Coma: an intermediate verification language with explicit abstraction barriers

Andrei Paskevich and Paul Patault

with thanks to Jean-Christophe Filliâtre

LMF, Université Paris-Saclay • Toccata, Inria Saclay

Frama-C days • 13 jun 2024

```
type tree = Node tree elt tree
          | Leaf

let removeRoot (t: tree) : tree




= match t with
  | Node l _ r → mergeTree l r
  | Leaf → fail
```

```
type tree = Node tree elt tree
          | Leaf

let removeRoot (t: tree) : tree
  requires { t ≠ Leaf }
  ensures  { match t with
    | Node l _ r → ∀e:elt. e ∈ result ↔ e ∈ l ∨ e ∈ r
    | Leaf → false }
= match t with
  | Node l _ r → mergeTree l r
  | Leaf → fail
```

```
type tree = Node tree elt tree
          | Leaf

removeRoot (Node l _ r)
  ensures { ∀e:elt. e ∈ result ↔ e ∈ l ∨ e ∈ r }
= mergeTree l r

removeRoot Leaf = fail
```

x, y, z			variable
s, t	$::=$	$x \mid 0 \ldots \mid s + t \ldots$	term
φ, ψ	$::=$	$s = t \ldots \mid \varphi \wedge \psi \ldots$	formula

data

x, y, z			variable
s, t	$::=$	$x \mid 0 \ldots \mid s + t \ldots$	term
φ, ψ	$::=$	$s = t \ldots \mid \varphi \wedge \psi \ldots$	formula

data

code

h, g, f			handler name
e, d	$::=$	$h \ \bar{s} \ \bar{g}$	application
	$\mid$	$e \ / \ h \ \bar{x} \ \bar{g} = d$	definition

x, y, z			variable
s, t	$::=$	$x \mid 0 \ldots \mid s + t \ldots$	term
φ, ψ	$::=$	$s = t \ldots \mid \varphi \wedge \psi \ldots$	formula

data

---

code

h, g, f			handler name
k, o	$::=$	$h \mid \bar{x}\ \bar{g} \to e$	handler
e, d	$::=$	$k\ \bar{s}\ \bar{o}$	application
	$\mid$	$e\ /\ h\ \bar{x}\ \bar{g} = d$	definition

x, y, z			variable
s, t	$::=$	$x \mid 0 \ldots \mid s + t \ldots$	term
φ, ψ	$::=$	$s = t \ldots \mid \varphi \wedge \psi \ldots$	formula

data

---

code

h, g, f			handler name
k, o	$::=$	$h \mid \bar{x}\ \bar{g} \rightarrow e$	handler
e, d	$::=$	$k\ \bar{s}\ \bar{o}$	application
	$\mid$	$e\ /\ h\ \bar{x}\ \bar{g} = d$	definition
	$\mid$	$\varphi\ e$	assertion

x, y, z			variable
s, t	$::=$	$x \mid 0 \ldots \mid s + t \ldots$	term
φ, ψ	$::=$	$s = t \ldots \mid \varphi \wedge \psi \ldots$	formula

data

code

h, g, f			handler name
k, o	$::=$	$h \mid \bar{x}\ \bar{g} \rightarrow e$	handler
e, d	$::=$	$k\ \bar{s}\ \bar{o}$	application
	$\mid$	$e\ /\ h\ \bar{x}\ \bar{g} = d$	definition
	$\mid$	$\varphi\ e$	assertion
	$\mid$	$\uparrow\ e$	barrier

```
factorial (n: int) (return (m: int)) =

  loop 1 n
  / loop (r: int) (k: int) =

      if (k > 0) (→ loop (r * k) (k - 1))
                 (→ return r)
```

```
factorial (n: int) (return (m: int)) =
  { n ⩾ 0 }
  loop 1 n
  / loop (r: int) (k: int) =
      { 0 ⩽ k ⩽ n ∧ r · k! = n! }
      if (k > 0) (→ loop (r * k) (k - 1))
                 (→ { r = n! } return r)
```

piecewise specification

```
removeRoot (t: tree) (return (s: tree)) =
  unTree t ((l: tree) (_: elt) (r: tree) →
             mergeTree l r ((s: tree) →
               { ∀e:elt. e ∈ s ↔ e ∈ l ∨ e ∈ r }
               return s))
           fail
```

$$\mathcal{C}(\varphi\ \mathsf{e}) \triangleq \varphi \wedge (\varphi \rightarrow \mathcal{C}(\mathsf{e}))$$

VC(Coma)

$$\mathcal{C}(k\ \bar{s}\ \bar{o}) \triangleq \mathcal{C}(k)\ \ \bar{s}\ \ \mathcal{C}(o_1)\ \cdots\ \mathcal{C}(o_n)$$

$$\mathcal{C}(\varphi\ e) \triangleq \varphi \wedge (\varphi \rightarrow \mathcal{C}(e))$$

VC(COMA)

$$\mathcal{C}(h) \triangleq h$$

$$\mathcal{C}(\bar{x}\,\bar{g} \to e) \triangleq \lambda \bar{x}\bar{g}.\, \mathcal{C}(e)$$

$$\mathcal{C}(k\;\bar{s}\;\bar{o}) \triangleq \mathcal{C}(k)\;\;\bar{s}\;\;\mathcal{C}(o_1)\;\cdots\;\mathcal{C}(o_n)$$

$$\mathcal{C}(\varphi\; e) \triangleq \varphi \wedge (\varphi \longrightarrow \mathcal{C}(e))$$

$$\begin{aligned}
\mathcal{C}(h) &\triangleq h \\
\mathcal{C}(\bar{x}\,\bar{g} \rightarrow e) &\triangleq \lambda \bar{x}\bar{g}.\,\mathcal{C}(e) \\
\mathcal{C}(k\;\bar{s}\;\bar{o}) &\triangleq \mathcal{C}(k)\;\;\bar{s}\;\;\mathcal{C}(o_1)\;\cdots\;\mathcal{C}(o_n)
\end{aligned}$$

$$\mathcal{C}(\varphi\; e) \triangleq \varphi \wedge (\varphi \longrightarrow \mathcal{C}(e))$$

$$\texttt{halt} \triangleq \top \qquad\qquad \texttt{fail} \triangleq \bot$$

$$\begin{aligned}
\texttt{if} &\triangleq \lambda \texttt{cfg}.\,(\texttt{c} \longrightarrow \texttt{f}) \wedge (\neg\texttt{c} \longrightarrow \texttt{g}) \\
\texttt{unTree} &\triangleq \lambda \texttt{tfg}.\,(\forall \texttt{lvr}.\,\texttt{t} = \mathit{Node}\;\texttt{l}\;\texttt{v}\;\texttt{r} \longrightarrow \texttt{f}\;\texttt{l}\;\texttt{v}\;\texttt{r}) \wedge \\
&\qquad (\texttt{t} = \mathit{Leaf} \longrightarrow \texttt{g})
\end{aligned}$$

$$\mathcal{C}(h) \triangleq h$$

$$\mathcal{C}(\bar{x}\,\bar{g} \to e) \triangleq \lambda \bar{x}\bar{g}.\,\mathcal{C}(e)$$

$$\mathcal{C}(k\ \bar{s}\ \bar{o}) \triangleq \mathcal{C}(k)\ \ \bar{s}\ \ \mathcal{C}(o_1)\ \cdots\ \mathcal{C}(o_n)$$

$$\mathcal{C}(e\ /\ h\ \bar{x}\ \bar{g} = d) \triangleq (\lambda h.\,\mathcal{C}(e))\,(\lambda \bar{x}\bar{g}.\,\mathcal{C}(d))$$

$$\mathcal{C}(\varphi\ e) \triangleq \varphi \wedge (\varphi \longrightarrow \mathcal{C}(e))$$

$$\texttt{halt} \triangleq \top \qquad\qquad \texttt{fail} \triangleq \bot$$

$$\texttt{if} \triangleq \lambda \texttt{cfg}.\,(\texttt{c} \longrightarrow \texttt{f}) \wedge (\neg\texttt{c} \longrightarrow \texttt{g})$$

$$\texttt{unTree} \triangleq \lambda \texttt{tfg}.\,(\forall \texttt{lvr}.\,\texttt{t} = \textit{Node}\,\texttt{l v r} \longrightarrow \texttt{f l v r}) \wedge (\texttt{t} = \textit{Leaf} \longrightarrow \texttt{g})$$

VC(Coma)

$$\mathcal{C}(h) \triangleq h$$

$$\mathcal{C}(\bar{x}\,\bar{g} \to e) \triangleq \lambda \bar{x}\bar{g}.\,\mathcal{C}(e)$$

$$\mathcal{C}(k\ \bar{s}\ \bar{o}) \triangleq \mathcal{C}(k)\ \ \bar{s}\ \ \mathcal{C}(o_1)\ \cdots\ \mathcal{C}(o_n)$$

$$\mathcal{C}(e\ /\ h\ \bar{x}\ \bar{g} = d) \triangleq \texttt{let}\ h\ \bar{x}\ \bar{g}\ =\ \mathcal{C}(d)\ \texttt{in}\ \mathcal{C}(e)$$

$$\mathcal{C}(\varphi\ e) \triangleq \varphi \land (\varphi \to \mathcal{C}(e))$$

$$\texttt{halt} \triangleq \top \qquad\qquad \texttt{fail} \triangleq \bot$$

$$\texttt{if} \triangleq \lambda \texttt{cfg}.\,(\texttt{c} \longrightarrow \texttt{f}) \land (\neg\texttt{c} \longrightarrow \texttt{g})$$

$$\texttt{unTree} \triangleq \lambda \texttt{tfg}.\,(\forall \texttt{lvr}.\,\texttt{t} = \mathit{Node}\ \texttt{l}\ \texttt{v}\ \texttt{r} \longrightarrow \texttt{f}\ \texttt{l}\ \texttt{v}\ \texttt{r}) \land (\texttt{t} = \mathit{Leaf} \longrightarrow \texttt{g})$$

VC(Coma)

$$\mathcal{C}(h) \triangleq h$$

$$\mathcal{C}(\bar{x}\,\bar{g} \to e) \triangleq \lambda \bar{x}\bar{g}.\,\mathcal{C}(e)$$

$$\mathcal{C}(k\;\bar{s}\;\bar{o}) \triangleq \mathcal{C}(k)\;\;\bar{s}\;\;\mathcal{C}(o_1)\;\cdots\;\mathcal{C}(o_n)$$

$$\mathcal{C}(e \;/\; h\;\bar{x}\;\bar{g} = d) \triangleq \mathtt{let}\;h\;\bar{x}\;\bar{g} = \mathcal{C}(d)\;\mathtt{in}\;\mathcal{C}(e)$$

$$\mathcal{C}(\varphi\;e) \triangleq \varphi \wedge (\varphi \longrightarrow \mathcal{C}(e))$$

$$\mathcal{C}(\uparrow e) \triangleq \mathcal{C}(e)$$

$$\mathtt{halt} \triangleq \top \qquad\qquad \mathtt{fail} \triangleq \bot$$

$$\mathtt{if} \triangleq \lambda \mathtt{cfg}.\,(\mathtt{c} \longrightarrow \mathtt{f}) \wedge (\neg\mathtt{c} \longrightarrow \mathtt{g})$$

$$\mathtt{unTree} \triangleq \lambda \mathtt{tfg}.\,(\forall \mathtt{lvr}.\,\mathtt{t} = \mathit{Node}\;\mathtt{l}\;\mathtt{v}\;\mathtt{r} \longrightarrow \mathtt{f}\;\mathtt{l}\;\mathtt{v}\;\mathtt{r}) \wedge (\mathtt{t} = \mathit{Leaf} \longrightarrow \mathtt{g})$$

$$\mathcal{C}(h) \triangleq h$$

$$\mathcal{C}(\bar{x}\,\bar{g} \to e) \triangleq \lambda \bar{x}\bar{g}.\, \mathcal{C}(e)$$

$$\mathcal{C}(k\ \bar{s}\ \bar{o}) \triangleq \mathcal{C}(k)\ \ \bar{s}\ \ \mathcal{C}(o_1)\ \cdots\ \mathcal{C}(o_n)$$

$$\mathcal{C}(e\ /\ h\ \bar{x}\ \bar{g} = d) \triangleq \texttt{let}\ h\ \bar{x}\ \bar{g}\ =\ \mathcal{E}(d)\ \texttt{in}\ \mathcal{C}(e) \land \forall \bar{x}\bar{g}.\, \mathcal{D}(d)$$

$$\mathcal{C}(\varphi\ e) \triangleq \varphi \land (\varphi \longrightarrow \mathcal{C}(e))$$

$$\mathcal{C}(\uparrow e) \triangleq \mathcal{C}(e)$$

$$\texttt{halt} \triangleq \top \qquad\qquad \texttt{fail} \triangleq \bot$$

$$\texttt{if} \triangleq \lambda \texttt{cfg}.\, (\texttt{c} \longrightarrow \texttt{f}) \land (\neg \texttt{c} \longrightarrow \texttt{g})$$

$$\texttt{unTree} \triangleq \lambda \texttt{tfg}.\, (\forall \texttt{lvr}.\, \texttt{t} = \mathit{Node}\ \texttt{l}\ \texttt{v}\ \texttt{r} \longrightarrow \texttt{f}\ \texttt{l}\ \texttt{v}\ \texttt{r}) \land (\texttt{t} = \mathit{Leaf} \longrightarrow \texttt{g})$$

```
factorial (n: int) (return (m: int)) =
  { n ⩾ 0 }
  ↑ loop 1 n
    / loop (r: int) (k: int) =
        { 0 ⩽ k ⩽ n ∧ r · k! = n! }
        ↑ if (k > 0) (→ loop (r * k) (k - 1))
                     (→ break r)
  / break (m: int) = { m = n! } ↑ return m
```

```
factorial (n: int) (return (m: int)) =
  { n ⩾ 0 }



  / break (m: int) = { m = n! } ↑ return m
```

```
factorial (n: int) (return (m: int)) =
  { n ⩾ 0 }

    ↑ loop 1 n
      / loop (r: int) (k: int) =
          { 0 ⩽ k ⩽ n ∧ r · k! = n! }
          ↑ if (k > 0) (→ loop (r * k) (k - 1))
                       (→ break r)

  / break (m: int) = { m = n! } ↑ return m
```

$$\mathcal{E}(\varphi\ \mathsf{e}) \triangleq \varphi \land (\varphi \longrightarrow \mathcal{E}(\mathsf{e}))$$

$$\frac{\text{application-side}}{\text{definition-side}}$$

$$\mathcal{D}(\varphi\ \mathsf{e}) \triangleq \varphi \longrightarrow \mathcal{D}(\mathsf{e})$$

$$\mathcal{E}(e \mathbin{/} h\ \bar{x}\ \bar{g} = d) \triangleq \texttt{let}\ h\ \bar{x}\ \bar{g} = \mathcal{E}(d)\ \texttt{in}\ \mathcal{E}(e) \land \forall \bar{x}\bar{g}.\, \mathcal{D}(d)$$

$$\mathcal{E}(\varphi\ e) \triangleq \varphi \land (\varphi \rightarrow \mathcal{E}(e))$$

$$\frac{\text{application-side}}{\text{definition-side}}$$

$$\mathcal{D}(e \mathbin{/} h\ \bar{x}\ \bar{g} = d) \triangleq \texttt{let}\ h\ \bar{x}\ \bar{g} = \mathcal{E}(d)\ \texttt{in}\ \mathcal{D}(e)$$

$$\mathcal{D}(\varphi\ e) \triangleq \varphi \rightarrow \mathcal{D}(e)$$

$$\begin{aligned}
\mathcal{E}(e\ /\ h\ \bar{x}\ \bar{g} = d) &\triangleq \texttt{let}\ h\ \bar{x}\ \bar{g} = \mathcal{E}(d)\ \texttt{in}\ \mathcal{E}(e) \land \forall \bar{x}\bar{g}.\, \mathcal{D}(d) \\
\mathcal{E}(\varphi\ e) &\triangleq \varphi \land (\varphi \longrightarrow \mathcal{E}(e)) \\
\mathcal{E}(\uparrow e) &\triangleq \top
\end{aligned}$$

application-side

definition-side

$$\begin{aligned}
\mathcal{D}(e\ /\ h\ \bar{x}\ \bar{g} = d) &\triangleq \texttt{let}\ h\ \bar{x}\ \bar{g} = \mathcal{E}(d)\ \texttt{in}\ \mathcal{D}(e) \\
\mathcal{D}(\varphi\ e) &\triangleq \varphi \longrightarrow \mathcal{D}(e) \\
\mathcal{D}(\uparrow e) &\triangleq \mathcal{C}(e)
\end{aligned}$$

$$\mathcal{E}(k\ \bar{s}\ \bar{o}) \triangleq \mathcal{E}(k)\ \ \bar{s}\ \ \mathcal{E}(o_1)\ \cdots\ \mathcal{E}(o_n)$$

$$\mathcal{E}(e\ /\ h\ \bar{x}\ \bar{g} = d) \triangleq \texttt{let}\ h\ \bar{x}\ \bar{g}\ = \mathcal{E}(d)\ \texttt{in}\ \mathcal{E}(e) \wedge \forall \bar{x}\bar{g}.\, \mathcal{D}(d)$$

$$\mathcal{E}(\varphi\ e) \triangleq \varphi \wedge (\varphi \longrightarrow \mathcal{E}(e))$$

$$\mathcal{E}(\uparrow e) \triangleq \top$$

application-side

---

definition-side

$$\mathcal{D}(k\ \bar{s}\ \bar{o}) \triangleq \mathcal{D}(k)\ \ \bar{s}\ \ \mathcal{D}(o_1)\ \cdots\ \mathcal{D}(o_n)$$

$$\mathcal{D}(e\ /\ h\ \bar{x}\ \bar{g} = d) \triangleq \texttt{let}\ h\ \bar{x}\ \bar{g}\ = \mathcal{E}(d)\ \texttt{in}\ \mathcal{D}(e)$$

$$\mathcal{D}(\varphi\ e) \triangleq \varphi \longrightarrow \mathcal{D}(e)$$

$$\mathcal{D}(\uparrow e) \triangleq \mathcal{C}(e)$$

$$\mathcal{E}(h) \triangleq h$$

$$\mathcal{E}(k\ \bar{s}\ \bar{o}) \triangleq \mathcal{E}(k)\ \ \bar{s}\ \ \mathcal{E}(o_1)\ \cdots\ \mathcal{E}(o_n)$$

$$\mathcal{E}(e\ /\ h\ \bar{x}\ \bar{g} = d) \triangleq \texttt{let}\ h\ \bar{x}\ \bar{g}\ = \mathcal{E}(d)\ \texttt{in}\ \mathcal{E}(e) \land \forall \bar{x}\bar{g}.\, \mathcal{D}(d)$$

$$\mathcal{E}(\varphi\ e) \triangleq \varphi \land (\varphi \longrightarrow \mathcal{E}(e))$$

$$\mathcal{E}(\uparrow e) \triangleq \top$$

application-side

---

definition-side

$$\mathcal{D}(h) \triangleq \natural h$$

$$\mathcal{D}(k\ \bar{s}\ \bar{o}) \triangleq \mathcal{D}(k)\ \ \bar{s}\ \ \mathcal{D}(o_1)\ \cdots\ \mathcal{D}(o_n)$$

$$\mathcal{D}(e\ /\ h\ \bar{x}\ \bar{g} = d) \triangleq \texttt{let}\ h\ \bar{x}\ \bar{g}\ = \mathcal{E}(d)\ \texttt{in}\ \mathcal{D}(e)$$

$$\mathcal{D}(\varphi\ e) \triangleq \varphi \longrightarrow \mathcal{D}(e)$$

$$\mathcal{D}(\uparrow e) \triangleq \mathcal{C}(e)$$

VC(CoMa)

$$
\begin{aligned}
\mathcal{E}(h) &\triangleq h \\
\mathcal{E}(\bar{x}\,\bar{g} \to e) &\triangleq \lambda \bar{x}\bar{g}.\, \mathcal{E}(e) \\
\mathcal{E}(k\,\bar{s}\,\bar{o}) &\triangleq \mathcal{E}(k)\ \bar{s}\ \mathcal{E}(o_1)\ \cdots\ \mathcal{E}(o_n) \\
\mathcal{E}(e\ /\ h\,\bar{x}\,\bar{g} = d) &\triangleq \texttt{let}\ h\,\bar{x}\,\bar{g} = \mathcal{E}(d)\ \texttt{in}\ \mathcal{E}(e) \land \forall \bar{x}\bar{g}.\, \mathcal{D}(d) \\
\mathcal{E}(\varphi\ e) &\triangleq \varphi \land (\varphi \longrightarrow \mathcal{E}(e)) \\
\mathcal{E}(\uparrow e) &\triangleq \top
\end{aligned}
$$

application-side

---

definition-side

$$
\begin{aligned}
\mathcal{D}(h) &\triangleq \natural h \\
\mathcal{D}(\bar{x}\,\bar{g} \to e) &\triangleq \lambda \bar{x}\bar{g}.\, \mathcal{D}(e) \\
\mathcal{D}(k\,\bar{s}\,\bar{o}) &\triangleq \mathcal{D}(k)\ \bar{s}\ \mathcal{D}(o_1)\ \cdots\ \mathcal{D}(o_n) \\
\mathcal{D}(e\ /\ h\,\bar{x}\,\bar{g} = d) &\triangleq \texttt{let}\ h\,\bar{x}\,\bar{g} = \mathcal{E}(d)\ \texttt{in}\ \mathcal{D}(e) \\
\mathcal{D}(\varphi\ e) &\triangleq \varphi \longrightarrow \mathcal{D}(e) \\
\mathcal{D}(\uparrow e) &\triangleq \mathcal{C}(e)
\end{aligned}
$$

VC(Coma)

$$
\begin{aligned}
\mathcal{E}(h) &\triangleq h \\
\mathcal{E}(\bar{x}\,\bar{g} \to e) &\triangleq (\lambda\bar{x}\bar{g}.\,\mathcal{E}(e)) \wedge (\ \lambda\bar{x}\bar{g}.\,\mathcal{D}(e)) \\
\mathcal{E}(k\,\bar{s}\,\bar{o}) &\triangleq \mathcal{E}(k)\ \ \bar{s}\ \ \mathcal{E}(o_1)\ \cdots\ \mathcal{E}(o_n) \\
\mathcal{E}(e\ /\ h\ \bar{x}\ \bar{g} = d) &\triangleq \texttt{let}\ h\ \bar{x}\ \bar{g}\ = \mathcal{E}(d)\ \texttt{in}\ \mathcal{E}(e) \wedge \forall\bar{x}\bar{g}.\,\mathcal{D}(d) \\
\mathcal{E}(\varphi\ e) &\triangleq \varphi \wedge (\varphi \longrightarrow \mathcal{E}(e)) \\
\mathcal{E}(\uparrow e) &\triangleq \top
\end{aligned}
$$

application-side

---

definition-side

$$
\begin{aligned}
\mathcal{D}(h) &\triangleq \natural h \\
\mathcal{D}(\bar{x}\,\bar{g} \to e) &\triangleq (\lambda\bar{x}\bar{g}.\,\mathcal{D}(e)) \wedge (\ \lambda\bar{x}\bar{g}.\,\mathcal{E}(e)) \\
\mathcal{D}(k\,\bar{s}\,\bar{o}) &\triangleq \mathcal{D}(k)\ \ \bar{s}\ \ \mathcal{D}(o_1)\ \cdots\ \mathcal{D}(o_n) \\
\mathcal{D}(e\ /\ h\ \bar{x}\ \bar{g} = d) &\triangleq \texttt{let}\ h\ \bar{x}\ \bar{g}\ = \mathcal{E}(d)\ \texttt{in}\ \mathcal{D}(e) \\
\mathcal{D}(\varphi\ e) &\triangleq \varphi \longrightarrow \mathcal{D}(e) \\
\mathcal{D}(\uparrow e) &\triangleq \mathcal{C}(e)
\end{aligned}
$$

VC(COMA)

$$\mathcal{E}(h) \triangleq h$$

$$\mathcal{E}(\bar{x}\,\bar{g} \to e) \triangleq (\lambda\bar{x}\bar{g}.\,\mathcal{E}(e)) \land (\natural\lambda\bar{x}\bar{g}.\,\mathcal{D}(e))$$

$$\mathcal{E}(k\,\bar{s}\,\bar{o}) \triangleq \mathcal{E}(k)\;\;\bar{s}\;\;\mathcal{E}(o_1)\;\cdots\;\mathcal{E}(o_n)$$

$$\mathcal{E}(e\;/\;h\;\bar{x}\;\bar{g} = d) \triangleq \texttt{let}\;h\;\bar{x}\;\bar{g}\;=\mathcal{E}(d)\;\texttt{in}\;\mathcal{E}(e) \land \forall\bar{x}\bar{g}.\,\mathcal{D}(d)$$

$$\mathcal{E}(\varphi\;e) \triangleq \varphi \land (\varphi \longrightarrow \mathcal{E}(e))$$

$$\mathcal{E}(\uparrow e) \triangleq \top$$

application-side

---

definition-side

$$\mathcal{D}(h) \triangleq \natural h$$

$$\mathcal{D}(\bar{x}\,\bar{g} \to e) \triangleq (\lambda\bar{x}\bar{g}.\,\mathcal{D}(e)) \land (\natural\lambda\bar{x}\bar{g}.\,\mathcal{E}(e))$$

$$\mathcal{D}(k\,\bar{s}\,\bar{o}) \triangleq \mathcal{D}(k)\;\;\bar{s}\;\;\mathcal{D}(o_1)\;\cdots\;\mathcal{D}(o_n)$$

$$\mathcal{D}(e\;/\;h\;\bar{x}\;\bar{g} = d) \triangleq \texttt{let}\;h\;\bar{x}\;\bar{g}\;=\mathcal{E}(d)\;\texttt{in}\;\mathcal{D}(e)$$

$$\mathcal{D}(\varphi\;e) \triangleq \varphi \longrightarrow \mathcal{D}(e)$$

$$\mathcal{D}(\uparrow e) \triangleq \mathcal{C}(e)$$

piecewise specification

```
removeRoot (t: tree) (return (s: tree)) =
  unTree t ((l: tree) (_: elt) (r: tree) →
                 ↑ mergeTree l r out
                 / out (s: tree) =
                     { ∀e:elt. e ∈ s ↔ e ∈ l ∨ e ∈ r }
                     ↑ return s)
          fail
```

$\mathcal{E}$: $\lambda \mathtt{tk}. (\forall \mathtt{lvr}. \mathtt{t} = \mathit{Node}\ \mathtt{l}\ \mathtt{v}\ \mathtt{r} \rightarrow$
$\forall \mathtt{s}. (\forall \mathtt{e}.\ \mathtt{e} \in \mathtt{s} \leftrightarrow \mathtt{e} \in \mathtt{l} \vee \mathtt{e} \in \mathtt{r}) \rightarrow \mathtt{k}\ \mathtt{s}) \wedge \mathtt{t} \neq \mathit{Leaf}$

$\mathcal{D}$: $\forall \mathtt{t}. \forall \mathtt{lvr}. \mathtt{t} = \mathit{Node}\ \mathtt{l}\ \mathtt{v}\ \mathtt{r} \rightarrow$
$\mathtt{mergeTree}\ \mathtt{l}\ \mathtt{r}\ (\lambda \mathtt{s}. \forall \mathtt{e}.\ \mathtt{e} \in \mathtt{s} \leftrightarrow \mathtt{e} \in \mathtt{l} \vee \mathtt{e} \in \mathtt{r})$

or none at all

```
removeRoot (t: tree) (return (s: tree)) =
  unTree t ((l: tree) (_: elt) (r: tree) →
             mergeTree l r return)
           fail
```

$\mathcal{E}: \quad \lambda \mathtt{tk}. (\forall \mathtt{lvr}. \mathtt{t} = \mathit{Node}\ \mathtt{l}\ \mathtt{v}\ \mathtt{r} \longrightarrow \mathtt{mergeTree}\ \mathtt{l}\ \mathtt{r}\ \mathtt{k}) \wedge \mathtt{t} \neq \mathit{Leaf}$

Fin

$$\langle \Sigma, M\,N \rangle \circ \ell \;\triangleq\; \langle \Sigma, M \rangle \circ \langle \Sigma, N \rangle, \ell$$

$$\langle \Sigma, M\,N \rangle \circ \ell \;\triangleq\; \langle \Sigma, M \rangle \circ \langle \Sigma, N \rangle, \ell$$

$$\langle \Sigma, \lambda h.\, M \rangle \circ \langle \Delta, N \rangle, \ell \;\triangleq\; \langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], M \rangle \circ \ell$$

$$\langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], h \rangle \circ \ell \triangleq \langle \Delta, N \rangle \circ \ell$$

$$\langle \Sigma, M\, N \rangle \circ \ell \triangleq \langle \Sigma, M \rangle \circ \langle \Sigma, N \rangle, \ell$$

$$\langle \Sigma, \lambda h.\, M \rangle \circ \langle \Delta, N \rangle, \ell \triangleq \langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], M \rangle \circ \ell$$

$$\begin{aligned}
\langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], h \rangle \circ \ell &\triangleq \langle \Delta, N \rangle \circ \ell \\
\langle \Sigma, M\, s \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ s, \ell \\
\langle \Sigma, M\, N \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ \langle \Sigma, N \rangle, \ell \\
\langle \Sigma, \lambda x. M \rangle \circ s, \ell &\triangleq \langle \Sigma, M[x \mapsto s] \rangle \circ \ell \\
\langle \Sigma, \lambda h. M \rangle \circ \langle \Delta, N \rangle, \ell &\triangleq \langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], M \rangle \circ \ell
\end{aligned}$$

verification conditions

$$
\begin{aligned}
\langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], h \rangle \circ \ell &\triangleq \langle \Delta, N \rangle \circ \ell \\
\langle \Sigma, M\, s \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ s, \ell \\
\langle \Sigma, M\, N \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ \langle \Sigma, N \rangle, \ell \\
\langle \Sigma, \lambda x.\, M \rangle \circ s, \ell &\triangleq \langle \Sigma, M[x \mapsto s] \rangle \circ \ell \\
\langle \Sigma, \lambda h.\, M \rangle \circ \langle \Delta, N \rangle, \ell &\triangleq \langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], M \rangle \circ \ell \\
\langle \Sigma, M \wedge N \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ \ell \;\wedge\; \langle \Sigma, N \rangle \circ \ell
\end{aligned}
$$

$$
\begin{aligned}
\langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], h \rangle \circ \ell &\triangleq \langle \Delta, N \rangle \circ \ell \\
\langle \Sigma, M\, s \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ s, \ell \\
\langle \Sigma, M\, N \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ \langle \Sigma, N \rangle, \ell \\
\langle \Sigma, \lambda x. M \rangle \circ s, \ell &\triangleq \langle \Sigma, M[x \mapsto s] \rangle \circ \ell \\
\langle \Sigma, \lambda h. M \rangle \circ \langle \Delta, N \rangle, \ell &\triangleq \langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], M \rangle \circ \ell \\
\langle \Sigma, M \wedge N \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ \ell \ \wedge \ \langle \Sigma, N \rangle \circ \ell \\
\langle \Sigma, \varphi \rangle \circ \varepsilon &\triangleq \varphi
\end{aligned}
$$

$$
\begin{aligned}
\langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], h \rangle \circ \ell &\triangleq \langle \Delta, N \rangle \circ \ell \\
\langle \Sigma, M\, s \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ s, \ell \\
\langle \Sigma, M\, N \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ \langle \Sigma, N \rangle, \ell \\
\langle \Sigma, \lambda x. M \rangle \circ s, \ell &\triangleq \langle \Sigma, M[x \mapsto s] \rangle \circ \ell \\
\langle \Sigma, \lambda h. M \rangle \circ \langle \Delta, N \rangle, \ell &\triangleq \langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], M \rangle \circ \ell \\
\langle \Sigma, M \wedge N \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ \ell \; \wedge \; \langle \Sigma, N \rangle \circ \ell \\
\langle \Sigma, \varphi \rangle \circ \varepsilon &\triangleq \varphi \\
\langle \Sigma, \varphi \to M \rangle \circ \varepsilon &\triangleq \varphi \to \langle \Sigma, M \rangle \circ \varepsilon
\end{aligned}
$$

$$
\begin{aligned}
\langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], h \rangle \circ \ell &\triangleq \langle \Delta, N \rangle \circ \ell \\
\langle \Sigma, M\, s \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ s, \ell \\
\langle \Sigma, M\, N \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ \langle \Sigma, N \rangle, \ell \\
\langle \Sigma, \lambda x.\, M \rangle \circ s, \ell &\triangleq \langle \Sigma, M[x \mapsto s] \rangle \circ \ell \\
\langle \Sigma, \lambda h.\, M \rangle \circ \langle \Delta, N \rangle, \ell &\triangleq \langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], M \rangle \circ \ell \\
\langle \Sigma, M \wedge N \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ \ell \;\wedge\; \langle \Sigma, N \rangle \circ \ell \\
\langle \Sigma, \varphi \rangle \circ \varepsilon &\triangleq \varphi \\
\langle \Sigma, \varphi \rightarrow M \rangle \circ \varepsilon &\triangleq \varphi \rightarrow \langle \Sigma, M \rangle \circ \varepsilon \\
\langle \Sigma, \forall x.\, M \rangle \circ \varepsilon &\triangleq \forall x.\, \langle \Sigma, M \rangle \circ \varepsilon
\end{aligned}
$$

$$
\begin{aligned}
\langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], h \rangle \circ \ell &\triangleq \langle \Delta, N \rangle \circ \ell \\
\langle \Sigma, M\, s \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ s, \ell \\
\langle \Sigma, M\, N \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ \langle \Sigma, N \rangle, \ell \\
\langle \Sigma, \lambda x. M \rangle \circ s, \ell &\triangleq \langle \Sigma, M[x \mapsto s] \rangle \circ \ell \\
\langle \Sigma, \lambda h. M \rangle \circ \langle \Delta, N \rangle, \ell &\triangleq \langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], M \rangle \circ \ell \\
\langle \Sigma, M \wedge N \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ \ell \;\wedge\; \langle \Sigma, N \rangle \circ \ell \\
\langle \Sigma, \varphi \rangle \circ \varepsilon &\triangleq \varphi \\
\langle \Sigma, \varphi \to M \rangle \circ \varepsilon &\triangleq \varphi \to \langle \Sigma, M \rangle \circ \varepsilon \\
\langle \Sigma, \forall x. M \rangle \circ \varepsilon &\triangleq \forall x.\, \langle \Sigma, M \rangle \circ \varepsilon
\end{aligned}
$$

$$
\forall h. M \triangleq \texttt{let}\ h\ \bar{x}\ \bar{f} = \bot \wedge \left(\bigwedge_{f} \forall \bar{z}\bar{g}. f\ \bar{z}\ \bar{g} \right)\ \texttt{in}\ M
$$

$$
\begin{aligned}
\langle \Sigma, \natural M \rangle_n \circ \ell &\triangleq \langle \Sigma, M \rangle_{n+1} \circ \ell \\
\langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], h \rangle \circ \ell &\triangleq \langle \Delta, N \rangle \circ \ell \\
\langle \Sigma, M\, s \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ s, \ell \\
\langle \Sigma, M\, N \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ \langle \Sigma, N \rangle, \ell \\
\langle \Sigma, \lambda x.\, M \rangle \circ s, \ell &\triangleq \langle \Sigma, M[x \mapsto s] \rangle \circ \ell \\
\langle \Sigma, \lambda h.\, M \rangle \circ \langle \Delta, N \rangle, \ell &\triangleq \langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], M \rangle \circ \ell \\
\langle \Sigma, M \wedge N \rangle \circ \ell &\triangleq \langle \Sigma, M \rangle \circ \ell \;\wedge\; \langle \Sigma, N \rangle \circ \ell \\
\langle \Sigma, \varphi \rangle \circ \varepsilon &\triangleq \varphi \\
\langle \Sigma, \varphi \rightarrow M \rangle \circ \varepsilon &\triangleq \varphi \rightarrow \langle \Sigma, M \rangle \circ \varepsilon \\
\langle \Sigma, \forall x.\, M \rangle \circ \varepsilon &\triangleq \forall x.\, \langle \Sigma, M \rangle \circ \varepsilon
\end{aligned}
$$

$$
\forall h.M \triangleq \texttt{let}\ h\ \bar{x}\ \bar{f} = \bot \wedge \left(\bigwedge_{f} \forall \bar{z}\bar{g}.\, f\ \bar{z}\ \bar{g} \right)\ \texttt{in}\ M
$$

$$\langle \Sigma, \natural M \rangle_n \circ \ell \triangleq \langle \Sigma, M \rangle_{n+1} \circ \ell$$

$$\langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], h \rangle \circ \ell \triangleq \langle \Delta, N \rangle \circ \ell$$

$$\langle \Sigma, M\, s \rangle \circ \ell \triangleq \langle \Sigma, M \rangle \circ s, \ell$$

$$\langle \Sigma, M\, N \rangle \circ \ell \triangleq \langle \Sigma, M \rangle \circ \langle \Sigma, N \rangle, \ell$$

$$\langle \Sigma, \lambda x. M \rangle \circ s, \ell \triangleq \langle \Sigma, M[x \mapsto s] \rangle \circ \ell$$

$$\langle \Sigma, \lambda h. M \rangle \circ \langle \Delta, N \rangle, \ell \triangleq \langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], M \rangle \circ \ell$$

$$\langle \Sigma, M \wedge N \rangle \circ \ell \triangleq \langle \Sigma, M \rangle \circ \ell \;\wedge\; \langle \Sigma, N \rangle \circ \ell$$

$$\langle \Sigma, \varphi \rangle_0 \circ \varepsilon \triangleq \varphi \qquad \langle \Sigma, \varphi \rangle_{n+1} \circ \varepsilon \triangleq \top$$

$$\langle \Sigma, \varphi \rightarrow M \rangle \circ \varepsilon \triangleq \varphi \rightarrow \langle \Sigma, M \rangle \circ \varepsilon$$

$$\langle \Sigma, \forall x. M \rangle \circ \varepsilon \triangleq \forall x.\, \langle \Sigma, M \rangle \circ \varepsilon$$

$$\forall h. M \triangleq \texttt{let}\ h\ \bar{x}\ \bar{f} = \bot \wedge \left(\bigwedge_f \forall \bar{z}\bar{g}. f\ \bar{z}\ \bar{g} \right) \texttt{in}\ M$$

$$\langle \Sigma, \natural M \rangle_n \circ \ell \triangleq \langle \Sigma, M \rangle_{n+1} \circ \ell$$

$$\langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle_n], h \rangle_m \circ \ell \triangleq \langle \Delta, N \rangle_{n+m} \circ \ell$$

$$\langle \Sigma, M\, s \rangle \circ \ell \triangleq \langle \Sigma, M \rangle \circ s, \ell$$

$$\langle \Sigma, M\, N \rangle \circ \ell \triangleq \langle \Sigma, M \rangle \circ \langle \Sigma, N \rangle, \ell$$

$$\langle \Sigma, \lambda x. M \rangle \circ s, \ell \triangleq \langle \Sigma, M[x \mapsto s] \rangle \circ \ell$$

$$\langle \Sigma, \lambda h. M \rangle \circ \langle \Delta, N \rangle, \ell \triangleq \langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle], M \rangle \circ \ell$$

$$\langle \Sigma, M \wedge N \rangle \circ \ell \triangleq \langle \Sigma, M \rangle \circ \ell \;\wedge\; \langle \Sigma, N \rangle \circ \ell$$

$$\langle \Sigma, \varphi \rangle_0 \circ \varepsilon \triangleq \varphi \qquad \langle \Sigma, \varphi \rangle_{n+1} \circ \varepsilon \triangleq \top$$

$$\langle \Sigma, \varphi \to M \rangle \circ \varepsilon \triangleq \varphi \to \langle \Sigma, M \rangle \circ \varepsilon$$

$$\langle \Sigma, \forall x. M \rangle \circ \varepsilon \triangleq \forall x.\, \langle \Sigma, M \rangle \circ \varepsilon$$

$$\forall h. M \triangleq \texttt{let}\ h\ \bar{x}\ \bar{f} = \bot \wedge \left(\bigwedge_f \forall \bar{z} \bar{g}. f\ \bar{z}\ \bar{g} \right)\ \texttt{in}\ M$$

$$\langle \Sigma, \natural M \rangle_n \circ \ell \triangleq \langle \Sigma, M \rangle_{n+1} \circ \ell$$

$$\langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle_n], h \rangle_m \circ \ell \triangleq \langle \Delta, N \rangle_{n+m} \circ \ell$$

$$\langle \Sigma, M\, s \rangle \circ \ell \triangleq \langle \Sigma, M \rangle \circ s, \ell$$

$$\langle \Sigma, M\, N \rangle \circ \ell \triangleq \langle \Sigma, M \rangle \circ \langle \Sigma, N \rangle, \ell$$

$$\langle \Sigma, \lambda x. M \rangle \circ s, \ell \triangleq \langle \Sigma, M[x \mapsto s] \rangle \circ \ell$$

$$\langle \Sigma, \lambda h. M \rangle_m \circ \langle \Delta, N \rangle_n, \ell \triangleq \langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle_{n-m}], M \rangle_m \circ \ell$$

$$\langle \Sigma, M \wedge N \rangle \circ \ell \triangleq \langle \Sigma, M \rangle \circ \ell \wedge \langle \Sigma, N \rangle \circ \ell$$

$$\langle \Sigma, \varphi \rangle_0 \circ \varepsilon \triangleq \varphi \qquad \langle \Sigma, \varphi \rangle_{n+1} \circ \varepsilon \triangleq \top$$

$$\langle \Sigma, \varphi \to M \rangle \circ \varepsilon \triangleq \varphi \to \langle \Sigma, M \rangle \circ \varepsilon$$

$$\langle \Sigma, \forall x. M \rangle \circ \varepsilon \triangleq \forall x. \langle \Sigma, M \rangle \circ \varepsilon$$

$$\forall h. M \triangleq \texttt{let}\ h\ \bar{x}\ \bar{f} = \bot \wedge \left(\bigwedge_f \forall \bar{z} \bar{g}. f\ \bar{z}\ \bar{g} \right)\ \texttt{in}\ M$$

$$
\begin{aligned}
\langle \Sigma, \natural M \rangle_n \circ \ell &\triangleq \langle \Sigma, M \rangle_{n+1} \circ \ell \\
\langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle_n], h \rangle_m \circ \ell &\triangleq \langle \Delta, N \rangle_{n+m} \circ \ell \\
\langle \Sigma, M\, s \rangle_n \circ \ell &\triangleq \langle \Sigma, M \rangle_n \circ s, \ell \\
\langle \Sigma, M\, N \rangle_n \circ \ell &\triangleq \langle \Sigma, M \rangle_n \circ \langle \Sigma, N \rangle_n, \ell \\
\langle \Sigma, \lambda x. M \rangle_n \circ s, \ell &\triangleq \langle \Sigma, M[x \mapsto s] \rangle_n \circ \ell \\
\langle \Sigma, \lambda h. M \rangle_m \circ \langle \Delta, N \rangle_n, \ell &\triangleq \langle \Sigma \uplus [h \mapsto \langle \Delta, N \rangle_{n-m}], M \rangle_m \circ \ell \\
\langle \Sigma, M \wedge N \rangle_n \circ \ell &\triangleq \langle \Sigma, M \rangle_n \circ \ell \;\wedge\; \langle \Sigma, N \rangle_n \circ \ell \\
\langle \Sigma, \varphi \rangle_0 \circ \varepsilon \triangleq \varphi \qquad & \langle \Sigma, \varphi \rangle_{n+1} \circ \varepsilon \triangleq \top \\
\langle \Sigma, \varphi \rightarrow M \rangle_n \circ \varepsilon &\triangleq \varphi \rightarrow \langle \Sigma, M \rangle_n \circ \varepsilon \\
\langle \Sigma, \forall x. M \rangle_n \circ \varepsilon &\triangleq \forall x.\, \langle \Sigma, M \rangle_n \circ \varepsilon
\end{aligned}
$$

$$
\forall h. M \triangleq \texttt{let}\ h\ \bar{x}\ \bar{f} = \bot \wedge \left(\bigwedge_f \forall \bar{z} \bar{g}. f\ \bar{z}\ \bar{g} \right)\ \texttt{in}\ M
$$

On-the-fly factorization of selected handlers:

$$(\forall x.\, \varphi \rightarrow h\ s) \wedge (\forall y.\, \psi \rightarrow h\ t) \quad \Longrightarrow$$
$$\forall z.\, ((\exists x.\, \varphi \wedge z = s) \vee (\exists y.\, \psi \wedge z = t)) \rightarrow h\ z$$

- no factorized handlers $\approx$ traditional WP
- factorize all eligible handlers $\approx$ compact VC à la Flanagan & Saxe

```
factorial (n: int) (return (m: int)) =
  { n ⩾ 0 }
  allocate int 1 ((&r: int) →
    ↑ allocate int n ((&k: int) →
        loop
        / loop [r k] =
            { 0 ⩽ k ⩽ n ∧ r · k! = n! }
            ↑ if (k > 0) (→ assign int &r (r * k)
                           (→ assign int &k (k - 1)
                             (→ loop)))
                         (→ break))
    / break [r] = { r = n! } ↑ return r)
```

```
allocate α (v: α) (return (&r: α) { r = v })
assign α (&r: α) (v: α) (return [r] { r = v })
```

No-alias type system:

$$\frac{\Gamma, \Delta' \vdash e \text{ wt} \qquad \Delta' \textit{ is } \Delta \textit{ with all handler prototypes removed}}{\Gamma, \&r, \Delta \vdash (e\ \&r) \text{ wt}}$$

- can be further refined by tracking actual reference dependencies

Effect computation — to verify and infer the pre-write annotations

Transformation into an equivalent pure program:

```
assign &r (r * k)                    assign r (r * k)
  (→ assign &k (k - 1)      ⇒          (r′ → assign k (k - 1)
    (→ loop))                             (k′ → loop r′ k′))
```

- pre-writes are converted into term parameters
- fine-grained state monad: send only the relevant part of the state

(cont.)

Further into control structures: iterators, coroutines, unstructured code?

Further into mutable state: ownership, borrowing, prophecy variables?

Scalable implementation, good heuristics for subgoal factorization

Nice surface syntax, extensive case studies, integration into WHY3