

Eliminating Redundant Checks

Alex Aiken

January 25, 1989

$f: x = \begin{cases} D_e \\ \perp \\ \text{error} \end{cases}$
 $S: f: x = \begin{cases} x \in D_e \text{ then } x \\ f.x \in D_e \text{ then } \perp_{\text{err}} \\ \text{else } f: x \end{cases}$
 $\perp_{\text{err}}$
 $\perp$

1 An Example

"S" is used for "Safe". Several new transformations are used.

$$\begin{aligned}
 K: ((S: (\Delta: f)): x) &= S: (\Delta: f) \circ K: x \text{ in context} \\
 [S: (\Delta: p_1) \circ f_1, \dots, S: (\Delta: p_n) \circ f_n] &= S: (\Delta: [p_1, \dots, p_n]) \circ [f_1, \dots, f_n] \text{ in context} \\
 \text{sub1} &= S: (\Delta: \text{isreal}) \circ \text{sub1}
 \end{aligned}$$

The example is the familiar factorial function.

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

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

$$\text{def } f \equiv \text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; * \circ [h \circ \text{sub1}, \text{id}] \quad (3)$$

$$\text{def } h \equiv (\text{eq} \circ [\sim 1, \text{id}] \rightarrow \sim 1; * \circ [f \circ \text{sub1}, \text{id}]) \circ S: (\Delta: \text{isreal}) \quad (4)$$

Note that at this point, we know $h = f \circ S: (\Delta: \text{isreal})$.

$$\begin{aligned}
 \text{def } h &\equiv \text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isreal}) \rightarrow \quad (5) \\
 &\quad \sim 1 \circ S: (\Delta: \text{isreal}); * \circ [f \circ \text{sub1}, \text{id}] \circ S: (\Delta: \text{isreal})
 \end{aligned}$$

$$\begin{aligned}
 \text{def } h &\equiv \text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isreal}) \rightarrow \quad (6) \\
 &\quad \sim 1 \circ S: (\Delta: \text{isreal}); * \circ [f \circ \text{sub1} \circ S: (\Delta: \text{isreal}), \text{id} \circ S: (\Delta: \text{isreal})]
 \end{aligned}$$

$$\begin{aligned}
 \text{def } h &\equiv \text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isreal}) \rightarrow \quad (7) \\
 &\quad \sim 1 \circ S: (\Delta: \text{isreal}); * \circ [f \circ \text{sub1} \circ S: (\Delta: \text{isreal}), S: (\Delta: \text{isreal})]
 \end{aligned}$$

$$\begin{aligned}
 \text{def } h &\equiv \text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isreal}) \rightarrow \quad (8) \\
 &\quad \sim 1 \circ S: (\Delta: \text{isreal}); * \circ [f \circ S: (\Delta: \text{isreal}) \circ \text{sub1} \circ S: (\Delta: \text{isreal}), S: (\Delta: \text{isreal})]
 \end{aligned}$$

$$\begin{aligned}
 \text{def } h &\equiv \text{eq} \circ [\sim 1, \text{id}] \circ S: (\Delta: \text{isreal}) \rightarrow \quad (9) \\
 &\quad \sim 1 \circ S: (\Delta: \text{isreal}); * \circ [h \circ \text{sub1} \circ S: (\Delta: \text{isreal}), S: (\Delta: \text{isreal})]
 \end{aligned}$$

$$\text{def } h \equiv \text{eq} \circ [\sim 1 \circ S : (\Delta : \text{isreal}), \text{id} \circ S : (\Delta : \text{isreal})] \rightarrow \quad (10)$$

$$\sim 1 \circ S : (\Delta : \text{isreal}); * \circ [h \circ \text{sub1} \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})]$$

$$\text{def } h \equiv \text{eq} \circ [\sim 1 \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})] \rightarrow \quad (11)$$

$$\sim 1 \circ S : (\Delta : \text{isreal}); * \circ [h \circ \text{sub1} \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})]$$

$$\text{def } h \equiv \text{eq} \circ [K : 1 \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})] \rightarrow \quad (12)$$

$$K : 1 \circ S : (\Delta : \text{isreal}); * \circ [h \circ \text{sub1} \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})]$$

$$\text{def } h \equiv \text{eq} \circ [K : (S : (\Delta : \text{isreal}) : 1) \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})] \rightarrow \quad (13)$$

$$K : (S : (\Delta : \text{isreal}) : 1) \circ S : (\Delta : \text{isreal}); * \circ [h \circ \text{sub1} \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})]$$

$$\text{def } h \equiv \text{eq} \circ [S : (\Delta : \text{isreal}) \circ K : 1 \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})] \rightarrow \quad (14)$$

$$S : (\Delta : \text{isreal}) \circ K : 1 \circ S : (\Delta : \text{isreal});$$

$$* \circ [h \circ \text{sub1} \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})]$$

$$\text{def } h \equiv \text{eq} \circ S : (\Delta : [\text{isreal}, \text{isreal}]) \circ [K : 1 \circ S : (\Delta : \text{isreal}), \text{id}] \rightarrow \quad (15)$$

$$S : (\Delta : \text{isreal}) \circ K : 1 \circ S : (\Delta : \text{isreal});$$

$$* \circ [h \circ \text{sub1} \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})]$$

$$\text{def } h \equiv \text{eq} \circ S : (\Delta : [\text{isreal}, \text{isreal}]) \circ [K : 1 \circ S : (\Delta : \text{isreal}), \text{id}] \rightarrow \quad (16)$$

$$S : (\Delta : \text{isreal}) \circ K : 1 \circ S : (\Delta : \text{isreal});$$

$$* \circ S : (\Delta : [\text{TT}, \text{isreal}]) \circ [h \circ \text{sub1} \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})]$$

$$\text{def } h \equiv \text{eq} \circ S : (\Delta : [\text{isreal}, \text{isreal}]) \circ [K : 1 \circ S : (\Delta : \text{isreal}), \text{id}] \rightarrow \quad (17)$$

$$S : (\Delta : \text{isreal}) \circ K : 1 \circ S : (\Delta : \text{isreal});$$

$$S : (\Delta : \text{isreal}) \circ * \circ S : (\Delta : [\text{TT}, \text{isreal}]) \circ [h \circ \text{sub1} \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})]$$

$$\text{def } h \equiv S : (\Delta : \text{isreal}) \circ (\text{eq} \circ S : (\Delta : [\text{isreal}, \text{isreal}]) \circ [K : 1 \circ S : (\Delta : \text{isreal}), \text{id}] \rightarrow \quad (18)$$

$$K : 1 \circ S : (\Delta : \text{isreal});$$

$$* \circ S : (\Delta : [\text{TT}, \text{isreal}]) \circ [h \circ \text{sub1} \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})])$$

We have now shown that $h = S : (\Delta : \text{isreal}) \circ h$. This fact (transformation) is exploited in the next series of transformations.

$$\text{def } h \equiv S : (\Delta : \text{isreal}) \circ (\text{eq} \circ S : (\Delta : [\text{isreal}, \text{isreal}]) \circ [K : 1 \circ S : (\Delta : \text{isreal}), \text{id}] \rightarrow \quad (19)$$

$$K : 1 \circ S : (\Delta : \text{isreal});$$

$$* \circ S : (\Delta : [\text{TT}, \text{isreal}]) \circ [S : (\Delta : \text{isreal}) \circ h \circ \text{sub1} \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})])$$

$$\text{def } h \equiv S : (\Delta : \text{isreal}) \circ (\text{eq} \circ S : (\Delta : [\text{isreal}, \text{isreal}]) \circ [K : 1 \circ S : (\Delta : \text{isreal}), \text{id}] \rightarrow \quad (20)$$

$$K : 1 \circ S : (\Delta : \text{isreal});$$

$$* \circ S : (\Delta : [\text{TT}, \text{isreal}]) \circ S : \Delta : ([\text{isreal}, \text{isreal}]) \circ [h \circ \text{sub1} \circ S : (\Delta : \text{isreal}), S : (\Delta : \text{isreal})])$$

$$\text{def } h \equiv S:(\Delta:\text{isreal}) \circ (\text{eq} \circ S:(\Delta:[[\text{isreal}, \text{isreal}]]) \circ [K:1 \circ S:(\Delta:\text{isreal}), \text{id}] \rightarrow \quad (21)$$

$$K:1 \circ S:(\Delta:\text{isreal});$$

$$* \circ S:(\Delta:([[\text{TT}, \text{isreal}] \circ \Delta:[[\text{isreal}, \text{isreal}]]) \circ [h \circ \text{sub1} \circ S:(\Delta:\text{isreal}), S:(\Delta:\text{isreal})])$$

$$\text{def } h \equiv S:(\Delta:\text{isreal}) \circ (\text{eq} \circ S:(\Delta:[[\text{isreal}, \text{isreal}]]) \circ [K:1 \circ S:(\Delta:\text{isreal}), \text{id}] \rightarrow \quad (22)$$

$$K:1 \circ S:(\Delta:\text{isreal});$$

$$* \circ S:(\Delta:([\text{TT}, \text{isreal}] \wedge [\text{isreal}, \text{isreal}])) \circ [h \circ \text{sub1} \circ S:(\Delta:\text{isreal}), S:(\Delta:\text{isreal})])$$

$$\text{def } h \equiv S:(\Delta:\text{isreal}) \circ (\text{eq} \circ S:(\Delta:[[\text{isreal}, \text{isreal}]]) \circ [K:1 \circ S:(\Delta:\text{isreal}), \text{id}] \rightarrow \quad (23)$$

$$K:1 \circ S:(\Delta:\text{isreal});$$

$$* \circ S:(\Delta:([\text{TT} \wedge \text{isreal}, \text{isreal} \wedge \text{isreal}])) \circ [h \circ \text{sub1} \circ S:(\Delta:\text{isreal}), S:(\Delta:\text{isreal})])$$

$$\text{def } h \equiv S:(\Delta:\text{isreal}) \circ (\text{eq} \circ S:(\Delta:[[\text{isreal}, \text{isreal}]]) \circ [K:1 \circ S:(\Delta:\text{isreal}), \text{id}] \rightarrow \quad (24)$$

$$K:1 \circ S:(\Delta:\text{isreal});$$

$$* \circ S:(\Delta:([\text{isreal}, \text{isreal}])) \circ [h \circ \text{sub1} \circ S:(\Delta:\text{isreal}), S:(\Delta:\text{isreal})])$$

2 Case Construct

The last function in the derivation has “annotations” of the form $g \circ S:(\Delta:p)$ showing the values that can be arguments of g . To take advantage of this information, g must be transformed into a function which only performs tests on values passing $\Delta:p$. I propose that this be accomplished by implementing every primitive transformation by a *Case* statement. Case is just a restricted form of conditional. Some sequences of transformations are probably more efficient using case, and the generated code (at least in C) should be more efficient as well. Case is defined in terms of conditional.

$$\text{case:} \langle p_1 \rightarrow f_1; \dots; p_n \rightarrow f_n; f_{n+1} \rangle = p_1 \rightarrow f_1; (\dots (p_n \rightarrow f_n; f_{n+1}) \dots)$$

Some properties of case

$$\text{case:} \langle p_1 \rightarrow f_1; \dots; p_n \rightarrow f_n; f_{n+1} \rangle \circ S:(\Delta:p) = \text{case:} \langle p_1 \circ S:(\Delta:p) \rightarrow f_1; \dots; p_n \circ S:(\Delta:p) \rightarrow f_n; f_{n+1} \rangle$$

$$\text{case:} \langle p_1 \rightarrow f_1; \dots; p_{i-1} \rightarrow f_{i-1}; \text{TT} \rightarrow f_i; \dots; p_n \rightarrow f_n; f_{n+1} \rangle = \text{case:} \langle p_1 \rightarrow f_1; \dots; p_{i-1} \rightarrow f_{i-1}; f_i \rangle$$

$$\text{case:} \langle \dots; p_{i-1} \rightarrow f_{i-1}; \text{FF} \rightarrow f_i; p_{i+1} \rightarrow f_{i+1} \dots \rangle = \text{case:} \langle \dots; p_{i-1} \rightarrow f_{i-1}; p_{i+1} \rightarrow f_{i+1} \dots \rangle$$

Here is an example of its use. The functions `sublint` and `sublreal` are equivalent to `sub1` on integers and reals respectively and produce `⊥err` everywhere else.

$$\text{sub1} = \text{case:} \langle \text{isint} \rightarrow \text{sublint}; \text{isreal} \circ S:(\Delta:(\text{not} \circ \text{isint})) \rightarrow \text{sublreal}; \text{mkerr:} \langle \text{“error”} \rangle \rangle$$

$$\text{sub1} \circ S: (\Delta: \text{isreal}) \quad (25)$$

$$= \text{case: } \langle \text{isint} \rightarrow \text{sub1int}; \text{isreal} \circ S: (\Delta: (\text{not} \circ \text{isint})) \rightarrow \text{sub1real}; \text{mkerr: } \langle \text{"error"} \rangle \rangle \circ S: (\Delta: \text{isreal}) \quad (26)$$

$$= \text{case: } \langle \text{isint} \circ S: (\Delta: \text{isreal}) \rightarrow \text{sub1int}; \text{isreal} \circ S: (\Delta: (\text{not} \circ \text{isint})) \circ S: (\Delta: \text{isreal}) \rightarrow \text{sub1real}; \text{mkerr: } \langle \text{"error"} \rangle \rangle \quad (27)$$

$$= \text{case: } \langle \text{isint} \wedge \text{isreal} \rightarrow \text{sub1int}; \text{isreal} \circ S: (\Delta: (\text{not} \circ \text{isint})) \circ S: (\Delta: \text{isreal}) \rightarrow \text{sub1real}; \text{mkerr: } \langle \text{"error"} \rangle \rangle \quad (28)$$

$$= \text{case: } \langle \text{isint} \rightarrow \text{sub1int}; \text{isreal} \circ S: (\Delta: (\text{not} \circ \text{isint})) \circ S: (\Delta: \text{isreal}) \rightarrow \text{sub1real}; \text{mkerr: } \langle \text{"error"} \rangle \rangle \quad (29)$$

$$= \text{case: } \langle \text{isint} \rightarrow \text{sub1int}; \text{isreal} \circ S: (\Delta: \text{isreal}) \circ S: (\Delta: (\text{not} \circ \text{isint})) \rightarrow \text{sub1real}; \text{mkerr: } \langle \text{"error"} \rangle \rangle \quad (30)$$

$$= \text{case: } \langle \text{isint} \rightarrow \text{sub1int}; \text{TT} \circ S: (\Delta: (\text{not} \circ \text{isint})) \rightarrow \text{sub1real}; \text{mkerr: } \langle \text{"error"} \rangle \rangle \quad (31)$$

$$= \text{case: } \langle \text{isint} \rightarrow \text{sub1int}; \text{TT} \circ \text{id} \rightarrow \text{sub1real}; \text{mkerr: } \langle \text{"error"} \rangle \rangle \quad (32)$$

$$= \text{case: } \langle \text{isint} \rightarrow \text{sub1int}; \text{TT} \rightarrow \text{sub1real}; \text{mkerr: } \langle \text{"error"} \rangle \rangle \quad (33)$$

$$= \text{case: } \langle \text{isint} \rightarrow \text{sub1int}; \text{sub1real} \rangle \quad (34)$$