A Proof Sketch Of Something Which May Possibly Be A Conjecture of Oege de Moor

Nick Benton
Microsoft Research
nick@microsoft.com
December 6, 2000

This note purports to prove something which Oege de Moor presented as an open problem in a talk entitled “Pointwise Relations” at the Computer Laboratory on December 1st. Since I’ve rephrased everything in terms with which I’m more familiar1 (and may well have misunderstood or misremembered what he said), it’s entirely possible that it doesn’t, however.

Oege starts with a simply-typed lambda calculus. This is given two interpretations, one in $\text{Set}$ and one in $\mathbb{B}$. Now $\mathbb{B}$ is the Kleisli category of the powerset monad $\mathbb{P}$ on $\text{Set}$ and I believe that Oege’s direct relational semantics is the same one as you get by factoring through the call-by-value translation into Moggi’s computational metalanguage and then interpreting that in $\text{Set}$ with $T = \mathbb{P}$. The call-by-value translation has the following shape:

$$(\Gamma \vdash M : A)^* = \Gamma^* \vdash M^* : T(A^*)$$

where

<table>
<thead>
<tr>
<th>Types</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$G^*$</td>
<td>$G\quad G$ a ground type</td>
</tr>
<tr>
<td>$(A \times B)^*$</td>
<td>$A^* \times B^*$</td>
</tr>
<tr>
<td>$(A \to B)^*$</td>
<td>$A^* \to T(B^*)$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Terms in Context</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>$(\Gamma, x : A \vdash x : A)^*$</td>
<td>$\Gamma^<em>, x : A^</em> \vdash \text{val} \ x : T(A^*)$</td>
</tr>
<tr>
<td>$(\Gamma \vdash (M \ N) : B)^*$</td>
<td>$\Gamma^* \vdash (\text{let } x \leftarrow M^* \text{ in } (\text{let } y \leftarrow N^* \text{ in } x\ y)) : T(B^*)$</td>
</tr>
<tr>
<td>$(\Gamma \vdash (\lambda x : A . M) : A \to B)^*$</td>
<td>$\Gamma^* \vdash \text{val} (\lambda x : A^<em>.M^</em>) : A^* \to T(B^*)$</td>
</tr>
</tbody>
</table>

The $\text{val}(\cdot)$ form is interpreted by the unit of the monad and $\text{let} \cdot \leftarrow \cdot \text{ in } \cdot$ by Kleisli composition.

I don’t think that what follows depends on anything that’s very specific to $\text{Set}$ or the powerset monad, but I haven’t got around to rewriting it in an element-free way in terms of CCCs with relations and seeing just what the

---

1 “Mathematicians are like Frenchmen: whatever you say to them, they translate into their own language and forthwith it is something entirely different.” – Goethe
conditions are. Not only will I be frightfully uncategorical, but I’ll also confuse syntax and semantics all over the place, confident that the ‘s can be dotted and the ‘l’s crossed if there’s any interest . . .

We start by defining a relation $\mathcal{R}_A$ between (the interpretations of) $A$ and $A^*$ for each type $A$ of the source language. To deal with the fact that we’ve got computation types around, we’ll also need a trivial auxiliary relation $\mathcal{R}^T_A$ which relates $A$ with $T(A^*)$:

$$
\begin{align*}
x \mathcal{R}_G y & \iff x = y \\
f \mathcal{R}_{A \rightarrow B} g & \iff \forall x \in A, y \in A^*, x \mathcal{R}_A y \Rightarrow (f x) \mathcal{R}^T_{B}(g y) \\
x \mathcal{R}^T_A y & \iff \exists y' \in A^*, (y = \text{val } y') \land (x \mathcal{R}_A y')
\end{align*}
$$

(Probably hiding ‘$\eta$ is mono’ in the computation type case.) A simple induction on terms in context yields the usual “fundamental theorem of logical relations”:

**Lemma 1.** If $x_1 : A_1, \ldots, x_n : A_n \vdash M : B$ and for all $1 \leq i \leq n \vdash V_i : A_i$, $\vdash W_i : A_i^*$, and $V_i \mathcal{R}_A W_i$, then $M[V_i/x_i] \mathcal{R}^T_A M^*[W_i/x_i]$. ∎

The above should be read with semantic brackets in appropriate places and probably with $W$ and $V$ being elements of the model rather than terms (and thus composition instead of substitution), but it doesn’t make any difference.

But Oege’s theorem actually looked something like this:

```
A  M  B

A^-  M^-  B^+

A^0  M^0  B^0
```

Where $A^0$ and $B^0$ are the relational interpretations of the types $A$ and $B$, $M^0$ is the relational interpretation of the term $M$ with one free variable. The $(\cdot)^+$ and $(\cdot)^-$ are inductively defined translations which replace function spaces in the original type by ‘relation spaces’ in all positive (resp. negative) positions. There are canonical coercion functions $A^- \rightarrow A$, $A \rightarrow A^+$, $A^- \rightarrow A^*$ and $A^0 \rightarrow A^+$ which are defined in the ‘obvious’ way. Note that it’s relational composition along the bottom of the diagram.

What does that look like in terms of explicit computational types? I confi-
I claim that this is implied by Lemma 1, which requires me to connect the logical relation and all those funny es and ps:

**Proposition 2.** For any type $A$

1. $\forall x \in A^- . e_A(x) \ R_A \ e_A^*(x)$;
2. $\forall x \in A , y \in A^+ . x \ R_A y \Rightarrow p_A(x) = p_A^*(y)$.

**Proof.** The two parts are proved simultaneously by induction on $A$. The base case is trivial, whilst for function types we reason as follows:

1. If $f \in (A \rightarrow B)^-$, we want to know that $e_{A \rightarrow B}(f) \ R_{A \rightarrow B} \ e_{A \rightarrow B}(f)$.

   Expanding the definitions that's

   
   $$(e_B \circ f \circ p_A) \ R_{A \rightarrow B} (\eta \circ e_B^* \circ f \circ p_A^*)$$

   

Where

$$G^+ = G$$
$$G^- = G$$
$$(A \rightarrow B)^+ = A^- \rightarrow T(B^+)$$
$$(A \rightarrow B)^- = A^+ \rightarrow B^-$$

and

$$e_G(g) = g$$
$$p_G(g) = g$$
$$e_G^*(g) = g$$
$$p_G^*(g) = g$$
$$e_{A \rightarrow B}(f) = e_B \circ f \circ p_A$$
$$p_{A \rightarrow B}(f) = \eta \circ e_B \circ f \circ e_A$$
$$e_{A \rightarrow B}^*(f) = \eta \circ e_B^* \circ f \circ p_A^*$$
$$p_{A \rightarrow B}^*(f) = T(p_B^*) \circ f \circ e_A^*$$
By the definition of $\mathcal{R}_{A\to B}$ that means we have to show that for any $a, b$ with $a \mathcal{R}_A b$
\[(e_B \circ f \circ p_A)(a) \mathcal{R}_B (\eta \circ e_B^* \circ f \circ p_A^*)(b)\]

By induction (second part), we know $p_A(a) = p_A^*(b)$ so the above is
\[e_B(f(p_A(a))) \mathcal{R}_B^T \eta(\epsilon^*_B(f(p_A(a))))\]

By the definition of $\mathcal{R}_B^T$ (definitely do want $\eta$ mono) that holds if
\[e_B(f(p_A(a))) \mathcal{R}_B \epsilon^*_B(f(p_A(a)))\]

which holds by induction (first part).

2. Now assume $f \mathcal{R}_{A\to B} g$ and we want $p_{A\to B}(f) = p_{A\to B}(g)$. That’s
\[(\eta \circ p_B \circ f \circ e_A) = (T(p_B^*) \circ g \circ e_A^*)\]

so pick an arbitrary $x \in A^-$, then we need show
\[(\eta \circ p_B \circ f \circ e_A)(x) = (T(p_B^*) \circ g \circ e_A^*)(x) \quad (1)\]

By induction (first part), we know $(e_A x) \mathcal{R}_A (e_A^* x)$ and hence, as $f$ and $g$ are related, $(f(e_A x)) \mathcal{R}_B^T (g(e_A^* x))$. By the definition of $\mathcal{R}_B^T$, that means $g(e_A^* x) = \eta(v)$ for some $v$ such that $(f(e_A x)) \mathcal{R}_B v$. But then
\[T(p_B^*)(g(e_A^* x)) = T(p_B^*)(\eta v) = \eta(p_B^* v) \quad \text{(monad defn.)}\]

So we can establish Equation 1 if we can show
\[(p_B(f(e_A x))) = (p_B^* v)\]

which follows immediately from the fact that $(f(e_A x)) \mathcal{R}_B v$ and induction (second part).

Now, look back at my version of Oege’s diagram.

**Corollary 3.** If $x : A \vdash M : B$ then
\[e_A; [M]; p_B; \eta = e_A^*; [M^*]; T(p_B^*)\]

**Proof.** If $x \in A^-$ then $(e_A x) \mathcal{R}_A (e_A^* x)$ by part 1 of Proposition 2. Hence, by Lemma 1, $[M](e_A x) \mathcal{R}_B^T [M^*](e_A^* x)$. Hence we’re done by part 2 of Proposition 2, just as we were in that proof. (Not surprising, since we’re in a CCC.)