

Using structure-valued formulae

Against philosophy

Philosophy is alive and well in the calculational style, unsurprisingly to our detriment. Here, I would like to focus on the philosophical notion of the “assumption”, and show how this notion has prevented us from exploiting a very natural and powerful way of calculating.

* *

 *

A few words on our calculational style

In the name of separation of concerns, we do not calculate with all our information simultaneously. We keep most of it in what we call “the context”, and calculate within that context, meaning that a proof step is viewed as an implication: the context is the antecedent, the step itself is the consequent.

In many circles, even calculational ones, contextual properties are called assumptions. The problem with this terminology is that in natural language, ‘assumptions’ are boolean scalars. And indeed, it seems as if to date people have only been comfortable calculating in scalar contexts.

In *Predicate Calculus and Program Semantics*, Edsger Dijkstra and Carel Scholten are clearly of this mind as they explain their enhancements to Wim Feijen’s proof format. They explain that a step like:

$$\begin{array}{l}
 P \\
 \equiv \quad \{ \text{using } [E] \} \\
 Q
 \end{array}$$

is to be understood as:

$$[E] \Rightarrow [P \equiv Q] \quad ,$$

or in our philosophical terminology: “assuming $[E]$, $[P \equiv Q]$ holds”. Here $[E]$ is drawn from the context.

One can only imagine that this philosophical terminology held them back from interpreting the above proof step equivalently as:

$$[[E] \Rightarrow (P \equiv Q)] \quad ,$$

which would have catered as well to a structure-valued hint, say E . Mathematically, there is nothing wrong with this approach, but notice that a sentence like “assuming E , $P \equiv Q$ holds” is in general nonsense, unless E , P , and Q are scalar.

In what follows, I interpret:

$$\begin{array}{c} P \\ \rightarrow \{ E \} \\ Q \end{array}$$

as:

$$[E \Rightarrow (P \rightarrow Q)] \quad ,$$

which I emphasize is equivalent to the Dijkstra–Scholten convention when E is scalar.

* *

A glorious example

The change of convention given above seems almost trivial, but the consequences of the change are quite striking. In this section, I wish to illustrate the benefits of this new convention.

I do so by proving that (a predicate transformer is punctually monotonic) equivaless (it is punctual and monotonic). In symbols, $\mathbf{PM} \equiv \mathbf{P} \wedge \mathbf{M}$, with:

$$\begin{array}{ll} \mathbf{PM}: & [(x \Rightarrow y) \Rightarrow (f.x \Rightarrow f.y)] \quad (\forall x, y) \\ \mathbf{P}: & [(x \equiv y) \Rightarrow (f.x \equiv f.y)] \quad (\forall x, y) \\ \mathbf{M}: & [x \Rightarrow y] \Rightarrow [f.x \Rightarrow f.y] \quad (\forall x, y) \quad . \end{array}$$

Our proof is by mutual implication. The first half, $\mathbf{PM} \Rightarrow \mathbf{P} \wedge \mathbf{M}$, we establish by proving $\mathbf{PM} \Rightarrow \mathbf{P}$ and $\mathbf{PM} \Rightarrow \mathbf{M}$ separately.

- **PM \Rightarrow P**

We put **PM** and $x \equiv y$ into the context, and calculate $f.x \equiv f.y$.

[[Context: **PM** \wedge ($x \equiv y$)

$f.x$

\Rightarrow { **PM** and $x \Rightarrow y$ (follows from $x \equiv y$) }

$f.y$

\Rightarrow { **PM** and $y \Rightarrow x$ (follows from $x \equiv y$) }

$f.x$

]]

- **PM \Rightarrow M**

We put **PM** and $[x \Rightarrow y]$ into the context, and calculate $[f.x \Rightarrow f.y]$.

[[Context: **PM** \wedge $[x \Rightarrow y]$

$f.x$

\Rightarrow { **PM** and $x \Rightarrow y$ (follows from $[x \Rightarrow y]$) }

$f.y$

]]

- **P \wedge M \Rightarrow PM**

We put **P** , **M** , and $x \Rightarrow y$ into the context, and calculate $f.x \Rightarrow f.y$.

[[Context: **P** \wedge **M** \wedge ($x \Rightarrow y$)

$f.x$

\equiv { **P** and $x \equiv x \wedge y$ (equivalens $x \Rightarrow y$) }

$f.(x \wedge y)$

\Rightarrow { **M** and $[x \wedge y \Rightarrow y]$ }

$f.y$

]]

JAW89-3

(The reader may enjoy designing a variant of this last calculation, where \mathbf{M} is used first, and \mathbf{P} second.)

Three calculations, five simple steps: the whole thing has the flavor of a walk-over! We would not have achieved anywhere near this level of brevity and elegance, had we not allowed ourselves the use of structure-valued formulae in our proof steps.

The moral of the story is: let us throw off our philosophical and linguistic shackles, and simply calculate!

Santa Cruz, 9 November 2006

Jeremy Weissmann
11260 Overland Ave. #21A
Culver City, CA 90230
USA
jeremy@mathmeth.com