Boolean connectives yield punctual expressions

Let all through this little note f, g stand for predicate transformers. In that case, we formulate Leibniz's principle as

(0) $[x \equiv y] \Rightarrow [f.x \equiv f.y]$ for all x, y

or -in the style of [GS94] "if $x = y$ is [valid, i.e.] true in all states, then so is $f.x = f.y$".

A function f is punctual means that it satisfies the stronger

(1) $[(x \equiv y) \Rightarrow (f.x \equiv f.y)]$ for all x, y

Remark Property (1) is justly called "stronger", since $(1) \Rightarrow (0)$, as follows from the monotonicity of $[\ldots]$:

$$[x \Rightarrow y] \Rightarrow ([x] \Rightarrow [y]) \quad .$$

(End of Remark)

An equivalent definition of f's punctuality is

(2) $[(x \equiv y) \wedge f.x \equiv (x \equiv y) \wedge f.y]$.

Proof. To demonstrate the equivalence of (1) and (2) we observe for any a, b, c

$$\begin{array}{ll} & [a \Rightarrow (b \equiv c)] \\ = & \quad \{\wedge \ \Rightarrow \ \equiv\} \\ & [a \wedge (b \equiv c) \equiv a \\ = & \quad \{\wedge \text{ over } \equiv\equiv\} \\ & [a \wedge b \equiv a \wedge c] \quad . \end{array}$$

(By omitting in the above the square brackets, we could have proved a stronger theorem.)
(End of Proof)

In the remainder of this note, the assumption of g's punctuality is expressed analogously

(3) $[(x \equiv y) \wedge g.x \ \equiv \ (x \equiv y) \wedge g.y]$.

The simple theorem to which this note is devoted is

<u>Theorem</u> An expression built from variables and the boolean connectives —quantification included— is a punctional function of its global —sometimes called "free"— variables.

Such a theorem has to be proved by "mathematical induction over the syntax", i.e. for the base one proves the property for any expression without subexpressions —i.e. without connectives—, and for the step one proves for each connective the punctuality of the expression it forms, under the assumption that the connective's operands are punctual.

For the base we have to consider:
(i) the constant function, i.e. $[f.x = z]$, for which, according to, say, (1) we have to show

$$[(x \equiv y) \Rightarrow (z \equiv z)] \quad , \text{and}$$

(ii) the identity function, i.e. $[f.x = x]$, for which, according to, say, (1) we have to show

$$[(x \equiv y) \Rightarrow (x \equiv y)] \quad .$$

Both proofs are trivial.

For the step we have to consider the connectives in turn.

For the equivalence it suffices to derive

$$[(x \equiv y) \wedge (f.x \equiv g.x) \;\equiv\; (x \equiv y) \wedge (f.y \equiv g.y)]$$

from (2) and (3). We observe

$$\begin{array}{ll}
 & (x \equiv y) \wedge (f.x \equiv g.x) \\
= & \quad \{\wedge \text{ over } \equiv\equiv\} \\
 & (x \equiv y) \wedge f.x \;\equiv\; (x \equiv y) \wedge g.x \;\equiv\; (x \equiv y) \\
= & \quad \{(2) \text{ and } (3)\} \\
 & (x \equiv y) \wedge f.y \;\equiv\; (x \equiv y) \wedge g.y \;\equiv\; (x \equiv y)
\end{array}$$

$$\{\wedge \text{ over } \equiv\equiv\}$$
$$= \quad (x\equiv y) \wedge (f.y \equiv g.y) \quad .$$

For the disjunction we have to derive

$$[(x\equiv y) \wedge (f.x \vee g.x) \;\equiv\; (x\equiv y) \wedge (f.y \vee g.y)]$$

from (2) & (3); the exercise is left to the reader. Since $\wedge$, $\Rightarrow$, and $\neg$ can be expressed in terms of $\equiv$, $\vee$ and the constant <u>false</u>, only quantification is left to be dealt with; because of de Morgan's Law, it suffices to deal with existential quantification only. That is, to be precise, we have to show

$$[(x\equiv y) \wedge \langle \exists i :: f.i.x \rangle \;\equiv\; (x\equiv y) \wedge \langle \exists i :: f.i.y \rangle]$$

under the generalized assumption that

(2') $[(x\equiv y) \wedge f.i.x \;\equiv\; (x\equiv y) \wedge f.i.y]$ for all x, y, i

i.e. we assume the function $f.i$ in the term to be punctual, independently of the value of the dummy i .

The proof is very similar to the previous ones. We observe for any f satisfying (2') and any x, y

$$(x\equiv y) \wedge \langle \exists i :: f.i.x \rangle$$
$$= \quad \{\wedge \text{ over } \exists\}$$

$$\begin{array}{ll} & \langle \exists i :: (x \equiv y) \wedge f.i.x \rangle \\ = & \quad \{ (2') \} \\ & \langle \exists i :: (x \equiv y) \wedge f.i.y \rangle \\ = & \quad \{ \wedge \text{ over } \exists \} \\ & (x \equiv y) \wedge \langle \exists i :: f.i.y \rangle \end{array}$$

Note that there is no constraint at all on the domain of the dummy; as far as we are concerned it could be uncountably infinite, and as "ill founded" as the reals. We are carrying out "induction on the grammar" and $\langle \exists i :: f.i.x \rangle$ is definitely a finite formula.

* * *

The above has been written down in such detail because [GS94] is here rather confusing. I quote from p. 60

"LEIBNIZ'S RULE AS AN AXIOM

On p. 12, we introduced Leibniz (1,5):

$$\frac{X = Y}{E[z := X] = E[z := Y]} \quad \text{or} \quad \frac{X = Y}{E^z_X = E^z_Y}$$

[On p. 14, they "reformulate (1.5) as

$$\frac{X = Y}{g.X = g.Y}$$

EWD]

Now that we have introduced operator ⇒, we can give a version of Leibniz as an axiom scheme:

(3.83) Axiom, Leibniz: $(e=f) \Rightarrow (E^z_e = E^z_f)$

(E any expression)

Inference rule Leibniz says, "if $X=Y$ is valid, i.e. true in all states, then so is $E[z:=X] = E[z:=Y]$." Axiom (3.83), on the other hand, says "if $e=f$ is true in a state, then $E[z:=e] = E[z:=f]$ is true in that state." Thus, the inference rule and the axiom are not quite the same."

The above quotation is so confusing that all by itself it justifies the writing of this note. The verbal explanation suggests that their (1,5) "inference rule Leibniz" corresponds to our (0), whereas (3.83) "axiom Leibniz" corresponds to our (1). But ..... here is my problem.

If in "E any expression" E may really be "any expression", I suggest $[E \equiv g.z]$ for a non-punctual g. In that case, $E[z:=e] = E[z:=f]$ becomes $g.e = g.f$, which can be false in a state where $e=f$ is true. So then the Axiom is wrong.

We can try to save the Axiom by explicitly restricting expressions to what can be built from boolean variables, constants and the (punctual!) connectives.

But then my problem is that under those constraints, their (3.83) is not an axiom but a theorem.

Comparison of their (1,5) & (3.83) with our (0) & (1) respectively suggests that [GS94] suffers from the implicit scopes of the universal quantifications over all states. Has the 2-line format of the inference rules been chosen with the understanding that the scope of the universal quantification does not extend over both lines?

[GS94] David Gries and Fred B. Schneider
"A Logical Approach to Discrete Math"
Springer Verlag, 1994

Pedernales Falls State Park
& Austin, 19 September 1994

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