A Stateful Time-Aware Operational Semantics for Temporal Resources

Danel Ahman (University of Tartu, Estonia)

Gašper Žajdela (University of Ljubljana, Slovenia)

MSFP 2024

8 July 2024

Plan for the talk

- Motivation
- Core calculus for temporal resources
- Stateful time-aware operational semantics
- Equational soundness

Motivation

```
let (body, door, windshield) = disassemble (car) in
let (body', door') = paint (body, door) in
delay τ_dry
assemble (body', door', windshield)
```

Motivation

```
let (body, door, windshield) = disassemble (car) in
let (body', door') = paint (body, door) in
delay τ_dry
assemble (body', door', windshield)
```

```
let (body, door, windshield) = disassemble (car) in
let (body', door') = paint (body, door) in
let windshield' = clean (windshield) in      (* τ_dry ≤ τ_clean *)
assemble (body', door', windshield')
```

Core Calculus

Core calculus

Based on:

D. Ahman. *When programs have to watch paint dry*, FoSSaCS (2023) 1-23.

Value	V, W	$::= x$	variable
		$\mid \mathsf{f}(V_1, \ldots, V_n)$	constant
		$\mid () \mid (V, W)$	unit and pair
		$\mid \mathsf{fun}\ (x : X) \mapsto M$	function
Effect handler	H	$::= (x \mathbin{.} k \mathbin{.} M_{\mathsf{op}})_{\mathsf{op} \in \mathcal{O}}$	operation clauses

Core calculus

Computation

$M, N ::=$	$\mathsf{return}\ V$	returning a value
$\mid$	$\mathsf{let}\ x = M\ \mathsf{in}\ N$	sequential composition
$\mid$	$V\ W$	function application
$\mid$	$\mathsf{match}\ V\ \mathsf{with}\ \{(x, y) \mapsto N\}$	product elimination
$\mid$	$\mathsf{op}\ V\ (x\ .\ M)$	algebraic operation call
$\mid$	$\mathsf{handle}\ M\ \mathsf{with}\ H\ \mathsf{to}\ z\ \mathsf{in}\ N$	effect handling
$\mid$	$\mathsf{delay}\ \tau\ M$	**time delay operation**
$\mid$	$\mathsf{box}_{[\tau]\ X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ N$	**boxing up**
$\mid$	$\mathsf{unbox}_{[\tau]\ X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ N$	**unboxing**

Core calculus - **Types**

Time grade: $\tau \in \mathbb{N}$

Ground type $A, B, C ::= \mathsf{b} \mid \mathsf{unit} \mid A \times B \mid [\tau]\, A$

Value type $X, Y, Z ::= A \mid X \times Y \mid X \to Y \,!\, \tau \mid [\tau]\, X$

Computation type: $X \,!\, \tau$

(Variable) context $\Gamma ::= \emptyset \mid \Gamma, x : X \mid \Gamma, \langle \tau \rangle$

Core calculus - **Typing rules**

Important rules

$$\textsc{Let}\quad \frac{\Gamma \vdash M : X \,!\, \tau \qquad \Gamma, \langle\tau\rangle, x : X \vdash N : Y \,!\, \tau'}{\Gamma \vdash \mathsf{let}\ x = M\ \mathsf{in}\ N : Y \,!\, \tau + \tau'}$$

Core calculus - **Typing rules**

Important rules

$$\textsc{Let}\ \frac{\Gamma \vdash M : X \,!\, \tau \qquad \Gamma, \langle \tau \rangle, x : X \vdash N : Y \,!\, \tau'}{\Gamma \vdash \mathsf{let}\ x = M\ \mathsf{in}\ N : Y \,!\, \tau + \tau'}$$

$$\textsc{Op}\ \frac{\Gamma \vdash V : A_{\mathsf{op}} \qquad \Gamma, \langle \tau_{\mathsf{op}} \rangle, x : B_{\mathsf{op}} \vdash M : X \,!\, \tau}{\Gamma \vdash \mathsf{op}\ V\ (x\,.\,M) : X \,!\, \tau_{\mathsf{op}} + \tau}$$

Core calculus - **Typing rules**

Delay

$$\frac{\Gamma, \langle \tau \rangle \vdash M : X \,!\, \tau'}{\Gamma \vdash \mathsf{delay}\ \tau\ M : X \,!\, \tau + \tau'}$$

Core calculus - **Typing rules**

Delay

$$\frac{\Gamma, \langle\tau\rangle \vdash M : X \,!\, \tau'}{\Gamma \vdash \mathsf{delay}\ \tau\ M : X \,!\, \tau + \tau'}$$

Box

$$\frac{\Gamma, \langle\tau\rangle \vdash V : X \qquad \Gamma, x : [\tau]\, X \vdash N : Y \,!\, \tau'}{\Gamma \vdash \mathsf{box}_{[\tau]\, X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ N : Y \,!\, \tau'}$$

Core calculus - **Typing rules**

DELAY

$$\frac{\Gamma, \langle \tau \rangle \vdash M : X \,!\, \tau'}{\Gamma \vdash \textsf{delay}\ \tau\ M : X \,!\, \tau + \tau'}$$

BOX

$$\frac{\Gamma, \langle \tau \rangle \vdash V : X \qquad \Gamma, x : [\tau]\, X \vdash N : Y \,!\, \tau'}{\Gamma \vdash \textsf{box}_{[\tau]\, X}\ V\ \textsf{as}\ x\ \textsf{in}\ N : Y \,!\, \tau'}$$

UNBOX

$$\frac{\tau \leq \tau_{\Gamma} \qquad \Gamma - \tau \vdash V : [\tau]\, X \qquad \Gamma, x : X \vdash N : Y \,!\, \tau'}{\Gamma \vdash \textsf{unbox}_{[\tau]\, X}\ V\ \textsf{as}\ x\ \textsf{in}\ N : Y \,!\, \tau'}$$

Core calculus - **Contexts**

Time substraction

$$\Gamma - 0 \stackrel{\text{def}}{=} \Gamma$$

$$\emptyset - \tau_+ \stackrel{\text{def}}{=} \emptyset$$

$$(\Gamma, x : X) - \tau_+ \stackrel{\text{def}}{=} \Gamma - \tau_+$$

$$(\Gamma, \langle \tau' \rangle) - \tau_+ \stackrel{\text{def}}{=} \begin{cases} \Gamma, \langle \tau' - \tau_+ \rangle, & \text{if } \tau_+ \leq \tau' \\ \Gamma - (\tau_+ - \tau'), & \text{otherwise} \end{cases}$$

Context time

$$\tau_\emptyset \stackrel{\text{def}}{=} 0 \qquad \tau_{(\Gamma, x:X)} \stackrel{\text{def}}{=} \tau_\Gamma \qquad \tau_{(\Gamma, \langle \tau \rangle)} \stackrel{\text{def}}{=} \tau_\Gamma + \tau$$

Core calculus - **Typing rules**

HANDLE

$$\frac{\begin{array}{c}\Gamma \vdash M : X \,!\, \tau \\ \Gamma, \langle\tau\rangle, z : X \vdash N : Y \,!\, \tau' \qquad H = (x \,.\, k \,.\, M_{\mathsf{op}})_{\mathsf{op} \in \mathcal{O}} \\ \left(\forall \tau'' \,.\, \Gamma, x : A_{\mathsf{op}}, k : [\tau_{\mathsf{op}}]\,(B_{\mathsf{op}} \to Y \,!\, \tau'') \vdash M_{\mathsf{op}} : Y \,!\, \tau_{\mathsf{op}} + \tau''\right)_{\mathsf{op} \in \mathcal{O}}\end{array}}{\Gamma \vdash \mathsf{handle}\ M\ \mathsf{with}\ H\ \mathsf{to}\ z\ \mathsf{in}\ N : Y \,!\, \tau + \tau'}$$

Example

```
H := handler {
    | (prepare, body, door, k) → (
        let (body',door') = clean (body, door) in
        let (body'',door'') = paint (body',door') in
        k (body'',door'')
      )
    | (disassemble, car, k) → let y = disassemble (car) in k y
    | ...
} (* Important thing is that τ_clean + τ_paint = τ_prepare *)
handle (
    let (body, door, windshield) = disassemble (car) in
    let (body', door') = prepare (body, door) in
    let windshield' = clean (windshield) in
    assemble (body', door', windshield)
) with H to car in return car
```

Renamings and Admissible Rules

Proposotion

Standard structural rules are admissible

$$\frac{\Gamma, \Gamma' \vdash J \qquad x : X \notin \Gamma, \Gamma'}{\Gamma, x : X, \Gamma' \vdash J} \qquad \frac{\Gamma, x : X, y : Y, \Gamma' \vdash J}{\Gamma, y : Y, x : X, \Gamma' \vdash J}$$

$$\frac{\Gamma, x : X, x' : X, \Gamma' \vdash J}{\Gamma, x : X, \Gamma' \vdash J[x/x']}$$

Renamings and Admissible Rules

Proposotion

Additionally, admissible for the time-graded context modalities

$$\frac{\Gamma, \langle 0 \rangle, \Gamma' \vdash J}{\Gamma, \Gamma' \vdash J} \qquad \frac{\Gamma, \langle \tau_1 + \tau_2 \rangle, \Gamma' \vdash J}{\Gamma, \langle \tau_1 \rangle, \langle \tau_2 \rangle, \Gamma' \vdash J}$$

$$\frac{\Gamma, \langle \tau \rangle, \Gamma' \vdash J \quad \tau \leq \tau'}{\Gamma, \langle \tau' \rangle, \Gamma' \vdash J} \qquad \frac{\Gamma, \langle \tau \rangle, x : X, \Gamma' \vdash J}{\Gamma, x : X, \langle \tau \rangle, \Gamma' \vdash J}$$

Renamings and Admissible Rules

$$\mathsf{Ren}\;\Gamma\;\Gamma' \stackrel{\text{def}}{=} \left\{ \rho : \mathit{vars}(\Gamma) \to \mathit{vars}(\Gamma') \;\middle|\; \begin{array}{c} \tau_{\Gamma} \leq \tau_{\Gamma'} \\ \text{and} \\ \forall (x : X \in \Gamma).\ \rho(x) : X \in \Gamma' \\ \text{and} \\ \tau_{\Gamma_{x,2}} \leq \tau_{\Gamma'_{\rho(x),2}} \end{array} \right\}$$

Note: $\Gamma = \Gamma_{x,1}, x : X, \Gamma_{x,2}$

Stateful Time-Aware Operational Semantics

$$\langle \mathbb{S} \mid M \rangle \rightsquigarrow \langle \mathbb{S}' \mid M' \rangle$$

Stateful Time-Aware Operational Semantics - **States**

States:

$$\mathbb{S} \ ::= \ \emptyset \ \big| \ \mathbb{S}, \langle \tau \rangle \ \big| \ \mathbb{S}, x \mapsto_{[\tau]\,X} V$$

Stateful Time-Aware Operational Semantics - **States**

States:

$$\mathbb{S} \ ::= \ \emptyset \ \big| \ \mathbb{S}, \langle \tau \rangle \ \big| \ \mathbb{S}, x \mapsto_{[\tau]\, X} V$$

Operations on states:

- $\mathbb{S} - \tau$
- $\tau_{\mathbb{S}}$
- $\Gamma_{\mathbb{S}} \overset{\text{def}}{=} \begin{cases} \emptyset, & \text{if } \mathbb{S} = \emptyset \\ \Gamma_{\mathbb{S}'}, \langle \tau \rangle, & \text{if } \mathbb{S} = \mathbb{S}', \langle \tau \rangle \\ \Gamma_{\mathbb{S}'}, x : [\tau]\, X, & \text{if } \mathbb{S} = \mathbb{S}', x \mapsto_{[\tau]\, X} V \end{cases}$

Stateful Time-Aware Operational Semantics - **States**

Proposotion

If $x : X \in \Gamma_{\mathbb{S}}$*, then*

- $X = [\tau]\, Y$ *for some* τ *and* Y*, and*
- $x \mapsto_{[\tau]\, Y} V \in \mathbb{S}$*, for some* V*.*

Proposotion

- *For all* $\mathbb{S}$ *and* τ*, we have* $\Gamma_{\mathbb{S} - \tau} = \Gamma_{\mathbb{S}} - \tau$*.*
- *For all* $\mathbb{S}$ *and* $\mathbb{S}'$*, we have* $\Gamma_{\mathbb{S}, \mathbb{S}'} = \Gamma_{\mathbb{S}}, \Gamma_{\mathbb{S}'}$*.*
- *For all* $\mathbb{S}$*, we have* $\tau_{\Gamma_{\mathbb{S}}} = \tau_{\mathbb{S}}$*.*
- *For all* $\mathbb{S}$ *and* $\mathbb{S}'$*, we have* $\tau_{\mathbb{S}, \mathbb{S}'} = \tau_{\mathbb{S}} + \tau_{\mathbb{S}'}$*.*

Stateful Time-Aware Operational Semantics - **Reduction rules**

Small-step reduction relation $\langle \mathbb{S} \mid M \rangle \rightsquigarrow \langle \mathbb{S}' \mid M' \rangle$.

Stateful Time-Aware Operational Semantics - **Reduction rules**

Small-step reduction relation $\langle \mathbb{S} \mid M \rangle \rightsquigarrow \langle \mathbb{S}' \mid M' \rangle$.

SEM-LET-CONG

$$\frac{\langle \mathbb{S} \mid M \rangle \rightsquigarrow \langle \mathbb{S}' \mid M' \rangle}{\langle \mathbb{S} \mid \mathsf{let}\ x = M\ \mathsf{in}\ N \rangle \rightsquigarrow \langle \mathbb{S}' \mid \mathsf{let}\ x = M'\ \mathsf{in}\ N \rangle}$$

SEM-LET-RET

$$\frac{}{\langle \mathbb{S} \mid \mathsf{let}\ x = (\mathsf{return}\ V)\ \mathsf{in}\ N \rangle \rightsquigarrow \langle \mathbb{S} \mid N[V/x] \rangle}$$

SEM-LET-OP

$$\frac{}{\langle \mathbb{S} \mid \mathsf{let}\ x = (\mathsf{op}\ V\ (y\ .\ M))\ \mathsf{in}\ N \rangle \rightsquigarrow \langle \mathbb{S} \mid \mathsf{op}\ V\ (y\ .\ \mathsf{let}\ x = M\ \mathsf{in}\ N) \rangle}$$

Stateful Time-Aware Operational Semantics - **Reduction rules**

Sem-Delay

$$\frac{}{\langle \mathbb{S} \mid \textsf{delay}\ \tau\ M \rangle \rightsquigarrow \langle \mathbb{S}, \langle \tau \rangle \mid M \rangle}$$

Sem-Box

$$\frac{}{\left\langle \mathbb{S} \mid \textsf{box}_{[\tau]\,X}\ V\ \textsf{as}\ x\ \textsf{in}\ N \right\rangle \rightsquigarrow \left\langle \mathbb{S}, x \mapsto_{[\tau]\,X} V \mid N \right\rangle}$$

Stateful Time-Aware Operational Semantics - **Reduction rules**

SEM-UNBOX

$$\frac{y \in \mathbb{S}}{\left\langle \mathbb{S} \mid \mathsf{unbox}_{[\tau]\,X}\ y\ \mathsf{as}\ x\ \mathsf{in}\ N \right\rangle \rightsquigarrow \langle \mathbb{S} \mid N[\mathbb{S}[y]/x] \rangle}$$

$$\mathbb{S}[x] \stackrel{\text{def}}{=} \begin{cases} V, & \text{if } \mathbb{S} = \mathbb{S}', x \mapsto_{[\tau]\,X} V \\ \mathbb{S}'[x], & \text{if } \mathbb{S} = \mathbb{S}', \langle \tau \rangle \text{ or } \mathbb{S} = \mathbb{S}', y \mapsto_{[\tau]\,X} V \text{ and } x \neq y \\ \text{undefined}, & \text{if } \mathbb{S} = \emptyset \end{cases}$$

Stateful Time-Aware Operational Semantics - **Reduction rules**

SEM-HANDLE-OP

$$\frac{H = (x \,.\, k \,.\, M_{\mathsf{op}})_{\mathsf{op} \in \mathcal{O}}}{\begin{array}{l}\langle \mathbb{S} \mid \mathsf{handle}\ (\mathsf{op}\ V\ (y \,.\, M))\ \mathsf{with}\ H\ \mathsf{to}\ z\ \mathsf{in}\ N \rangle \rightsquigarrow \\ \langle \mathbb{S} \mid \mathsf{box}\ \big(\mathsf{fun}\ (y : B_{\mathsf{op}}) \mapsto \mathsf{handle}\ M\ \mathsf{with}\ H\ \mathsf{to}\ z\ \mathsf{in}\ N\big) \\ \qquad\qquad \mathsf{as}\ w\ \mathsf{in}\ M_{\mathsf{op}}[V/x, w/k] \rangle\end{array}}$$

$$\frac{\begin{array}{c}\Gamma \vdash M : X \,!\, \tau \\ \Gamma, \langle \tau \rangle, z : X \vdash N : Y \,!\, \tau' \qquad H = (x \,.\, k \,.\, M_{\mathsf{op}})_{\mathsf{op} \in \mathcal{O}} \\ \big(\forall \tau'' \,.\, \Gamma, x : A_{\mathsf{op}}, k : [\tau_{\mathsf{op}}]\,(B_{\mathsf{op}} \to Y \,!\, \tau'') \vdash M_{\mathsf{op}} : Y \,!\, \tau_{\mathsf{op}} + \tau''\big)_{\mathsf{op} \in \mathcal{O}}\end{array}}{\Gamma \vdash \mathsf{handle}\ M\ \mathsf{with}\ H\ \mathsf{to}\ z\ \mathsf{in}\ N : Y \,!\, \tau + \tau'}$$

Type Safety

Stateful Time-Aware Operational Semantics - **Progress**

Theorem (Progress theorem)

If $\vdash \mathbb{S}$ *and* $\Gamma_{\mathbb{S}} \vdash M : X \,!\, \tau$*, then either*

- *M is in a result form, or*
- *we can make step* $\langle \mathbb{S} \mid M \rangle \rightsquigarrow \langle \mathbb{S}' \mid M' \rangle$*, for some* $\mathbb{S}'$ *and* M'*.*

Result form is either an **operation call** or a **returned value**.

Stateful Time-Aware Operational Semantics - **Preservation**

Theorem (Preservation theorem)

If $\vdash \mathbb{S}$ *and* $\Gamma_{\mathbb{S}} \vdash M : X \,!\, \tau$*, and if* $\langle \mathbb{S} \mid M \rangle \rightsquigarrow \langle \mathbb{S}' \mid M' \rangle$*, for some* $\mathbb{S}'$ *and* M'*, then*

- $\vdash \mathbb{S}'$,
- *there exists a* τ'*, such that* $\tau_{\mathbb{S}} + \tau = \tau_{\mathbb{S}'} + \tau'$*, and*
- $\Gamma_{\mathbb{S}'} \vdash M' : X \,!\, \tau'$.

Equational Soundness

$$\langle \mathbb{S} \mid M \rangle \rightsquigarrow \langle \mathbb{S}' \mid M' \rangle$$
$$\Downarrow$$
$$\vdash \mathbb{K}_{\mathbb{S}}[M] \equiv \mathbb{K}_{\mathbb{S}'}[M'] : X \,!\, (\tau_{\mathbb{S}} + \tau)$$

Equational Soundness - **Equational theory**

Equations for well-typed terms:

$$\Gamma \vdash V \equiv W : X \qquad\qquad \Gamma \vdash M \equiv N : X\,!\,\tau.$$

Equational Soundness - **Equational theory**

Equations for well-typed terms:

$$\Gamma \vdash V \equiv W : X \qquad \Gamma \vdash M \equiv N : X \,!\, \tau.$$

We have:

- congruence rules
- standard β-equations and η-equations for the non-modal $\lambda_{[\tau]}$-values and $\lambda_{[\tau]}$-computations as in FGCBV

Equational Soundness - **Equational theory**

- standard equations for computation terms (let, handle)

Equational Soundness - **Equational theory**

- standard equations for computation terms (let, handle)

$$\text{handle } (\text{return } V) \text{ with } H \text{ to } z \text{ in } N \equiv N[V/z]$$

Equational Soundness - **Equational theory**

- standard equations for computation terms (let, handle)

$$\text{handle } (\text{return } V) \text{ with } H \text{ to } z \text{ in } N \equiv N[V/z]$$

$$\text{handle } (\mathsf{op}\ V\ (y\ .\ M)) \text{ with } H \text{ to } z \text{ in } N \equiv$$

$$\text{box } \big(\text{fun } (y : B_{\mathsf{op}}) \mapsto \text{handle } M \text{ with } H \text{ to } z \text{ in } N\big)$$

$$\text{as } w \text{ in } M_{\mathsf{op}}[V/x, w/k],$$

where $H = (x\ .\ k\ .\ M_{\mathsf{op}})_{\mathsf{op} \in \mathcal{O}}$ and $y \notin fv(H), y \notin fv(N)$

Equational Soundness - **Equational theory**

- equations describing interactions of delay

$$\mathsf{let}\ x = (\mathsf{delay}\ \tau\ M)\ \mathsf{in}\ N \equiv \mathsf{delay}\ \tau\ (\mathsf{let}\ x = M\ \mathsf{in}\ N)$$

$$\mathsf{handle}\ (\mathsf{delay}\ \tau\ M)\ \mathsf{with}\ H\ \mathsf{to}\ z\ \mathsf{in}\ N \equiv \mathsf{delay}\ \tau\ (\mathsf{handle}\ M\ \mathsf{with}\ H\ \mathsf{to}\ z\ \mathsf{in}\ N)$$

$$\mathsf{delay}\ 0\ M \equiv M$$

$$\mathsf{delay}\ \tau\ (\mathsf{delay}\ \tau'\ M) \equiv \mathsf{delay}\ (\tau + \tau')\ M$$

- equations describing behaviour of box and unbox (displayed later)

Equational Soundness - **Computational context**

$$
\begin{aligned}
\textbf{Computational context } \mathbb{K} \;::=\;& [\,] \\
\mid\;& \mathsf{op}\ V\ (x\,.\,\mathbb{K}) \\
\mid\;& \mathsf{delay}\ \tau\ \mathbb{K} \\
\mid\;& \mathsf{box}_{[\tau]\,X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ \mathbb{K} \\
\mid\;& \mathsf{unbox}_{[\tau]\,X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ \mathbb{K}
\end{aligned}
$$

Comp. context time: $\tau_{\mathbb{K}}$

Bounded variables: $\Gamma_{\mathbb{K}}$

Equational soundness - **Computational context**

Composition operation: $\mathbb{K}[\mathbb{K}']$

Hole filling operation: $\mathbb{K}[M]$

Proposotion

- *If* $\Gamma \vdash \mathbb{K} : \tau$ *and* $\Gamma, \Gamma_{\mathbb{K}} \vdash \mathbb{K}' : \tau'$, *then* $\Gamma \vdash \mathbb{K}[\mathbb{K}'] : \tau + \tau'$.
- *If* $\Gamma \vdash \mathbb{K} : \tau$ *and* $\Gamma, \Gamma_{\mathbb{K}} \vdash M : X \,!\, \tau'$, *then* $\Gamma \vdash \mathbb{K}[M] : X \,!\, \tau + \tau'$.

Judgements are polymorphic in type of return values!

Equational soundness - **Equational theory**

Equations of box and unbox:

$$\mathsf{let}\ x = (\mathsf{box}_{[\tau]\,X}\ V\ \mathsf{as}\ y\ \mathsf{in}\ M)\ \mathsf{in}\ N \equiv \mathsf{box}_{[\tau]\,X}\ V\ \mathsf{as}\ y\ \mathsf{in}\ (\mathsf{let}\ x = M\ \mathsf{in}\ N)$$

$$\mathsf{let}\ x = (\mathsf{unbox}_{[\tau]\,X}\ V\ \mathsf{as}\ y\ \mathsf{in}\ M)\ \mathsf{in}\ N \equiv \mathsf{unbox}_{[\tau]\,X}\ V\ \mathsf{as}\ y\ \mathsf{in}\ (\mathsf{let}\ x = M\ \mathsf{in}\ N)$$

$$\mathsf{handle}\ (\mathsf{box}_{[\tau]\,X}\ V\ \mathsf{as}\ y\ \mathsf{in}\ M)\ \mathsf{with}\ H\ \mathsf{to}\ z\ \mathsf{in}\ N \equiv \mathsf{box}_{[\tau]\,X}\ V\ \mathsf{as}\ y\ \mathsf{in}\ (\mathsf{handle}\ M\ \mathsf{with}\ H\ \mathsf{to}\ z\ \mathsf{in}\ N)$$

$$\mathsf{handle}\ (\mathsf{unbox}_{[\tau]\,X}\ V\ \mathsf{as}\ y\ \mathsf{in}\ M)\ \mathsf{with}\ H\ \mathsf{to}\ z\ \mathsf{in}\ N \equiv \mathsf{unbox}_{[\tau]\,X}\ V\ \mathsf{as}\ y\ \mathsf{in}\ (\mathsf{handle}\ M\ \mathsf{with}\ H\ \mathsf{to}\ z\ \mathsf{in}\ N)$$

(with $y \notin fv(N)$ in all four equations)

Equational soundness - **Equational theory**

Equations of box and unbox:

$$\text{box}_{[\tau]\,X}\ V\ \text{as}\ x\ \text{in}\ (\text{box}_{[\tau']\,Y}\ W\ \text{as}\ y\ \text{in}\ N) \equiv$$
$$\text{box}_{[\tau']\,Y}\ W\ \text{as}\ y\ \text{in}\ (\text{box}_{[\tau]\,X}\ V\ \text{as}\ x\ \text{in}\ N)$$

$$\text{unbox}_{[\tau]\,X}\ V\ \text{as}\ x\ \text{in}\ (\text{unbox}_{[\tau']\,X'}\ W\ \text{as}\ y\ \text{in}\ N) \equiv$$
$$\text{unbox}_{[\tau']\,X'}\ W\ \text{as}\ y\ \text{in}\ (\text{unbox}_{[\tau]\,X}\ V\ \text{as}\ x\ \text{in}\ N)$$

$$\text{box}_{[\tau]\,X}\ V\ \text{as}\ x\ \text{in}\ (\text{unbox}_{[\tau']\,X'}\ W\ \text{as}\ y\ \text{in}\ N) \equiv$$
$$\text{unbox}_{[\tau']\,X'}\ W\ \text{as}\ y\ \text{in}\ (\text{box}_{[\tau]\,X}\ V\ \text{as}\ x\ \text{in}\ N)$$

(with $x \notin fv(W), y \notin fv(V)$ in all three equations)

Equational soundness - **Equational theory**

Equations of box and unbox:

$$\mathsf{box}_{[\tau]\,X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ \mathbb{K}[\mathsf{unbox}_{[\tau]\,X}\ x\ \mathsf{as}\ y\ \mathsf{in}\ N] \equiv \mathsf{box}_{[\tau]\,X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ \mathbb{K}[N[V/y]] \quad (\tau_{\mathbb{K}} \geq \tau)$$

$$\mathsf{box}_{[\tau]\,X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ N \equiv N \qquad (x \notin fv(N))$$

$$\mathsf{unbox}_{[\tau]\,X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ N \equiv N \qquad (x \notin fv(N))$$

$$\mathsf{unbox}_{[\tau]\,X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ (\mathsf{unbox}_{[\tau]\,X}\ V\ \mathsf{as}\ y\ \mathsf{in}\ N) \equiv \mathsf{unbox}_{[\tau]\,X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ N[x/y]$$

Equational soundness - **Computational context**

Proposotion

If $\Gamma \vdash \mathbb{K} : \tau$ *and* $\Gamma, \Gamma_{\mathbb{K}} \vdash M \equiv N : X \,!\, \tau'$*, then we have*

$$\Gamma \vdash \mathbb{K}[M] \equiv \mathbb{K}[N] : X \,!\, \tau + \tau'.$$

Proposotion

If $\Gamma \vdash \mathbb{K} : \tau$ *and* $\Gamma, \Gamma_{\mathbb{K}} \vdash M : X \,!\, \tau'$ *and* $\Gamma, \langle \tau + \tau' \rangle, x : X \vdash N : Y \,!\, \tau''$*, then we have the algebraicity equation*

$$\Gamma \vdash \mathsf{let}\ x = \mathbb{K}[M]\ \mathsf{in}\ N \equiv \mathbb{K}[\mathsf{let}\ x = M\ \mathsf{in}\ N] : Y \,!\, \tau + \tau' + \tau''.$$

Equational soundness - **Computational context**

Translation from state to computational context:

$$\mathbb{K}_{\mathbb{S}} \stackrel{\text{def}}{=} \begin{cases} [\,], & \text{if } \mathbb{S} = \emptyset \\ \mathbb{K}_{\mathbb{S}'}[\textsf{delay}\ \tau\ [\,]], & \text{if } \mathbb{S} = \mathbb{S}', \langle\tau\rangle \\ \mathbb{K}_{\mathbb{S}'}[\textsf{box}_{[\tau]\,X}\ V\ \textsf{as}\ x\ \textsf{in}\ [\,]], & \text{if } \mathbb{S} = \mathbb{S}', x \mapsto_{[\tau]\,X} V \end{cases}$$

Equational soundness - **Computational context**

Translation from state to computational context:

$$\mathbb{K}_{\mathbb{S}} \stackrel{\text{def}}{=} \begin{cases} [\,], & \text{if } \mathbb{S} = \emptyset \\ \mathbb{K}_{\mathbb{S}'}[\mathsf{delay}\ \tau\ [\,]], & \text{if } \mathbb{S} = \mathbb{S}', \langle\tau\rangle \\ \mathbb{K}_{\mathbb{S}'}[\mathsf{box}_{[\tau]\,X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ [\,]], & \text{if } \mathbb{S} = \mathbb{S}', x \mapsto_{[\tau]\,X} V \end{cases}$$

Proposotion

- *For all* $\mathbb{S}$ *and* $\mathbb{S}'$*, we have* $\mathbb{K}_{\mathbb{S},\mathbb{S}'} = \mathbb{K}_{\mathbb{S}}[\mathbb{K}_{\mathbb{S}'}]$ *and* $\Gamma_{\mathbb{K}_{\mathbb{S}}} = \Gamma_{\mathbb{S}}$.
- $\Rightarrow$ *If* $\mathbb{S} = \mathbb{S}', x \mapsto_{[\tau]\,X} V, \mathbb{S}''$*, then we have* $\mathbb{K}_{\mathbb{S}} = \mathbb{K}_{\mathbb{S}'}[\mathsf{box}_{[\tau]\,X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ \mathbb{K}_{\mathbb{S}''}]$.

Equational soundness - **Soundness theorem**

Theorem

If $\vdash \mathbb{S}$ *and* $\Gamma_{\mathbb{S}} \vdash M : X \,!\, \tau$ *and* $\langle \mathbb{S} \mid M \rangle \rightsquigarrow \langle \mathbb{S}' \mid M' \rangle$*, then*

$$\vdash \mathbb{K}_{\mathbb{S}}[M] \equiv \mathbb{K}_{\mathbb{S}'}[M'] : X \,!\, (\tau_{\mathbb{S}} + \tau).$$

Equational soundness - **Soundness theorem**

Theorem

If $\vdash \mathbb{S}$ *and* $\Gamma_{\mathbb{S}} \vdash M : X \,!\, \tau$ *and* $\langle \mathbb{S} \mid M \rangle \rightsquigarrow \langle \mathbb{S}' \mid M' \rangle$, *then*

$$\vdash \mathbb{K}_{\mathbb{S}}[M] \equiv \mathbb{K}_{\mathbb{S}'}[M'] : X \,!\, (\tau_{\mathbb{S}} + \tau).$$

Almost works ...

Equational soundness - **Soundness theorem**

Case SEM-LET-CONG

We have:

- $M \rightsquigarrow M'$
- $\Rightarrow \vdash \mathbb{K}_{\mathbb{S}}[M] \equiv \mathbb{K}_{\mathbb{S}'}[M']$ (induction hypothesis)
- $\Rightarrow \vdash \mathbb{K}_{\mathbb{S}}[M] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{K}_{\mathbb{S}''}[M']]$

Equational soundness - **Soundness theorem**

Case Sem-Let-Cong

We have:

- $M \leadsto M'$
- $\Rightarrow\ \vdash \mathbb{K}_{\mathbb{S}}[M] \equiv \mathbb{K}_{\mathbb{S}'}[M']$ (induction hypothesis)
- $\Rightarrow\ \vdash \mathbb{K}_{\mathbb{S}}[M] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{K}_{\mathbb{S}''}[M']]$

We want:

- $\vdash \mathbb{K}_{\mathbb{S}}[\mathsf{let}\ x = M\ \mathsf{in}\ N] \equiv \mathbb{K}_{\mathbb{S}'}[\mathsf{let}\ x = M'\ \mathsf{in}\ N]$
- $\iff \vdash \mathbb{K}_{\mathbb{S}}[\mathsf{let}\ x = M\ \mathsf{in}\ N] \equiv \mathbb{K}_{\mathbb{S}}[\mathsf{let}\ x = \mathbb{K}_{\mathbb{S}''}[M']\ \mathsf{in}\ N]$
- $\Leftarrow \Gamma_{\mathbb{K}_{\mathbb{S}}} \vdash \mathsf{let}\ x = M\ \mathsf{in}\ N \equiv \mathsf{let}\ x = \mathbb{K}_{\mathbb{S}''}[M']\ \mathsf{in}\ N$

We are stuck with $\Gamma_{\mathbb{K}_{\mathbb{S}}} \vdash M \equiv \mathbb{K}_{\mathbb{S}''}[M']$

Equational soundness - **Evaluation context**

Evaluation context $\mathbb{E} ::= [\,]$

$\quad\mid \text{let } x = \mathbb{E} \text{ in } N$

$\quad\mid \text{handle } \mathbb{E} \text{ with } H \text{ to } z \text{ in } N$

Equational soundness - **Evaluation context**

$$\mathbb{E} ::= [\,] \;\big|\; \textsf{let } x = \mathbb{E} \textsf{ in } N \;\big|\; \textsf{handle } \mathbb{E} \textsf{ with } H \textsf{ to } z \textsf{ in } N$$

Proposotion

If $\Gamma \vdash_{[X!\tau]} \mathbb{E} : Y \,!\, \tau'$ *and* $\Gamma \vdash M \equiv N : X \,!\, \tau$*, then*

$$\Gamma \vdash \mathbb{E}[M] \equiv \mathbb{E}[N] : Y \,!\, \tau'.$$

Equational soundness - **Evaluation context**

$$\mathbb{E} ::= [\,] \mid \text{let } x = \mathbb{E} \text{ in } N \mid \text{handle } \mathbb{E} \text{ with } H \text{ to } z \text{ in } N$$

Proposotion

If $\Gamma \vdash_{[X!\tau]} \mathbb{E} : Y \,!\, \tau'$ *and* $\Gamma \vdash M \equiv N : X \,!\, \tau$*, then*

$$\Gamma \vdash \mathbb{E}[M] \equiv \mathbb{E}[N] : Y \,!\, \tau'.$$

Proposotion

If $\Gamma \vdash_{[Y!\tau']} \mathbb{E} : Z \,!\, \tau''$ *and* $\Gamma - \tau \vdash V : [\tau]\, X$ *and* $\Gamma, x : X \vdash N : Y \,!\, \tau'$*,*
then we have the equation

$$\Gamma \vdash \mathbb{E}[\text{unbox}_{[\tau]\,X}\; V \text{ as } x \text{ in } N] \equiv \text{unbox}_{[\tau]\,X}\; V \text{ as } x \text{ in } \mathbb{E}[N] : Z \,!\, \tau'',$$

and similarly for box *and* delay.

Equational soundness - **Soundness theorem**

Theorem

If

- $\vdash \mathbb{S}$, *and*
- $\Gamma_{\mathbb{S}} \vdash M : X \,!\, \tau$, *and*
- $\langle \mathbb{S} \mid M \rangle \rightsquigarrow \langle \mathbb{S}' \mid M' \rangle$, *for some* $\mathbb{S}'$ *and* M', *with* $\mathbb{S}' = \mathbb{S}, \mathbb{S}''$,

then for every evaluation context $\Gamma_{\mathbb{S}} \vdash_{[X!\tau]} \mathbb{E} : Y \,!\, \tau'$, *we have*

$$\vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}[M]] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathbb{K}_{\mathbb{S}''}[M']]] : Y \,!\, (\tau_{\mathbb{S}} + \tau').$$

Proof of soundness theorem.

SEM-LET-CONG

- $M = \mathsf{let}\ x = N\ \mathsf{in}\ P$ and $M' = \mathsf{let}\ x = N'\ \mathsf{in}\ P$

Proof of soundness theorem.

SEM-LET-CONG

- $M = \mathsf{let}\ x = N\ \mathsf{in}\ P$ and $M' = \mathsf{let}\ x = N'\ \mathsf{in}\ P$
- $\langle \mathbb{S} \mid N \rangle \rightsquigarrow \langle \mathbb{S}' \mid N' \rangle$

Proof of soundness theorem.

SEM-LET-CONG

- $M = \text{let } x = N \text{ in } P$ and $M' = \text{let } x = N' \text{ in } P$
- $\langle \mathbb{S} \mid N \rangle \rightsquigarrow \langle \mathbb{S}' \mid N' \rangle$
- $\Rightarrow \forall \mathbb{E}' .\ \vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}'[N]] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}'[\mathbb{K}_{\mathbb{S}''}[N']]] : Z \,!\, (\tau_{\mathbb{S}} + \tau'')$ (I. H.)

Proof of soundness theorem.

SEM-LET-CONG

- $M = \textsf{let}\ x = N\ \textsf{in}\ P$ and $M' = \textsf{let}\ x = N'\ \textsf{in}\ P$
- $\langle \mathbb{S} \mid N \rangle \rightsquigarrow \langle \mathbb{S}' \mid N' \rangle$
- $\Rightarrow \forall \mathbb{E}' .\ \vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}'[N]] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}'[\mathbb{K}_{\mathbb{S}''}[N']]] : Z\,!\,(\tau_{\mathbb{S}} + \tau'')$ (I. H.)
- $\mathbb{E}' \stackrel{\text{def}}{=} \mathbb{E}[\textsf{let}\ x = [\,]\ \textsf{in}\ P]$

Proof of soundness theorem.

SEM-LET-CONG

- $M = \mathsf{let}\ x = N\ \mathsf{in}\ P$ and $M' = \mathsf{let}\ x = N'\ \mathsf{in}\ P$
- $\langle \mathbb{S} \mid N \rangle \rightsquigarrow \langle \mathbb{S}' \mid N' \rangle$
- $\Rightarrow \forall \mathbb{E}' .\ \vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}'[N]] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}'[\mathbb{K}_{\mathbb{S}''}[N']]] : Z\,!\,(\tau_{\mathbb{S}} + \tau'')$ (I. H.)
- $\mathbb{E}' \stackrel{\text{def}}{=} \mathbb{E}[\mathsf{let}\ x = [\,]\ \mathsf{in}\ P]$
- $\Rightarrow \vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathsf{let}\ x = N\ \mathsf{in}\ P]] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathsf{let}\ x = \mathbb{K}_{\mathbb{S}''}[N']\ \mathsf{in}\ P]] : Y\,!\,(\tau_{\mathbb{S}} + \tau')$

Proof of soundness theorem.

Sem-Let-Cong

- $M = \mathsf{let}\ x = N\ \mathsf{in}\ P$ and $M' = \mathsf{let}\ x = N'\ \mathsf{in}\ P$
- $\langle \mathbb{S} \mid N \rangle \rightsquigarrow \langle \mathbb{S}' \mid N' \rangle$
- $\Rightarrow \forall \mathbb{E}' .\ \vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}'[N]] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}'[\mathbb{K}_{\mathbb{S}''}[N']]] : Z\,!\,(\tau_{\mathbb{S}} + \tau'')$ (I. H.)
- $\mathbb{E}' \stackrel{\text{def}}{=} \mathbb{E}[\mathsf{let}\ x = [\,]\ \mathsf{in}\ P]$
- $\Rightarrow \vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathsf{let}\ x = N\ \mathsf{in}\ P]] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathsf{let}\ x = \mathbb{K}_{\mathbb{S}''}[N']\ \mathsf{in}\ P]] : Y\,!\,(\tau_{\mathbb{S}} + \tau')$
- $\Rightarrow \vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}[M]] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathbb{K}_{\mathbb{S}''}[M']]] : Y\,!\,(\tau_{\mathbb{S}} + \tau')$

Proof of soundness theorem - continuation.

SEM-DELAY

- $M = \text{delay}\ \tau_1\ M'$
- $\Rightarrow \mathbb{K}_{\mathbb{S}''} = \text{delay}\ \tau_1\ [\,]$
- $\Rightarrow \vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}[M]] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\text{delay}\ \tau_1\ M']] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathbb{K}_{\mathbb{S}''}[M']]] : Y\,!\,(\tau_{\mathbb{S}} + \tau')$

Proof of soundness theorem - continuation.

SEM-DELAY

- $M = \text{delay}\ \tau_1\ M'$
- $\Rightarrow \mathbb{K}_{\mathbb{S}''} = \text{delay}\ \tau_1\ [\,]$
- $\Rightarrow \vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}[M]] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\text{delay}\ \tau_1\ M']] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathbb{K}_{\mathbb{S}''}[M']]] : Y\,!\,(\tau_{\mathbb{S}} + \tau')$

SEM-BOX

- $M = \text{box}_{[\tau'']X'}\ V \text{ as } x \text{ in } M'$
- $\Rightarrow \mathbb{K}_{\mathbb{S}''} = \text{box}_{[\tau'']X'}\ V \text{ as } x \text{ in } [\,]$
- $\Rightarrow \vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}[M]] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\text{box}_{[\tau'']X'}\ V \text{ as } x \text{ in } M']] \equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathbb{K}_{\mathbb{S}''}[M']]] : Y\,!\,(\tau_{\mathbb{S}} + \tau')$

Proof of soundness theorem - continuation.

SEM-UNBOX

- $M = \mathsf{unbox}_{[\tau''] X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ N$ and $M' = N[\mathbb{S}[y]/x]$ and $\mathbb{S}' = \mathbb{S}$

Proof of soundness theorem - continuation.

SEM-UNBOX

- $M = \mathsf{unbox}_{[\tau''] X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ N$ and $M' = N[\mathbb{S}[y]/x]$ and $\mathbb{S}' = \mathbb{S}$

- $\Rightarrow y : [\tau''] X' \in \Gamma_{\mathbb{S}} - \tau''$ and $\Gamma_{\mathbb{S}}, x : X' \vdash N : [\tau] X$ (inversion)

Proof of soundness theorem - continuation.

SEM-UNBOX

- $M = \text{unbox}_{[\tau''] X'}\ y\ \text{as}\ x\ \text{in}\ N$ and $M' = N[\mathbb{S}[y]/x]$ and $\mathbb{S}' = \mathbb{S}$
- $\Rightarrow y : [\tau''] X' \in \Gamma_{\mathbb{S}} - \tau''$ and $\Gamma_{\mathbb{S}}, x : X' \vdash N : [\tau] X$ (inversion)
- $\Rightarrow \Gamma_{\mathbb{S}} \vdash \mathbb{S}[y] : X'$

Proof of soundness theorem - continuation.

SEM-UNBOX

- $M = \mathsf{unbox}_{[\tau''] X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ N$ and $M' = N[\mathbb{S}[y]/x]$ and $\mathbb{S}' = \mathbb{S}$
- $\Rightarrow y : [\tau''] X' \in \Gamma_{\mathbb{S}} - \tau''$ and $\Gamma_{\mathbb{S}}, x : X' \vdash N : [\tau] X$ (inversion)
- $\Rightarrow \Gamma_{\mathbb{S}} \vdash \mathbb{S}[y] : X'$
- $\Gamma_{\mathbb{S}} = (\Gamma_{\mathbb{S}})_{y,1}, y : [\tau''] X', (\Gamma_{\mathbb{S}})_{y,2}$

Proof of soundness theorem - continuation.

Sem-Unbox

- $M = \mathsf{unbox}_{[\tau''] X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ N$ and $M' = N[\mathbb{S}[y]/x]$ and $\mathbb{S}' = \mathbb{S}$
- $\Rightarrow y : [\tau''] X' \in \Gamma_{\mathbb{S}} - \tau''$ and $\Gamma_{\mathbb{S}}, x : X' \vdash N : [\tau] X$ (inversion)
- $\Rightarrow \Gamma_{\mathbb{S}} \vdash \mathbb{S}[y] : X'$
- $\Gamma_{\mathbb{S}} = (\Gamma_{\mathbb{S}})_{y,1}, y : [\tau''] X', (\Gamma_{\mathbb{S}})_{y,2}$
- $\Rightarrow \mathbb{S} = \mathbb{S}_{y,1}, y \mapsto_{[\tau''] X'} \mathbb{S}[y], \mathbb{S}_{y,2}$

Proof of soundness theorem - continuation.

SEM-UNBOX

- $M = \mathsf{unbox}_{[\tau''] X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ N$ and $M' = N[\mathbb{S}[y]/x]$ and $\mathbb{S}' = \mathbb{S}$
- $\Rightarrow y : [\tau''] X' \in \Gamma_{\mathbb{S}} - \tau''$ and $\Gamma_{\mathbb{S}}, x : X' \vdash N : [\tau] X$ (inversion)
- $\Rightarrow \Gamma_{\mathbb{S}} \vdash \mathbb{S}[y] : X'$
- $\Gamma_{\mathbb{S}} = (\Gamma_{\mathbb{S}})_{y,1}, y : [\tau''] X', (\Gamma_{\mathbb{S}})_{y,2}$
- $\Rightarrow \mathbb{S} = \mathbb{S}_{y,1}, y \mapsto_{[\tau''] X'} \mathbb{S}[y], \mathbb{S}_{y,2}$
- $\mathbb{K}_{\mathbb{S}''} = [\,]$

Proof of soundness theorem - continuation.

$\vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathsf{unbox}_{[\tau'']\,X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ N]]$

Proof of soundness theorem - continuation.

$$\vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathsf{unbox}_{[\tau'']\,X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ N]]$$

$$\equiv \mathbb{K}_{\mathbb{S}}[\mathsf{unbox}_{[\tau'']\,X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ \mathbb{E}[N]]$$

Proof of soundness theorem - continuation.

$$\vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\textsf{unbox}_{[\tau'']\,X'}\; y \;\textsf{as}\; x \;\textsf{in}\; N]]$$

$$\equiv \mathbb{K}_{\mathbb{S}}[\textsf{unbox}_{[\tau'']\,X'}\; y \;\textsf{as}\; x \;\textsf{in}\; \mathbb{E}[N]]$$

$$\equiv \mathbb{K}_{\mathbb{S}_{y},1}[\textsf{box}_{[\tau'']\,X'}\; \mathbb{S}[y] \;\textsf{as}\; y \;\textsf{in}\; \mathbb{K}_{\mathbb{S}_{y},2}[\textsf{unbox}_{[\tau'']\,X'}\; y \;\textsf{as}\; x \;\textsf{in}\; \mathbb{E}[N]]]$$

Proof of soundness theorem - continuation.

$\vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathsf{unbox}_{[\tau'']\,X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ N]]$

$\equiv \mathbb{K}_{\mathbb{S}}[\mathsf{unbox}_{[\tau'']\,X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ \mathbb{E}[N]]$

$\equiv \mathbb{K}_{\mathbb{S}_{y},1}[\mathsf{box}_{[\tau'']\,X'}\ \mathbb{S}[y]\ \mathsf{as}\ y\ \mathsf{in}\ \mathbb{K}_{\mathbb{S}_{y},2}[\mathsf{unbox}_{[\tau'']\,X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ \mathbb{E}[N]]]$

$\equiv \mathbb{K}_{\mathbb{S}_{y},1}[\mathsf{box}_{[\tau'']\,X'}\ \mathbb{S}[y]\ \mathsf{as}\ y\ \mathsf{in}\ \mathbb{K}_{\mathbb{S}_{y},2}[\mathbb{E}[N[\mathbb{S}[y]/x]]]]$

Proof of soundness theorem - continuation.

$\vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathsf{unbox}_{[\tau'']\,X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ N]]$

$\equiv \mathbb{K}_{\mathbb{S}}[\mathsf{unbox}_{[\tau'']\,X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ \mathbb{E}[N]]$

$\equiv \mathbb{K}_{\mathbb{S}_{y},1}[\mathsf{box}_{[\tau'']\,X'}\ \mathbb{S}[y]\ \mathsf{as}\ y\ \mathsf{in}\ \mathbb{K}_{\mathbb{S}_{y},2}[\mathsf{unbox}_{[\tau'']\,X'}\ y\ \mathsf{as}\ x\ \mathsf{in}\ \mathbb{E}[N]]]$

$\equiv \mathbb{K}_{\mathbb{S}_{y},1}[\mathsf{box}_{[\tau'']\,X'}\ \mathbb{S}[y]\ \mathsf{as}\ y\ \mathsf{in}\ \mathbb{K}_{\mathbb{S}_{y},2}[\mathbb{E}[N[\mathbb{S}[y]/x]]]]$

$\equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}[N[\mathbb{S}[y]/x]]]$

Proof of soundness theorem - continuation.

$$\vdash \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\textsf{unbox}_{[\tau'']\,X'}\; y \;\textsf{as}\; x \;\textsf{in}\; N]]$$

$$\equiv \mathbb{K}_{\mathbb{S}}[\textsf{unbox}_{[\tau'']\,X'}\; y \;\textsf{as}\; x \;\textsf{in}\; \mathbb{E}[N]]$$

$$\equiv \mathbb{K}_{\mathbb{S}_{y,1}}[\textsf{box}_{[\tau'']\,X'}\; \mathbb{S}[y] \;\textsf{as}\; y \;\textsf{in}\; \mathbb{K}_{\mathbb{S}_{y,2}}[\textsf{unbox}_{[\tau'']\,X'}\; y \;\textsf{as}\; x \;\textsf{in}\; \mathbb{E}[N]]]$$

$$\equiv \mathbb{K}_{\mathbb{S}_{y,1}}[\textsf{box}_{[\tau'']\,X'}\; \mathbb{S}[y] \;\textsf{as}\; y \;\textsf{in}\; \mathbb{K}_{\mathbb{S}_{y,2}}[\mathbb{E}[N[\mathbb{S}[y]/x]]]]$$

$$\equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}[N[\mathbb{S}[y]/x]]]$$

$$\equiv \mathbb{K}_{\mathbb{S}}[\mathbb{E}[\mathbb{K}_{\mathbb{S}''}[M']]] : Y \,!\, (\tau_{\mathbb{S}} + \tau')$$

$\square$

Equational soundness - **Soundness theorem**

Take $\mathbb{E} = [\,]$ and we get soundness theorem as a colloraly.

Theorem

If $\vdash \mathbb{S}$ *and* $\Gamma_{\mathbb{S}} \vdash M : X \,!\, \tau$ *and* $\langle \mathbb{S} \mid M \rangle \rightsquigarrow \langle \mathbb{S}' \mid M' \rangle$, *then*

$$\vdash \mathbb{K}_{\mathbb{S}}[M] \equiv \mathbb{K}_{\mathbb{S}'}[M'] : X \,!\, (\tau_{\mathbb{S}} + \tau).$$

Future work

- Normalization
- Adequacy
- Concurrency
- Finite loops

Appendix

Typing rules for $\lambda_{[\tau]}$

VAR
$$\frac{x : X \in \Gamma}{\Gamma \vdash x : X}$$

CONST
$$\frac{(\Gamma \vdash V_i : \mathsf{b}_i)_{1 \leq i \leq n}}{\Gamma \vdash \mathsf{f}(V_1, \ldots, V_n) : \mathsf{b}}$$

PAIR
$$\frac{\Gamma \vdash V : X \qquad \Gamma \vdash W : Y}{\Gamma \vdash (V, W) : X \times Y}$$

UNIT
$$\frac{}{\Gamma \vdash () : \mathsf{unit}}$$

FUN
$$\frac{\Gamma, x : X \vdash M : Y \,!\, \tau}{\Gamma \vdash \mathsf{fun}\ (x : X) \mapsto M : X \to Y \,!\, \tau}$$

RETURN
$$\frac{\Gamma \vdash V : X}{\Gamma \vdash \mathsf{return}\ V : X \,!\, 0}$$

LET
$$\frac{\Gamma \vdash M : X \,!\, \tau \qquad \Gamma, \langle \tau \rangle, x : X \vdash N : Y \,!\, \tau'}{\Gamma \vdash \mathsf{let}\ x = M\ \mathsf{in}\ N : Y \,!\, \tau + \tau'}$$

Typing rules for $\lambda_{[\tau]}$

$$\textsc{Apply}\quad \frac{\Gamma \vdash V : X \to Y \,!\, \tau \qquad \Gamma \vdash W : X}{\Gamma \vdash V\,W : Y \,!\, \tau}$$

$$\textsc{Match}\quad \frac{\Gamma \vdash V : X \times Y \qquad \Gamma, x : X, y : Y \vdash N : Z \,!\, \tau}{\Gamma \vdash \mathsf{match}\ V\ \mathsf{with}\ \{(x, y) \mapsto N\} : Z \,!\, \tau}$$

$$\textsc{Op}\quad \frac{\Gamma \vdash V : A_{\mathsf{op}} \qquad \Gamma, \langle \tau_{\mathsf{op}} \rangle, x : B_{\mathsf{op}} \vdash M : X \,!\, \tau}{\Gamma \vdash \mathsf{op}\ V\ (x\,.\,M) : X \,!\, \tau_{\mathsf{op}} + \tau}$$

Typing rules for $\lambda_{[\tau]}$

Delay

$$\frac{\Gamma, \langle\tau\rangle \vdash M : X \,!\, \tau'}{\Gamma \vdash \mathsf{delay}\ \tau\ M : X \,!\, \tau + \tau'}$$

Handle

$$\frac{\begin{array}{c}\Gamma \vdash M : X \,!\, \tau \\ \Gamma, \langle\tau\rangle, z : X \vdash N : Y \,!\, \tau' \qquad H = (x \,.\, k \,.\, M_{\mathsf{op}})_{\mathsf{op} \in \mathcal{O}} \\ \left(\forall \tau'' \,.\, \Gamma, x : A_{\mathsf{op}}, k : [\tau_{\mathsf{op}}]\,(B_{\mathsf{op}} \to Y \,!\, \tau'') \vdash M_{\mathsf{op}} : Y \,!\, \tau_{\mathsf{op}} + \tau''\right)_{\mathsf{op} \in \mathcal{O}}\end{array}}{\Gamma \vdash \mathsf{handle}\ M\ \mathsf{with}\ H\ \mathsf{to}\ z\ \mathsf{in}\ N : Y \,!\, \tau + \tau'}$$

Typing rules for $\lambda_{[\tau]}$

$$\textsc{Box}\quad \frac{\Gamma, \langle\tau\rangle \vdash V : X \qquad \Gamma, x : [\tau]\, X \vdash N : Y \,!\, \tau'}{\Gamma \vdash \mathsf{box}_{[\tau]\,X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ N : Y \,!\, \tau'}$$

$$\textsc{Unbox}\quad \frac{\tau \leq \tau_\Gamma \qquad \Gamma - \tau \vdash V : [\tau]\, X \qquad \Gamma, x : X \vdash N : Y \,!\, \tau'}{\Gamma \vdash \mathsf{unbox}_{[\tau]\,X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ N : Y \,!\, \tau'}$$

Well-formed states $\Gamma \vdash \mathbb{S}$:

$$\frac{}{\Gamma \vdash \emptyset} \qquad \frac{\Gamma \vdash \mathbb{S}}{\Gamma \vdash \mathbb{S}, \langle\tau\rangle} \qquad \frac{\Gamma \vdash \mathbb{S} \qquad \Gamma, \Gamma_{\mathbb{S}}, \langle\tau\rangle \vdash V : X \qquad x \notin \Gamma, \Gamma_{\mathbb{S}}}{\Gamma \vdash \mathbb{S}, x \mapsto_{[\tau]\,X} V}$$

Small-step reduction relation

SEM-APP

$$\frac{}{\langle \mathbb{S} \mid (\textsf{fun}\ (x : X) \mapsto M)\ V \rangle \rightsquigarrow \langle \mathbb{S} \mid M[V/x] \rangle}$$

SEM-MATCH

$$\frac{}{\langle \mathbb{S} \mid \textsf{match}\ (V, W)\ \textsf{with}\ \{(x, y) \mapsto N\} \rangle \rightsquigarrow \langle \mathbb{S} \mid N[V/x, W/y] \rangle}$$

SEM-LET-CONG

$$\frac{\langle \mathbb{S} \mid M \rangle \rightsquigarrow \langle \mathbb{S}' \mid M' \rangle}{\langle \mathbb{S} \mid \textsf{let}\ x = M\ \textsf{in}\ N \rangle \rightsquigarrow \langle \mathbb{S}' \mid \textsf{let}\ x = M'\ \textsf{in}\ N \rangle}$$

SEM-LET-RET

$$\frac{}{\langle \mathbb{S} \mid \textsf{let}\ x = (\textsf{return}\ V)\ \textsf{in}\ N \rangle \rightsquigarrow \langle \mathbb{S} \mid N[V/x] \rangle}$$

Small-step reduction relation

SEM-LET-OP

$$\frac{}{\langle \mathbb{S} \mid \textsf{let}\ x = (\textsf{op}\ V\ (y\ .\ M))\ \textsf{in}\ N\rangle \rightsquigarrow \langle \mathbb{S} \mid \textsf{op}\ V\ (y\ .\ \textsf{let}\ x = M\ \textsf{in}\ N)\rangle}$$

SEM-HANDLE-CONG

$$\frac{\langle \mathbb{S} \mid M\rangle \rightsquigarrow \langle \mathbb{S}' \mid M'\rangle}{\langle \mathbb{S} \mid \textsf{handle}\ M\ \textsf{with}\ H\ \textsf{to}\ z\ \textsf{in}\ N\rangle \rightsquigarrow \langle \mathbb{S}' \mid \textsf{handle}\ M'\ \textsf{with}\ H\ \textsf{to}\ z\ \textsf{in}\ N\rangle}$$

SEM-HANDLE-RET

$$\frac{}{\langle \mathbb{S} \mid \textsf{handle}\ (\textsf{return}\ V)\ \textsf{with}\ H\ \textsf{to}\ z\ \textsf{in}\ N\rangle \rightsquigarrow \langle \mathbb{S} \mid N[V/z]\rangle}$$

Small-step reduction relation

SEM-DELAY

$$\frac{}{\langle \mathbb{S} \mid \textsf{delay}\ \tau\ M \rangle \rightsquigarrow \langle \mathbb{S}, \langle \tau \rangle \mid M \rangle}$$

SEM-BOX

$$\frac{}{\langle \mathbb{S} \mid \textsf{box}_{[\tau]\ X}\ V\ \textsf{as}\ x\ \textsf{in}\ N \rangle \rightsquigarrow \langle \mathbb{S}, x \mapsto_{[\tau]\ X} V \mid N \rangle}$$

SEM-UNBOX

$$\frac{y \in \mathbb{S}}{\langle \mathbb{S} \mid \textsf{unbox}_{[\tau]\ X}\ y\ \textsf{as}\ x\ \textsf{in}\ N \rangle \rightsquigarrow \langle \mathbb{S} \mid N[\mathbb{S}[y]/x] \rangle}$$

Proposotion

If $\vdash \mathbb{S}$ *and* $x : [\tau]\ X \in \Gamma_{\mathbb{S}}$, *then* $(\Gamma_{\mathbb{S}})_{x,1}, \langle \tau \rangle \vdash \mathbb{S}[x] : X$.

Computational context typing rules

$$\frac{}{\Gamma \vdash [\,] : 0} \qquad \frac{\Gamma \vdash V : A_{\mathsf{op}} \qquad \Gamma, \langle \tau_{\mathsf{op}} \rangle, x : B_{\mathsf{op}} \vdash \mathbb{K} : \tau}{\Gamma \vdash \mathsf{op}\ V\ (x\ .\ \mathbb{K}) : \tau_{\mathsf{op}} + \tau}$$

$$\frac{\Gamma, \langle \tau \rangle \vdash \mathbb{K} : \tau'}{\Gamma \vdash \mathsf{delay}\ \tau\ \mathbb{K} : \tau + \tau'} \qquad \frac{\Gamma, \langle \tau \rangle \vdash V : X \qquad \Gamma, x : [\tau]\, X \vdash \mathbb{K} : \tau'}{\Gamma \vdash \mathsf{box}_{[\tau]\, X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ \mathbb{K} : \tau'}$$

$$\frac{\tau \leq \tau_{\Gamma} \qquad \Gamma - \tau \vdash V : [\tau]\, X \qquad \Gamma, x : X \vdash \mathbb{K} : \tau'}{\Gamma \vdash \mathsf{unbox}_{[\tau]\, X}\ V\ \mathsf{as}\ x\ \mathsf{in}\ \mathbb{K} : \tau'}$$

Equational theory - Non-modal fragment

Unit Type

$$V \equiv ()$$

Product Type

$$\textsf{match}\ (V, W)\ \textsf{with}\ \{(x, y) \mapsto N\} \equiv N[V/x, W/y]$$

$$M[V/z] \equiv \textsf{match}\ V\ \textsf{with}\ \{(x, y) \mapsto M[(x, y)/z]\}$$

Function Type

$$(\textsf{fun}\ (x : X) \mapsto M)\ V \equiv M[V/x]$$

$$V \equiv \textsf{fun}\ (x : X) \mapsto V\, x$$

Equational theory - return, let, and handle fragment

Return Values

$$\text{let } x = (\text{return } V) \text{ in } N \equiv N[V/x]$$

$$\text{handle } (\text{return } V) \text{ with } H \text{ to } z \text{ in } N \equiv N[V/z]$$

Algebraicity ($y \notin fv(N)$)

$$\text{let } x = (\text{op } V\ (y\ .\ M)) \text{ in } N \equiv \text{op } V\ (y\ .\ (\text{let } x = M \text{ in } N))$$

Effect Handling

...

Associativity ($y \notin fv(P)$)

$$\text{let } x = (\text{let } y = M \text{ in } N) \text{ in } P \equiv \text{let } y = M \text{ in } (\text{let } x = N \text{ in } P)$$