HANDLE WITH CARE:

RELATIONAL INTERPRETATION OF ALGEBRAIC EFFECTS AND HANDLERS

DARIUSZ BIERNACKI, **MACIEJ PIRÓG**,
FILIP SIECZKOWSKI, and PIOTR POLESIUK

University of Wrocław, Poland

GAINING MOMENTUM

Programming with algebraic effects and handlers seems to be on the rise for a number of reasons:

- Elegant separation of syntax and semantics
- More flexibility in programming with multiple different effects at a time
- Closer to algebraic understanding of effects
- Attractive language for delimited control

PLENTY-OF-ROPE

Algebraic effects and handlers allow for a lot of flexibility and dynamic control over the computation.

How to make sure that we won’t shoot ourselves in the foot with all this flexibility?

GOAL OF THE PAPER

Reasoning about algebraic effects and handlers (e.g., contextual equivalence)

In particular: operational, relational reasoning

...about a calculus (out of many calculi that could be constructed for AE&H)

(Note the feedback loop!)

THE λ^{HL} CALCULUS

Based on Daan Leijen's core calculus of KOKA [POPL'17]:

- CBV λ-calculus + operations and handlers
- row-based type-and-effect system
- simply-typed in types
- polymorphic in rows of effects
- a novel "lift" construct

OPERATIONS AND HANDLERS

- Each effect ℓ is a set of (typed) operations, for example:
  Mutable state: S with $\mathit{put} : \sigma \to ()$, $\mathit{get} : () \to \sigma$
- Handlers tell us what to do with operations, for example:

$$\begin{array}{ll} \text{handle}_{\mathsf{S}}\ \square & \{\ \mathit{get}\ \_, r.\ \lambda s.\ r\ s\ s \\ & ;\ \mathit{put}\ s', r.\ \lambda s.\ r\ ()\ s' \\ & ;\ \text{return}\ x.\ \lambda \_.x\ \ \} \end{array}$$

- In general, the evaluation rule is as follows:

$$\begin{array}{l} \text{handle}_{\ell}\ E[op_{\ell}\ v]\ \{h; \text{return}\ x.\ e'\} \to \\ \qquad e\{v/x\}\{\lambda z.\text{handle}_{\ell}\ E[z]\ \{h; \text{return}\ x.\ e'\}/r\} \\ \qquad (\text{if } \ell \text{ appropriately free in } E \text{ and } op\ x, r.\ e \in h) \end{array}$$

$$\text{handle}_{\ell}\ v\ \{h; \text{return}\ x.\ e'\} \to e'\{v/x\}$$

TYPE-AND-EFFECT SYSTEM

In judgements, terms are given types and rows of effect names:

$$\cdots \vdash e : \tau / \varepsilon$$

For example, consider:

Reader: R with one operation $ask : 1 \to \sigma$

Then,

$$ask_{\mathsf{R}}\ () + get_{\mathsf{S}}\ () : int\ /\ \langle \mathsf{R}, \mathsf{S} \rangle$$

Arrows are decorated with rows of effects:

$$\lambda x.\ x + ask_{\mathsf{R}}\ () : int \to_{\langle \mathsf{R} \rangle} int$$

ROW POLYMORPHISM

Rows can be open, i.e., end with a variable, which we can instantiate with any row, for example

$$\cdots \vdash e : \tau \ / \ \langle \mathsf{R}, \mathsf{S} \mid \alpha \rangle$$

We can manage effect-polymorphic computation with Λ to generalise and $\cdot *$ to instantiate, for example

$$\vdash \Lambda.\lambda f.f\ () : \forall \alpha.(1 \rightarrow_\alpha \tau) \rightarrow_\alpha \tau / \varepsilon$$

(Note the sub-effecting)

WHAT ABOUT PARAMETRICITY?

- $f : \forall\alpha.(\tau_1 \to_\alpha \tau_2) \to_\alpha \tau_3$
- Given any $g : \tau_1 \to_\alpha \tau_2$, how many times $f\ g$ uses g?
  Let's try the T ('tick') effect with a single operation $\mathit{tick} : 1 \to 1$.

$$
\begin{aligned}
f_{cnt} = \Lambda.\lambda g.\mathrm{handle}_{\mathrm{T}}\ f * (\lambda x.\mathit{tick}_{\mathrm{T}}\ (); g\ x)\\
\{\mathit{tick}\ \_, r.\ \lambda n.r\ ()\ (n+1)\\
;\mathrm{return}\ \_.\ \lambda n.n\\
\}\ 0
\end{aligned}
$$

- Because of the dynamic nature of binding of handlers to operations, the above won't work as expected when g uses T.

THE LIFT OPERATOR

If $e : \tau / \langle \ell_1, \ell_2, \ldots \rangle$

then $[e]_{\ell} : \tau / \langle \ell, \ell_1, \ell_2, \ldots \rangle$

OPERATIONAL SEMANTICS OF LIFT

$$\mathit{ask}_{\mathsf{R}}\ () + [\mathit{ask}_{\mathsf{R}}\ ()]_{\mathsf{R}} : \mathit{int}\ /\ \langle \mathsf{R}, \mathsf{R} \rangle$$

OPERATIONAL SEMANTICS OF LIFT

$$\mathit{ask}_{\mathsf{R}}\ () + [\mathit{ask}_{\mathsf{R}}\ ()]_{\mathsf{R}} : \mathit{int} \,/\, \langle \mathsf{R}, \mathsf{R} \rangle$$

$$\mathsf{handle}_{\mathsf{R}}\ \mathsf{handle}_{\mathsf{R}}\ \mathit{ask}_{\mathsf{R}}\ () + [\mathit{ask}_{\mathsf{R}}\ ()]_{\mathsf{R}}\ \{\mathit{ask}\ \_, r.\, r\ 10\}\{\mathit{ask}\ \_, r.\, r\ 2\}$$

OPERATIONAL SEMANTICS OF LIFT

$$\mathit{ask}_{\mathsf{R}}\ () + [\mathit{ask}_{\mathsf{R}}\ ()]_{\mathsf{R}} : \mathit{int}\ /\ \langle \mathsf{R}, \mathsf{R} \rangle$$

$$\mathsf{handle}_{\mathsf{R}}\ \mathsf{handle}_{\mathsf{R}}\ \mathit{ask}_{\mathsf{R}}\ () + [\mathit{ask}_{\mathsf{R}}\ ()]_{\mathsf{R}}\ \{\mathit{ask}\ \_, r.\ r\ 10\}\{\mathit{ask}\ \_, r.\ r\ 2\}$$

OPERATIONAL SEMANTICS OF LIFT

$$ask_{\mathsf{R}}\ () + [ask_{\mathsf{R}}\ ()]_{\mathsf{R}} : int \,/\, \langle \mathsf{R}, \mathsf{R} \rangle$$

$$\mathsf{handle}_{\mathsf{R}}\ \mathsf{handle}_{\mathsf{R}}\ ask_{\mathsf{R}}\ () + [ask_{\mathsf{R}}\ ()]_{\mathsf{R}}\ \{ask\ \_, r.\ r\ 10\}\{ask\ \_, r.\ r\ 2\}$$

BACK TO TICK

- $f : \forall\alpha.(\tau_1 \to_\alpha \tau_2) \to_\alpha \tau_3$
- Given any $g : \tau_1 \to_\alpha \tau_2$, how many times $f\ g$ uses g? Let's try the T ('tick') effect with a single operation $tick : 1 \to 1$.

$$
\begin{aligned}
f_{cnt} = \Lambda.\lambda g.\mathrm{handle}_{\mathsf{T}}\ f * (\lambda x.tick_{\mathsf{T}}\ (); {\color{red}[g\ x]_{\mathsf{T}}})\\
&\{tick\ \_, r.\ \lambda n.r\ ()\ (n+1)\\
&;\mathrm{return}\ \_.\ \lambda n.n\\
&\}\ 0
\end{aligned}
$$

SUMMARY OF THE HARDSHIPS

Reasoning about algebraic effects and handlers even in the simple case of λ^{HL} seems to be non-trivial, because of:

- Control structure in the style of delimited continuations
- Non-termination (via recursive effects)
- Effect polymorphism
- Managing multiple effects in a row

RELATIONAL INTERPRETATION

We build a biorthogonal relational interpretation of λ^{HL}, which allows us to show contextual program approximations and equivalences, as well as type soundness of λ^{HL}.

The novel things are:

- Interpretation of effect rows
- Closure for “simple expressions”

CONTROL-STUCK EXPRESSIONS

- For example, *op* v is not a value, but we cannot reduce it without an appropriate handler around it.
- We use the standard technique of biorthogonality, but we add a separate closure for *simple expressions*, which are (things related to) such irreducible non-values.
- Two evaluation contexts are related if they are ovservationally equivalent when plugged with related values **and** with related simple expressions.

NON-TERMINATION

- We use a standard solution: step-indexed logical relations formalised as predicates in the category of complete ordered families of equivalences (COFE).
- COFE has a nice internal logic with a later modality ($\triangleright$) and Löb induction as a reasoning principle...
- ...although not consistent with LEM (if you care about such things)

COQ FORMALISATION

- Uses Polesiuk's IxFree library for step-indexed relations
- 4228 LOC:
  - Language: 1573 LOC
  - Logical relation: 2217 LOC
  - Examples: 438 LOC
- `bitbucket.org/pl-uwr/aleff-logrel`

A FEW EXAMPLES

STATE AS A COMPOSITION OF READER AND WRITER

- Reader: R with one operation *ask* $: 1 \to \sigma$
- Writer: W with one operation *tell* $: \sigma \to 1$
- $$\begin{aligned} &\lambda s.\mathsf{handle}_{\mathsf{R}} \\ &\qquad \mathsf{handle}_{\mathsf{W}}\ \Box \\ &\qquad \{tell\ s', r.\ [\mathsf{handle}_{\mathsf{R}}\ r\ ()\ \{ask\ \_, r.\ r\ s'\}]_{\mathsf{R}}\} \\ &\quad \{ask\ \_, r.\ r\ s\} \end{aligned}$$
- Is it equivalent to the usual handler for state?

THE RETURN CLAUSE IS REDUNDANT

With the lift construct, handlers of the shape

$$\text{handle}_\ell\ e\ \{h;\ \text{return}\ x.\ e_r\}$$

can be replaced by

$$\text{handle}_\ell\ (\lambda x.[e_r]_\ell)\ e\ \{h\}$$

THINGS TO DO NEXT

- More programming language constructs, e.g., base types, value polymorphism
- Shallow handlers
- Local definitions of effects and instancecs (Kripke logical relations maybe)

SUMMARY

- A study of a calculus with algebraic effects and row-polymorphic type-and-effect system
- A logical relation that allowed us to prove some contextual equivalences
- Fully formalised in Coq

`bitbucket.org/pl-uwr/aleff-logrel`

QUESTIONS?

Please, handle the speaker with care!

TECHNICAL STUFF

SYNTAX

$$\mathrm{Var} \ni f, r, x, y, \ldots \quad \mathrm{RVar} \ni \alpha, \beta, \ldots \quad \text{(variables, row variables)}$$

$$\mathcal{EN} \ni l \quad \mathcal{ON} \ni op \qquad \text{(effect names, operation names)}$$

$$\begin{aligned}
\mathrm{Exp} \ni e \;&::= v \mid e\ e \mid e\ * \mid [e]_l \mid \mathsf{handle}_l\ e\ \{h; \mathsf{return}\ x.\ e\} \\
\mathrm{Val} \ni u, v \;&::= x \mid \lambda x.e \mid \Lambda.e \mid op_l \mid () \\
h \;&::= \cdot \mid op_l\ x, r.\ e; h \\
\mathrm{ECont} \ni E \;&::= \square \mid E\ e \mid v\ E \mid E\ * \mid \\
&\quad\; [E]_l \mid \mathsf{handle}_l\ E\ \{h; \mathsf{return}\ x.\ e\}
\end{aligned}$$

$$\begin{aligned}
\mathrm{Type} \ni \sigma, \tau \;&::= 1 \mid \tau \to_\varepsilon \tau \mid \forall \alpha.\tau && \text{(types)} \\
\mathrm{Eff} \ni \varepsilon \;&::= \alpha \mid \langle\rangle \mid \langle l \mid \varepsilon \rangle && \text{(effects)}
\end{aligned}$$

$$\begin{aligned}
\Delta \;&::= \cdot \mid \Delta, \alpha && \text{(row contexts)} \\
\Gamma \;&::= \cdot \mid \Gamma, x : \tau && \text{(variable contexts)} \\
\Sigma \;&::= \cdot \mid \Sigma, l \mapsto \overline{op : \tau \to \tau} && \text{(effect contexts)}
\end{aligned}$$

n-FREENESS

$$\frac{}{0\text{--free}(l, \square)} \qquad \frac{n\text{--free}(l, E)}{n\text{--free}(l, E\ e)} \qquad \frac{n\text{--free}(l, E)}{n\text{--free}(l, v\ E)}$$

$$\frac{n\text{--free}(l, E)}{(n+1)\text{--free}(l, [E]_l)} \qquad \frac{n\text{--free}(l, E) \qquad l \neq l'}{n\text{--free}(l, [E]_{l'})}$$

$$\frac{(n+1)\text{--free}(l, E)}{n\text{--free}(l, \mathsf{handle}_l\ E\ \{h; \mathsf{return}\ x.\ e\})}$$

$$\frac{n\text{--free}(l, E) \qquad l \neq l'}{n\text{--free}(l, \mathsf{handle}_{l'}\ E\ \{h; \mathsf{return}\ x.\ e\})}$$

OPERATIONAL SEMANTICS

$$
\begin{array}{rcl}
E[(\lambda x.e)\ v] & \to & E[e\{v/x\}] \\
E[(\Lambda.e)\ *] & \to & E[e] \\
E[[v]_l] & \to & E[v] \\
E[\text{handle}_l\ v\ \{h; \text{return}\ x.\ e'\}] & \to & E[e'\{v/x\}] \\
E[\text{handle}_l\ E'[op_l\ v]\ \{h; \text{return}\ x.\ e'\}] & \to &
\end{array}
$$

$$
E[e\{v/x\}\{\lambda z.\text{handle}_l\ E'[z]\ \{h; \text{return}\ x.\ e'\}/r\}]
$$

$$
\text{if } 0{-}\mathrm{free}(l, E') \text{ and } op\ x, r.\ e \in h
$$

SUBTYPING AND EFFECT SUBSUMPTION

$$\frac{}{\Sigma; \Delta \vdash \varepsilon \leq \varepsilon} \qquad \frac{\Sigma; \Delta \vdash \varepsilon_1 \leq \varepsilon_2 \qquad \Sigma; \Delta \vdash \varepsilon_2 \leq \varepsilon_3}{\Sigma; \Delta \vdash \varepsilon_1 \leq \varepsilon_3}$$

$$\frac{}{\Sigma; \Delta \vdash \langle l_1, l_2 \mid \varepsilon \rangle \leq \langle l_2, l_1 \mid \varepsilon \rangle} \qquad \frac{}{\Sigma; \Delta \vdash \langle \rangle \leq \varepsilon}$$

$$\frac{\Sigma; \Delta \vdash \varepsilon_1 \leq \varepsilon_2}{\Sigma; \Delta \vdash \langle l \mid \varepsilon_1 \rangle \leq \langle l \mid \varepsilon_2 \rangle} \qquad \frac{}{\Sigma; \Delta \vdash \tau \leq \tau}$$

$$\frac{\Sigma; \Delta \vdash \tau_1 \leq \tau_2 \qquad \Sigma; \Delta \vdash \tau_2 \leq \tau_3}{\Sigma; \Delta \vdash \tau_1 \leq \tau_3} \qquad \frac{\Sigma; \Delta, \alpha \vdash \tau_1 \leq \tau_2}{\Sigma; \Delta \vdash \forall \alpha . \tau_1 \leq \forall \alpha . \tau_2}$$

$$\frac{\Sigma; \Delta \vdash \sigma_2 \leq \sigma_1 \qquad \Sigma; \Delta \vdash \varepsilon_1 \leq \varepsilon_2 \qquad \Sigma; \Delta \vdash \tau_1 \leq \tau_2}{\Sigma; \Delta \vdash \sigma_1 \rightarrow_{\varepsilon_1} \tau_1 \leq \sigma_2 \rightarrow_{\varepsilon_2} \tau_2}$$

TYPING RELATION (1/2)

$$\frac{}{\Sigma; \Delta; \Gamma \vdash () : 1 \ / \ \langle\rangle} \qquad \frac{x : \tau \in \Gamma}{\Sigma; \Delta; \Gamma \vdash x : \tau \ / \ \langle\rangle}$$

$$\frac{op : \sigma \to \tau \in \Sigma(l)}{\Sigma; \Delta; \Gamma \vdash op_l : \sigma \to_{\langle l \rangle} \tau \ / \ \langle\rangle}$$

$$\frac{\Sigma; \Delta; \Gamma, x : \sigma \vdash e : \tau \ / \ \varepsilon}{\Sigma; \Delta; \Gamma \vdash \lambda x.e : \sigma \to_\varepsilon \tau \ / \ \langle\rangle}$$

$$\frac{\Sigma; \Delta; \Gamma \vdash e_1 : \sigma \to_\varepsilon \tau \ / \ \varepsilon \qquad \Sigma; \Delta; \Gamma \vdash e_2 : \sigma \ / \ \varepsilon}{\Sigma; \Delta; \Gamma \vdash e_1 \ e_2 : \tau \ / \ \varepsilon}$$

$$\frac{\Sigma; \Delta, \alpha; \Gamma \vdash e : \tau \ / \ \langle\rangle}{\Sigma; \Delta; \Gamma \vdash \Lambda.e : \forall \alpha.\tau \ / \ \langle\rangle} \qquad \frac{\Sigma; \Delta; \Gamma \vdash e : \forall \alpha.\tau \ / \ \varepsilon}{\Sigma; \Delta; \Gamma \vdash e \ast : \tau\{\varepsilon'/\alpha\} \ / \ \varepsilon}$$

TYPING RELATION (2/2)

$$\frac{\Sigma; \Delta; \Gamma \vdash e : \tau_1 \;/\; \varepsilon_1 \qquad \Sigma; \Delta \vdash \tau_1 \leq \tau_2 \qquad \Sigma; \Delta \vdash \varepsilon_1 \leq \varepsilon_2}{\Sigma; \Delta; \Gamma \vdash e : \tau_2 \;/\; \varepsilon_2}$$

$$\frac{\Sigma; \Delta; \Gamma \vdash e : \tau \;/\; \varepsilon}{\Sigma; \Delta; \Gamma \vdash [e]_l : \tau \;/\; \langle l \mid \varepsilon \rangle}$$

$$\frac{\Sigma; \Delta; \Gamma \vdash e : \sigma \;/\; \langle l \mid \varepsilon \rangle \qquad \Sigma; \Delta; \Gamma \vdash_l h : \tau \;/\; \varepsilon \qquad \Sigma; \Delta; \Gamma, x : \sigma \vdash e_r : \tau \;/\; \varepsilon}{\Sigma; \Delta; \Gamma \vdash \mathrm{handle}_l\; e\; \{h; \mathrm{return}\; x.\, e_r\} : \tau \;/\; \varepsilon}$$

$$\frac{}{\Sigma; \Delta; \Gamma \vdash_l \cdot : \tau \;/\; \varepsilon}$$

$$\frac{\Sigma; \Delta; \Gamma \vdash_l h : \tau \;/\; \varepsilon \qquad \Sigma; \Delta; \Gamma, x : \tau_1, r : \tau_2 \rightarrow_\varepsilon \tau \vdash e : \tau \;/\; \varepsilon}{\Sigma; \Delta; \Gamma \vdash_l op\; x, r.\, e; h : \tau \;/\; \varepsilon}$$

INTERPRETATION OF TYPES

$$\textbf{Type} \equiv \textbf{UPred}(\mathrm{Val}^2)$$

$$\textbf{Eff} \equiv \textbf{UPred}(\mathrm{Exp}^2 \times (\mathcal{EN} \hookrightarrow \mathbb{N})^2 \times \textbf{UPred}(\mathrm{Exp}^2))$$

$$(v_1, v_2) \in [\![1]\!]_\eta \iff v_1 = v_2 = ()$$

$$(v_1, v_2) \in [\![\tau_1 \to_\varepsilon \tau_2]\!]_\eta \iff \forall (u_1, u_2) \in [\![\tau_1]\!]_\eta .\, (v_1\ u_1, v_2\ u_2) \in \mathcal{E}[\![\tau_2 \ / \ \varepsilon]\!]_\eta$$

$$(v_1, v_2) \in [\![\forall \alpha.\tau]\!]_\eta \iff \forall R \in \textbf{Eff}.\, (v_1 *, v_2 *) \in \mathcal{E}[\![\tau \ / \ \langle\rangle]\!]_{\eta[\alpha \mapsto R]}$$

CLOSURE OPERATIONS

$$
\begin{aligned}
(e_1, e_2) \in \mathcal{E}[\![\tau \;/\; \varepsilon]\!]_\eta \;\iff&\\
&\forall (E_1, E_2) \in \mathcal{K}[\![\tau \;/\; \varepsilon]\!]_\eta.\, (E_1[e_1], E_2[e_2]) \in \mathbf{Obs}
\end{aligned}
$$

$$
\begin{aligned}
(E_1, E_2) \in \mathcal{K}[\![\tau \;/\; \varepsilon]\!]_\eta \;\iff&\\
&\forall (v_1, v_2) \in [\![\tau]\!]_\eta.\, (E_1[v_1], E_2[v_2]) \in \mathbf{Obs} \land\\
&\forall (e_1, e_2) \in \mathcal{S}[\![\tau \;/\; \varepsilon]\!]_\eta.\, (E_1[e_1], E_2[e_2]) \in \mathbf{Obs}
\end{aligned}
$$

$$
\begin{aligned}
(E_1[e_1], E_2[e_2]) \in \mathcal{S}[\![\tau \;/\; \varepsilon]\!]_\eta \;\iff&\\
&\exists \rho_1, \rho_2, \mu.\, (e_1, e_2, \rho_1, \rho_2, \mu) \in [\![\varepsilon]\!]_\eta \land\\
&\qquad \rho_1 - \mathrm{free}(E_1) \land \rho_2 - \mathrm{free}(E_2) \land\\
&\qquad \forall (e_1', e_2') \in \mu.\, (E_1[e_1'], E_2[e_2']) \in \triangleright \mathcal{E}[\![\tau \;/\; \varepsilon]\!]_\eta
\end{aligned}
$$

$$
\begin{aligned}
(e_1, e_2) \in \mathbf{Obs} \;\iff&\\
&(e_1 = () \land e_2 \to^* ()) \lor \exists e_1'.(e_1 \to e_1' \land (e_1', e_2) \in \triangleright \mathbf{Obs})
\end{aligned}
$$

INTERPRETATION OF EFFECTS

$$(op_l\ v_1, op_l\ v_2, [l \mapsto 0], [l \mapsto 0], \triangleright[\![\tau_2]\!]_\emptyset) \in [\![l]\!] \iff$$
$$op : \tau_1 \to \tau_2 \in \Sigma(l) \wedge (v_1, v_2) \in \triangleright[\![\tau_1]\!]_\emptyset$$

$$\begin{aligned}
[\![\langle\rangle]\!]_\eta &\equiv \emptyset \\
[\![\alpha]\!]_\eta &\equiv \eta(\alpha) \\
[\![\langle l \mid \varepsilon\rangle]\!]_\eta &\equiv [\![l]\!] \cup [\![\varepsilon]\!]_\eta \uparrow l
\end{aligned}$$

$$(e_1, e_2, \rho_1 \uparrow l, \rho_2 \uparrow l, \mu) \in Q \uparrow l \iff (e_1, e_2, \rho_1, \rho_2, \mu) \in Q,$$

$$\begin{aligned}
(\rho \uparrow l)(l) &= \rho(l) + 1 \\
(\rho \uparrow l)(l') &= \rho(l') \qquad \text{for } l \neq l'.
\end{aligned}$$

THE LOGICAL RELATION

$$(\gamma_1, \gamma_2) \in \mathcal{G}[\![\Gamma]\!]_\eta \iff \text{dom}(\gamma_1) = \text{dom}(\gamma_2) = \text{dom}(\Gamma) \land$$
$$\forall x \in \text{dom}(\Gamma).\, (\gamma_1(x), \gamma_2(x)) \in [\![\Gamma(x)]\!]_\eta$$

$$\Sigma; \Delta; \Gamma \models e_1 \precsim e_2 : \tau \;/\; \varepsilon \equiv$$
$$\forall \eta \in \mathbf{Eff}^{\Delta}.\, \forall(\gamma_1, \gamma_2) \in \mathcal{G}[\![\Gamma]\!]_\eta.\, (e_1\gamma_1, e_2\gamma_2) \in \mathcal{E}[\![\tau \;/\; \varepsilon]\!]_\eta$$

$$\Sigma; \Delta; \Gamma \models e_1 \simeq e_2 : \tau \;/\; \varepsilon \equiv$$
$$\Sigma; \Delta; \Gamma \models e_1 \precsim e_2 : \tau \;/\; \varepsilon \land \Sigma; \Delta; \Gamma \models e_2 \precsim e_1 : \tau \;/\; \varepsilon$$

LEMMA 1

- $[\![\tau]\!]_\eta \subseteq \mathcal{E}[\![\tau \ / \ \varepsilon]\!]_\eta$
- $\mathcal{S}[\![\tau \ / \ \varepsilon]\!]_\eta \subseteq \mathcal{E}[\![\tau \ / \ \varepsilon]\!]_\eta$
- if $e_1 \to e_1'$ then $(e_1', e_2) \in \triangleright\mathcal{E}[\![\tau \ / \ \varepsilon]\!]_\eta \Longrightarrow (e_1, e_2) \in \mathcal{E}[\![\tau \ / \ \varepsilon]\!]_\eta$
- if $e_2 \to e_2'$ then $(e_1, e_2') \in \mathcal{E}[\![\tau \ / \ \varepsilon]\!]_\eta \Longrightarrow (e_1, e_2) \in \mathcal{E}[\![\tau \ / \ \varepsilon]\!]_\eta$

COMPATIBILITY LEMMAS

If $op : \sigma \to \tau \in \Sigma(l)$, then $\Sigma; \Delta; \Gamma \models op_l \precsim op_l : \sigma \to_{\langle l \rangle} \tau \ / \ \langle\rangle$.

If $\Sigma; \Delta; \Gamma \models e_1 \precsim e_2 : \tau \ / \ \varepsilon$, then
$\Sigma; \Delta; \Gamma \models [e_1]_l \precsim [e_2]_l : \tau \ / \ \langle l \mid \varepsilon \rangle$.

Take any expressions e_1, e_2, e_1', e_2' and handlers h_1, h_2 such that:

1. $\Sigma; \Delta; \Gamma \models e_1 \precsim e_2 : \sigma \ / \ \langle l \mid \varepsilon \rangle$,
2. for each $(op : \tau_1 \to \tau_2) \in \Sigma(l)$ there exist $(op\ x, r.\ e_1^h \in h_1)$ and $(op\ x, r.\ e_2^h) \in h_2$ such that
$\Sigma; \Delta; \Gamma, x : \tau_1, r : \tau_2 \to_\varepsilon \tau \models e_1^h \precsim e_2^h : \tau \ / \ \varepsilon$,
3. $\Sigma; \Delta; \Gamma, x : \sigma \models e_1' \precsim e_2' : \tau \ / \ \varepsilon$.

Then $\Sigma; \Delta; \Gamma \models \text{handle}_l\ e_1\ \{h_1; \text{return}\ x.\ e_1'\} \precsim$
$\text{handle}_l\ e_2\ \{h_2; \text{return}\ x.\ e_2'\} : \tau \ / \ \varepsilon$.

MAIN LEMMAS

FUNDAMENTAL: For any expression e, if $\Sigma; \Delta; \Gamma \vdash e : \tau \ / \ \varepsilon$, then $\Sigma; \Delta; \Gamma \models e \simeq e : \tau \ / \ \varepsilon$.

TYPE SOUNDNESS: For any expression e, if $\Sigma; \cdot; \cdot \vdash e : 1 \ / \ \langle\rangle$ and $e \to^* e' \not\to$, then e' is a unit value ($e' = ()$).

SOUNDNESS: For any expressions e_1 and e_2, if $\Sigma; \Delta; \Gamma \models e_1 \simeq e_2 : \tau \ / \ \varepsilon$ holds for all step-indices, then $\Sigma; \Delta; \Gamma \vdash e_1 \simeq e_2 : \tau \ / \ \varepsilon$.