv [\ X \Leftarrow F@Y\ ]\ .$$

<u>proof</u>: $[\ X \circ F \Leftarrow Y\ ]$

$=$ { definition of [···] and $\circ$ }

$(\forall u :: X.(F.u) \Leftarrow Y.u)$

$=$ { 1-pt rule, to obtain $X.v \Leftarrow \ldots$ }

$(\forall u,v : v = F.u : X.v \Leftarrow Y.u)$

$=$ { nesting }

$$
\begin{array}{ll}
 & (\forall v :: (\forall u : v = F.u : \ X.v \Leftarrow Y.u)) \\
= & \quad \{ \text{ predicate calculus } \} \\
 & (\forall v :: \ X.v \Leftarrow (\exists u : v = F.u : Y.u)) \\
= & \quad \{ \text{ introduction of } @ \text{, see below } \} \\
 & (\forall v :: \ X.v \Leftarrow (F@Y).v) \\
= & \quad \{ \text{ definition of } [\cdots] \ \} \\
 & [\ X \Leftarrow F@Y\ ] \ .
\end{array}
$$

For function F and predicate X, predicate $F@X$ is defined by

$$(\forall v :: \ (F@X).v \equiv (\exists u : v = F.u : X.u)) \ .$$

Notice that the right-hand side of this definition equivales $(\exists u : X.u : v = F.u)$, which in classical set notation would be read as $v \in \{ F.u \mid u \in X \}$. So, $@$ is nothing but the well-known "map" operator.

□

To some extent, the lemma defines $@$ in terms of $\circ$. For example, to prove that $(F@)$ is universally disjunctive the lemma is all we need to know about $@$. Whether or not the lemma really defines $@$ I do not know (yet).

Eindhoven, 11 october 1990
Rob R. Hoogerwoord
department of mathematics and computing science
Eindhoven University of Technology