

Return of the Redundant Checks

February 7, 1989

1 A Harder Example

This example demonstrates that when there is more information present in a program, that information can be harder to extract. Put another way, inferring more about a program requires more sophisticated techniques. The factorial function is again the vehicle. In the first derivation, we use the techniques of the previous handout with some added power (described below). Somewhat surprisingly, this does not yield a very satisfactory analysis of the function. In fact, in most respects the analysis is no better than for the “bad” factorial function. We introduce a new technique to get around this problem and present a second derivation.

The previous strategy is augmented with the following transformation:

$$p \rightarrow q; r \equiv p \rightarrow q \circ S: (\Delta: p); r \circ S: (\Delta: (\text{not} \circ p))$$

In this example, and probably many others, it is useful to say that the argument of a function is an element of a finite set, or that some finite set of elements cannot be the argument of a function. To allow us to do this in a concise and easily recognized way, we add a new EFL construct.

K

```
def Eqobj  ≡ isobj →' ~eq o' ['id, ~id]; ~FF
def NotEqobj ≡ not ∘ Eqobj
```

As before, “S” is used for “Safe”.

$$\text{def } f \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; * \circ [f \circ \text{sub1}, \text{id}]); \text{mkerr}: \langle f \rangle \quad (1)$$

$$\text{def } f \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; * \circ [f \circ \text{sub1}, \text{id}]) \circ S: (\Delta: \text{isposint}); \text{mkerr}: \langle f \rangle \quad (2)$$

$$\begin{aligned} \text{def } f \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \\ \sim 1 \circ S: (\Delta: \text{isposint}); * \circ [f \circ \text{sub1}, \text{id}] \circ S: (\Delta: \text{isposint})); \text{mkerr}: \langle f \rangle \end{aligned} \quad (3)$$

$$\text{def } f \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \quad (4)$$

$$\begin{aligned}
& * \circ \llbracket \text{TT}, S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})) \rrbracket \circ \\
& [h \circ \text{sub1} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})), \text{id} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1}))] \\
\text{def } h & \equiv \text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \quad (15)
\end{aligned}$$

$$\begin{aligned}
& S: (\Delta: (\text{Eqobj: 1})) \circ \sim 1 \circ S: (\Delta: (\text{Eqobj: 1})); \\
& S: (\Delta: \text{isnum}) \circ * \circ S: (\Delta: \llbracket \text{TT}, \text{isposint} \wedge \text{NotEqobj: 1} \rrbracket) \circ \\
& [h \circ \text{sub1} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})), \text{id} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1}))] \\
\text{def } h & \equiv (S: (\Delta: (\text{Eqobj: 1})) \vee S: (\Delta: \text{isnum})) \circ (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \quad (16) \\
& \sim 1 \circ S: (\Delta: (\text{Eqobj: 1})); \\
& * \circ S: (\Delta: \llbracket \text{TT}, \text{isposint} \wedge \text{NotEqobj: 1} \rrbracket) \circ \\
& [h \circ \text{sub1} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})), \text{id} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1}))])
\end{aligned}$$

$$\begin{aligned}
\text{def } h & \equiv S: (\Delta: \text{isnum}) \circ (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \sim 1 \circ S: (\Delta: (\text{Eqobj: 1})); \quad (17) \\
& * \circ S: (\Delta: \llbracket \text{TT}, \text{isposint} \wedge \text{NotEqobj: 1} \rrbracket) \circ \\
& [h \circ \text{sub1} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})), \text{id} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1}))])
\end{aligned}$$

$$\begin{aligned}
\text{def } h & \equiv S: (\Delta: \text{isnum}) \circ (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \sim 1 \circ S: (\Delta: (\text{Eqobj: 1})); \quad (18) \\
& * \circ S: (\Delta: \llbracket \text{TT}, \text{isposint} \wedge \text{NotEqobj: 1} \rrbracket) \circ \\
& [S: (\Delta: \text{isnum}) \circ h \circ \text{sub1} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})), \text{id} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1}))])
\end{aligned}$$

$$\begin{aligned}
\text{def } h & \equiv S: (\Delta: \text{isnum}) \circ (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \sim 1 \circ S: (\Delta: (\text{Eqobj: 1})); \quad (19) \\
& * \circ S: (\Delta: \llbracket \text{isnum}, \text{isposint} \wedge \text{NotEqobj: 1} \rrbracket) \circ \\
& [h \circ \text{sub1} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})), \text{id} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1}))]) \quad (20)
\end{aligned}$$

This hasn't gotten us very far—we still can't see that the multiplication is going to be applied to two integers. One solution is to “guess” that h might produce something more restrictive than an isnum , and try to prove it. To do this, we define a new function

$$g \equiv \cancel{S: (\Delta: p)} \circ h$$

where p passes a subset of isnum .

$$\begin{aligned}
\text{def } g & \equiv \Delta: \text{isposint} \circ (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \sim 1 \circ S: (\Delta: (\text{Eqobj: 1})); \quad (21) \\
& * \circ S: (\Delta: \llbracket \text{TT}, \text{isposint} \wedge \text{NotEqobj: 1} \rrbracket) \circ \\
& [g \circ \text{sub1} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})), \text{id} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1}))])
\end{aligned}$$

$$\begin{aligned}
\text{def } g & \equiv \Delta: \text{isposint} \circ (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \sim 1 \circ S: (\Delta: (\text{Eqobj: 1})); \quad (22) \\
& * \circ S: (\Delta: \llbracket \text{TT}, \text{isposint} \wedge \text{NotEqobj: 1} \rrbracket) \circ \\
& [S: (\Delta: \text{isposint}) \circ g \circ \text{sub1} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})), \text{id} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1}))])
\end{aligned}$$

$$\begin{aligned}
\text{def } g & \equiv \Delta: \text{isposint} \circ (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \sim 1 \circ S: (\Delta: (\text{Eqobj: 1})); \quad (23) \\
& * \circ S: (\Delta: \llbracket \text{isposint}, \text{isposint} \wedge \text{NotEqobj: 1} \rrbracket) \circ
\end{aligned}$$

$$\begin{aligned}
& [g \circ \text{sub1} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})), \text{id} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1}))]) \\
\text{def } g & \equiv \Delta: \text{isposint} \circ (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \\
& S: (\Delta: (\text{Eqobj: 1})) \circ \sim 1 \circ S: (\Delta: (\text{Eqobj: 1})); \\
& S: (\Delta: \text{isposint}) \circ * \circ S: (\Delta: [\text{isposint}, \text{isposint} \wedge \text{NotEqobj: 1}]) \circ \\
& [g \circ \text{sub1} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})), \text{id} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1}))])
\end{aligned} \tag{24}$$

$$\begin{aligned}
\text{def } g & \equiv \Delta: \text{isposint} \circ (S: (\Delta: (\text{Eqobj: 1})) \wedge S: (\Delta: \text{isposint})) \circ \\
& (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \sim 1 \circ S: (\Delta: (\text{Eqobj: 1})); \\
& * \circ S: (\Delta: [\text{isposint}, \text{isposint} \wedge \text{NotEqobj: 1}]) \circ \\
& [g \circ \text{sub1} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})), \text{id} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1}))])
\end{aligned} \tag{25}$$

$$\begin{aligned}
\text{def } g & \equiv \Delta: \text{isposint} \circ S: (\Delta: \text{isposint}) \circ (\text{eq} \circ [\sim 1, \text{id}] \circ \\
& S: (\Delta: \text{isposint}) \rightarrow \sim 1 \circ S: (\Delta: (\text{Eqobj: 1})); \\
& * \circ S: (\Delta: [\text{isposint}, \text{isposint} \wedge \text{NotEqobj: 1}]) \circ \\
& [g \circ \text{sub1} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})), \text{id} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1}))])
\end{aligned} \tag{26}$$

$$\begin{aligned}
\text{def } g & \equiv S: (\Delta: \text{isposint}) \circ (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \sim 1 \circ S: (\Delta: (\text{Eqobj: 1})); \\
& * \circ S: (\Delta: [\text{isposint}, \text{isposint} \wedge \text{NotEqobj: 1}]) \circ \\
& [g \circ \text{sub1} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1})), \text{id} \circ S: (\Delta: (\text{isposint} \wedge \text{NotEqobj: 1}))])
\end{aligned} \tag{27}$$

So $g \equiv S: (\Delta: \text{isposint}) \circ g \equiv h$

2 A Second Approach

The problem with the previous approach is determining what a recursively defined function can return. A better way to calculate this is to study approximations to the function. This eliminates the function variable and allows analysis of the results at points close to the termination condition. This approach is reminiscent of abstract interpretation.

$$\text{def } f \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; * \circ [f \circ \text{sub1}, \text{id}]); \text{mkerr}: \langle f \rangle \tag{28}$$

$$\text{def } f \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; * \circ [f \circ \text{sub1}, \text{id}]) \circ S: (\Delta: \text{isposint}); \text{mkerr}: \langle f \rangle \tag{29}$$

$$\begin{aligned} \text{def } f & \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \\ & \sim 1 \circ S: (\Delta: \text{isposint}); * \circ [f \circ \text{sub1}, \text{id}] \circ S: (\Delta: \text{isposint})); \text{mkerr}: \langle f \rangle \end{aligned} \tag{30}$$

$$\begin{aligned} \text{def } f & \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isposint}) \rightarrow \\ & \sim 1 \circ S: (\Delta: \text{isposint}) \circ S: (\Delta: (\text{Eqobj: 1})); \\ & * \circ [f \circ \text{sub1}, \text{id}] \circ S: (\Delta: \text{isposint}) \circ S: (\Delta: (\text{NotEqobj: 1})); \text{mkerr}: \langle f \rangle \end{aligned} \tag{31}$$

$$\text{def } f \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow \quad (32)$$

$$\begin{aligned} & \sim 1 \circ S : (\Delta : \text{isposint} \circ \Delta : (\text{Eqobj}: 1)); \\ & * \circ [f \circ \text{sub1}, \text{id}] \circ S : (\Delta : \text{isposint} \circ \Delta : (\text{NotEqobj}: 1)); \text{mkerr}: \langle f \rangle \end{aligned}$$

$$\text{def } f \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow \quad (33)$$

$$\begin{aligned} & \sim 1 \circ S : (\Delta : (\text{isposint} \wedge \text{Eqobj}: 1)); \\ & * \circ [f \circ \text{sub1}, \text{id}] \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)); \text{mkerr}: \langle f \rangle \end{aligned}$$

$$\text{def } f \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow \sim 1 \circ S : (\Delta : (\text{Eqobj}: 1)); \quad (34)$$

$$* \circ [f \circ \text{sub1}, \text{id}] \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)); \text{mkerr}: \langle f \rangle$$

$$\text{def } f \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow \sim 1 \circ S : (\Delta : (\text{Eqobj}: 1)); \quad (35)$$

$$\begin{aligned} & * \circ [f \circ \text{sub1} \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)), \\ & \text{id} \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1))]; \text{mkerr}: \langle f \rangle \end{aligned}$$

$$\text{def } f \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow \sim 1 \circ S : (\Delta : (\text{Eqobj}: 1)); \quad (36)$$

$$\begin{aligned} & * \circ [f \circ S : (\Delta : \text{isposint}) \circ \text{sub1} \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)), \\ & S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)) \circ \text{id} \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1))]; \text{mkerr}: \langle f \rangle \end{aligned}$$

$$\text{def } f \equiv \text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow \sim 1 \circ S : (\Delta : (\text{Eqobj}: 1)); \quad (37)$$

$$\begin{aligned} & * \circ [h \circ \text{sub1} \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)), \\ & S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)) \circ \text{id} \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1))]; \\ & \text{mkerr}: \langle f \rangle \end{aligned}$$

$$\text{def } h \equiv (\text{isposint} \rightarrow (\text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow \sim 1 \circ S : (\Delta : (\text{Eqobj}: 1)); \quad (38)$$

$$\begin{aligned} & * \circ [f \circ S : (\Delta : \text{isposint}) \circ \text{sub1} \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)), \\ & S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)) \circ \text{id} \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1))]; \\ & \text{mkerr}: \langle f \rangle \circ S : (\Delta : \text{isposint}) \end{aligned}$$

$$\text{def } h \equiv \text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow \sim 1 \circ S : (\Delta : (\text{Eqobj}: 1)); \quad (39)$$

$$\begin{aligned} & * \circ [f \circ S : (\Delta : \text{isposint}) \circ \text{sub1} \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)), \\ & S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)) \circ \text{id} \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1))] \end{aligned}$$

$$\text{def } h \equiv \text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow \sim 1 \circ S : (\Delta : (\text{Eqobj}: 1)); \quad (40)$$

$$\begin{aligned} & * \circ [h \circ \text{sub1} \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)), \\ & S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)) \circ \text{id} \circ S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1))] \end{aligned}$$

This much of the derivation is the same as the previous example through step 13. At this point we need to know something about the result of h in order to proceed. We do this by analyzing successive approximations to $h : h_0, h_1, h_2, \dots$

$$\text{def } h_0 \equiv \text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; * \circ [\sim \perp \circ \text{sub1}, \text{id}] \quad (41)$$

$$\text{def } h_0 \equiv \text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; \sim \perp \quad (42)$$

$$\text{def } h_1 \equiv \text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; * \circ [h_0 \circ \text{sub1}, \text{id}] \quad (43)$$

$$(44)$$

We now analyze h_0 . We use the fact that $h \equiv h \circ S : (\Delta : \text{isposint})$.

$$\text{def } h_0 \equiv (\text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; \sim \perp) \circ S : (\Delta : \text{isposint}) \quad (45)$$

$$\begin{aligned} \text{def } h_0 &\equiv \text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow \sim 1 \circ S : (\Delta : \text{isposint}); \\ &\sim \perp \circ S : (\Delta : \text{isposint}) \end{aligned} \quad (46)$$

$$\begin{aligned} \text{def } h_0 &\equiv \text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow S : (\Delta : (\text{Eqobj}: 1)) \circ \sim 1; \\ &S : (\Delta : \neg \text{FF}) \circ \sim \perp \end{aligned} \quad (47)$$

$$\text{def } h_0 \equiv (S : (\Delta : (\text{Eqobj}: 1)) \vee S : (\Delta : \neg \text{FF})) \circ \text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow \sim 1 \quad (48)$$

$$\text{def } h_0 \equiv (S : (\Delta : (\text{Eqobj}: 1 \vee \neg \text{FF}))) \circ \text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow \sim 1; \sim \perp \quad (49)$$

$$\text{def } h_0 \equiv (S : (\Delta : (\text{Eqobj}: 1))) \circ \text{eq} \circ [\sim 1, \text{id}] \circ S : (\Delta : \text{isposint}) \rightarrow \sim 1; \sim \perp \quad (50)$$

We now know that

$$h_0 \circ S : (\Delta : \text{isposint}) \equiv S : (\Delta : (\text{Eqobj}: 1)) \circ h_0 \circ S : (\Delta : \text{isposint})$$

We use h_0 to analyze h_1 .

$$\text{def } h_1 \equiv \text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; * \circ [h_0 \circ \text{sub1}, \text{id}] \circ S : (\Delta : \text{isposint}) \quad (51)$$

$$\text{def } h_1 \equiv \text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; * \circ [h_0 \circ \text{sub1}, \text{id}] \circ S : (\Delta : \text{isposint}) \quad (52)$$

$$\begin{aligned} \text{def } h_1 &\equiv \text{eq} \circ [\sim 1, \text{id}] \rightarrow S : (\Delta : (\text{Eqobj}: 1)) \circ \sim 1; \\ &* \circ [h_0 \circ S : (\Delta : \text{isposint}) \circ \text{sub1}, S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)) \circ \text{id}] \end{aligned} \quad (53)$$

$$\begin{aligned} \text{def } h_1 &\equiv \text{eq} \circ [\sim 1, \text{id}] \rightarrow S : (\Delta : (\text{Eqobj}: 1)) \circ \sim 1; \\ &* \circ [S : (\Delta : (\text{Eqobj}: 1)) \circ h_0 \circ \text{sub1}, S : (\Delta : (\text{isposint} \wedge \text{NotEqobj}: 1)) \circ \text{id}] \end{aligned} \quad (54)$$

$$\begin{aligned} \text{def } h_1 &\equiv \text{eq} \circ [\sim 1, \text{id}] \rightarrow S : (\Delta : (\text{Eqobj}: 1)) \circ \sim 1; \\ &* \circ S : (\Delta : [\text{Eqobj}: 1, \text{isposint} \wedge \text{NotEqobj}: 1]) \circ [h_0 \circ \text{sub1}, \text{id}] \end{aligned} \quad (55)$$

$$\begin{aligned} \text{def } h_1 &\equiv \text{eq} \circ [\sim 1, \text{id}] \rightarrow S : (\Delta : (\text{Eqobj}: 1)) \circ \sim 1; \\ &S : (\Delta : \text{isposint}) \circ * \circ S : (\Delta : [\text{Eqobj}: 1, \text{isposint} \wedge \text{NotEqobj}: 1]) \circ \\ &[h_0 \circ \text{sub1}, \text{id}] \end{aligned} \quad (56)$$

$$\begin{aligned} \text{def } h_1 &\equiv (S : (\Delta : (\text{Eqobj}: 1)) \vee S : (\Delta : \text{isposint})) \circ (\text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; \\ &* \circ S : (\Delta : [\text{Eqobj}: 1, \text{isposint} \wedge \text{NotEqobj}: 1]) \circ [h_0 \circ \text{sub1}, \text{id}]) \end{aligned} \quad (57)$$

$$\begin{aligned} \text{def } h_1 &\equiv S:(\Delta:\text{isposint}) \circ (\text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; \\ &\quad * \circ S:(\Delta: [\text{Eqobj}: 1, \text{isposint} \wedge \text{NotEqobj}: 1]) \circ [h_0 \circ \text{sub1}, \text{id}]) \end{aligned} \quad (58)$$

Thus,

$$h_1 \circ S:(\Delta:\text{isposint}) \equiv S:(\Delta:\text{isposint}) \circ h_1 \circ S:(\Delta:\text{isposint})$$

If we analyze h_2 in the same manner, we discover that

$$h_2 \circ S:(\Delta:\text{isposint}) \equiv S:(\Delta:\text{isposint}) \circ h_2 \circ S:(\Delta:\text{isposint})$$

Under suitable assumptions, this allows us to conclude that the same law holds for h .

3 A Third Approach

This analysis is based on the linear expansion theorem.

$$\text{def } f \equiv \text{eq} \circ [\text{id}, \sim 1] \rightarrow \sim 1; * \circ [f \circ \text{sub1}, \text{id}] \quad (59)$$

$$\equiv \dots; \text{eq} \circ [\text{id}, \sim 1] \circ \text{sub1}^n \rightarrow * \circ [\text{id}, \text{sub1}, \dots, \text{sub1}^n] \quad (60)$$

A useful fact to know is a set of values for which a function terminates. We focus on an arbitrary term in the linear expansion, and try to determine values for which the predicate is true.

$$\equiv \Delta:\text{istrue} \circ \text{eq} \circ [\text{id}, \sim 1] \circ \text{sub1}^n \quad (61)$$

$$\equiv \Delta:\text{istrue} \circ \text{eq} \circ [\text{id}, \sim 1] \circ \text{sub} \circ [\text{id}, \sim n] \quad (62)$$

$$\equiv \Delta:\text{istrue} \circ \text{eq} \circ [\text{id}, K: 1] \circ \text{sub} \circ [\text{id}, K: n] \quad (63)$$

$$\equiv \Delta: (\exists \beta. [\text{Eqobj}: \beta, \text{Eqobj}: \beta]) \circ [\text{id}, K: 1] \circ \text{sub} \circ [\text{id}, K: n] \quad (64)$$

$$\equiv \Delta: (\exists \beta. (\text{Eqobj}: \beta \circ \text{id}) \wedge (\text{Eqobj}: \beta \circ K: 1)) \circ \text{sub} \circ [\text{id}, K: n] \quad (65)$$

$$\equiv \Delta: (\exists \beta. \text{Eqobj}: \beta \wedge (\text{Eqobj}: \beta \circ K: 1)) \circ \text{sub} \circ [\text{id}, K: n] \quad (66)$$

$$\equiv \Delta: (\exists \beta. \text{Eqobj}: \beta \wedge (S: (\text{Eqobj}: \beta) \circ S: (K: 1))) \circ \text{sub} \circ [\text{id}, K: n] \quad (67)$$

$$\equiv \Delta: (\exists \beta. \text{Eqobj}: \beta \wedge S: (\text{Eqobj}: \beta \circ K: 1)) \circ \text{sub} \circ [\text{id}, K: n] \quad (68)$$

$$\equiv \Delta: (\exists \beta. \text{Eqobj}: \beta \wedge S: (K: ((\text{Eqobj}: \beta): 1))) \circ \text{sub} \circ [\text{id}, K: n] \quad (69)$$

$$\equiv \Delta: (\text{Eqobj}: 1 \wedge S: (K: ((\text{Eqobj}: 1): 1))) \circ \text{sub} \circ [\text{id}, K: n] \quad (70)$$

$$\equiv \Delta: (\text{Eqobj}: 1 \wedge S: (K: \text{TT})) \circ \text{sub} \circ [\text{id}, K: n] \quad (71)$$

$$\equiv \Delta: (\text{Eqobj}: 1 \wedge \sim \text{TT}) \circ \text{sub} \circ [\text{id}, K: n] \quad (72)$$

$$\equiv \Delta: (\text{Eqobj}: 1) \circ \text{sub} \circ [\text{id}, K: n] \quad (73)$$

$$\equiv \Delta: (\exists \gamma. [\text{isnum} \wedge \text{Eqobj}: \gamma, \text{Eqobj}: \gamma \circ \text{add1}]) \circ [\text{id}, K: n] \quad (74)$$

$$\equiv \Delta: (\exists \gamma. (\text{isnum} \wedge \text{Eqobj}: \gamma) \circ \text{id} \wedge \text{Eqobj}: \gamma \circ \text{add1} \circ K: n) \quad (75)$$

$$\equiv \Delta: (\exists \gamma. (\text{isnum} \wedge \text{Eqobj}: \gamma) \wedge \text{Eqobj}: \gamma \circ \text{add1} \circ K: n) \quad (76)$$

$$\equiv \Delta: (\exists \gamma. (\text{isnum} \wedge \text{Eqobj}:\gamma) \wedge \text{Eqobj}:\gamma \circ \text{add1} \circ \Delta: \text{isposint} \circ K:n) \quad (77)$$

$$\equiv \Delta: (\exists \gamma. (\text{isnum} \wedge \text{Eqobj}:\gamma) \wedge S: (\text{Eqobj}:\gamma) \circ S: \text{add1} \circ S: (K:n)) \quad (78)$$

$$\equiv \Delta: (\exists \gamma. (\text{isnum} \wedge \text{Eqobj}:\gamma) \wedge S: (\text{Eqobj}:\gamma \circ \text{add1} \circ K:n)) \quad (79)$$

$$\equiv \Delta: (\exists \gamma. (\text{isnum} \wedge \text{Eqobj}:\gamma) \wedge S: (K: ((\text{Eqobj}:\gamma): (\text{add1}:n)))) \quad (80)$$

$$\equiv \Delta: (\text{isnum} \wedge \text{Eqobj}: (\text{add1}:n) \wedge S: (K: ((\text{Eqobj}: (\text{add1}:n)): (\text{add1}:n)))) \quad (81)$$

$$\equiv \Delta: (\text{isnum} \wedge \text{Eqobj}: (\text{add1}:n) \wedge S: (K: \text{TT})) \quad (82)$$

$$\equiv \Delta: (\text{isnum} \wedge \text{Eqobj}: (\text{add1}:n) \wedge K: \text{TT}) \quad (83)$$

$$\equiv \Delta: (\text{isnum} \wedge \text{Eqobj}: (\text{add1}:n)) \quad (84)$$

$$\equiv \Delta: (\text{Eqobj}: (\text{add1}:n)) \quad (85)$$

At this point, we know that $\Delta: \text{istrue} \circ p_i \equiv \Delta: (\text{Eqobj}: (\text{add1}:i))$, where p_i is the i th guard in the linear expansion. From this, we can conclude that f terminates on all arguments in the set

$$\bigvee_{i \downarrow 0} \text{Eqobj}: (\text{add1}:i) = \bigvee_{i \downarrow 1} \text{Eqobj}:i = \text{isposint}$$

Usually we are interested in trying to “drive” a filter to the left; i.e., given some knowledge (a filter) about a function’s argument, we try to conclude something (another filter) about its result. In this example, we know something about the desired result (those values for which a predicate is true) and want to conclude something about the argument.