

Semantics for Modular Analysis

Joonhyup Lee

1 Abstract Syntax

In this section we define the abstract syntax for a simple language that captures the essence of modules and linking. The language is basically an extension of untyped lambda calculus with modules and the linking operator.

x	\in	ExprVar	
M	\in	ModVar	
e	\in	Expr	
e	$::=$	x	<i>identifier, expression</i>
		$ \lambda x.e$	<i>function</i>
		$ e e$	<i>application</i>
		$ e!e$	<i>linked expression</i>
		$ \varepsilon$	<i>empty module</i>
		$ M$	<i>identifier, module</i>
		$ \text{let } x e e$	<i>let-binding, expression</i>
		$ \text{let } M e e$	<i>let-binding, module</i>

1.1 Rationale for the design of the simple language

There are no recursive modules, first-class modules, or functors in the simple language that is defined. Also, note that the nonterminals for the modules and expressions are not separated. Why is this so?

The rationale for the exclusion of recursive modules/first-class modules/functors is because we want to enforce static scoping. That is, we need to be able to statically determine where variables were bound when using them. To enforce static scoping when function applications might return modules, we need to employ signatures to project the dynamically computed modules onto a statically known context. Concretely, we need to define signatures S where $\lambda M :> S.e$ statically resolves the context when M is used in the body e , and $e :> S$ enforces that a dynamic computation is resolved into one static form.

The rationale for not separating modules and expressions in the syntax is because we want to utilize the linking operator to link both modules to expressions and modules to modules. That is, we want expressions to be parsed as $(m_1!m_2)!e$. $m_1!m_2$ links a module with a module, and $(m_1!m_2)!e$ links a module with an expression. Why this is convenient will be clear when we explain separate analysis; we want to link modules with modules as well as expressions.

2 Big-Step Operational Semantics

In this section we give the big-step operational semantics for the dynamic execution of the module language. The big-step evaluation relation relates the initial configuration(context, memory and time) and expression with the resulting value and state.

This relation is nonstandard in that the *environment* that is often used to define closures in the call-by-value dynamics is not a finite map from variables to values. Rather, the surrounding *syntactic* context annotated with the *binding times* for the variables serve as the environment. To access the value of the variable x from the context C , one has to read off the closest binding time from the context and look up the value bound at that time from the memory. To access the exported context from the variable M , one has to look up the exported context from C , not from the memory.

This separation between where we store modules and where we store the evaluated values from expressions emphasizes the fact that *where* the variables are bound is guided by syntax. The only thing that is dynamic is *when* the variables are bound, which is represented by the time component.

Now, we start by defining what we mean by *time* and *context*, which is the essence of our model.

2.1 Time and Context

We first define sets that are parametrized by our choice of the time domain, mainly the *value*, *memory*, and *context* domains. Also, we present the notational conventions used in this paper to represent members of each domain.

t	\in	\mathbb{T}	
v	\in	$\text{Val } \mathbb{T}$	
C	\in	$\text{Ctx } \mathbb{T}$	
V	\in	$\text{Val } \mathbb{T} + \text{Ctx } \mathbb{T}$	
σ	\in	$\text{Mem } \mathbb{T} \triangleq \mathbb{T} \xrightarrow{\text{fin}} \text{Val } \mathbb{T}$	
C	$::=$	$[]$	<i>hole</i>
	$ $	$\lambda x^t. C$	<i>function parameter binding</i>
	$ $	$\text{let } x^t C$	<i>let expression binding</i>
	$ $	$\text{let } M C C$	<i>let module context binding</i>
v	$::=$	$\langle \lambda x.e, C \rangle$	<i>closure</i>

Above, there are no constraints placed upon the set \mathbb{T} . Now we give the conditions that the concrete time domain must satisfy.

Definition 2.1 (Concrete time). $(\mathbb{T}, \leq, \text{tick})$ is a *concrete time* when

1. (\mathbb{T}, \leq) is a total order.
2. $\text{tick} \in \text{Ctx } \mathbb{T} \rightarrow \text{Mem } \mathbb{T} \rightarrow \mathbb{T} \rightarrow \text{ExprVar} \rightarrow \text{Val } \mathbb{T} \rightarrow \mathbb{T}$ gives a strictly larger timestamp. That is,

$$\forall C \in \text{Ctx } \mathbb{T}, \sigma \in \text{Mem } \mathbb{T}, t \in \mathbb{T}, x \in \text{ExprVar}, v \in \text{Val } \mathbb{T} : t < \text{tick } C \sigma t x v.$$

tick updates the timestamp when v is bound to x under the context C and state (σ, t) .

Now for the auxiliary operators that is used when defining the evaluation relation. We first define the plugin operator for the dynamic context.

$$C_1[C_2] \triangleq \begin{cases} C_2 & (C_1 = []) \\ \lambda x^t. C'[C_2] & (C_1 = \lambda x^t. C') \\ \text{let } x^t C'[C_2] & (C_1 = \text{let } x^t C') \\ \text{let } M C' C''[C_2] & (C_1 = \text{let } M C' C'') \end{cases}$$

Next, the function that extracts the address for an ExprVar must be defined.

$$\text{addr}(C, x) \triangleq \begin{cases} \perp & (C = []) \\ \perp & (C = \lambda x'^t. C' \wedge x' \neq x \wedge \text{addr}(C', x) = \perp) \\ \perp & (C = \text{let } x'^t C' \wedge x' \neq x \wedge \text{addr}(C', x) = \perp) \\ t & (C = \lambda x'^t. C' \wedge x' = x \wedge \text{addr}(C', x) = \perp) \\ t & (C = \text{let } x'^t C' \wedge x' = x \wedge \text{addr}(C', x) = \perp) \\ t' & (C = \lambda x'^t. C' \wedge \text{addr}(C', x) = t') \\ t' & (C = \text{let } x'^t C' \wedge \text{addr}(C', x) = t') \\ \text{addr}(C'', x) & (C = \text{let } M C' C'') \end{cases}$$

Finally, the function that looks up the dynamic context bound to a module variable M must be defined.

$$\text{ctx}(C, M) \triangleq \begin{cases} \perp & (C = []) \\ C' & (C = \text{let } M' C' C'' \wedge M' = M \wedge \text{ctx}(C'', M) = \perp) \\ \text{ctx}(C'', M) & (C = \text{let } M' C' C'' \wedge \text{ctx}(C'', M) \neq \perp) \\ \text{ctx}(C'', M) & (C = \text{let } M' C' C'' \wedge M' \neq M) \\ \text{ctx}(C', M) & (C = \lambda x^t. C') \\ \text{ctx}(C', M) & (C = \text{let } x^t C') \end{cases}$$

2.2 The Evaluation Relation

Now we are in a position to define the big-step evaluation relation. The relation \Downarrow relates $(e, C, \sigma, t) \in \text{Expr} \times \text{Ctx } \mathbb{T} \times \text{Mem } \mathbb{T} \times \mathbb{T}$ with $(V, \sigma, t) \in (\text{Val } \mathbb{T} + \text{Ctx } \mathbb{T}) \times \text{Mem } \mathbb{T} \times \mathbb{T}$. Note that we constrain whether the evaluation relation returns $v \in \text{Val } \mathbb{T}$ (when the expression being evaluated is not a module) or $C \in \text{Ctx } \mathbb{T}$ by the definition of the relation.

$$[\text{EXPRVAR}] \frac{t_x = \text{addr}(C, x) \quad \sigma(t_x) = v}{(x, C, \sigma, t) \Downarrow (v, \sigma, t)} \quad [\text{FN}] \frac{}{(\lambda x.e, C, \sigma, t) \Downarrow (\langle \lambda x.e, C \rangle, \sigma, t)}$$

$$\begin{array}{c}
\frac{(e_1, C, \sigma, t) \Downarrow (\langle \lambda x. e_\lambda, C_\lambda \rangle, \sigma_\lambda, t_\lambda) \quad (e_2, C, \sigma_\lambda, t_\lambda) \Downarrow (v, \sigma_a, t_a)}{[APP] \frac{(e_\lambda, C_\lambda[\lambda x^{t_a}. []], \sigma_a[t_a \mapsto v], \text{tick } C \sigma_a t_a x v) \Downarrow (v', \sigma', t')}{(e_1 e_2, C, \sigma, t) \Downarrow (v', \sigma', t')}} \quad [LINKING] \frac{(e_1, C, \sigma, t) \Downarrow (C', \sigma', t') \quad (e_2, C', \sigma', t') \Downarrow (V, \sigma'', t'')}{(e_1!e_2, C, \sigma, t) \Downarrow (V, \sigma'', t'')}
\end{array}$$

Note that we do not constrain whether v or C is returned by e_2 in the linking case. That is, linking may return either values or modules.

$$\begin{array}{c}
[EMPTY] \frac{}{(\varepsilon, C, \sigma, t) \Downarrow (C, \sigma, t)} \quad [MODVAR] \frac{C' = \text{ctx}(C, M)}{(M, C, \sigma, t) \Downarrow (C', \sigma, t)} \\
[LETE] \frac{(e_1, C, \sigma, t) \Downarrow (v, \sigma', t') \quad (e_2, C[\text{let } x^{t'} []], \sigma'[t' \mapsto v], \text{tick } C \sigma' t' x v) \Downarrow (C', \sigma'', t'')}{(\text{let } x e_1 e_2, C, \sigma, t) \Downarrow (C', \sigma'', t'')} \quad [LETM] \frac{(e_1, C, \sigma, t) \Downarrow (C', \sigma', t') \quad (e_2, C[\text{let } M C' []], \sigma', t') \Downarrow (C'', \sigma'', t'')}{(\text{let } M e_1 e_2, C, \sigma, t) \Downarrow (C'', \sigma'', t'')}
\end{array}$$

The equivalence of the evaluation relation with a reference interpreter is formalized in Coq.

3 Collecting Semantics

To describe what happens when an expression e is executed under the context C , memory σ and initial time t , we need to collect all *reachable states* starting from (e, C, σ, t) and all values that are returned by the reachable states. We first define the one-step reachability relation \rightsquigarrow .

$$\begin{array}{c}
[APPL] \frac{}{(e_1 e_2, C, \sigma, t) \rightsquigarrow (e_1, C, \sigma, t)} \quad [APPR] \frac{(e_1, C, \sigma, t) \Downarrow (\langle \lambda x. e_\lambda, C_\lambda \rangle, \sigma_\lambda, t_\lambda)}{(e_1 e_2, C, \sigma, t) \rightsquigarrow (e_2, C, \sigma_\lambda, t_\lambda)} \\
[APPBODY] \frac{(e_1, C, \sigma, t) \Downarrow (\langle \lambda x. e_\lambda, C_\lambda \rangle, \sigma_\lambda, t_\lambda) \quad (e_2, C, \sigma_\lambda, t_\lambda) \Downarrow (v, \sigma_a, t_a)}{(e_1 e_2, C, \sigma, t) \rightsquigarrow (e_\lambda, C_\lambda[\lambda x^{t_a}. []], \sigma_a[t_a \mapsto v], \text{tick } C \sigma_a t_a x v)} \\
[LINKL] \frac{}{(e_1!e_2, C, \sigma, t) \rightsquigarrow (e_1, C, \sigma, t)} \quad [LINKR] \frac{(e_1, C, \sigma, t) \Downarrow (C', \sigma', t')}{(e_1!e_2, C, \sigma, t) \rightsquigarrow (e_2, C', \sigma', t')} \\
[LETEL] \frac{}{(\text{let } x e_1 e_2, C, \sigma, t) \rightsquigarrow (e_1, C, \sigma, t)} \quad [LETERR] \frac{(e_1, C, \sigma, t) \Downarrow (v, \sigma', t')}{(\text{let } x e_1 e_2, C, \sigma, t) \rightsquigarrow (e_2, C[\text{let } x^{t'} []], \sigma'[t' \mapsto v], \text{tick } C \sigma' t' x v)} \\
[LETML] \frac{}{(\text{let } M e_1 e_2, C, \sigma, t) \rightsquigarrow (e_1, C, \sigma, t)} \quad [LETMR] \frac{(e_1, C, \sigma, t) \Downarrow (C', \sigma', t')}{(\text{let } M e_1 e_2, C, \sigma, t) \rightsquigarrow (e_2, C[\text{let } M C' []], \sigma', t')}
\end{array}$$

The well-definedness of the reachability relation with respect to a reference interpreter is formalized in Coq.

We want to enable separate analysis without making any assumptions on the free variables. That is, there may be stuck states because the value of free variables are not known in the given context. Since we want to collect the most precise information that describes the execution of the program, we have to collect all reachable states. The relation that collects the reachable states \rightsquigarrow^* is defined as the reflexive and transitive closure of \rightsquigarrow .

Definition 3.1 (Reachable states).

$$\underline{e}^*(C, \sigma, t) \triangleq \{(e', C', \sigma, t') \mid (e, C, \sigma, t) \rightsquigarrow^* (e', C', \sigma, t')\}$$

Definition 3.2 (Resolved states).

$$\underline{e}^\circ(C, \sigma, t) \triangleq \{((e', C', \sigma', t'), (V, \sigma'', t'')) \mid (e, C, \sigma, t) \rightsquigarrow^* (e', C', \sigma', t') \wedge (e', C' \sigma', t') \Downarrow (V, \sigma'', t'')\}$$

Definition 3.3 (Collecting semantics). The semantics for an expression e under context C , memory σ and time t is:

$$[e](C, \sigma, t) \triangleq (\underline{e}^\circ(C, \sigma, t), \underline{e}^*(C, \sigma, t))$$

To justify separate analysis, we first decompose the collecting semantics of the linking expression into a composition of the semantics of the left and right expressions.

Lemma 3.1 (Separation of linking, resolved part).

- Let $E = \{(C', \sigma', t') \mid (e_1, C, \sigma, t) \Downarrow (C', \sigma', t')\}$ (exported configurations).

$$\underline{e_1!e_2}^\circ(C, \sigma, t) = \underline{e_1}^\circ(C, \sigma, t) \cup \bigcup_{(C', \sigma', t') \in E} (\underline{e_2}^\circ(C', \sigma', t') \cup \underbrace{\{((e_1!e_2, C, \sigma, t), (V, \sigma'', t'')) \mid (e_2, C', \sigma', t') \Downarrow (V, \sigma'', t'')\}}_{\text{The final evaluation}})$$

Lemma 3.2 (Separation of linking, reached part).

- Let $E = \{(C', \sigma', t') \mid (e_1, C, \sigma, t) \Downarrow (C', \sigma', t')\}$ (exported configurations).

$$\underline{e_1!e_2}^*(C, \sigma, t) = \{(e_1!e_2, C, \sigma, t)\} \cup \underline{e_1}^*(C, \sigma, t) \cup \bigcup_{(C', \sigma', t') \in E} \underline{e_2}^*(C', \sigma', t')$$

Now we only need a way to calculate $\llbracket e_2 \rrbracket(C', \sigma', t')$ by utilizing the separately calculated $\llbracket e_2 \rrbracket([], \emptyset, t_0)$. The problem here is that when we calculate the two modules separately, we cannot enforce the order of the time component of each component. The order is important, because the *equivalence* of the concrete semantics depends on the fact that the tick function always generates a fresh timestamp larger than the times in the context and in the memory. The notion of equivalence between concrete configurations and the notion of soundness between the concrete and abstract configurations is essential in developing a formal guarantee that our modular separate analysis does generate some sound abstract state.

Definition 3.4 (Domain of a configuration). We define the domain of a configuration given by C, σ, t to be

$$\text{Dom}(C, \sigma, t) \triangleq \{t' \mid t' \in C \vee t' \in \text{Dom}(\sigma) \vee t' = t\}$$

Definition 3.5 (Equivalence between concrete configurations).

- Let $(\mathbb{T}, \leq, \text{tick})$ and $(\mathbb{T}', \leq', \text{tick}')$ be two concrete times.
- Let (C, σ, t) be a configuration in the first time domain and (C', σ', t') be a configuration in the second time domain.

The two configurations are equivalent if there exists a strictly increasing function $f \in \text{Dom}(C, \sigma, t) \rightarrow \text{Dom}(C', \sigma', t')$ that translates (C, σ, t) into (C', σ', t') .

$$(C, \sigma, t) \equiv (C', \sigma', t') \triangleq \exists f \in \text{Dom}(C, \sigma, t) \rightarrow \text{Dom}(C', \sigma', t') : f \text{ strictly increases} \wedge f(C) = C' \wedge f(t) = t' \wedge f \circ \sigma = \sigma' \circ f$$

Furthermore, we extend the definition of \equiv to a relation between $(\text{Val } \mathbb{T} + \text{Ctx } \mathbb{T}) \times \text{Mem } \mathbb{T} \times \mathbb{T}$ and $(\text{Val } \mathbb{T}' + \text{Ctx } \mathbb{T}') \times \text{Mem } \mathbb{T}' \times \mathbb{T}'$ to mean that

$$(V, \sigma, t) \equiv (V', \sigma', t') \triangleq \begin{cases} x = x' \wedge e = e' \wedge (C, \sigma, t) \equiv (C', \sigma', t') & (V = \langle \lambda x.e, C \rangle \wedge V' = \langle \lambda x'.e', C' \rangle) \\ (C, \sigma, t) \equiv (C', \sigma', t') & (V = C \wedge V' = C') \\ \text{False} & (\text{otherwise}) \end{cases}$$

We can prove that this relation indeed defines an equivalence relation, since such a function f automatically becomes a bijection between $\text{Dom}(C, \sigma, t)$ and $\text{Dom}(C', \sigma', t')$.

Lemma 3.3 (Preservation of equivalence).

- Let $(\mathbb{T}, \leq, \text{tick})$ and $(\mathbb{T}', \leq', \text{tick}')$ be two concrete times.
- Let (C, σ, t) be a configuration in the first time domain and (C', σ', t') be a configuration in the second time domain.
- Let all timestamps in C and $\text{Dom}(\sigma)$ be strictly less than t .
- Let $(C, \sigma, t) \equiv (C', \sigma', t')$.

Then for all e , if $(e, C, \sigma, t) \Downarrow (V, \sigma'', t'')$, there exists V', σ''', t''' such that $(e, C', \sigma', t') \Downarrow (V', \sigma''', t''')$ and $(V, \sigma'', t'') \equiv (V', \sigma''', t''')$. Likewise, if $(e, C, \sigma, t) \rightsquigarrow (e', C'', \sigma'', t'')$, there exists C''', σ''', t''' such that $(e, C', \sigma', t') \rightsquigarrow (e', C''', \sigma''', t''')$ and $(C'', \sigma'', t'') \equiv (C''', \sigma''', t''')$.

Now we need to define a concrete time on $\mathbb{T} + \mathbb{T}'$, when the first time domain exports C', σ' to the second time domain. What we want to prove is: $(C', \sigma', t') \equiv (C', \sigma', t_0)$, when the first configuration is in \mathbb{T} and the second configuration is in $\mathbb{T} + \mathbb{T}'$, with t_0 being the initial time in \mathbb{T}' . Then the reachable states from (e_2, C', σ', t_0) under the sum domain are equivalent to the reachable states from (e_2, C', σ', t') . Thus, because we can obtain a subset of the reachable states from (e_2, C', σ', t_0) by simply *injecting* C' and σ' into the reachable states obtained from $\llbracket e_2 \rrbracket([], \emptyset, t_0)$, we can compute a set *equivalent to* $\llbracket e_2 \rrbracket(C', \sigma', t')$ starting from the *separately analyzed* results.

Before elaborating on how to link the time domains, we need to define the injection and deletion operators that inject the exported context into the separately analyzed results. The notation for injecting C_1 into C_2 is $C_1\langle C_2 \rangle$, similar to the plugin operator defined above.

$$\text{map_inject}(C_1, C_2) \triangleq \begin{cases} [] & (C_2 = []) \\ \lambda x^t. \text{map_inject}(C_1, C') & (C_2 = \lambda x^t. C') \\ \text{let } x^t \text{ map_inject}(C_1, C') & (C_2 = \text{let } x^t C') \\ \text{let } M C_1[\text{map_inject}(C_1, C')] \text{ map_inject}(C_1, C'') & (C_2 = \text{let } M C' C'') \end{cases}$$

$$C_1\langle C_2 \rangle \triangleq C_1[\text{map_inject}(C_1, C_2)]$$

We extend the injection operator to map over all closures in a memory so that $C\langle\sigma\rangle$ can be defined naturally.

$$\text{delete_prefix}(C_1, C_2) \triangleq \begin{cases} \text{delete_prefix}(C'_1, C'_2) & ((C_1, C_2) = (\lambda x^t. C'_1, \lambda x^t. C'_2)) \\ \text{delete_prefix}(C'_1, C'_2) & ((C_1, C_2) = (\text{let } x^t C'_1, \text{let } x^t C'_2)) \\ \text{delete_prefix}(C'_1, C'_2) & ((C_1, C_2) = (\text{let } M C' C'_1, \text{let } M C' C'_2)) \\ C_2 & (\text{otherwise}) \end{cases}$$

$$\text{delete_map}(C_1, C_2) \triangleq \begin{cases} [] & (C_2 = []) \\ \lambda x^t. \text{delete_map}(C_1, C') & (C_2 = \lambda x^t. C') \\ \text{let } x^t \text{ delete_map}(C_1, C') & (C_2 = \text{let } x^t C') \\ \text{let } M \text{ delete_map}(C_1, \text{delete_prefix}(C_1, C')) \text{ delete_map}(C_1, C'') & (C_2 = \text{let } M C' C'') \end{cases}$$

$$\text{delete}(C_1, C_2) \triangleq \text{delete_map}(C_1, \text{delete_prefix}(C_1, C_2))$$

The deletion operation has the expected property that $\text{delete}(C, C\langle C' \rangle) = C'$.

Finally, before delving into the definition of the linked time domain, we need to define a filter function that filters the context and memory by membership in each time domain.

$$\text{filter}(C, \mathbb{T}) \triangleq \begin{cases} [] & (C = []) \\ \lambda x^t. \text{filter}(C', \mathbb{T}) & (C = \lambda x^t. C' \wedge t \in \mathbb{T}) \\ \text{let } x^t \text{ filter}(C', \mathbb{T}) & (C = \text{let } x^t C' \wedge t \in \mathbb{T}) \\ \text{let } M \text{ filter}(C', \mathbb{T}) \text{ filter}(C'', \mathbb{T}) & (C = \text{let } M C' C'') \\ \text{filter}(C', \mathbb{T}) & (C = \lambda x^t. C' \wedge t \notin \mathbb{T}) \\ \text{filter}(C', \mathbb{T}) & (C = \text{let } x^t C' \wedge t \notin \mathbb{T}) \end{cases}$$

$$\text{filter}(\sigma, \mathbb{T}) \triangleq \lambda t \in \mathbb{T}. \text{let } \langle \lambda x.e, C \rangle := \sigma(t) \text{ in } \langle \lambda x.e, \text{filter}(C, \mathbb{T}) \rangle$$

Lemma 3.4 (Linking of time domains).

- Let $(\mathbb{T}, \leq, \text{tick})$ and $(\mathbb{T}', \leq', \text{tick}')$ be two concrete times.
- Let $C_0 \in \text{Ctx } \mathbb{T}$ be the injected context.
- Define the \leq_+ order by

$$t \leq_+ t' \triangleq \begin{cases} t \leq t' & (t, t' \in \mathbb{T}) \\ t \leq' t' & (t, t' \in \mathbb{T}') \\ \text{True} & (t \in \mathbb{T}, t' \in \mathbb{T}') \\ \text{False} & (t \in \mathbb{T}', t' \in \mathbb{T}) \end{cases}$$

- Define the tick_+ function so that the timestamps produced from the *injected* context and state are exactly the timestamps produced before injection.

$$\text{tick}_+(C, \sigma, t, x, v) \triangleq \begin{cases} \text{tick}(\text{filter}(C, \mathbb{T}), \text{filter}(\sigma, \mathbb{T}), t, x, \text{filter}(v, \mathbb{T})) & (t \in \mathbb{T}) \\ \text{tick}'(\text{filter}(\text{delete}(C_0, C), \mathbb{T}'), \text{filter}(\text{delete}(C_0, \sigma), \mathbb{T}'), t, x, \text{filter}(\text{delete}(C_0, v), \mathbb{T}')) & (t \in \mathbb{T}') \end{cases}$$

Then $(\mathbb{T} + \mathbb{T}', \leq_+, \text{tick}_+)$ is a concrete time.

Lemma 3.5 (Preservation of timestamps under linked time).

- Let $(\mathbb{T}, \leq, \text{tick})$ and $(\mathbb{T}', \leq', \text{tick}')$ be two concrete times.
- Let $C_0 \in \text{Ctx } \mathbb{T}$ be the injected context.
- Let $\sigma_0 \in \text{Mem } \mathbb{T}$ be the injected memory, and let

$$\sigma; \sigma_0 \triangleq \lambda t. \begin{cases} \sigma(t) & (t \in \mathbb{T}') \\ \sigma_0(t) & (t \in \mathbb{T}) \end{cases}$$

for $\sigma \in \text{Mem } \mathbb{T}'$.

Now, if $(e, C, \sigma, t) \Downarrow (V, \sigma', t')$ under \mathbb{T}' , then $(e, C_0\langle C \rangle, C_0\langle \sigma \rangle; \sigma_0, t) \Downarrow (C_0\langle V \rangle, C_0\langle \sigma' \rangle; \sigma_0, t')$ under $\mathbb{T} + \mathbb{T}'$.

Likewise, if $(e, C, \sigma, t) \rightsquigarrow^* (e', C', \sigma', t')$ under \mathbb{T}' , then $(e, C_0\langle C \rangle, C_0\langle \sigma \rangle; \sigma_0, t) \rightsquigarrow^* (e', C_0\langle C' \rangle, C_0\langle \sigma' \rangle; \sigma_0, t')$ under $\mathbb{T} + \mathbb{T}'$.

Definition 3.6 (Subset to an equivalent set).

- $A \subseteq B$ in the context when $A, B \in (\text{Expr} \times \text{Ctx } \mathbb{T} \times \text{Mem } \mathbb{T} \times \mathbb{T})$ is defined as

$$(e, C, \sigma, t) \in A \Rightarrow \exists C', \sigma', t' : (C, \sigma, t) \equiv (C', \sigma', t') \wedge (e, C', \sigma', t') \in B$$

- $A \subseteq B$ in the context when $A, B \in (\text{Expr} \times \text{Ctx } \mathbb{T} \times \text{Mem } \mathbb{T} \times \mathbb{T}) \times (\text{Val } \mathbb{T} \times \text{Mem } \mathbb{T} \times \mathbb{T})$ is defined as

$$((e, C, \sigma, t), (V, \sigma', t')) \in A \Rightarrow \exists C', \sigma'', t'', V', \sigma''', t''' : (C, \sigma, t) \equiv (C', \sigma'', t'') \wedge (V, \sigma', t') \equiv (V', \sigma''', t''') \wedge ((e, C', \sigma'', t''), (V', \sigma''', t''')) \in B$$

Before going into the formulation of linking in the concrete semantics, we need to cast $\llbracket e \rrbracket$ into a fixpoint computation form. We define a transfer function \mathcal{F} that takes $(R^\circ, R^*) \in \wp((\text{Expr} \times \text{Ctx } \mathbb{T} \times \text{Mem } \mathbb{T} \times \mathbb{T}) \times (\text{Val } \mathbb{T} \times \text{Mem } \mathbb{T} \times \mathbb{T})) \times \wp(\text{Expr} \times \text{Ctx } \mathbb{T} \times \text{Mem } \mathbb{T} \times \mathbb{T})$ and outputs (R'°, R'^*) that are one step away from the original sets.

Definition 3.7 (Transfer function).

- Given $(R^\circ, R^*) \in \wp((\text{Expr} \times \text{Ctx } \mathbb{T} \times \text{Mem } \mathbb{T} \times \mathbb{T}) \times (\text{Val } \mathbb{T} \times \text{Mem } \mathbb{T} \times \mathbb{T})) \times \wp(\text{Expr} \times \text{Ctx } \mathbb{T} \times \text{Mem } \mathbb{T} \times \mathbb{T})$,
- Let the relations \Downarrow_{R° and \rightsquigarrow_{R^*} be defined as exactly the relations \Downarrow and \rightsquigarrow with all assumptions of the form $a \Downarrow b$ replaced with the assumptions $(a, b) \in R^\circ$.
- Let $\Delta R^\circ = \{(a, b) \mid a \in R^* \wedge a \Downarrow_{R^\circ} b\}$ and $\Delta R^* = \{b \mid \exists a \in R^* : a \rightsquigarrow_{R^*} b\}$
- The definition of the transfer function is $\mathcal{F}(R^\circ, R^*) \triangleq (R^\circ \cup \Delta R^\circ, R^* \cup \Delta R^*)$.

Lemma 3.6 (Collecting semantics as a least fixpoint).

$$\llbracket e \rrbracket(C, \sigma, t) = \text{lfp}(\lambda(R^\circ, R^*). \mathcal{F}(R^\circ, R^* \cup \{(e, C, \sigma, t)\}))$$

Theorem 3.1 (Linking of collected states). We want to compute $\llbracket e_1!e_2 \rrbracket(C, \sigma, t)$.

- Given R° and R^* that satisfies $\underline{e_1}^\circ(C, \sigma, t) \subseteq R^\circ$ and $\underline{e_1}^*(C, \sigma, t) \subseteq R^*$,
- Let $E = \{(C_0, \sigma_0, t'') \mid \exists C', \sigma', t' : (C, \sigma, t) \equiv (C', \sigma', t') \wedge ((e_1, C', \sigma', t'), (C_0, \sigma_0, t'')) \in R^\circ\}$ (exported configurations).
- Let $R^\circ(C_0, \sigma_0) = \{((e_2, C_0, \sigma_0, t_0), (C_0\langle V \rangle, C_0\langle \sigma' \rangle; \sigma_0, t')) \mid ((e_2, [], \emptyset, t_0), (V, \sigma', t')) \in \underline{e_2}^\circ([], \emptyset, t_0)\}$ (separate resolved).
- Let $R^*(C_0, \sigma_0) = \{(e', C_0\langle C' \rangle, C_0\langle \sigma' \rangle; \sigma_0, t') \mid (e', C', \sigma', t') \in \underline{e_2}^*([], \emptyset, t_0)\}$ (separate reached).

We have:

$$\llbracket e_2 \rrbracket(C_0, \sigma_0, t_0) = \text{lfp}(\lambda(R^\circ, R^*). \mathcal{F}(R^\circ \cup R^\circ(C_0, \sigma_0), R^* \cup R^*(C_0, \sigma_0)))$$

Thus:

$$\underline{e_1!e_2}^\circ(C, \sigma, t) \subseteq R^\circ \cup \bigcup_{(C_0, \sigma_0, t') \in E} \underbrace{(\underline{e_2}^\circ(C_0, \sigma_0, t_0) \cup \{((e_1!e_2, C, \sigma, t), (V, \sigma'', t'')) \mid ((e_2, C_0, \sigma_0, t_0), (V, \sigma'', t'')) \in \underline{e_2}^\circ(C_0, \sigma_0, t_0)\})}_{\text{The final evaluation}}$$

$$\underline{e_1!e_2}^*(C, \sigma, t) \subseteq \{(e_1!e_2, C, \sigma, t)\} \cup R^* \cup \bigcup_{(C_0, \sigma_0, t') \in E} \underline{e_2}^*(C_0, \sigma_0, t_0)$$

4 Abstract Semantics

The abstract semantics is almost exactly the same as the concrete semantics, except for the fact that the memory domain is now a finite map from the abstract time domain to a *set* of abstract values.

$$\begin{array}{ll}
t^\# & \in \mathbb{T}^\# \\
v^\# & \in \text{Val}^\# \mathbb{T}^\# \\
C^\# & \in \text{Ctx } \mathbb{T}^\# \\
V^\# & \in \text{Val}^\# \mathbb{T}^\# + \text{Ctx } \mathbb{T}^\# \\
\sigma^\# & \in \text{Mem}^\# \mathbb{T} \triangleq \mathbb{T}^\# \xrightarrow{\text{fin}} \wp(\text{Val}^\# \mathbb{T}^\#) \\
v^\# & ::= \langle \lambda x.e, C^\# \rangle \quad \text{closure}
\end{array}$$

Definition 4.1 (Soundness).

- Given two configurations (C, σ, t) in \mathbb{T} and $(C^\#, \sigma^\#, t^\#)$ in $\mathbb{T}^\#$, we say that the latter is a sound approximation of the former when there exists an $\alpha : \mathbb{T} \rightarrow \mathbb{T}^\#$ such that $\alpha(t) = t^\# \wedge \alpha(C) = C^\# \wedge \forall t : \alpha(\sigma(t)) \in \sigma^\#(\alpha(t))$. We write this as $(C, \sigma, t) \triangleleft (C^\#, \sigma^\#, t^\#)$.
- Given two states (e, C, σ, t) and $(e', C^\#, \sigma^\#, t^\#)$, the latter is said to be a sound approximation of the former when $e = e'$ and $(C, \sigma, t) \triangleleft (C^\#, \sigma^\#, t^\#)$.
- Given two results (V, σ, t) and $(V^\#, \sigma^\#, t^\#)$, the latter is said to be a sound approximation of the former either if they are both of the form (C, σ, t) and $(C^\#, \sigma^\#, t^\#)$ and the latter is a sound approximation of the former, or if they are of the form $(\langle \lambda x.e, C \rangle, \sigma, t)$ and $(\langle \lambda x'.e', C^\# \rangle, \sigma^\#, t^\#)$ satisfying $x = x' \wedge (C, \sigma, t) \triangleleft (C^\#, \sigma^\#, t^\#)$.
- Given two sets S and $S^\#$, we write $S \subseteq^\# S^\#$ when for every element of S , there exists a sound approximation in $S^\#$.

We define the abstract evaluation relation $\Downarrow^\#$ and abstract reachability relation $\rightsquigarrow^\#$ exactly as their concrete counterparts, except that the update for the memory is now a weak update and variables can evaluate to any value in $\sigma^\#(\text{addr})$.

Lemma 4.1 (Preservation of soundness).

- Let (C, σ, t) be a concrete configuration and $(C^\#, \sigma^\#, t^\#)$ be an abstract configuration.
- Let all timestamps in C and $\text{Dom}(\sigma)$ be strictly less than t .
- Let $(C, \sigma, t) \triangleleft (C^\#, \sigma^\#, t^\#)$.

Then for all e , if $(e, C, \sigma, t) \Downarrow (V, \sigma', t')$, there exists $V^\#, \sigma'^\#, t'^\#$ such that $(e, C^\#, \sigma^\#, t^\#) \Downarrow^\# (V^\#, \sigma'^\#, t'^\#)$ and $(V, \sigma', t') \triangleleft (V^\#, \sigma'^\#, t'^\#)$. Likewise, if $(e, C, \sigma, t) \rightsquigarrow (e', C', \sigma', t')$, there exists $C'^\#, \sigma'^\#, t'^\#$ such that $(e, C^\#, \sigma^\#, t^\#) \rightsquigarrow^\# (e', C'^\#, \sigma'^\#, t'^\#)$ and $(C', \sigma', t') \triangleleft (C'^\#, \sigma'^\#, t'^\#)$.

Lemma 4.2 (Equivalence preserves soundness).

- Let (C, σ, t) and (C', σ', t') be concrete configurations and $(C^\#, \sigma^\#, t^\#)$ be an abstract configuration.
- Let $(C, \sigma, t) \equiv (C', \sigma', t')$ and $(C, \sigma, t) \triangleleft (C^\#, \sigma^\#, t^\#)$.

Then $(C', \sigma', t') \triangleleft (C^\#, \sigma^\#, t^\#)$.

Theorem 4.1 (Abstract linking). We want to compute sets $\tilde{R}^\#$ and $R^{\circ\#}$ satisfying

$$\underline{e_1!e_2}^\circ(C, \sigma, t) \subseteq^\# \tilde{R}^{\circ\#} \quad \wedge \quad \underline{e_1!e_2}^*(C, \sigma, t) \subseteq^\# \tilde{R}^{*\#}$$

- Given $R^{\circ\#}$ and $R^{*\#}$ that satisfies $\underline{e_1}^\circ(C, \sigma, t) \subseteq^\# R^{\circ\#}$ and $\underline{e_1}^*(C, \sigma, t) \subseteq^\# R^{*\#}$,
- Let $E^\# = \{(C_0^\#, \sigma_0^\#, t_0^\#) \mid \exists C^\#, \sigma^\#, t^\# : (C, \sigma, t) \triangleleft (C^\#, \sigma^\#, t^\#) \wedge ((e_1, C^\#, \sigma^\#, t^\#), (C_0^\#, \sigma_0^\#, t_0^\#)) \in R^{\circ\#}\}$.
- Let $R^{\circ\#}(C_0^\#, \sigma_0^\#) = \{((e_2, C_0^\#, \sigma_0^\#, t_0^\#), (C_0^\# \langle V^\# \rangle, C_0^\# \langle \sigma^\# \rangle; \sigma_0^\#, t_0^\#)) \mid ((e_2, [], \emptyset, t_0^\#), (V^\#, \sigma^\#, t^\#)) \in \underline{e_2}^\circ([], \emptyset, t_0^\#)\}$.
- Let $R^{*\#}(C_0^\#, \sigma_0^\#) = \{(e', C_0^\# \langle C^\# \rangle, C_0^\# \langle \sigma^\# \rangle; \sigma_0^\#, t_0^\#) \mid (e', C^\#, \sigma^\#, t^\#) \in \underline{e_2}^*(([], \emptyset, t_0^\#))\}$.

We have:

$$\llbracket e_2 \rrbracket^\#(C_0^\#, \sigma_0^\#, t_0^\#) = \text{lfp}(\lambda(R^\circ^\#, R^{*\#}). \mathcal{F}^\#(R^\circ^\# \cup R^\circ^\#(C_0^\#, \sigma_0^\#), R^{*\#} \cup R^{*\#}(C_0^\#, \sigma_0^\#)))$$

Thus, if we pick some $(C^\#, \sigma^\#, t^\#)$ satisfying $(C, \sigma, t) \triangleleft (C^\#, \sigma^\#, t^\#)$:

$$\underline{e_1!e_2}^\circ(C, \sigma, t) \subseteq^\# R^\circ^\# \cup \bigcup_{(C_0^\#, \sigma_0^\#, t'^\#) \in E^\#} (\underline{e_2}^\circ(C_0^\#, \sigma_0^\#, t_0^\#) \cup \underbrace{\{((e_1!e_2, C^\#, \sigma^\#, t^\#), (V^\#, \sigma'^\#, t'^\#)) | (e_2, C_0^\#, \sigma_0^\#, t_0^\#) \Downarrow^\# (V^\#, \sigma'^\#, t'^\#)\}}_{\text{The final evaluation}})$$

$$\underline{e_1!e_2}^*(C, \sigma, t) \subseteq^\# \{(e_1!e_2, C^\#, \sigma^\#, t^\#)\} \cup R^{*\#} \cup \bigcup_{(C_0^\#, \sigma_0^\#, t'^\#) \in E^\#} \underline{e_2}^{*\#}(C_0^\#, \sigma_0^\#, t_0^\#)$$

Theorem 4.2 (Finiteness of time implies finiteness of abstraction). If $\mathbb{T}^\#$ is finite,

$$\forall e, C^\#, \sigma^\#, t^\# : |\underline{e}^\circ^\#(C^\#, \sigma^\#, t^\#)| < \infty \wedge |\underline{e}^{*\#}(C^\#, \sigma^\#, t^\#)| < \infty$$