Free style spec wrestling II : preorders

Free style spec wrestling II: preorders

Jaap van der Woude

18-10-1991

1 Introduction

Some games seem truely masochistic, for instance: give a pointfree proof of something that is easily proved with pointwise reasoning. With a pointfree proof I mean a proof in a pointless world, not just a proof without points in the formulae to be manipulated. Such games are not played just for fun or to keep us from other popular pastimes like ramriding. They kind of test the calculational power of the spec algebra and they may induce further streamlining of the spec calculus. I do admit that I am not spec wizard enough to conclude that the outrageous prooftime I needed until now is sufficient reason to abandon the spec calculus, but I do have my doubts on the current state of affairs.

An almost ridiculous sample-game was presented in the Liber Amicorum for Lambert Meertens (pp 110–115), constructing those proofs took me about three days (not counting the time to shape things up). An easier one (took me six hours, so at least five too many) is the following challenge from Richard Bird, transferred to me by Wim Feijen:

Define for a preorder X , i.e. X is reflexive and transitive, the *leasting* λX by

$$\lambda X.S \;=\; \{m \in S \mid (\mathbf{A}\, s \;:\; s \in S \;:\; m\, X\, s)\}$$

So, λX fed with a set S returns the X-least points of S (by lack of antisymmetry this may be a substantial subset of S).

(1) Challenge *Prove for preorders* X *and* Y *the existence of a preorder* Z *with*

$$\lambda Z \;=\; \lambda Y \circ \lambda X$$

By pointwise reasoning one finds such a Z quite easily: $X \sqcap (\neg X^{\cup} \sqcup Y)$, and it turns out to be unique (thanks Wim).

One way to meet the challenge is to prove that the proposed candidate is a good one (that is what I did first), but that smells like cheating. Here I want to present a proof that at least makes it sweetly reasonable that one could have arrived at the candidate by careful calculation.

2 Translation and technique

Since set theory can be played in an extensional (monotypical) spec algebra, where points are represented as impish leftconditions, we represent sets as leftconditions; so, without name changes, the set S is represented as a spec S such that $S = S \circ \top\!\!\top$. A subset A of S is a leftcondition $A \sqsubseteq S$ and a full relation $A \times B$ on S is given by $A \circ B^{\cup}$. A preorder X is of course a spec such that $I \sqcup X \circ X \sqsubseteq X$.

The definition of λX amounts to: $\lambda X.S$ is the greatest solution of

$$A :: \quad A \sqsubseteq S \quad \wedge \quad A \circ S^{\cup} \sqsubseteq X$$

Thus, by definition of the division operator,

(2) $$\lambda X.S \;=\; S \sqcap X/S^{\cup}$$

The challenge is to construct for preorders X and Y a preorder Z such that *for every* S

(3) $$S \sqcap Z/S^{\cup} \;=\; S \sqcap X/S^{\cup} \sqcap Y/(S \sqcap X/S^{\cup})^{\cup}$$

Since $/S^{\cup}$ is conjunctive we are led to believe that $Z = X \sqcap Z'$ for some Z' probably depending on Y .

Oh ... you are right, it is very well possible you don't know all calculation rules for the division operator by heart. Let me give you a few:

(4) $$P/Q \sqsupseteq R \;\equiv\; P \sqsupseteq R \circ Q$$

(5) $$P \;\sqsupseteq\; (P/Q) \circ Q$$

The first is the defining characterisation of $/Q$ as an "adjoint" of $\circ\, Q$, the second is a direct consequence: the *cancellation* rule. Two junctivity rules are:

(6) $$(P \sqcap Q)/R \;=\; P/R \sqcap Q/R$$

(7) $$P/(Q \sqcup R) \;=\; P/Q \sqcap P/R$$

The observation that the numerator of $\lambda X.S$ is a preorder invites the following rule to join in:

(8) $$X/P \;=\; X \circ (X/P) \;\Leftarrow\; X \text{ is a preorder}$$

Since in the denominator of $\lambda X.S$ a wokked leftcondition (so a rightcondition) occurs, it might be useful to note for leftcondition L , rightcondition R and arbitrary P and Q :

(9) $$P/R \text{ is a leftcondition}$$

(10) $$P \circ (R \sqcap Q) \;=\; P \circ R \sqcap P \circ Q$$

(11) $$L \circ R \;=\; L \sqcap R$$

(12) $$L_{<} \circ Q \;=\; L \sqcap Q$$

(13) $$L_{<} \;\sqsubseteq\; L \sqcap L^{\cup}$$

I do assume familiarity with the (left) domain operator.

3 Let's do it

First consider the RHS of (3); direct manipulation fails because of lack of suitable rules with conjunctions in the denominator of a division. So I try

$$(\text{LHS} \sqsupseteq P \equiv \text{RHS} \sqsupseteq P) \equiv (\text{LHS} = \text{RHS})$$

a good possibility since "/" occurs in both sides.

$$\begin{array}{l} S \sqcap X/S^{\cup} \sqcap Y/(S \sqcap X/S^{\cup})^{\cup} \sqsupseteq P \\ = \{ \text{ assume } S \sqcap X/S^{\cup} \sqsupseteq P \ ; (4) \} \\ Y \sqsupseteq P \circ (S \sqcap X/S^{\cup})^{\cup} \\ = \{ \ S^{\cup} \text{ is rightcondition } ; (10) \} \\ Y \sqsupseteq P \circ S^{\cup} \sqcap P \circ (X/S^{\cup})^{\cup} \\ \Leftarrow \{ \text{ get rid of } /S^{\cup} \text{ by cancellation } ; \ P \sqsubseteq S \ \} \\ Y \sqsupseteq P \circ S^{\cup} \sqcap X^{\cup} \\ = \{ \text{ shunting } ; (4) ; \text{ assumption on } P \ \} \\ S \sqcap X/S^{\cup} \sqcap (\neg X^{\cup} \sqcup Y)/S^{\cup} \sqsupseteq P \\ = \{ (6) \} \\ S \sqcap (X \sqcap (\neg X^{\cup} \sqcup Y))/S^{\cup} \sqsupseteq P \end{array}$$

So, indeed, I arrived at the candidate $X \sqcap (\neg X^{\cup} \sqcup Y)$ with only one little rabbit: remove $/S^{\cup}$ in order to construct a candidate that does *not* depent on S . However, the price is an implication! while an equivalence was needed. It is by no means clear that such an equivalence is possible. To obtain it, it would be nice if

(14) $$P \circ S^{\cup} \sqcap X^{\cup} \sqsubseteq P \circ S^{\cup} \sqcap P \circ (X/S^{\cup})^{\cup}$$

under the assumption put on P in the above calculation. Since in (14) P is only composed with rightconditions and P is contained in a leftcondition by assumption, P may even be assumed to be a leftcondition.
Reintroduction of $/S^{\cup}$ in the LHS of (14) while enlarging it leaves me no other choice than exploiting $P \sqsubseteq X/S^{\cup}$, but where? Ah..., in that situation $X^{\cup}$ has to be removed! so (8) may help. This asks for introduction of a $(P^{\cup} \circ)$-translation of $X^{\cup}$, indeed:

$$\begin{array}{l} P \circ S^{\cup} \sqcap X^{\cup} \\ = \{ (11) ; (12) \} \\ P \sqcap S^{\cup} \sqcap P_{<} \circ X^{\cup} \end{array}$$

$\sqsubseteq$ { $P_< \sqsubseteq$ {(13)} $P^\cup \sqsubseteq (X/S^\cup)^\cup$ }
$P \sqcap S^\cup \sqcap (X/S^\cup)^\cup \circ X^\cup$
$=$ { (8) }
$P \sqcap S^\cup \sqcap (X/S^\cup)^\cup$
$=$ { (11) ; "wok" }
$P \circ (S \sqcap X/S^\cup)^\cup$

This proves the wish and so the equation (3) for the candidate $Z = X \sqcap (\neg X^\cup \sqcup Y)$. The heuristics may have shrunk the rabbits, but I think they still are alive.

The candidate may be perfect for the equation (3) (that was why it was constructed the way it is), but that doesn't mean that the challenge is met: is the candidate a preorder? Reflexivity is for free, how about transitivity?
For transitivity the distributed form of the candidate is helpful:

$$(X \sqcap \neg X^\cup) \sqcup (X \sqcap Y)$$

The first disjunct is the well-known nonreflexive partial order generated by the preorder X and so it is transitive. The second disjunct is the conjunction of transitive specs, thus transitive; so the cross-compositions remain. It turns out that the cross-compositions are all contained in the first disjunct. The proof thereof and the proof of the transitivity of the first disjunct follow immediately from

(15) Note $(X \sqcap \neg X^\cup) \circ X \ \sqcup \ X \circ (X \sqcap \neg X^\cup) \ \sqsubseteq \ X \sqcap \neg X^\cup$

Proof. $(X \sqcap \neg X^\cup) \circ X \sqsubseteq X \sqcap \neg X^\cup$
$\Leftarrow$ { $\circ X$ is monotonic }
$X \circ X \sqcap \neg X^\cup \circ X \sqsubseteq X \sqcap \neg X^\cup$
$\Leftarrow$ { X is preorder }
$\neg X^\cup \circ X \sqsubseteq \neg X^\cup$
$=$ { left exchange }
$X^\cup \circ X^\cup \sqsubseteq X^\cup$
$=$ { X is preorder }
true

□

Transitivity of $X \sqcap \neg X^\cup$ follows from (15) since $X \sqcap \neg X^\cup \sqsubseteq X$.
Inclusion of the cross-compositions in $X \sqcap \neg X^\cup$ follows from (15) via $X \sqcap Y \sqsubseteq X$.

More challenges are anxiously awaited.

4 Comparison

Appreciation of the spec approach depends also on the alternative pointwise treatment of the challenge, but note that the pointwise approach does not cover the general situation.

First the derivation of Z such that

$$(\mathbf{A}\, S\ ::\ \lambda Z.S\ =\ \lambda Y.(\lambda X.S)\,)$$

The candidate is derived by instantiating doubletons for S in the above, using the fact that

(16) $$aXb\ \equiv\ a \in \lambda X.\{a,b\}$$

as follows:

$$
\begin{array}{ll}
 & aZb \\
\equiv & \{\ (16)\ ;\ \text{instantiation}\ ;\ \text{def.}\ \lambda Y\ \} \\
 & a \in \lambda X.\{a,b\} \quad \wedge \quad a \times \lambda X.\{a,b\} \subseteq Y \\
\equiv & \{\ (16)\ ;\ \text{case analysis}\ \} \\
 & aXb \quad \wedge \quad (aYb \quad \vee \quad b \notin \lambda X.\{a,b\}) \\
\equiv & \{\ (16)\ \} \\
 & aXb \quad \wedge \quad (aYb \quad \vee \quad b \neg X a) \\
\equiv & \{\ \text{calc.}\ \} \\
 & a(X \sqcap (Y \sqcup \neg X^{\cup}))b
\end{array}
$$

The derived candidate indeed does the job (for transitivity see the former section):

$$
\begin{array}{ll}
 & m \in \lambda(X \sqcap (Y \sqcup \neg X^{\cup})).S \\
\equiv & \{\ \text{def.}\ \lambda\ \} \\
 & m \in S \quad \wedge \quad m \times S \subseteq X \quad \wedge \quad m \times S \subseteq Y \sqcup \neg X^{\cup} \\
\equiv & \{\ \text{def.}\ \lambda\ ;\ \text{calc.}\ \} \\
 & m \in \lambda X.S \quad \wedge \quad (\mathbf{A}\, s\ :\ s \in S\ :\ mX^{\cup}s\ \Rightarrow\ mYs\,) \\
\equiv & \{\ \text{calc.}\ \} \\
 & m \in \lambda X.S \quad \wedge \quad (\mathbf{A}\, s\ :\ s \in S \quad \wedge \quad sXm\ :\ mYs\,) \\
\equiv & \{\ m \in \lambda X.S\ \Rightarrow\ (sXm\ \equiv\ s \in \lambda X.S)\ \} \\
 & m \in \lambda X.S \quad \wedge \quad m \times \lambda X.S \subseteq Y \\
\equiv & \{\ \text{def.}\ \lambda\ \} \\
 & m \in \lambda Y.(\lambda X.S)
\end{array}
$$

This proof is not really shorter than the spec proof, but it is a lot easier if not straightforward. Does this mean that the calculational system of the spec algebra is too extravagant, or is it extra evidence that I lack sufficient adroitness?

Thank you Richard for this interesting challenge. I feel that there is a lot to do to turn the spec calculus into an acceptable alternative for this kind of exercises; these challenges may help. I hope others will make my solution look ridiculous in the near future.