Pilsner: A Compositionally Verified Compiler for a Higher-Order Imperative Language
Technical Appendix

Georg Neis Chung-Kil Hur
Jan-Oliver Kaiser Craig McLaughlin Derek Dreyer Viktor Vafeiadis

February 28, 2015

Contents

1 Notice

The following sections contain detailed definitions of languages and models as well as statements of key theorems. Given the amount of symbols, it is possible that there are typos or other mistakes here. If in doubt, please consult the Coq code. Many parts are annotated with the identifiers and file names of the corresponding Coq definitions.

2 Differences From the Paper

The paper omits many definitions that are shown here (*e.g.,* module similarity itself). The paper also shows several definitions in a simplified form, which are shown in its full form here. In particular:

- A local world can depend on the global world (see WorldL).
- A local world can give a relational interpretation to type names (see MN). Like in PBs, this is used for reasoning about parametric polymorphism.
- Worlds feature the distinction between public and private state transitions. This also affects the definition of **E**.
- **E** includes the validity assumption (see **U**).
- **E** contains machinery to enable the reasoning principles discussed in Section 6 in the paper. The main pieces are:
  - **E** carries around a flag (σ) indicating whether configure cares about the world being currently satisfied.
  - **E** is indexed by an order and an element i of that order to allow stuttering.

3 Abstract Language and Concrete Instances

(In **lang_common.v**)

$$t \in \text{Evt} ::= \epsilon \mid ?n \mid !n \qquad\qquad F_1, F_2, \ldots \in \text{Lbl}$$

3.1 Language Specification

(**Lang_Spec** in **lang_spec.v**)

Domains: $\mathbf{Val}, \mathbf{Cont}, \mathbf{Conf}, \mathbf{Mach}, \mathbf{Mod}, \mathbf{Anch}$

Operators and relations:

- vload $\in \mathbf{Mod} \to \mathbf{Anch} \to (\mathrm{Lbl} \times \mathbf{Val})^* \to \mathrm{Lbl} \to \mathcal{P}(\mathbf{Val})$
- cload $\in \mathbf{Mod} \to \mathbf{Anch} \to (\mathrm{Lbl} \times \mathbf{Val})^* \to \mathcal{P}(\mathbf{Conf}^2)$
- $\cdot \in \mathbf{Conf} \to \mathbf{Conf} \to \mathbf{Conf}$
- $\emptyset \in \mathbf{Conf}$
- $\hookrightarrow \in \mathcal{P}(\mathrm{Evt} \times \mathbf{Mach} \times \mathbf{Mach})$
- real $\in \mathbf{Conf} \to \mathcal{P}(\mathbf{Mach})$
- extra $\in \mathcal{P}(\mathbf{Conf})$
- core $\in \mathcal{P}(\mathbf{Conf})$
- halted $:= \{m \in \mathbf{Mach} \mid \nexists t, m'.\ m \overset{t}{\hookrightarrow} m'\}$
- error $:= \{m \in \mathbf{Mach} \mid \forall c.\ m \notin \mathrm{real}(c)\}$

Properties:

- $\mathbf{Conf}$ forms commutative monoid with $\cdot$ and $\emptyset$.
- $\forall t, m, m'.\ m \overset{t}{\hookrightarrow} m' \land m' \notin \mathrm{error} \implies m \notin \mathrm{error}$
- $\forall t, m, m'.\ m \notin \mathrm{error} \land m \overset{t}{\hookrightarrow} m' \land m' \in \mathrm{error} \implies t = \epsilon$
- $\emptyset \in \mathrm{extra}$
- $\forall c, c' \in \mathrm{extra}.\ c \cdot c' \in \mathrm{extra}$
- $\forall c.\ \exists m.\ \forall c' \in \mathrm{extra}.\ \forall m' \in \mathrm{real}(c \cdot c').\ m \in \mathrm{real}(c)$
- $\forall c_1, c_2, c_1', c_2', m.\ c_1 \in \mathrm{core} \land c_2 \in \mathrm{core} \land m \in \mathrm{real}(c_1 \cdot c_1') \cap \mathrm{real}(c_2 \cdot c_2') \implies c_1 = c_2 \land c_1' = c_2'$
- $\forall m, c, m'.\ m' \in m \cdot c \land c \in \mathrm{extra} \land m' \in \mathrm{halted} \implies m \in \mathrm{halted}$

3.2 Source Language

(Semantics in lang_src.v, language specification in lang_src_lsi.v, types in types.v)

$$\tau ::= \nu \mid \alpha \mid \mathsf{unit} \mid \mathsf{nat} \mid \tau_1 \to \tau_2 \mid \tau_1 \times \tau_2 \mid \tau_1 + \tau_2 \mid \mu\alpha.\,\tau \mid \forall\alpha.\,\tau \mid \exists\alpha.\,\tau \mid \mathsf{ref}\;\tau$$

$$e ::= x \mid \langle\rangle \mid n \mid \mathsf{input} \mid \mathsf{output}\;e \mid \mathsf{fix}\,f(x).\,e \mid e_1\;e_2 \mid \langle e_1, e_2\rangle \mid e.1 \mid e.2 \mid \mathsf{inl}\;e \mid \mathsf{inr}\;e \mid \mathsf{case}\,e\,(x.\,e_1)\,(x.\,e_2) \mid \mathsf{roll}\;e \mid \mathsf{unroll}\;e \mid F \mid e_1 \circ e_2 \mid \mathsf{ifnz}\;e\;\mathsf{then}\;e_1\;\mathsf{else}\;e_2 \mid \Lambda.\,e \mid e[] \mid \mathsf{pack}\;e \mid \mathsf{unpack}\;e_1\;\mathsf{as}\;x\;\mathsf{in}\;e_2 \mid l \mid \mathsf{ref}\;e \mid !e \mid e_1 := e_2 \mid e_1 == e_2$$

$$v ::= \langle\rangle \mid n \mid \mathsf{fix}\,f(x).\,e \mid \langle v_1, v_2\rangle \mid \mathsf{inl}\;v \mid \mathsf{inr}\;v \mid \mathsf{roll}\;v \mid \Lambda.e \mid \mathsf{pack}\;v \mid l$$

$$\begin{array}{lll}
\mathbf{Val} & := & \{v \mid \mathrm{FV}(v) = \emptyset\} \\
\mathbf{Mod} \ni M & ::= & [F_1{=}v_1, \ldots, F_n{=}v_n] \\
\mathbf{Anch} & := & 1 \\
\mathbf{Cont} \ni K & ::= & \bullet \mid K\;e \mid v\;K \mid \ldots \\
\mathrm{Env} & := & \mathrm{Lbl} \rightharpoonup \mathbf{Val} \\
\mathrm{Heap} & := & (\mathrm{Loc} \rightharpoonup \mathbf{Val})_\bot \\
\mathbf{Mach} & := & \mathrm{Heap} \times \mathrm{Env} \times \mathrm{Exp} \\
\mathbf{Conf} & := & \mathrm{Heap} \times \mathrm{Env}_{\bot,\emptyset} \times \mathrm{Exp}_{\bot,\emptyset} \\
 & & \text{where } X_{\bot,\emptyset} = X \mathbin{\dot\cup} \{\emptyset, \bot\}
\end{array}$$

$$\emptyset := (\emptyset, \emptyset, \emptyset) \qquad (h, \sigma, e) \cdot (h', \sigma', e') := (h \cdot h', \sigma \cdot \sigma', e \cdot e')$$

$$\mathrm{cload}(M)(\_)(\sigma) := \{(c, \emptyset) \mid \exists\sigma'.\; c = (\emptyset, (\sigma, M, \sigma'), \emptyset)\}$$
$$\mathrm{vload}(M)(\_)(\_)(F) := \{v \mid (F, v) \in M\}$$

$$\mathrm{real}(c) := \{m \mid m = c \wedge m.\mathrm{hp} \neq \bot \wedge m.\mathrm{hp}\text{ finite}\}$$
$$\mathrm{core} := \{(\emptyset, \emptyset, e)\}$$
$$\mathrm{extra} := \{(h, \emptyset, \emptyset)\}$$
$$\mathrm{halted} := \{(\_, v) \mid v \in \mathbf{Val}\}$$

$$\begin{array}{rcll}
(h, \sigma, K[F]) & \hookrightarrow & (h, \sigma, K[v]) & (\text{if } \sigma(F) = v) \\
(h, \sigma, K[\mathsf{input}]) & \overset{?n}{\hookrightarrow} & (h, \sigma, K[n]) & \\
(h, \sigma, K[\mathsf{output}\;n]) & \overset{!n}{\hookrightarrow} & (h, \sigma, K[\langle\rangle]) & \\
(h, \sigma, K[v\;v']) & \hookrightarrow & (h, \sigma, K[e[v'/x][v/f]]) & (\text{if } v = \mathsf{fix}\,f(x).\,e) \\
(h, \sigma, K[\mathsf{ref}\;v]) & \hookrightarrow & (h{\cdot}\{l{\mapsto}v\}, \sigma, K[l]) & (\text{if } h{\cdot}\{l{\mapsto}v\} \neq \bot) \\
 & \ldots & & \\
(h, \sigma, e) & \hookrightarrow & (\bot, \sigma, e) & (\text{if } e \neq v \text{ and no other rule applicable})
\end{array}$$

$\boxed{\Gamma \vdash e : \tau}$ $\boxed{\Gamma \vdash M : \Gamma'}$ $\boxed{M_1 \bowtie M_2}$ $\boxed{\mathrm{Behav}(M)}$

3.3 Intermediate Language

(Semantics and language specification in **lang_mid.v**)

$$
\begin{array}{lll}
a & ::= & \langle\rangle \mid n \mid \langle x_1, x_2\rangle \mid x.1 \mid x.2 \mid \mathsf{inl}\, x \mid \mathsf{inr}\, x \mid \\
 & & \mathsf{fix}\, f(y,k).\, e \mid \Lambda k.\, e \mid x_1 == x_2 \mid x_1 \circ x_2 \\
e & ::= & \mathsf{let}\ y = a\ \mathsf{in}\ e \mid \mathsf{let}\ k\ y = e_1\ \mathsf{in}\ e_2 \mid y \leftarrow \mathsf{input};\ e \mid \\
 & & \mathsf{output}\ x;\ e \mid y \leftarrow \mathsf{ref}\ x;\ e \mid x_1 := x_2;\ e \mid y \leftarrow !x;\ e \mid \\
 & & \mathsf{ifnz}\ x\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 \mid \mathsf{case}\, x\, (y.\ e_1)\, (y.\ e_2) \mid \\
 & & x_1\ x_2\ k \mid x[]\ k \mid k\ x
\end{array}
$$

$$
\begin{array}{lll}
\mathbf{Val} \ni v & := & \langle\rangle \mid n \mid l \mid \langle v_1, v_2\rangle \mid \mathsf{inl}\, v \mid \mathsf{inr}\, v \mid \\
 & & \langle \sigma, \mathsf{fix}\, f(y,k).e\rangle \mid \langle \sigma, \lambda y.e\rangle \\
\mathrm{Loc} \ni l & := & l_1 \ldots l_n \\
\mathbf{Mod} \ni M & := & [F_1{=}e_1, \ldots, F_n{=}e_n] \\
\mathbf{Anch} & := & 1 \\
\mathbf{Cont} & := & \mathbf{Val} \\
\mathrm{Env} & := & \mathrm{Lbl} \uplus \mathrm{TVar} \uplus \mathrm{KVar} \rightharpoonup \mathbf{Val} \\
\mathrm{Heap} & := & (\mathrm{Loc} \rightharpoonup \mathbf{Val})_\bot \\
\mathbf{Mach} & := & \mathrm{Heap} \times (\mathrm{Env} \times \mathrm{Exp}) \\
\mathbf{Conf} & := & \mathrm{Heap} \times (\mathrm{Env} \times \mathrm{Exp})_{\bot,\emptyset}
\end{array}
$$

$\emptyset := (\emptyset, \emptyset) \qquad (h, ee) \cdot (h', ee') := (h \cdot h', ee \cdot ee')$

$$
\begin{array}{l}
\mathrm{cload}(M)(\_)(\_) := \{((\emptyset,\emptyset),(\emptyset,\emptyset))\} \\
\mathrm{vload}(M)(\mathrm{imports})(\_)(F) := \{\langle \mathrm{imports} +\!\!+ [F_1 = e_1, \ldots, F_{m-1} = e_{m-1}], e\rangle \\
\qquad\qquad \mid M = [F_1 = e_1, \ldots, F_{m-1} = e_{m-1}, F = e, \ldots] \land \\
\qquad\qquad\ \ F \notin \{F_1, \ldots, F_{m-1}\}\} \\
\quad \text{where } [a_1, \ldots, a_m] +\!\!+ [b_1, \ldots, b_n] := [a_1, \ldots, a_m, b_1, \ldots, b_n]
\end{array}
$$

$\mathrm{real}(c) := \{m \mid m = c \land c.\mathrm{hp} \neq \bot \land c.\mathrm{hp}\ \mathrm{finite}\}$

$\mathrm{core} := \{(\_, (\sigma, e))\}$

$\mathrm{extra} := \{(\_, \emptyset)\}$

$\mathrm{halted} := \{(h, (\_, n))\}$

$$
\begin{aligned}
(h, (\sigma, \mathsf{let}\ x = y\ \mathsf{in}\ e_1)) &\hookrightarrow (h, (\sigma[x \mapsto \sigma(y)], e_1)) \\
(h, (\sigma, \mathsf{let}\ k\ y = e_1\ \mathsf{in}\ e_2)) &\hookrightarrow (h, (\sigma[k \mapsto \langle \sigma, \lambda y. e_1 \rangle], e_2)) \\
(h, (\sigma, y \leftarrow \mathsf{input};\ e)) &\overset{?n}{\hookrightarrow} (h, (\sigma[y \mapsto n], e)) \\
(h, (\sigma, \mathsf{output}\ y;\ e)) &\overset{!n}{\hookrightarrow} (h, (\sigma, e)) \\
(h, (\sigma, \mathsf{ifnz}\ x\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2)) &\hookrightarrow (h, (\sigma, e_1)) && (\text{if } \sigma(x) \neq 0) \\
(h, (\sigma, \mathsf{ifnz}\ x\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2)) &\hookrightarrow (h, (\sigma, e_2)) && (\text{if } \sigma(x) = 0) \\
(h, (\sigma, \mathsf{case}\, x\ (y.\ e_1)\ (y.\ e_2))) &\hookrightarrow (h, (\sigma[y \mapsto v], e_1)) && (\text{if } \sigma(x) = \mathsf{inl}\ v) \\
(h, (\sigma, \mathsf{case}\, x\ (y.\ e_1)\ (y.\ e_2))) &\hookrightarrow (h, (\sigma[y \mapsto v], e_2)) && (\text{if } \sigma(x) = \mathsf{inr}\ v) \\
(h, (\sigma, k\ x)) &\hookrightarrow (h, (\sigma'[y \mapsto \sigma(x)], e)) \\
& && (\text{if } \sigma(k) = \langle \sigma', \lambda y. e \rangle) \\
(h, (\sigma, x_1\ x_2\ k)) &\hookrightarrow (h, (\sigma'[f, y, k' \mapsto \sigma(x_1), \sigma(x_2), \sigma(k)], e)) \\
& && (\text{if } \sigma(x_1) = \langle \sigma', \mathsf{fix}\, f(y, k').\ e \rangle) \\
(h, (\sigma, x[]\ k)) &\hookrightarrow (h, (\sigma[y \mapsto \sigma(k)], e)) \\
& && (\text{if } \sigma(x) = \langle \sigma', \Lambda y.\ e \rangle) \\
&\dots \\
(h, (\sigma, e)) &\hookrightarrow (\bot, (\sigma, e)) && (\text{if no other rule applicable})
\end{aligned}
$$

3.4 Target Language

(Semantics and language specification in lang_tgt.v)

$$
\begin{array}{lll}
\text{Reg} \ni r & ::= & \mathsf{sp} \mid \mathsf{clo} \mid \mathsf{arg} \mid \mathsf{env} \mid \mathsf{ret} \mid \mathsf{aux} \mid \mathsf{i} \\
\text{Oper} \ni o & ::= & n \mid r \mid \langle r \pm n \rangle \mid [r \pm n] \\
\text{Instr} \ni z & ::= & \mathsf{jmp}\ o \mid \mathsf{jnz}\ r\ o \mid \mathsf{ld}\ r\ o \mid \mathsf{sto}\ o\ r \mid \mathsf{lpc}\ r \mid \\
 & & \mathsf{bop}\ \circ\ r\ o_1\ o_2 \mid \mathsf{input}\ r \mid \mathsf{output}\ r \mid \mathsf{alloc}\ r_1\ r_2 \\
 & & \\
\textbf{Val} & := & \text{Word} \\
\textbf{Anch} \ni a & := & \text{Word} \\
\text{Seg} \ni \text{seg} & ::= & (n, n_1 \ldots n_k) \\
\textbf{Mod} \ni M(n, [a_1, \ldots, a_k]) & ::= & [F_1 = \text{seg}_1, \ldots, F_m = \text{seg}_m] \\
\textbf{Cont} & := & \text{Word} \\
\text{RegFile} & := & \text{Reg} \to \text{Word} \\
\text{Stack} & := & (\text{Word} \rightharpoonup \text{Word})_\bot \\
\text{Heap} & := & (\text{Word} \rightharpoonup \text{Word})_\bot \\
\textbf{Mach} & := & \text{Heap}_\bot \times \text{Stack} \times \text{RegFile} \times \text{Word} \\
 & & \text{where Heap}_\bot = \text{Heap} \,\dot{\cup} \{\bot\} \\
\textbf{Conf} & := & \text{Heap} \times \text{Stack} \times \text{RegFile}_{\bot,\emptyset} \times \text{Word}_{\bot,\emptyset}
\end{array}
$$

$\emptyset := (\emptyset, \emptyset, \emptyset, \emptyset) \qquad (h, st, R, n) \cdot (h, st, R, n) := (h \cdot h', st \cdot st', R \cdot R', n \cdot n')$

$\text{vload}(M)(n)([F_1 = \text{seg}_1, \ldots, F_1 = \text{seg}_n])(F) := \{v \mid (F, (v, \_)) \in M(n)([\text{seg}_1, \ldots, \text{seg}_n])\}$

$\text{real}(c) := \{m \mid m = c \wedge c.\text{hp} \neq \bot \wedge c.\text{hp finite} \wedge c.\text{st} \neq \bot\}$

$$
\begin{aligned}
\text{eval}((\text{h}, \text{st}, \text{R}, \text{pc})) := {} & \{(n, n)\} \ \cup \ \{(r, R(r))\} \ \cup \\
& \{(\langle r \pm n \rangle, n) \mid st(R(r) \pm n) = w\} \ \cup \\
& \{(\langle r \pm n \rangle, n) \mid h(R(r) \pm n) = w\}
\end{aligned}
$$

For $m = (h, st, R, \text{pc})$ with $\text{pc} > 0$ we define:

$$
\begin{array}{ll}
m \hookrightarrow (h, st, R, \text{pc}') & (\text{if } h(\text{pc}) = \mathsf{jmp}\ o \wedge (o, \text{pc}') \in \text{eval(m)}) \\
m \hookrightarrow (h, st, R, \text{pc} + 1) & (\text{if } h(\text{pc}) = \mathsf{jnz}\ r\ o \wedge R(r) = 0) \\
m \hookrightarrow (h, st, R, \text{pc}') & \\
 & (\text{if } h(\text{pc}) = \mathsf{jnz}\ r\ o \wedge R(r) \neq 0 \wedge (o, \text{pc}') \in \text{eval(m)}) \\
m \hookrightarrow (h, st, R[r \mapsto n], \text{pc} + 1) & (\text{if } h(\text{pc}) = \mathsf{ld}\ r\ o \wedge (o, n) \in \text{eval(m)}) \\
m \hookrightarrow (h, st, R[r' \mapsto R(r)], \text{pc} + 1) & (\text{if } h(\text{pc}) = \mathsf{sto}\ r'\ r) \\
m \hookrightarrow (h, st[n' \pm n \mapsto R(r)], R, \text{pc} + 1) & \\
 & (\text{if } h(\text{pc}) = \mathsf{sto}\ \langle r' \pm n \rangle\ r \wedge (\langle r' \pm n \rangle, n') \in \text{eval(m)}) \\
m \hookrightarrow (h[n' \pm n \mapsto R(r)], st, R, \text{pc} + 1) & \\
 & (\text{if } h(\text{pc}) = \mathsf{sto}\ [r' \pm n]\ r \wedge (\langle r' \pm n \rangle, n') \in \text{eval(m)}) \\
m \hookrightarrow (h, st, R[r \mapsto \text{pc}], \text{pc} + 1) & (\text{if } h(\text{pc}) = \mathsf{lpc}\ r) \\
m \hookrightarrow (h, st, R[r \mapsto n_1 \circ n_2], \text{pc} + 1) & \\
 & (\text{if } h(\text{pc}) = \mathsf{bop}\ \circ\ r\ o_1\ o_2 \wedge (o_1, n_1) \in \text{eval(m)} \wedge (o_2, n_2) \in \text{eval(m)}) \\
m \overset{?n}{\hookrightarrow} (h, st, R[r \mapsto n], \text{pc} + 1) & (\text{if } h(\text{pc}) = \mathsf{input}\ r) \\
m \overset{!R(r)}{\hookrightarrow} (h, st, R, \text{pc} + 1) & (\text{if } h(\text{pc}) = \mathsf{output}\ r) \\
m \hookrightarrow (\bot, m_2, m_3, m_4) & (\text{if no other rule applicable})
\end{array}
$$

4 Generic Model and Concrete Instances

(**model_common.v**, unless specified otherwise)

$$T \in \mathrm{TrSys} := \{(\mathsf{S}, \sqsupseteq_{\mathrm{pub}}, \sqsupseteq) \in \mathrm{Set} \times \mathcal{P}(\mathsf{S} \times \mathsf{S}) \times \mathcal{P}(\mathsf{S} \times \mathsf{S}) \mid \sqsupseteq_{\mathrm{pub}}, \sqsupseteq \text{ pre-orders} \wedge \sqsupseteq_{\mathrm{pub}} \subseteq \sqsupseteq\}$$ **transys**

$$\mathrm{TyName} := \{\nu_1, \nu_2, \ldots\}$$
$$\mathrm{TypeF} := \{\tau \to \tau' \in \mathrm{Type}, \nu \in \mathrm{Type}, \forall \tau. \in \mathrm{Type}\}$$ **model.flextyp**
$$\mathrm{VRelF}_{A,B} := \mathrm{TypeF} \to \mathcal{P}(A.\mathbf{Val} \times B.\mathbf{Val})$$ **model.vrelf**
$$\mathrm{VRel}_{A,B} := \mathrm{Type} \to \mathcal{P}(A.\mathbf{Val} \times B.\mathbf{Val})$$ **model.vrel**
$$\mathrm{KRel}_{A,B} := \mathrm{Type} \to \mathrm{Type} \to \mathcal{P}(A.\mathbf{Cont} \times B.\mathbf{Cont})$$ **model.krel**

$$\mathsf{VQry}_L := \mathsf{unit} \mid \mathsf{nat}\, n \mid \mathsf{pair}\, v\, v' \mid \mathsf{inl}\, v \mid \mathsf{inr}\, v \mid \mathsf{roll}\, v \mid \mathsf{fun} \mid \mathsf{goodfun} \mid \mathsf{goodgen} \mid \mathsf{pack}\, v \mid \mathsf{name}$$ **vquery**
$$\mathsf{CQry}_L := \mathsf{app}\, v\, v'\, k \mid \mathsf{ret}\, v\, k \mid \mathsf{inst}\, v\, k \quad (\text{where } v, v' \in L.\mathbf{Val} \text{ and } k \in L.\mathbf{Cont})$$ **cquery**

$$\begin{aligned}\mathrm{QH}^T_{A,B} := \{(&\mathsf{rqh} \in T.\mathsf{S} \xrightarrow{\text{mon}} \mathrm{VRel}_{A,B} \\ ,&\mathsf{vqha} \in T.\mathsf{S} \xrightarrow{\text{mon}} \mathsf{VQry}_A \to \mathcal{P}(A.\mathbf{Val}) \\ ,&\mathsf{vqhb} \in T.\mathsf{S} \xrightarrow{\text{mon}} \mathsf{VQry}_B \to \mathcal{P}(B.\mathbf{Val}) \\ ,&\mathsf{cqha} \in T.\mathsf{S} \to \mathsf{CQry}_A \to \mathcal{P}(A.\mathbf{Conf}) \\ ,&\mathsf{cqhb} \in T.\mathsf{S} \to \mathsf{CQry}_B \to \mathcal{P}(B.\mathbf{Conf})) \\ \mid& \forall s, U.\ \mathsf{cqha}(s)(U) \subseteq A.\mathrm{core} \wedge \mathsf{cqhb}(s)(U) \subseteq B.\mathrm{core}\}\end{aligned}$$ **model.method_query**

$$\mathrm{CR}^T_{A,B} := \{\mathsf{crel} \in (T.\mathsf{S} \to \mathrm{VRelF}_{A,B}) \xrightarrow{\text{mon}} T.\mathsf{S} \to \mathcal{P}(A.\mathbf{Conf} \times B.\mathbf{Conf})\}$$ **model.method_conf**

$$\begin{aligned}\mathrm{MN}^T_{A,B} := \{(&\mathsf{supp} \in \mathcal{P}(\mathrm{TyName}) \\ ,&\mathsf{name} \in (T.\mathsf{S} \to \mathrm{VRelF}_{A,B}) \xrightarrow{\text{mon}} T.\mathsf{S} \to \mathrm{TyName} \to \mathcal{P}(A.\mathbf{Val} \times B.\mathbf{Val})) \\ \mid& \forall U, s.\ \forall (\nu, \_, \_) \in \mathsf{name}(U)(s).\ \nu \in \mathsf{supp}\}\end{aligned}$$ **model.method_name**

We define algebraic, well-founded orders as follows

$$\begin{aligned}\mathrm{awfo} := \{(O, <, 0, 1, +) \in \mathrm{Set} \times O \times O \times ((O \times O) \to O) \\ \mid (< \text{ well-founded on } O) \wedge \\ (\forall i.\ 0 + i = i) \wedge (\forall i.\ i + 0 = i) \wedge \\ (\forall i, j.\ i + j = j + i) \wedge \\ (\forall i.\ 0 < i) \wedge \\ (\forall i, i', j.\ i < i' \implies i + j \le i' + j) \wedge \\ (\forall i, j, j'.\ j < j' \implies i + j \le i + j') \wedge \\ (0 \ne 1)\}\end{aligned}$$ **gwfo.awfo**

$$\mathrm{World}_{A,B} := \{(T \in \mathrm{TrSys}, \_ \in \mathrm{CR}^T_{A,B}, \_ \in \mathrm{QH}^T_{A,B}, \_ \in \mathrm{awfo}, \_ \in \mathrm{MN}^T_{A,B})\}$$ **world**
$$\mathrm{WorldG}_{A,B} := \{(T \in \mathrm{TrSys}, \_ \in \mathrm{CR}^T_{A,B}, \_ \in \mathrm{QH}^T_{A,B})\}$$ **world_glob**

For $W \in \mathrm{WorldG}_{A,B}$ we define

$$\mathrm{WorldL}_{A,B}(W) := \{(T \in \mathrm{TrSys}, \_ \in \mathrm{CR}^{W.T \times T}_{A,B}, \_ \in \mathrm{awfo}, \_ \in \mathrm{MN}^{W.T \times T}_{A,B})\}$$ **world_loca**

$$R_1 \star R_2 := \{(c^a_1 \cdot c^a_2, c^b_1 \cdot c^b_2) \mid (c^a_1, c^b_1) \in R_1 \wedge (c^a_2, c^b_2) \in R_2\}$$

$$\begin{aligned}w{\uparrow}.T &:= W.T \times w.T \qquad (\text{where } w \in \mathrm{WorldL}_{A,B}(W)) \\ w{\uparrow}.\mathsf{crel}(U)(s_g, s) &:= W.\mathsf{crel}(U(-, s))(s_g) \star w.\mathsf{crel}(U)(s_g, s) \\ w{\uparrow}.\mathsf{vqha}(s_g, \_) &:= W.\mathsf{vqha}(s_g) \qquad \textit{(analogously for the rest)} \\ w{\uparrow}.\mathsf{supp} &:= w.\mathsf{supp} \\ w{\uparrow}.\mathsf{name} &:= w.\mathsf{name}\end{aligned}$$ **wlift**

4.1 Global Worlds

(In gw_common.v)

$$
\begin{aligned}
T^{A,B}_{\text{ref}} := \{(s \in \mathcal{P}(\text{Type} \times \text{Loc} \times \text{Loc}), \sqsupseteq, \sqsupseteq) \mid \\
& s \text{ finite } \wedge \\
& (\forall \tau, \tau', v_a, v_a', v_b, v_b'.\ (\tau, v_a, v_b) \in s \wedge (\tau',, v_a', v_b') \in s \implies \\
& \quad (v_a' = v_a \implies \tau' = \tau \wedge v_b' = v_b) \\
& \wedge\ (v_b' = v_b \implies \tau' = \tau \wedge v_a' = v_a)\}
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{crel}^{\mathbf{T},\mathbf{S}}_{\text{ref}}(U)(s) := \{((\emptyset, \emptyset, \emptyset, h_{\mathbf{T}}), (h_{\mathbf{S}}, \emptyset, \emptyset)) \mid \\
& h_{\mathbf{T}} \neq \bot \wedge h_{\mathbf{S}} \neq \bot \wedge \\
& \text{dom}(h_{\mathbf{T}}) = \{l_{\mathbf{T}} \mid \exists \tau, l_{\mathbf{S}}.\ (\tau, l_{\mathbf{T}}, l_{\mathbf{S}}) \in s.\text{refdb}\} \wedge \\
& \text{dom}(h_{\mathbf{S}}) = \{l_{\mathbf{S}} \mid \exists \tau, l_{\mathbf{T}}.\ (\tau, l_{\mathbf{T}}, l_{\mathbf{S}}) \in s.\text{refdb}\} \wedge \\
& \forall (\tau, l_{\mathbf{T}}, l_{\mathbf{S}}) \in s.\text{refdb}.\ (\tau, h_{\mathbf{T}}(l_{\mathbf{T}}), h_{\mathbf{S}}(l_{\mathbf{T}})) \in \langle\!\langle U(s) \rangle\!\rangle^s\}
\end{aligned}
$$

(analogously for the other pairs of languages)

$$
\begin{aligned}
&W^{A,B}.T := T^A \times T^{A,B}_{\text{ref}} \times T^B && W^{A,B}.\mathsf{rqh} := \mathsf{rqh} \\
&W^{A,B}.\mathsf{vqha} := \mathsf{vqh}^A && W^{A,B}.\mathsf{vqhb} := \mathsf{vqh}^B \\
&W^{A,B}.\mathsf{cqha} := \mathsf{cqh}^A && W^{A,B}.\mathsf{cqhb} := \mathsf{cqh}^B \\
&W^{A,B}.\mathsf{crel}(U)(s) := (\mathsf{cpred}^A(s^A) \times \mathsf{cpred}^B(s^B)) \star \mathsf{crel}^{A,B}_{\text{ref}}(U)(s)
\end{aligned}
$$

$$
T^{\mathbf{S}}.\mathsf{S} := \text{Lbl} \rightharpoonup \mathbf{Val_S} \qquad T^{\mathbf{S}}.\sqsupseteq := T^{\mathbf{S}}.\sqsupseteq_{\text{pub}} := \{(s, s)\}
$$

$$
T^{\mathbf{I}}.\mathsf{S} := 1
$$

$$
\begin{aligned}
&\text{query}_{\mathbf{T}} := \{\mathsf{pair}_{\mathbf{T}}\, v\, v'\} \cup \{\mathsf{inl}_{\mathbf{T}}\, v\} \cup \{\mathsf{inr}_{\mathbf{T}}\, v\} \cup \{\mathsf{fun}_{\mathbf{T}}\, v\} \\
&\text{ValDb} := \text{query}_{\mathbf{T}} \to \mathcal{P}(\mathbf{T}.\mathbf{Val})
\end{aligned}
$$

$$
\begin{aligned}
&T^{\mathbf{T}}.\mathsf{S} := \text{RegFile} \times \text{ValDb} \qquad T^{\mathbf{T}}.\sqsupseteq := \{(s', s) \mid s'.2 \supseteq s.2\} \\
&T^{\mathbf{T}}.\sqsupseteq_{\text{pub}} := \{(s', s) \in T^{\mathbf{T}}.\sqsupseteq \mid \forall r \in \{\mathsf{sp}, \mathsf{env}\}.\ s'.1(r) = s.1(r)\}
\end{aligned}
$$

$$
\begin{aligned}
&\mathsf{cpred}^{\mathbf{S}}(s) := (\emptyset, s, \bot) \\
&\mathsf{cpred}^{\mathbf{I}}(s) := (\emptyset, \bot)
\end{aligned}
$$

$$
\begin{aligned}
&\text{repr} \in \text{Heap} \to \mathcal{P}(\text{query}_{\mathbf{T}} \times \text{Word}) \\
&\text{repr}(h) := \{(\mathsf{pair}_{\mathbf{T}}\, v\, v', n) \mid h(n) = v \wedge h(n+1) = v'\} \cup \\
&\qquad \{(\mathsf{inl}_{\mathbf{T}}\, v, n) \mid h(n) = 0 \wedge h(n+1) = v\} \cup \\
&\qquad \{(\mathsf{inr}_{\mathbf{T}}\, v, n) \mid \exists n'.\ n' \neq 0 \wedge h(n) = n' \wedge h(n+1) = v\} \cup \\
&\qquad \{(\mathsf{fun}_{\mathbf{T}}\, v, n) \mid h(n) = v\}
\end{aligned}
$$

$$
\begin{aligned}
\mathsf{cpred}^{\mathbf{T}}((R, \text{valdb})) := \{(h, st, R, \bot) \mid & (\forall n.\ n >= R(\mathsf{sp}) \iff \exists v, st(a) = v) \\
& \wedge (\forall q, v.\ v \in \text{valdb}(q) \implies (q, v) \in \text{repr}(h))\}
\end{aligned}
$$

$$
\begin{array}{ll}
\mathsf{vqh}_{\mathbf{S}}(\_)(\mathsf{pair}\, v\, v') := \{\langle v, v'\rangle\} & \mathsf{vqh}_{\mathbf{I}}(\_)(\mathsf{pair}\, v\, v') := \{\langle v, v'\rangle\} \\
\mathsf{vqh}_{\mathbf{S}}(\_)(\mathsf{roll}\, v) := \{\mathsf{roll}\ v\} & \mathsf{vqh}_{\mathbf{I}}(\_)(\mathsf{roll}\, v) := \{v\} \\
\mathsf{vqh}_{\mathbf{S}}(\_)(\mathsf{fun}) := \{\mathsf{fix}\, f(x).\, e\} & \mathsf{vqh}_{\mathbf{I}}(\_)(\mathsf{fun}) := \{\langle \sigma, \mathsf{fix}\, f(y,k).\, e\rangle\} \\
\mathsf{vqh}_{\mathbf{S}}(\_)(\mathsf{unit}) := \{\langle\rangle\} & \mathsf{vqh}_{\mathbf{I}}(\_)(\mathsf{unit}) := \{\langle\rangle\} \\
\mathsf{vqh}_{\mathbf{S}}(\_)(\mathsf{nat}\, n) := \{n\} & \mathsf{vqh}_{\mathbf{I}}(\_)(\mathsf{nat}\, n) := \{n\} \\
\mathsf{vqh}_{\mathbf{S}}(\_)(\mathsf{inl}\, v) := \{\mathsf{inl}\ v\} & \mathsf{vqh}_{\mathbf{I}}(\_)(\mathsf{inl}\, v) := \{\mathsf{inl}\ v\} \\
\mathsf{vqh}_{\mathbf{S}}(\_)(\mathsf{inr}\, v) := \{\mathsf{inr}\ v\} & \mathsf{vqh}_{\mathbf{I}}(\_)(\mathsf{inr}\, v) := \{\mathsf{inr}\ v\} \\
\mathsf{vqh}_{\mathbf{S}}(\_)(\mathsf{pack}\, v) := \{\mathsf{pack}\ v\} & \mathsf{vqh}_{\mathbf{I}}(\_)(\mathsf{pack}\, v) := \{\mathsf{pack}\ v\} \\
\mathsf{vqh}_{\mathbf{S}}(\_)(\mathsf{gen}) := \{\Lambda.\, e\} & \mathsf{vqh}_{\mathbf{I}}(\_)(\mathsf{gen}) := \{\langle \sigma, \Lambda.\, e\rangle\} \\
\mathsf{vqh}_{\mathbf{S}}(\_)(\mathsf{name}) := \{v\} & \mathsf{vqh}_{\mathbf{I}}(\_)(\mathsf{name}) := \{\langle \sigma, n\rangle\} \\
\mathsf{vqh}_{\mathbf{S}}(\_)(\mathsf{goodfun}) := \{v\} & \mathsf{vqh}_{\mathbf{I}}(\_)(\mathsf{goodfun}) := \{\langle \sigma, \mathsf{fix}\, f(y,k).\, e\rangle \mid (\langle \sigma, \mathsf{fix}\, f(y,k).\, e\rangle) \notin \mathrm{badfun}\} \\
\mathsf{vqh}_{\mathbf{S}}(\_)(\mathsf{goodgen}) := \{v\} & \mathsf{vqh}_{\mathbf{I}}(\_)(\mathsf{goodgen}) := \{\langle \sigma, \Lambda k.\, e\rangle \mid (\langle \sigma, \Lambda k.\, e\rangle) \notin \mathrm{badgen}\} \\
 & \text{where } \mathrm{badfun} := \{\langle [], \mathsf{fix}\, 0(0,0).\, n\rangle\} \text{ and} \\
 & \qquad\quad \mathrm{badgen} := \{\langle [], \Lambda 0.\, n\rangle\}
\end{array}
$$

$$
\begin{array}{lcl}
\mathsf{vqh}_{\mathbf{T}}(s)(\mathsf{pair}\, v\, v') & := & \{n \mid n \in s.\mathrm{valdb}(\mathsf{pair}\, v\, v')\} \\
\mathsf{vqh}_{\mathbf{T}}(\_)(\mathsf{roll}\, v) & := & \{v\} \\
\mathsf{vqh}_{\mathbf{T}}(s)(\mathsf{fun}) & := & \{n \mid \exists n'.\ n \in s.\mathrm{valdb}(\mathsf{fun}\, n')\} \\
\mathsf{vqh}_{\mathbf{T}}(\_)(\mathsf{unit}) & := & \{n\} \\
\mathsf{vqh}_{\mathbf{T}}(\_)(\mathsf{nat}\, n) & := & \{n\} \\
\mathsf{vqh}_{\mathbf{T}}(s)(\mathsf{inl}\, v) & := & \{n \mid n \in s.\mathrm{valdb}(\mathsf{inl}\,, v)\} \\
\mathsf{vqh}_{\mathbf{T}}(s)(\mathsf{inr}\, v) & := & \{n \mid n \in s.\mathrm{valdb}(\mathsf{inr}\,, v)\} \\
\mathsf{vqh}_{\mathbf{T}}(\_)(\mathsf{pack}\, v) & := & \{\ n\} \\
\mathsf{vqh}_{\mathbf{T}}(s)(\mathsf{gen}) & := & \{n \mid \exists n'.\ n \in s.\mathrm{valdb}(\mathsf{fun}\, n')\} \\
\mathsf{vqh}_{\mathbf{T}}(\_)(\mathsf{name}) & := & \{n\} \\
\mathsf{vqh}_{\mathbf{T}}(\_)(\mathsf{goodfun}) & := & \{n\} \\
\mathsf{vqh}_{\mathbf{T}}(\_)(\mathsf{goodfun}) & := & \{n\}
\end{array}
$$

$$
\begin{array}{lcl}
\mathsf{cqh}_{\mathbf{S}}(\_)(\mathsf{app}\, v\, v'\, k) & := & \{(\emptyset, \emptyset, k[e[v/f][v'/x]]) \mid v = \mathsf{fix}\, f(x).\, e\} \\
\mathsf{cqh}_{\mathbf{S}}(\_)(\mathsf{inst}\, v\, k) & := & \{(\emptyset, \emptyset, k[e]) \mid v = \Lambda x.\, e\} \\
\mathsf{cqh}_{\mathbf{S}}(\_)(\mathsf{ret}\, v\, k) & := & \{(\emptyset, \emptyset, k[v])\}
\end{array}
$$

$$
\begin{array}{lcl}
\mathsf{cqh}_{\mathbf{I}}(\_)(\mathsf{app}\, v\, v'\, k) & := & \{(\emptyset, (\sigma', e)) \mid v = \langle \sigma, \mathsf{fix}\, f(y,k').\, e\rangle \wedge \\
 & & \qquad\qquad \sigma' = \sigma[f \mapsto v, y \mapsto v', k' \mapsto k]\} \\
\mathsf{cqh}_{\mathbf{I}}(\_)(\mathsf{inst}\, v\, k) & := & \{(\emptyset, (\sigma', e)) \mid v = \langle \sigma, \Lambda k'.\, e\rangle \wedge \sigma' = \sigma[k' \mapsto k]\} \\
\mathsf{cqh}_{\mathbf{I}}(\_)(\mathsf{ret}\, v\, k) & := & \{(\emptyset, (\sigma, k'\ x)) \mid \sigma(k') = k \wedge \sigma(x) = v\}
\end{array}
$$

$$
\begin{array}{lcl}
\mathsf{cqh}_{\mathbf{T}}(s)(\mathsf{app}\, v\, v'\, k) & := & \{(\emptyset, \emptyset, \emptyset, n) \mid v = s.R(\mathsf{clo}) \wedge v' = s.R(\mathsf{arg}) \\
 & & \qquad\qquad \wedge\, k = s.R(\mathsf{ret}) \wedge n \in s.\mathrm{db}(\mathsf{fun}\, v)\} \\
\mathsf{cqh}_{\mathbf{T}}(s)(\mathsf{inst}\, v\, k) & := & \{(\emptyset, \emptyset, \emptyset, n) \mid v = s.R(\mathsf{clo}) \\
 & & \qquad\qquad \wedge\, k = s.R(\mathsf{ret}) \wedge n \in s.\mathrm{db}(\mathsf{fun}\, v)\} \\
\mathsf{cqh}_{\mathbf{T}}(s)(\mathsf{ret}\, v\, k) & := & \{(\emptyset, \emptyset, \emptyset, k) \mid v = s.R(\mathsf{arg})\}
\end{array}
$$

5 Simulations

(In **model.v**)

Suppose $A, B \in \text{LangSpec}$, $T \in \text{TrSys}$, and $W \in \text{QH}^T_{A,B}$.

$$\langle - \rangle^{(-)} \in T.\mathsf{S} \to \text{VRelF}_{A,B} \to \text{VRelF}_{A,B} \qquad \textbf{vclos\_thunk}$$

$$\begin{aligned}\langle R \rangle^s := &\{(\tau \to \tau', v_a, v_b) \in R \mid v_a \in W.\mathsf{vqha}(s)(\mathsf{fun}) \land v_b \in W.\mathsf{vqhb}(s)(\mathsf{fun})\} \\ \cup\ &\{(\forall \alpha.\, \tau, v_a, v_b)\} \in R \mid v_a \in W.\mathsf{vqha}(s)(\mathsf{gen}) \land v_b \in W.\mathsf{vqhb}(s)(\mathsf{gen})\}\end{aligned}$$

$$\langle\!\langle - \rangle\!\rangle^{(-)} \in T.\mathsf{S} \to \text{VRelF}_{A,B} \to \text{VRel}_{A,B} \qquad \textbf{vclos\_, vclos}$$

$$\begin{aligned}\langle\!\langle R \rangle\!\rangle^s := \langle R \rangle^s &\cup \{(\mathsf{unit}, v_a, v_b) \mid v_a \in W.\mathsf{vqha}(s)(\mathsf{unit}) \land v_b \in W.\mathsf{vqhb}(s)(\mathsf{unit})\} \\ &\cup \{(\mathsf{nat}, v_a, v_b) \mid \exists n.\ v_a \in W.\mathsf{vqha}(s)(\mathsf{nat}\, n) \land v_b \in W.\mathsf{vqhb}(s)(\mathsf{nat}\, n)\} \\ &\cup \{(\tau_1 \times \tau_2, v_a, v_b) \mid \exists v_a^1, v_a^2, v_b^1, v_b^2.\ (v_a^1, v_b^1) \in \langle\!\langle R \rangle\!\rangle^s(\tau_1) \land (v_a^2, v_b^2) \in \langle\!\langle R \rangle\!\rangle^s(\tau_2) \land \\ &\qquad\qquad v_a \in W.\mathsf{vqha}(s)(\mathsf{pair}\, v_a^1\, v_a^2) \land v_b \in W.\mathsf{vqhb}(s)(\mathsf{pair}\, v_b^1\, v_b^2)\} \\ &\cup \{(\tau_1 + \tau_2, v_a, v_b) \mid \exists v_a^1, v_b^1.\ (v_a^1, v_b^1) \in \langle\!\langle R \rangle\!\rangle^s(\tau_1) \land v_a \in W.\mathsf{vqha}(s)(\mathsf{inl}\, v_a^1) \land v_b \in W.\mathsf{vqhb}(s)(\mathsf{inl}\, v_b^1)\} \\ &\cup \{(\tau_1 + \tau_2, v_a, v_b) \mid \exists v_a^2, v_b^2.\ (v_a^2, v_b^2) \in \langle\!\langle R \rangle\!\rangle^s(\tau_2) \land v_a \in W.\mathsf{vqha}(s)(\mathsf{inr}\, v_a^2) \land v_b \in W.\mathsf{vqhb}(s)(\mathsf{inr}\, v_b^2)\} \\ &\cup \{(\mu\alpha.\, \tau, v_a, v_b) \mid \exists v_a', v_b'.\ (v_a', v_b') \in \langle\!\langle R \rangle\!\rangle^s(\tau[\mu\alpha.\, \tau/\alpha]) \land \\ &\qquad\qquad v_a \in W.\mathsf{vqha}(s)(\mathsf{roll}\, v_a') \land v_b \in W.\mathsf{vqhb}(s)(\mathsf{roll}\, v_b')\} \\ &\cup \{(\exists \alpha.\, \tau, v_a, v_b) \mid \exists \tau', v_a', v_b'.\ (v_a', v_b') \in \langle\!\langle R \rangle\!\rangle^s(\tau[\tau'/\alpha]) \land \text{FV}(\tau) = \emptyset \land \\ &\qquad\qquad v_a \in W.\mathsf{vqha}(s)(\mathsf{pack}\, v_a') \land v_b \in W.\mathsf{vqhb}(s)(\mathsf{pack}\, v_b')\} \\ &\cup \{(\nu, v_a, v_b) \mid v_b \in W.\mathsf{vqhb}(s)(\mathsf{name}) \land (v_a, v_b) \in R(\nu)\} \\ &\cup \{(\mathsf{ref}\, \tau, v_a, v_b) \mid (v_a, v_b) \in W.\mathsf{rqh}(s)(\tau)\}\end{aligned}$$

Given $W \in \text{World}_{A,B}$, we define:

$$\begin{aligned}\text{configure} \in\ &(W.\mathsf{S} \to \text{VRelF}_{A,B}) \to W.\mathsf{S} \to \mathbb{B} \to (A.\mathbf{Conf} \times B.\mathbf{Conf}) \to \\ &(A.\mathbf{Conf} \times B.\mathbf{Conf}) \to (A.\mathbf{Conf} \times B.\mathbf{Conf}) \to \mathcal{P}(A.\mathbf{Mach} \times B.\mathbf{Mach})\end{aligned} \qquad \textbf{configure}$$

$$\begin{aligned}\text{configure}(U)(s)(\sigma)(e_a, e_b)(c_a, c_b)(c_a', c_b') := \{&(m_a, m_b) \in A.\text{real}(e_a \cdot c_a \cdot c_a') \times B.\text{real}(e_b \cdot c_b \cdot c_b') \\ \mid\ &(\neg\sigma \implies c_a = c_b = \emptyset) \land \\ &(\sigma \implies (c_a, c_b) \in W.\mathsf{crel}(U)(s) \land e_a \in A.\text{core} \land e_b \in B.\text{core}) \land \\ &(c_a, c_b) \in W.\mathsf{crel}(U)(s)\}\end{aligned}$$

$$\text{call} \in W.\mathsf{S} \to \text{VRelF}_{A,B} \to \text{VRelF}_{A,B} \to \text{KRel}_{A,B} \to \text{Type} \to \mathcal{P}(A.\mathbf{Conf} \times B.\mathbf{Conf}) \qquad \textbf{call}$$

$$\begin{aligned}\text{call}(s)(R_f)(R_v)(R_k)(\tau) := &\{(e_a, e_b) \in W.\mathsf{cqha}(s)(\mathsf{app}\, f_a\, v_a\, k_a) \times W.\mathsf{cqhb}(s)(\mathsf{app}\, f_b\, v_b\, k_b) \mid \exists \tau_v, \tau_r. \\ &\quad \exists f_a, f_b, v_a, v_b, k_a, k_b. \\ &\quad (f_a, f_b) \in \langle R_f \rangle^s(\tau_v \to \tau_r) \land (v_a, v_b) \in \langle\!\langle R_v \rangle\!\rangle^s(\tau_v) \land (k_a, k_b) \in R_k(\tau_r)(\tau)\} \\ \cup\ &\{(e_a, e_b) \in W.\mathsf{cqha}(s)(\mathsf{inst}\, v_a\, k_a) \times W.\mathsf{cqhb}(s)(\mathsf{inst}\, v_b\, k_b) \mid \exists \alpha, \tau_v, \tau_r. \\ &\quad \exists f_a, f_b, k_a, k_b. \\ &\quad (f_a, f_b) \in \langle R_f \rangle^s(\forall \alpha.\, \alpha\tau_r) \land \text{FV}(\tau_v) = \emptyset \land (k_a, k_b) \in R_k(\tau_r[\tau_v/\alpha])(\tau)\}\end{aligned}$$

$$[\tau, v_a, v_b] := \{(\tau, v_a, v_b)\} \qquad [k_a, k_b] := \{(\tau, \tau, k_a, k_b) \mid \tau \in \text{Type}\} \qquad \textbf{vsingle, ksingle}$$

Given $W \in \text{World}_{A,B}$, we define coinductively:

$\mathbf{E}_{\text{prog}} \in W.O \to A.\mathbf{Cont} \times B.\mathbf{Cont} \to (W.\mathsf{S} \to \text{VRelF}_{A,B}) \to W.\mathsf{S} \to W.\mathsf{S} \to \mathbb{B} \to$ **esim_progress**
$\quad \text{Evt} \to A.\mathbf{Mach} \times B.\mathbf{Mach} \to \text{Type} \to \mathcal{P}(A.\mathbf{Conf} \times B.\mathbf{Conf})$
$\mathbf{E}_{\text{prog}}(i)(k_a^0, k_b^0)(U)(s^0)(s)(\sigma)(t)(m_b, m_b')(\tau) :=$
$\quad \{(e_a, e_b) \mid \exists i', (m_b \overset{t}{\hookrightarrow}_B m_b') \vee (t = \epsilon \wedge m_b = m_b' \wedge i' <^* i) \wedge (e_a, e_b) \in \mathbf{E}(i')(k_a^0, k_b^0)(U)(s^0)(s)(\sigma)(\tau) \wedge \sigma = 0\}$

$\mathbf{E} \in W.O \to A.\mathbf{Cont} \times B.\mathbf{Cont} \to (W.\mathsf{S} \to \text{VRelF}_{A,B}) \to W.\mathsf{S} \to W.\mathsf{S} \to \mathbb{B} \to \text{Type} \to \mathcal{P}(A.\mathbf{Conf} \times B.\mathbf{Conf})$
$\mathbf{E}(i)(k_a^0, k_b^0)(U)(s^0)(s)(\sigma)(\tau) :=$ **esim_call, esim_main, esim_, pesim**
$\{(e_a, e_b) \mid U \in \mathbf{U} \implies \forall c_a, c_b, \eta_a, \eta_b.$
$\quad \eta_a \in A.\text{extra} \wedge \eta_b \in B.\text{extra} \implies \quad \forall (m_a, m_b) \in \text{configure}(U)(s)(\sigma)(e_a, e_b)(c_a, c_b)(\eta_a, \eta_b).$
$\quad\quad$ (ERR) $\exists m_b'.\ m_b \overset{\epsilon}{\hookrightarrow}^* m_b' \wedge m_b' \in B.\text{error}$
$\quad \vee$ (RET) $\exists s', v_a, v_b, e_a', e_b', c_a', c_b'.\ s' \sqsupseteq s \wedge s' \sqsupseteq_{\text{pub}} s^0 \wedge$
$\quad\quad m_b \overset{\epsilon}{\hookrightarrow}^* m_b' \wedge$
$\quad\quad (e_a', e_b') \in W.\mathsf{cqha}(s')(\mathsf{ret}\, v_a\, k_a^0) \times W.\mathsf{cqhb}(s')(\mathsf{ret}\, v_b\, k_b^0) \wedge$
$\quad\quad (v_a, v_b) \in \langle\!\langle U(s') \rangle\!\rangle^{s'}(\tau) \wedge (m_a, m_b') \in \text{configure}(U)(s')(1)(e_a', e_b')(c_a', c_b')(\eta_a, \eta_b)$
$\quad \vee$ (STEP) $(m_a \notin A.\text{halted}) \wedge \forall t, m_a'.\ m_a \overset{t}{\hookrightarrow} m_a' \implies$
$\quad\quad \exists i', e_a', e_b', c_a', c_b', m_b', m_b'', \sigma', s'.\ s' \sqsupseteq s \wedge$
$\quad\quad (m_a', m_b'') \in \text{configure}(U)(s')(\sigma')(e_a, e_b)(c_a', c_b')(\eta_a, \eta_b) \wedge m_b \overset{\epsilon}{\hookrightarrow}^* m_b' \wedge$
$\quad\quad\quad$ (REC) $(e_a', e_b') \in \mathbf{E}_{\text{prog}}(i')(k_a^0, k_b^0)(U)(s^0)(s')(\sigma')(t)(m_b', m_b'')(\tau)$
$\quad\quad \vee$ (CALL) $m_b' \overset{t}{\hookrightarrow} m_b'' \wedge (e_a', e_b') \in \text{call}(s')(U(s'))(U(s'))(\mathbf{K}(i')(k_a^0, k_b^0)(U)(s^0)(s'))(\tau) \wedge \sigma' = 1$
$\}$

$\mathbf{U} \in \mathcal{P}(W.\mathsf{S} \to \text{VRelF}_{A,B})$ **gknow_, gknow**
$\mathbf{U} := \{U \mid U \text{ monotone w.r.t. } \sqsupseteq\ \wedge \mathbf{F}(U) \subseteq U \wedge \forall \nu \in W.\mathsf{supp}.\ U(s)(\nu) = W.\mathsf{name}(U)(s)(\nu)\}$

$\text{goodthunk}(W)(s) :=$
$\quad \{(\tau \to \tau', v_a, v_b) \mid v_a \in W.\mathsf{vqha}(s)(\mathsf{goodfun}) \wedge v_b \in W.\mathsf{vqhb}(s)(\mathsf{goodfun})\} \cup$
$\quad \{(\forall \alpha.\, \tau, v_a, v_b) \mid v_a \in W.\mathsf{vqha}(s)(\mathsf{goodgen}) \wedge v_b \in W.\mathsf{vqhb}(s)(\mathsf{goodgen})\}$

$\mathbf{F} \in (W.\mathsf{S} \to \text{VRelF}_{A,B}) \to W.\mathsf{S} \to \text{VRelF}_{A,B}$ **lsim_, lsim**
$\mathbf{F}(U)(s) := \{(\tau, v_a, v_b) \in \text{goodthunk}(W)(s) \mid \forall \tau', k_a, k_b.\ \forall U' \sqsupseteq U.\ \forall s' \sqsupseteq s.$
$\quad \text{call}(s')([\tau, v_a, v_b])(U'(s'))([k_a, k_b])(\tau') \subseteq \mathbf{E}(i)(k_a, k_b)(U')(s')(s')(\sigma)(\tau')\}$

$\mathbf{K} \in W.O \to A.\mathbf{Cont} \times B.\mathbf{Cont} \to (W.\mathsf{S} \to \text{VRelF}_{A,B}) \to W.\mathsf{S} \to W.\mathsf{S} \to \text{KRel}_{A,B}$ **ksim_, ksim**
$\mathbf{K}(i)(k_a^0, k_b^0)(U)(s^0)(s) := \{(\tau', \tau, k_a, k_b) \mid \forall U' \sqsupseteq U.\ \forall s' \sqsupseteq_{\text{pub}} s.\ \forall (v_a, v_b) \in \langle\!\langle U'(s') \rangle\!\rangle^{s'}(\tau').$
$\quad W.\mathsf{cqha}(s')(\mathsf{ret}\, v_a\, k_a) \times W.\mathsf{cqhb}(s')(\mathsf{ret}\, v_b\, k_b) \subseteq \mathbf{E}(i)(k_a^0, k_b^0)(U')(s^0)(s')(1)(\tau)\}$

Given $W \in \text{WorldG}_{A,B}$ and $w \in \text{WorldL}(W)_{A,B}$, we define:

$\text{realizableG}(W) \in (A.\mathbf{Conf} \times B.\mathbf{Conf}) \to \mathbf{U} \to \mathcal{P}(W.T)$ **realizable_global_state**
$\text{realizableG}(W)(c_a, c_b)(U) := \{s \mid \exists e_a, e_b, c_a', c_b', \eta_a, \eta_b, m_a, m_b.$
$\quad\quad \text{configure}(U)(s)(1)(e_a, e_b)(c_a', c_b')(c_a \cdot \eta_a, c_b \cdot \eta_b)\}$
$\text{realizableL}(w) \in \mathbf{U} \to \mathcal{P}(w.T)$ **realizable_local_state**
$\text{realizableL}(w)(U) := \{s \mid \exists c_a, c_b.\ (c_a, c_b) \in w.\mathsf{crel}(U)(s)\}$

$\text{stable}(W) \in \mathcal{P}(\text{WorldL}_{A,B}(W))$ **stable**
$\text{stable}(W) := \{w \mid \forall U, s_{\text{g}}, s, s_{\text{g}}', c_a, c_b.\ U \in \mathbf{U} \wedge (c_a, c_b) \in w.\mathsf{crel}(U)(s_{\text{g}}, s) \wedge s_{\text{g}}' \sqsupseteq s_{\text{g}} \wedge$
$\quad s_{\text{g}}' \in \text{realizableG}(W)(c_a, c_b)(U(-, s)) \implies$
$\quad \exists s' \sqsupseteq_{\text{pub}} s.\ (c_a, c_b) \in w.\mathsf{crel}(U)(s_{\text{g}}', s')\}$

5.1 Module Simulation

Given $W \in \text{WorldG}_{A,B}$, $M_a \in A.\mathbf{Mod}$ and $M_b \in B.\mathbf{Mod}$ we define the module simulation:

$$\begin{aligned}
&\Gamma \vdash M_a \precsim_W M_b : \Gamma' := \qquad \textbf{tlsim, msim}\\
&\quad \forall \mathcal{N}.\ \mathcal{N} \text{ countably infinite} \implies \exists w \in \text{WorldL}_{A,B}(W).\ \forall \Psi_a, \Psi_b, \gamma_a, \gamma_b, c_a^g, c_b^g, c_a^l, c_b^l.\\
&\quad (c_a^g, c_a^l) \in A.\text{cload}(M_a)(\Psi_a)(\gamma_a) \wedge (c_b^g, c_b^l) \in B.\text{cload}(M_b)(\Psi_b)(\gamma_b) \wedge\\
&\quad \text{map}\ \Pi_1\ \gamma_a = \text{map}\ \Pi_1\ \Gamma = \text{map}\ \Pi_1\ \gamma_b \implies \exists s^0.\ w \in \text{stable}(W) \wedge w.\mathsf{supp} \subseteq \mathcal{N} \wedge\\
&\quad (\forall U \in \mathbf{U}.\ (c_a^g, c_b^g) \in W.\mathsf{crel}(U(-, \Pi_2 s^0))(\Pi_1 s^0)) \wedge (\forall U \in \mathbf{U}.\ (c_a^l, c_b^l) \in w.\mathsf{crel}(U)(s^0)) \wedge\\
&\quad (\forall \tau, v_a, v_b.\ (v_a, v_b) \notin W.\mathsf{rqh}(s^0)(\tau)) \wedge\\
&\quad \forall f' {:} \tau \in \Gamma'.\ \exists (v_a, v_b) \in A.\text{vload}(M_a)(\Psi_a)(\gamma_a)(f') \times B.\text{vload}(M_b)(\Psi_b)(\gamma_b)(f').\\
&\quad \forall s \sqsupseteq s^0.\ \forall U \in \mathbf{U}.\ s \in \text{realizableL}(w)(U) \implies\\
&\quad (\forall f {:} \tau' \in \Gamma.\ (\gamma_a f, \gamma_b f) \in \langle U(s) \rangle^s(\tau')) \implies (v_a, v_b) \in \langle U(s) \rangle^s(\tau)
\end{aligned}$$

6 Key Results

Theorem 1 (Transitivity).

$$\frac{|\Gamma| \vdash M_{\mathbf{T}} \precsim_{\mathbf{TI}} M_{\mathbf{I}} : |\Gamma'| \qquad \Gamma \vdash M_{\mathbf{I}} \precsim_{\mathbf{IS}} M_{\mathbf{S}} : \Gamma'}{\Gamma \vdash M_{\mathbf{T}} \precsim_{\mathbf{TS}} M_{\mathbf{S}} : \Gamma'} \text{ vcomp\_tms}$$

$$\frac{|\Gamma| \vdash M_{\mathbf{I}} \precsim_{\mathbf{II}} M'_{\mathbf{I}} : |\Gamma'| \qquad \Gamma \vdash M'_{\mathbf{I}} \precsim_{\mathbf{IS}} M_{\mathbf{S}} : \Gamma'}{\Gamma \vdash M_{\mathbf{I}} \precsim_{\mathbf{IS}} M_{\mathbf{S}} : \Gamma'} \text{ vcomp\_mms}$$

(Here $|-|$ erases the types from the given context, leaving just a list of variables.)

Note that from the second property we immediately get the following:

$$\frac{|\Gamma| \vdash M_{\mathbf{I}} \precsim^{*}_{\mathbf{II}} M'_{\mathbf{I}} : |\Gamma'| \qquad \Gamma \vdash M'_{\mathbf{I}} \precsim_{\mathbf{IS}} M_{\mathbf{S}} : \Gamma'}{\Gamma \vdash M_{\mathbf{I}} \precsim_{\mathbf{IS}} M_{\mathbf{S}} : \Gamma'} \text{ vcomp\_mms\_rtc}$$

Theorem 2 (Linking). We define linking of modules in source and target language:

$$\begin{array}{l}
\bowtie_{\mathbf{T}} \ \in \ \mathbf{Mod_T} \times \mathbf{Mod_T} \to \mathbf{Mod_T} \qquad \text{tgt_link} \\
(M_a \bowtie_{\mathbf{T}} M_b)(\Psi)(\text{imports}) := \text{segs}_1 +\!\!+ \text{segs}_2 \\
\quad \text{where} \\
\quad \text{segs}_1 := M_a(\Psi)([n_1, \ldots, n_m]) \\
\quad \text{size} \ := \sum_{\text{seg} \in \text{map } (\Pi_2 \circ \Pi_2) \text{ segs}_1} (1 + |\text{seg}|) \\
\quad \text{segs}_2 := M_b(\Psi + \text{size})(\text{imports} +\!\!+ \text{map } (\Pi_1 \circ \Pi_2) \text{ segs}_1)
\end{array}$$

$$\begin{array}{l}
\bowtie_{\mathbf{S}} \ \in \ \mathbf{Mod_S} \times \mathbf{Mod_S} \to \mathbf{Mod_S} \qquad \text{src_link} \\
M_a \bowtie_{\mathbf{S}} M_b := M_a +\!\!+ M_b
\end{array}$$

$$\frac{\begin{array}{cc} \vdash M^1_{\mathbf{T}} : \Gamma_1 & \Gamma_1 = \mathit{map}\ \Pi_1\ M^1_{\mathbf{S}} \\ \vdash M^2_{\mathbf{T}} : \Gamma_2 & \Gamma_2 = \mathit{map}\ \Pi_1\ M^2_{\mathbf{S}} \\ \Gamma_1 \cap \Gamma = \emptyset & \Gamma_1 \cap \Gamma_2 = \emptyset \\ \Gamma \vdash M^1_{\mathbf{T}} \precsim_{\mathbf{TS}} M^1_{\mathbf{S}} : \Gamma_1 & \Gamma, \Gamma_1 \vdash M^2_{\mathbf{T}} \precsim_{\mathbf{TS}} M^2_{\mathbf{S}} : \Gamma_2 \end{array}}{\Gamma \vdash (M^1_{\mathbf{T}} \bowtie_{\mathbf{T}} M^2_{\mathbf{T}}) \precsim_{\mathbf{TS}} (M^1_{\mathbf{S}} \bowtie_{\mathbf{S}} M^2_{\mathbf{S}}) : \Gamma_1, \Gamma_2} \text{ hcomp\_msim\_linking}$$

6.1 Adequacy

(In adequacy.v)

We define OBS and Behav as greatest fixed points in the following way:

$$\begin{array}{l}
\text{OBS} \in \text{Set} \qquad \text{obs_event, observation} \\
\text{OBS} := \{\text{done}, \infty_\epsilon\} \ \cup \ (\{?n, !n\} \times \text{OBS})
\end{array}$$

$$\begin{array}{ll}
\multicolumn{2}{l}{\text{Behav}_L \in \mathcal{P}(\mathbf{Mach}_L \times \text{OBS}) \qquad \text{behmatch, behave_, behave}} \\
\multicolumn{2}{l}{\text{Behav}_L := \{(m, o) \mid} \\
\quad (\textsc{Err}) & \exists m'.\ m \overset{\epsilon}{\hookrightarrow}^{*} m' \wedge m' \in L.\text{error} \\
\vee\ (\textsc{Halt}) & o = \text{done} \wedge \exists m''.\ m \overset{\epsilon}{\hookrightarrow}^{*} m'' \wedge m'' \in L.\text{halted} \\
\vee\ (\epsilon) & o = \infty_\epsilon \wedge \exists m'.\ m \overset{\epsilon}{\hookrightarrow}_L m' \wedge (m', \infty_\epsilon) \in \text{Behav}_L \\
\vee\ (\textsc{Evt}) & \exists m', m'', t, o'.\ o = (t, o') \wedge m \overset{\epsilon}{\hookrightarrow}^{*} m'' \wedge m'' \overset{t}{\hookrightarrow}_L m' \wedge t \in \{?n, !n\} \wedge (m', o') \in \text{Behav}_L\}
\end{array}$$

For convenience, we write $\text{Behav}(m_L)$ for $\{o \mid (m_L, o) \in \text{Behav}_L\}$.

Theorem 3 (Adequacy)**.**

$$\frac{\begin{array}{c}\Gamma[F_{\text{main}}] = \mathsf{unit} \to \tau \qquad \vdash M_{\mathbf{T}} : |\Gamma| \\ \text{load}_{\mathbf{T}}(M_{\mathbf{T}}) = m_{\mathbf{T}} \qquad \cdot \vdash M_{\mathbf{T}} \precsim_{\mathbf{TS}} M_{\mathbf{S}} : \Gamma \qquad \text{load}_{\mathbf{S}}(M_{\mathbf{S}}) = m_{\mathbf{S}}\end{array}}{\text{Behav}(m_{\mathbf{T}}) \subseteq \text{Behav}(m_{\mathbf{S}})} \text{ adequacy\_msim}$$

6.2 Compiler Correctness

(In **compiler.v**)

Theorem 4 (Reinheitsgebot: Compositional correctness of Pilsner)**.**

$$\frac{\Gamma \vdash M_{\mathbf{S}} : \Gamma'}{\Gamma \vdash \text{Pilsner}(M_{\mathbf{S}}) \precsim_{\mathbf{TS}} M_{\mathbf{S}} : \Gamma'} \text{ compile\_correct}$$

$$\frac{\Gamma \vdash M_{\mathbf{S}} : \Gamma'}{\vdash \text{Pilsner}(M_{\mathbf{S}}) : |\Gamma'|} \text{ compile\_correct}$$