Designing a Security-typed Language with Certificate-based Declassification

Stephen Tse Steve Zdancewic

University of Pennsylvania
Technical report: MS-CIS-04-16

Abstract

This paper presents the design of a programming language that supports information-flow security policies and certificate-based declassification.

The language uses monadic information-flow annotations in the style of Abadi et al.'s dependency core calculus, and has an effects system and fixpoints. The type system conflates security concepts such as labels, principals, and privileges with abstract types, allowing a uniform treatment of lattice structures throughout the language. Myers' and Liskov's decentralized label model is encoded using type constructors that describe confidentiality and integrity policies, and label refinements and principal groups follow naturally from intersection and union types. Singleton types, combined with bounded universal and existential quantifications, connect the type system with public-key infrastructures whose digital certificates provide authorization for privileged operations such as declassification. These features allow specification of security policies in term of dynamic entities such as run-time user identities and file access permissions.

Besides showing that the language is sound, we present a security theorem that generalizes standard noninterference to account for information flows introduced by declassification. Although this result gives only a coarse approximation to the information potentially leaked, it captures our intuitions about certificate-based declassification.

1 Introduction

Information-flow policies specify constraints on the propagation of confidential data and provide an end-to-end guarantee of security. Security-typed languages have become a promising approach for specifying and enforcing such policies with type systems [45]. However, designing a *sound* and *secure* information-flow type system is still a challenging problem: programmers want to express fine-grained security policies with advanced types, but reasoning about security guarantees in such complex systems is non-trivial.

This paper presents a security-typed language with well-studied constructs such as polymorphism, subtyping, effects, and fixpoints. Most importantly, these language features are isolated in a monadic style. This makes typing and evaluation rules easy to understand and the proof of *noninterference* [19, 29] for security modular. The language presented here is intended to serve as a simple core calculus that lets us experiment with the design of new security policy constructs and their interaction with advanced type features.

Another challenge of designing a security-typed language is to provide downgrading mechanisms that intentionally break the security guarantees, if such actions can be justified externally. Downgrading mechanisms, such as *delegating* to another principal or *declassifying* secret data to public, are important in practical programming [58]. The decentralized label model by Myers and Liskov [35, 36] addresses this problem and introduces the notion of principals and reader sets such that the type system controls authority for downgrading.

Our type system conflates labels, principals and privileges as abstract types so that standard type constructs can be used to integrate the decentralized label model. For example, subtyping naturally models principal delegations, while intersection and union types give rise to principal groups and label refinements. A security language with such encoding allows expressive and decentralized policies, yet the semantics remains easy to understand and implement.

The last challenge addressed in this paper is to connect the compile-time security type system with the run-time security infrastructure. Public-key infrastructure is a standard choice for distributed access control.

Stephen Tse <stse@cis.upenn.edu> and Steve Zdancewic <stevez@cis.upenn.edu>. Last update: October 1, 2004.

Our language uses *singleton types* such that a principal is represented as a public key, and the authority of a principal granting a privilege is represented as a digital certificate signed by the principal's private key [49]. Given these semantics, the type system can interpret verifying certificate as *extending* the subtyping relation, which in turn means delegation or declassification. We formalize the intuition that the certificate externally justifies the information leaks due to declassification in a *conditioned* version of the standard noninterference theorem.

The main contributions of our paper are:

1. the design of a sound and secure information-flow type system with bounded quantifications, effects, fixpoints in a monadic style;
2. the integration of the decentralized label model with type constructors and the use of extensible subtyping to study delegation, declassification, and endorsement;
3. a conditioned version of the noninterference theorem that justifies certificate-based declassification;
4. the uniform treatment of labels, principals, and privileges as abstract types, and the application of intersection and union types for principal groups and policy refinements.

We have proved the soundness and the noninterference theorems and written a small prototype interpreter, called *Apollo*, for our language. We are also working on formalizing the semantics and the soundness proof in Twelf (a logical framework) [37]. The interested reader is invited to visit our homepage at `http://www.cis.upenn.edu/~stse/apollo`.

For brevity, the main body of this paper only shows the interesting cases of rules and proof excerpts. The full details are in the appendix.

The rest of the paper is organized as follows. Section 2 starts with a core calculus with labels to study noninterference and extends it with effects and fixpoints. Section 3 introduces the decentralized label model and shows how the core calculus supports the same notion of principals, confidentiality and integrity. Furthermore, downgrading mechanisms are studied as extensible subtyping and certificate-based declassification is justified using constructs from public-key infrastructures. The paper then concludes with related work in Section 4 and discussion in Section 5.

2 Core label calculus

Let us start by introducing a core calculus with monadic labels and effects for analyzing program dependency. This section proves two important security theorems, *soundness* and *noninterference*, for our core calculus. We then enrich the language with fixpoints and refine the theorems to account for *strong noninterference* and *weak noninterference* in the presence of computational effects.

2.1 Monadic labels

The first part of our core label calculus is the *dependency core calculus* (DCC) introduced by Abadi et al. [1]. The motivation behind DCC is to use *monadic labels* as a unifying framework to study many important program analyses such as binding time, information flow, slicing, and function call tracking. DCC uses a lattice of monads and a special typing rule for their associated *bind* operations to describe the dependency of computations in a program.

Unlike DCC, which is based on call-by-name simply-typed lambda calculus, our core calculus is based on the call-by-value polymorphic lambda calculus with subtyping (System $F_{\preceq}$) [14]. Universal and existential quantifications ($\forall\alpha \preceq \mathtt{t}.\mathtt{t}$ and $\exists\alpha \preceq \mathtt{t}.\mathtt{t}$) will become essential in later sections describing the connection between the static security policies and the run-time public-key infrastructures (Section 3.3), while subtyping naturally models principal delegations and policy refinements (Section 3).

The following grammar defines the syntax for the types and terms of the basic calculus.

$$
\begin{array}{rcl}
\mathtt{t} & ::= & \mathtt{<>} \mid \mathtt{<t,t>} \mid \mathtt{t}+\mathtt{t} \mid \mathtt{t}\to\mathtt{t} \\
 & & \mid \top \mid \bot \mid \alpha \mid \forall\alpha \preceq \mathtt{t}.\mathtt{t} \mid \exists\alpha \preceq \mathtt{t}.\mathtt{t} \\
\mathtt{m} & ::= & \mathtt{<>} \mid \mathtt{<m,m>} \mid \mathtt{prj}_1\ \mathtt{m} \mid \mathtt{prj}_2\ \mathtt{m} \mid \mathtt{inj}_1\ \mathtt{m} \mid \mathtt{inj}_2\ \mathtt{m} \\
 & & \mid \mathtt{case\ m\ m\ m} \mid \mathtt{x} \mid \lambda\mathtt{x{:}t.m} \mid \mathtt{m\ m} \mid \Lambda\alpha \preceq \mathtt{t.m} \mid \mathtt{m\ [t]} \\
 & & \mid \mathtt{pack\ (t,m)\ as\ t} \mid \mathtt{open\ }(\alpha,\mathtt{x}) = \mathtt{m\ in\ m}
\end{array}
$$

The types consists of unit, products, sums, functions, top, bottom, variables, universal and existential quantifications, while the terms consists of unit, products, projections, injections, cases, variables, functions, applications, type abstractions, instantiations, package packings, and package openings.

We use the standard semantics of Kernel $F_{\preceq}$ [9, 38]. We denote the evaluation judgement by $\mathtt{m} \longrightarrow \mathtt{m}$, the typing judgements by $\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t}$ and the subtyping judgement by $\Delta \vdash \mathtt{t} \preceq \mathtt{t}$, where type contexts Δ and term contexts Γ are defined as:

$$
\begin{array}{rcl}
\Delta & ::= & \cdot \mid \Delta, \alpha \preceq \mathtt{t} \\
\Gamma & ::= & \cdot \mid \Gamma, \mathtt{x{:}t}
\end{array}
$$

We omit rules for the standard constructs above. Let us focus on the new type and terms for monadic labels: monadic label types $\mathtt{t}\{\ell\}$ and their corresponding unit $\mathtt{m}\{\ell\}$ and `bind` operator for each label ℓ.

We conflate labels and types as the same syntactic class and use a kind system to rule out ill-formed types. The only kinds now are types `T` and labels `L`, but later we will add principals `P` and privileges `J` (Section 3), so that all four constructs uniformly share mechanisms such as polymorphism and subtyping. Formally, we define kinds and extend types and terms as follows:

$$\begin{array}{lcl} \ell & \equiv & \mathtt{t} \\ \mathtt{k} & ::= & \mathtt{T} \mid \mathtt{L} \mid \mathtt{P} \mid \mathtt{J} \\ \mathtt{t} & ::= & \ldots \mid \ell \wedge \ell \mid \ell \vee \ell \mid \mathtt{t}\{\ell\} \\ \mathtt{m} & ::= & \ldots \mid \mathtt{m}\{\ell\} \mid \mathtt{bind\ x = m\ in\ m} \end{array}$$

The straight-forward kinding rules ($\Delta \vdash \mathtt{t} :: \mathtt{k}$) are omitted here. Note that we also add intersection and union types [39, 40, 6], which precisely model policy sets and principal groups. Section 3.1 explains how confidentiality and integrity policies make use of both intersection and union types.

Intersection and union types in this paper are needed only for our *abstract types* (labels, effects, principals, and privileges); hence, we do not provide the introduction or elimination forms of intersection and union for *concrete types* (such as products and functions). This decision helps keeping the language and the type checking algorithm simple.

We follow Pottier's notation [43] for specifying the subtyping polarities Ⓢ of type constructors: $\oplus$ for covariant, $\ominus$ for contravariant, and $\odot$ for invariant:

$$\begin{array}{rcl} Ⓢ & = & \texttt{<}\oplus,\oplus\texttt{>} \mid \oplus + \oplus \mid \ominus \to \oplus \mid \forall \alpha \preceq \odot.\oplus \\ & & \mid \exists \alpha \preceq \odot.\oplus \mid \oplus \wedge \oplus \mid \oplus \vee \oplus \mid \oplus\{\oplus\} \end{array}$$

In addition, intersection and union types satisfy the following standard subtyping rules:

$$\frac{\Delta \vdash \mathtt{t}_1 \preceq \mathtt{t}}{\Delta \vdash \mathtt{t}_1 \wedge \mathtt{t}_2 \preceq \mathtt{t}} \qquad \frac{\Delta \vdash \mathtt{t} \preceq \mathtt{t}_1}{\Delta \vdash \mathtt{t} \preceq \mathtt{t}_1 \vee \mathtt{t}_2}$$

$$\frac{\Delta \vdash \mathtt{t}_2 \preceq \mathtt{t}}{\Delta \vdash \mathtt{t}_1 \wedge \mathtt{t}_2 \preceq \mathtt{t}} \qquad \frac{\Delta \vdash \mathtt{t} \preceq \mathtt{t}_2}{\Delta \vdash \mathtt{t} \preceq \mathtt{t}_1 \vee \mathtt{t}_2}$$

$$\frac{\Delta \vdash \mathtt{t} \preceq \mathtt{t}_1 \quad \Delta \vdash \mathtt{t} \preceq \mathtt{t}_2}{\Delta \vdash \mathtt{t} \preceq \mathtt{t}_1 \wedge \mathtt{t}_2} \qquad \frac{\Delta \vdash \mathtt{t}_1 \preceq \mathtt{t} \quad \Delta \vdash \mathtt{t}_2 \preceq \mathtt{t}}{\Delta \vdash \mathtt{t}_1 \vee \mathtt{t}_2 \preceq \mathtt{t}}$$

Now let us see how the type system prevents low-level computation from depending on high-level computation:

$$\frac{\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t} \quad \Delta \vdash \ell :: \mathtt{L}}{\Delta;\ \Gamma \vdash \mathtt{m}\{\ell\} : \mathtt{t}\{\ell\}} \qquad \text{(T-Lab)}$$

$$\frac{\begin{array}{l}\Delta;\ \Gamma \vdash \mathtt{m}_1 : \mathtt{t}_1\{\ell\} \\ \Delta;\ \Gamma, \mathtt{x}{:}\mathtt{t}_1 \vdash \mathtt{m}_2 : \mathtt{t}_2 \quad \Delta \vdash \mathtt{t}_2 \gg \ell\end{array}}{\Delta;\ \Gamma \vdash \mathtt{bind\ x = m_1\ in\ m_2} : \mathtt{t}_2} \qquad \text{(T-Bind)}$$

The label monad $\mathtt{m}\{\ell\}$ marks the computation `m` with the label ℓ, restricting how it interacts with the rest of the program (T-Bind). The term $\mathtt{bind\ x = m_1\ in\ m_2}$ exposes the computation $\mathtt{m}_1$ protected inside the label type $\mathtt{t}\{\ell\}$ to the scope of $\mathtt{m}_2$ (T-Bind).

The label protection judgement $\Delta \vdash \mathtt{t}_2 \gg \ell$ ensures that the result of `bind` still protects the data from labels lower than or incomparable to ℓ in the lattice.

Example 1. *The following term*

$$\Lambda\alpha \preceq \top.\ \lambda \mathtt{x}{:}\texttt{<}\alpha,\alpha\texttt{>}\{\mathtt{H}\}.\ \mathtt{bind\ y = x\ in\ (prj}_1\ \mathtt{y)}\{\mathtt{H}\}$$

is well-typed to be $\forall\alpha \preceq \top.\ \texttt{<}\alpha,\alpha\texttt{>}\{\mathtt{H}\} \to \alpha\{\mathtt{H}\}$. *The return type of the function has the high label* `H`*, which protects the confidential input.*

This requirement of label protection is formally specified by the following rules:

$$\Delta \vdash \texttt{<>} \gg \ell \qquad \text{(P-Unit)}$$

$$\frac{\Delta \vdash \mathtt{t}_2 \gg \ell}{\Delta \vdash \mathtt{t}_1 \to \mathtt{t}_2 \gg \ell} \qquad \text{(P-Fun)}$$

$$\frac{\Delta, \alpha \preceq \mathtt{t}_1 \vdash \mathtt{t}_2 \gg \ell}{\Delta \vdash \forall\alpha \preceq \mathtt{t}_1.\mathtt{t}_2 \gg \ell} \qquad \text{(P-All)}$$

$$\frac{\Delta \vdash \ell_2 \preceq \ell_1}{\Delta \vdash \mathtt{t}\{\ell_1\} \gg \ell_2} \qquad \text{(P-Lab1)}$$

$$\frac{\Delta \vdash \mathtt{t} \gg \ell_2}{\Delta \vdash \mathtt{t}\{\ell_1\} \gg \ell_2} \qquad \text{(P-Lab2)}$$

Terms of type unit `<>` never leaks information, hence such type protects any label (P-Fun). A function protects the data as long as the return type of the function protects the data (P-Fun). Quantified types introduce bounded assumptions into the contexts (P-All). However, since we do not have lower bounds for quantifications, a type variable does not protect a label.

The interesting cases are those for the monadic label types. A label at a *higher* (or equal) level in the lattice sufficiently protects the results at a lower level (P-Lab1). On the other hand, a label at a *lower* (or *incomparable*) level of computation does not protect data at a *higher* label in the lattice, unless the contents are already protected at the higher level (P-Lab2).

Example 2. *The following term*

$$\lambda \mathtt{x}{:}\mathtt{bool}\{\mathtt{H}\}.\ \mathtt{bind\ y = x\ in\ if\ y\ then\ 0\ else\ 1}$$

is not *well-typed because it leaks information about the high boolean input without protecting the return value .*

Operationally, the label monad $\mathtt{m}\{\ell\}$ evaluates the term inside until it becomes a value $\mathtt{v}\{\ell\}$, while `bind` evaluates $\mathtt{m}_1$ to a value $\mathtt{v}\{\ell\}$ and substitutes `v` for `x` in $\mathtt{m}_2$. We specify the dynamic semantics by the following syntax of values `v` and evaluation contexts `E` in additional to the small-step computation rules [54]. We use

$\mathtt{m}\{\mathtt{v}/\mathtt{x}\}$ to denote capture-free substitution of $\mathtt{v}$ for $\mathtt{x}$ in $\mathtt{m}$.

$$\begin{array}{rcl} \mathtt{v} & ::= & \ldots \mid \mathtt{v}\{\ell\} \\ \mathtt{E} & ::= & \ldots \mid \mathtt{E}\{\ell\} \mid \mathtt{bind\ x = E\ in\ m} \end{array}$$

$$\mathtt{bind\ x = v}\{\ell\}\ \mathtt{in\ m} \longrightarrow \mathtt{m}\{\mathtt{v}/\mathtt{x}\} \quad \text{(E-Bind)}$$

DCC has also fixpoints and pointed types, which we will add to our core calculus in Section 2.4, after introducing an effect system in Section 2.3.

2.2 Security theorems

Before we go on to enrich the language with features such as effects and fixpoints, let us state and prove two important theorems that guarantee the security of programs written in our language.

The first theorem is the soundness property of the language, which we have proved using the standard progress and preservation theorems. Soundness states that if a program is well-typed, the evaluation will not get stuck or generate any error. Proofs can also be found in standard references [9, 39, 14, 6, 1, 38].

Theorem 3 (Progress and preservation).

1. *If* $\cdot;\ \cdot \vdash \mathtt{m}_1 : \mathtt{t}$, *then either* $\mathtt{m}_1 = \mathtt{v}$ *or* $\mathtt{m}_1 \longrightarrow \mathtt{m}_2$.
2. *If* $\Delta;\ \Gamma \vdash \mathtt{m}_1 : \mathtt{t}$ *and* $\mathtt{m}_1 \longrightarrow \mathtt{m}_2$, *then* $\Delta;\ \Gamma \vdash \mathtt{m}_2 : \mathtt{t}$.

The second theorem is the noninterference property of the language, which states that if a program is well-typed, a low-level observer cannot distinguish the high-level computations. The theorem requires a model of *observers*, or *adversaries*, to specify what information leaks are possible. Our model here is that, given a predefined equivalence relation over values of the same type, a well-typed observer cannot distinguish *equivalent values*, which are parameterized by the security label of the observer.

For example, if we encode Booleans in our language using unit and sums, we should have these equivalences:

$$\begin{array}{rcll} \mathtt{true} & \sim_\zeta & \mathtt{true} & : \mathtt{bool} \\ \mathtt{true} & \not\sim_\zeta & \mathtt{false} & : \mathtt{bool} \\ \mathtt{true\{H\}} & \sim_\mathtt{L} & \mathtt{false\{H\}} & : \mathtt{bool\{H\}} \end{array}$$

The first two lines say that any observers at the level ζ cannot distinguish `true` from `true` as they are syntactically the same, but can tell the difference between `true` and `false`. More interestingly, the third line says that if the values are protected under the high label `H`, then different Boolean values become indistinguishable to the low-level observer `L`, assuming $\mathtt{H} \not\preceq \mathtt{L}$.

Based on the intuition above, we generalize the equivalence relation in the following ways: (1) extend the relation to be higher-order, to account for functions; (2) parameterize the relation with arbitrary labels; (3) cover all types and values in the relation; and, (4) lift the relation from values to terms by evaluation.

Formally, this logical equivalence relation is defined by the following rules. We denote the value equivalence relation at type $\mathtt{t}$ by $\mathtt{v} \sim_\zeta \mathtt{v} : \mathtt{t}$ and the term equivalence relation at type $\mathtt{t}$ by $\mathtt{m} \approx_\zeta \mathtt{m} : \mathtt{t}$:

$$\frac{\forall(\mathtt{v}_3 \sim_\zeta \mathtt{v}_4 : \mathtt{t}_1).\ \mathtt{v}_1\ \mathtt{v}_3 \approx_\zeta \mathtt{v}_2\ \mathtt{v}_4 : \mathtt{t}_2}{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}_1 \to \mathtt{t}_2} \quad \text{(R-Fun)}$$

$$\frac{\ell \preceq \zeta \quad \mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}}{\mathtt{v}_1\{\ell\} \sim_\zeta \mathtt{v}_2\{\ell\} : \mathtt{t}\{\ell\}} \quad \text{(R-Lab1)}$$

$$\frac{\ell \not\preceq \zeta}{\mathtt{v}_1\{\ell\} \sim_\zeta \mathtt{v}_2\{\ell\} : \mathtt{t}\{\ell\}} \quad \text{(R-Lab2)}$$

$$\frac{\forall(\mathtt{t}_2 \preceq \mathtt{t}_1).\ \mathtt{v}_1\ [\mathtt{t}_2] \approx_\zeta \mathtt{v}_2\ [\mathtt{t}_2] : \mathtt{t}\{\mathtt{t}_2/\alpha\}}{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \forall\alpha \preceq \mathtt{t}_1.\ \mathtt{t}} \quad \text{(R-All)}$$

$$\frac{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}\{\mathtt{t}_1/\alpha\}}{\begin{array}{l}\mathtt{pack\ (t_1, v_1)\ as}\ \exists\alpha \preceq \mathtt{t}_2.\mathtt{t} \\ \sim_\zeta \mathtt{pack\ (t_1, v_2)\ as}\ \exists\alpha \preceq \mathtt{t}_2.\mathtt{t} : \exists\alpha \preceq \mathtt{t}_2.\mathtt{t}\end{array}} \quad \text{(R-Some)}$$

$$\frac{\mathtt{m}_1 \longrightarrow^* \mathtt{v}_1 \quad \mathtt{m}_2 \longrightarrow^* \mathtt{v}_2 \quad \mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}}{\mathtt{m}_1 \approx_\zeta \mathtt{m}_2 : \mathtt{t}} \quad \text{(R-Term)}$$

The rule R-Term is well-founded because our calculus is normalizing. Note that we do not deal with parametricity of polymorphic functions [52] nor the behavioral equivalence of existential packages [41]. That is, we assume that an observer can differentiate different implementations of polymorphic functions or existential packages. This assumption simplifies the equivalence relations and suffices for the proof for noninterference. This is, in fact, the key difference between noninterference and relational parametricity.

The last step is to model an arbitrary observer as an open term with type variables and term variables, and model observations as type substitutions δ and term substitutions γ, which are defined as:

$$\begin{array}{rcl} \delta & ::= & \cdot \mid \delta, \alpha \mapsto \mathtt{t} \\ \gamma & ::= & \cdot \mid \gamma, \mathtt{x} \mapsto \mathtt{v} \end{array}$$

A new judgement $\delta \models \Delta$ says that a type substitution models a type context Δ, meaning that, for all $\alpha \in \mathtt{dom}(\delta) = \mathtt{dom}(\Delta)$, if $\delta(\alpha) = \mathtt{t}_1$ and $\alpha \preceq \mathtt{t}_2 \in \Delta$, then $\mathtt{t}_1$ is closed, has the same kind as $\mathtt{t}_2$, and $\Delta \vdash \mathtt{t}_1 \preceq \mathtt{t}_2$.

Similarly, a new judgement $\gamma_1 \sim_\zeta \gamma_2 : \delta(\Gamma)$ says that two term substitutions are equivalent at the term context of closed types, meaning that, for all $\mathtt{x} \in \mathtt{dom}(\gamma_1) = \mathtt{dom}(\gamma_2) = \mathtt{dom}(\delta(\Gamma))$, if $\gamma_1(\mathtt{x}) = \mathtt{v}_1$, $\gamma_2(\mathtt{x}) = \mathtt{v}_2$ and $\mathtt{x}{:}\mathtt{t} \in \delta(\Gamma)$, then $\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}$.

With the logical relations and the substitutions above, we can formally state the main theorem of the core label calculus: related substitutions preserve the logical equivalence. In other words, an arbitrary observer cannot distinguish values higher in the lattice.

Theorem 4 (Noninterference for terms). *If* $\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t}$ *and* $\delta \models \Delta$ *and* $\gamma_1 \sim_\zeta \gamma_2 : \delta(\Gamma)$*, then* $\delta\gamma_1(\mathtt{m}) \approx_\zeta \delta\gamma_2(\mathtt{m}) : \delta(\mathtt{t})$.

Proof. By induction on the typing derivation. Case T-Bind: We are given $\Delta;\ \Gamma \vdash \mathtt{bind\ x = m_1\ in\ m_2} : \mathtt{t_2}$. By inversion, we have $\Delta;\ \Gamma \vdash \mathtt{m_1} : \mathtt{t_1}\{\ell\}$ (*1) and $\Delta;\ \Gamma, \mathtt{x}:\mathtt{t_1} \vdash \mathtt{m_2} : \mathtt{t_2}$ (*2) and $\Delta \vdash \mathtt{t_2} \gg \ell$ (*3). By induction hypothesis with (*1), we have

$$\delta\gamma_1(\mathtt{m_1}) \approx_\zeta \delta\gamma_2(\mathtt{m_2}) : \delta(\mathtt{t_1}\{\ell\})$$

By inversion of T-Term, $\delta\gamma_1(\mathtt{m_1}) \longrightarrow^* \mathtt{v_2}$ (*4) and $\delta\gamma_2(\mathtt{m_1}) \longrightarrow^* \mathtt{v_2}$ (*5) and $\mathtt{v_1} \sim_\zeta \mathtt{v_2} : \delta(\mathtt{t_1}\{\ell\})$.

Subcase $\delta(\ell) \preceq \zeta$: By the inversion of R-Lab1, $\mathtt{v_1} = \mathtt{v_3}\{\ell\}$ and $\mathtt{v_2} = \mathtt{v_4}\{\ell\}$ and $\mathtt{v_3} \sim_\zeta \mathtt{v_4} : \delta(\mathtt{t_1})$ (*6). We then extend the term substitutions as

$$\begin{array}{rcl} \gamma_1' & = & \gamma_1, \mathtt{x} \mapsto \mathtt{v_3} \\ \gamma_2' & = & \gamma_2, \mathtt{x} \mapsto \mathtt{v_4} \end{array}$$

such that, by (*6), we have $\gamma_1' \sim_\zeta \gamma_2' : \delta(\Gamma, \mathtt{x}:\mathtt{t_1})$ (*7). By induction hypothesis with (*2,*7), we have

$$\delta\gamma_1'(\mathtt{m_2}) \approx_\zeta \delta\gamma_2'(\mathtt{m_2}) : \delta(\mathtt{t_2})$$

which means that $\delta\gamma_1(\mathtt{m_2})\{\mathtt{v_3/x}\} \approx_\zeta \delta\gamma_2(\mathtt{m_2})\{\mathtt{v_4/x}\} : \delta(\mathtt{t_2})$ (*8). By (*4,*5),

$$\begin{array}{rl} & \delta\gamma_1(\mathtt{bind\ x = m_1\ in\ m_2}) \\ = & \mathtt{bind\ x} = \delta\gamma_1(\mathtt{m_1})\ \mathtt{in}\ \delta\gamma_1(\mathtt{m_2}) \\ \longrightarrow^* & \mathtt{bind\ x} = \mathtt{v_3}\{\ell\}\ \mathtt{in}\ \delta\gamma_1(\mathtt{m_2}) \\ \longrightarrow & \delta\gamma_1(\mathtt{m_2})\{\mathtt{v_3/x}\} \end{array}$$

$$\begin{array}{rl} & \delta\gamma_2(\mathtt{bind\ x = m_1\ in\ m_2}) \\ = & \mathtt{bind\ x} = \delta\gamma_2(\mathtt{m_1})\ \mathtt{in}\ \delta\gamma_2(\mathtt{m_2}) \\ \longrightarrow^* & \mathtt{bind\ x} = \mathtt{v_4}\{\ell\}\ \mathtt{in}\ \delta\gamma_2(\mathtt{m_2}) \\ \longrightarrow & \delta\gamma_2(\mathtt{m_2})\{\mathtt{v_4/x}\} \end{array}$$

Therefore, by R-Term and (*8), we conclude that $\delta\gamma_1(\mathtt{bind\ x = m_1\ in\ m_2}) \approx_\zeta \delta\gamma_2(\mathtt{bind\ x = m_1\ in\ m_2}) : \delta(\mathtt{t_2})$.

Subcase $\delta(\ell) \not\preceq \zeta$: by Lemma 5 with (*3). □

Lemma 5 (Noninterference for protected terms). *If* $\Delta \vdash \mathtt{t} \gg \ell$*,* $\delta \models \Delta$ *and* $\delta(\ell) \not\preceq \zeta$*, then* $\mathtt{m_1} \approx_\zeta \mathtt{m_2} : \mathtt{t}$.

2.3 Monadic effects

We now turn to study information flows in the presence of computational effects. Practical programs interact with external systems and produce effects (Section 3.5). Therefore, we need to refine the type system in order to prevent information leaks through such side effects.

We again follows the monadic style of adding new types for computation effects [53, 23, 30, 12], allowing a modular presentation of the full calculus. We introduce a new syntactic class $\mathtt{e}$ for *effectful expressions* to distinguish from $\mathtt{m}$ for *pure terms* in Section 2.1:

$$\begin{array}{rcl} \epsilon & \equiv & \ell \\ \mathtt{t} & ::= & \ldots \mid \mathtt{t!}\epsilon \\ \text{Ⓢ} & ::= & \ldots \mid \oplus\,!\ominus \\ \mathtt{e} & ::= & \mathtt{return\ m} \mid \mathtt{run\ x = m\ in\ e} \\ \mathtt{m} & ::= & \ldots \mid \mathtt{e!}\epsilon \end{array}$$

We treat effects as outputs at a given label ℓ, which are visible to an observer of level ζ if $\ell \preceq \zeta$. An observer cannot tell the difference between effects of different labels, but can count the number of visible effects happening in the program. This treatment gives us a uniform way of modeling language features with effects and could easily be extended to effects that carry additional values.

Effectful expressions are $\mathtt{return\ m}$ and $\mathtt{run\ x = m\ in\ e}$, which explicitly specify the order the execution. The term $\mathtt{e!}\epsilon$ delays the effects ϵ in $\mathtt{e}$ and thus can be considered pure, but has the monadic effect type $\mathtt{t!}\epsilon$. Here ϵ is a lower bound on the labels of observable effects happening in $\mathtt{e}$.

The typing judgement for effectful expressions is $\Delta;\ \Gamma \vdash \mathtt{e} : \mathtt{t!}\epsilon$, which says under the type context Δ and term context Γ, the effectful expression $\mathtt{e}$ has the monadic effect type $\mathtt{t!}\epsilon$. The following are the typing rules for the new constructs:

$$\frac{\Delta;\ \Gamma \vdash \mathtt{e} : \mathtt{t!}\epsilon \quad \Delta \vdash \epsilon :: \mathtt{L}}{\Delta;\ \Gamma \vdash \mathtt{e!}\epsilon : \mathtt{t!}\epsilon} \quad \text{(T-Eff)}$$

$$\frac{\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t}}{\Delta;\ \Gamma \vdash \mathtt{return\ m} : \mathtt{t!}\top} \quad \text{(T-Ret)}$$

$$\frac{\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t_1!}\epsilon \quad \Delta;\ \Gamma, \mathtt{x}:\mathtt{t_1} \vdash \mathtt{e} : \mathtt{t_2!}\epsilon}{\Delta;\ \Gamma \vdash \mathtt{run\ x = m\ in\ e} : \mathtt{t_2!}\epsilon} \quad \text{(T-Run)}$$

As we *encapsulate* an expression $\mathtt{e}$ of type $\mathtt{t!}\epsilon$, the term $\mathtt{e!}\epsilon$ also has type $\mathtt{t!}\epsilon$ (T-Eff). We just need to make sure the effect is well-kinded to be a label. The expression $\mathtt{return\ m}$ has no effect, as the computation is over, and hence it has the empty effect $\top$ (T-Ret). We interpret the effect at $\top$ to be visible to no-one, while the effect at $\bot$ to be visible to everyone. The typing rule for $\mathtt{run}$ simply threads the types and effects through the judgement (T-Run); it could have been written as

$$\frac{\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t_1!}\epsilon_1 \quad \Delta;\ \Gamma, \mathtt{x}:\mathtt{t_1} \vdash \mathtt{e} : \mathtt{t_2!}\epsilon_2}{\Delta;\ \Gamma \vdash \mathtt{run\ x = m\ in\ e} : \mathtt{t_2!}\epsilon_1 \wedge \epsilon_2} \quad \text{(T-Run')}$$

but instead we take advantage of the following subsumption rule to make the notation slightly lighter:

$$\frac{\Delta;\ \Gamma \vdash \mathtt{e} : \mathtt{t_1!}\epsilon_1 \quad \Delta \vdash \mathtt{t_1} \preceq \mathtt{t_2} \quad \Delta \vdash \epsilon_2 \preceq \epsilon_1}{\Delta;\ \Gamma \vdash \mathtt{e} : \mathtt{t_2!}\epsilon_2} \quad \text{(T-Sub)}$$

The evaluation judgement for expressions is $\mathtt{e} \xrightarrow{\epsilon} \mathtt{e}$, where ϵ accounts for the side effect during the computation:

$$\mathtt{run\ x = (return\ v)!}\epsilon\ \mathtt{in\ e} \xrightarrow{\epsilon} \mathtt{e}\{\mathtt{v/x}\} \quad \text{(E-Run)}$$

$$\begin{array}{rcl} \mathtt{u} & ::= & \mathtt{return\ v} \\ \mathtt{E} & ::= & \ldots \mid \mathtt{return\ E} \mid \mathtt{run\ x = E\ in\ e} \\ & & \mid \mathtt{run\ x = (return\ E)!}\epsilon\ \mathtt{in\ e} \\ \mathtt{v} & ::= & \ldots \mid \mathtt{e!}\epsilon \end{array}$$

We use $\mathtt{u}$ to denote the values for expressions, which for now contains `return v` only. Since the small-step congruence rules for expressions have no computational effects, we can still use evaluation contexts $\mathtt{E}$ to describe the order of evaluation for expressions. The term $\mathtt{e!}\epsilon$ is a value because it is a closure that delays computation.

Example 6. *The following expression of type* `bool!L` *evaluates as:*

$$
\begin{array}{rl}
 & \mathtt{run\ x = (run\ y = (return\ prj_2\ <true,false>)!L} \\
 & \quad \mathtt{in\ return\ y)!H\ in\ return\ x} \\
\longrightarrow & \mathtt{run\ x = (run\ y = (return\ false)!L} \\
 & \quad \mathtt{in\ return\ y)!H\ in\ return\ x} \\
\xrightarrow{\mathtt{L}} & \mathtt{run\ x = (return\ y)\{false/y\}!H\ in\ return\ x} \\
= & \mathtt{run\ x = (return\ false)!H\ in\ return\ x} \\
\xrightarrow{\mathtt{H}} & \mathtt{(return\ x)\{false/x\}!H} \\
= & \mathtt{return\ false}
\end{array}
$$

Let us consider the interaction between labels and effects, and extend the observer model to prove the noninterference theorem for expressions. First, the label protection rule for `bind` has to account for the new type:

$$\frac{\Delta \vdash \mathtt{t} \gg \ell \quad \Delta \vdash \ell \preceq \epsilon}{\Delta \vdash \mathtt{t!}\epsilon \gg \ell} \quad \text{(P-Eff)}$$

The rule says that the underlying type must protect the label and the computation must generate effects higher than the label. In other words, once the program has bound high-security data, it may not produce low observable effects.

Example 7. *Let* $\mathtt{c} \equiv \mathtt{return\ <>}$*. Under the term context* $\Gamma = \mathtt{x{:}bool\{H\}}$*, the program* $\mathtt{e}$

$$\mathtt{bind\ y = x\ in\ if\ y\ then\ c!\{H\}\ else\ c!\{L\}\ in\ c}$$

whose the body of the bind has type `<>!L`*, is insecure. The program leaks information about the high boolean through side effect: a low-level observer can distinguish* $\gamma_1(\mathtt{e})$ *from* $\gamma_2(\mathtt{e})$ *where*

$$\gamma_1 = \mathtt{x} \mapsto \mathtt{true\{H\}} \qquad \gamma_2 = \mathtt{x} \mapsto \mathtt{false\{H\}}$$

But $\gamma_1 \sim_{\mathtt{L}} \gamma_2 : \Gamma$ *because* $\mathtt{true\{H\}} \sim_{\mathtt{L}} \mathtt{false\{H\}} : \mathtt{bool\{H\}}$.

To model that an observer can now distinguish programs due to computational effects [28], we need the following new equivalence judgements for effectful terms and effectful values: $\mathtt{e} \approx_\zeta \mathtt{e} : \mathtt{t!}\epsilon$ and $\mathtt{u} \sim_\zeta \mathtt{u} : \mathtt{t!}\epsilon$. The rules for expressions make use of a new evaluation relation, $\mathtt{e} \overset{\zeta}{\Longrightarrow}^{\mathtt{n}} \mathtt{u}$, which will be explained soon.

$$\frac{\mathtt{e_1} \approx_\zeta \mathtt{e_2} : \mathtt{t}\epsilon}{\mathtt{e_1!}\epsilon \sim_\zeta \mathtt{e_2!}\epsilon : \mathtt{t!}\epsilon} \quad \text{(R-Eff)}$$

$$\frac{\mathtt{v_1} \sim_\zeta \mathtt{v_2} : \mathtt{t}}{\mathtt{return\ v_1} \sim_\zeta \mathtt{return\ v_2} : \mathtt{t!}\epsilon} \quad \text{(R-Ret)}$$

$$\frac{\mathtt{e_1} \overset{\zeta}{\Longrightarrow}^{\mathtt{n}} \mathtt{u_1} \quad \mathtt{e_2} \overset{\zeta}{\Longrightarrow}^{\mathtt{n}} \mathtt{u_2} \quad \mathtt{u_1} \sim_\zeta \mathtt{u_2} : \mathtt{t!}\epsilon}{\mathtt{e_1} \approx_\zeta \mathtt{e_2} : \mathtt{t!}\epsilon} \quad \text{(R-Exp)}$$

The first two rules simply connect the term equivalence and the expression equivalence of monadic effects (R-Eff and R-Ret). Expressions are equivalent if they produce the same number of effects visible to the observer and halt at equivalent values (R-Exp).

To formalize such a notion of equivalence, we first partition evaluation steps into those that are *visible* and those that are *invisible* to the observer:

$$
\begin{array}{rcl}
\xrightarrow{\preceq\zeta} & \equiv & \bigcup_{\ell \preceq \zeta} \xrightarrow{\ell} \\
\xrightarrow{\not\preceq\zeta} & \equiv & \bigcup_{\ell \not\preceq \zeta} \xrightarrow{\ell}
\end{array}
$$

Then, a visible evaluation step can be prefixed and suffixed with any number of invisible evaluation steps. The evaluation judgement we want is therefore the $\mathtt{n}$-step closure $\mathtt{e} \overset{\zeta}{\Longrightarrow}^{\mathtt{n}} \mathtt{u}$ of the following relation:

$$\overset{\zeta}{\Longrightarrow} \quad \equiv \quad \xrightarrow{\not\preceq\zeta}{}^{*} \circ \xrightarrow{\preceq\zeta} \circ \xrightarrow{\not\preceq\zeta}{}^{*}$$

Note that $\xrightarrow{\not\preceq\zeta}{}^{*} \circ \xrightarrow{\preceq\zeta}$ is the composition of the two relations, while $\xrightarrow{\not\preceq\zeta}{}^{*}$ is the reflexive and transitive closure of $\xrightarrow{\not\preceq\zeta}$.

Having refined our observer model as above, we proceed to proving noninterference for our core calculus with effectful expressions. The main idea is to keep track the number of visible effects produced during the evaluation.

Theorem 8 (Noninterference for expressions). *If* $\Delta;\ \Gamma \vdash \mathtt{e} : \mathtt{t!}\epsilon$ *and* $\delta \models \Delta$ *and* $\gamma_1 \sim_\zeta \gamma_2 : \delta(\Gamma)$*, then* $\delta\gamma_1(\mathtt{e}) \approx_\zeta \delta\gamma_2(\mathtt{e}) : \delta(\mathtt{t})!\delta(\epsilon)$.

Proof. By mutual induction with Theorem 4 (extended with T-Eff) on the typing derivation. Case T-Ret: We are given $\Delta;\ \Gamma \vdash \mathtt{return\ m} : \mathtt{t!}\top$. By inversion, we have $\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t}$. By Theorem 4, we have

$$\delta\gamma_1(\mathtt{m}) \approx_\zeta \delta\gamma_2(\mathtt{m}) : \delta(\mathtt{t})$$

By inversion of R-Term, $\delta\gamma_1(\mathtt{m}) \longrightarrow^* \mathtt{v_1}$ and $\delta\gamma_2(\mathtt{m}) \longrightarrow^* \mathtt{v_2}$ and $\mathtt{v_1} \sim_\zeta \mathtt{v_2} : \delta(\mathtt{t})$. Therefore, by R-Ret, we conclude that

$$\delta\gamma_1(\mathtt{return\ m}) \approx_\zeta \delta\gamma_2(\mathtt{return\ m}) : \delta(\mathtt{t})!\delta(\epsilon)$$

Case T-Run: We are given $\Delta;\ \Gamma \vdash \mathtt{run\ x = m\ in\ e} : \mathtt{t_2!}\epsilon$. By inversion, we have $\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t_1!}\epsilon$ (*1) and $\Delta;\ \Gamma, \mathtt{x{:}t_1} \vdash \mathtt{e} : \mathtt{t_2!}\epsilon$ (*2). By Theorem 4 with (*1), we have

$$\delta\gamma_1(\mathtt{m}) \approx_\zeta \delta\gamma_2(\mathtt{m}) : \delta(\mathtt{t_1})!\delta(\epsilon)$$

By inversion of R-Term, $\delta\gamma_1(\mathtt{m}) \longrightarrow^* \mathtt{v_1}$ (*3) and $\delta\gamma_2(\mathtt{m}) \longrightarrow^* \mathtt{v_2}$ (*4) and $\mathtt{v_1} \sim_\zeta \mathtt{v_2} : \delta(\mathtt{t_1})!\delta(\epsilon)$. By inversion of R-Ret, $\mathtt{v_1} = \mathtt{e_1}!\delta(\epsilon)$ and $\mathtt{v_2} = \mathtt{e_2}!\epsilon$ and $\mathtt{e_1} \approx_\zeta \mathtt{e_2} : \delta(\mathtt{t_1})!\delta(\epsilon)$. By inversion of R-Exp, $\mathtt{e_1} \overset{\zeta}{\Longrightarrow}^{\mathtt{n}} \mathtt{u_1}$ (*5) and $\mathtt{e_2} \overset{\zeta}{\Longrightarrow}^{\mathtt{n}} \mathtt{u_2}$ and $\mathtt{u_1} \sim_\zeta \mathtt{u_2} : \delta(\mathtt{t_1})$:

$\delta(\epsilon)$ (*6). By inversion of R-Ret, $u_1 = \texttt{return}\ v_3!\delta(\epsilon)$ and $u_2 = \texttt{return}\ v_4!\delta(\epsilon)$.

We then extend the term substitutions as

$$\begin{array}{rcl}\gamma_1' & = & \gamma_1, x \mapsto v_3 \\ \gamma_2' & = & \gamma_2, x \mapsto v_4\end{array}$$

such that $\gamma_1' \sim_\zeta \gamma_2' : \delta(\Gamma, x : t_1)$ (*7). By induction hypothesis with (*2,*7), we have

$$\delta\gamma_1'(e) \approx_\zeta \delta\gamma_2'(e) : \delta(t_2)!\delta(\epsilon)$$

which means that $\delta\gamma_1(e)\{v_3/x\} \approx_\zeta \delta\gamma_2(e)\{v_4/x\} : \delta(t_2)!\delta(\epsilon)$ (*8). By (*3,*4,*5,*6),

$$\begin{array}{rl} & \delta\gamma_1(\texttt{run}\ x = m\ \texttt{in}\ e) \\ = & \texttt{run}\ x = \delta\gamma_1(m)\ \texttt{in}\ \delta\gamma_1(e) \\ \longrightarrow^* & \texttt{run}\ x = e_1!\delta(\epsilon)\ \texttt{in}\ \delta\gamma_1(e) \\ \stackrel{\zeta}{\Longrightarrow}^n & \texttt{run}\ x = (\texttt{return}\ v_3)!\delta(\epsilon)\ \texttt{in}\ \delta\gamma_1(e) \\ \stackrel{\epsilon}{\longrightarrow} & \delta\gamma_1(e)\{v_3/x\} \end{array}$$

$$\begin{array}{rl} & \delta\gamma_2(\texttt{run}\ x = m\ \texttt{in}\ e) \\ = & \texttt{run}\ x = \delta\gamma_2(m)\ \texttt{in}\ \delta\gamma_2(e) \\ \longrightarrow^* & \texttt{run}\ x = e_2!\delta(\epsilon)\ \texttt{in}\ \delta\gamma_2(e) \\ \stackrel{\zeta}{\Longrightarrow}^n & \texttt{run}\ x = (\texttt{return}\ v_4)!\delta(\epsilon)\ \texttt{in}\ \delta\gamma_2(e) \\ \stackrel{\epsilon}{\longrightarrow} & \delta\gamma_2(e)\{v_4/x\} \end{array}$$

That means

$$\begin{array}{lll} \delta\gamma_1(\texttt{run}\ x = m\ \texttt{in}\ e) & \stackrel{\zeta}{\Longrightarrow}^{n+1} & \delta\gamma_1(e)\{v_3/x\} \\ \delta\gamma_2(\texttt{run}\ x = m\ \texttt{in}\ e) & \stackrel{\zeta}{\Longrightarrow}^{n+1} & \delta\gamma_2(e)\{v_4/x\} \end{array}$$

Therefore, by R-Exp and (*8), we conclude that $\delta\gamma_1(\texttt{run}\ x = m\ \texttt{in}\ e) \approx_\zeta \delta\gamma_2(\texttt{run}\ x = m\ \texttt{in}\ e) : \delta(t_2)!\delta(\epsilon)$. □

2.4 Fixpoints and divergence

The last feature we add to the core label calculus is fixpoints, which are important for recursive programming. Programs with fixpoints may diverge and our observer model cannot assume termination for testing the equivalence of terms any more (R-Term and R-Exp). Moreover, effects and divergence interact; an observer can distinguish an infinite loop with no effects from another loop that keeps producing effects. Again, our strategy is to extend our type system and equivalence relation to account for divergence in the presence of effects.

Based on ideas from DCC [1], we add fixpoints `fix m` and pointed types $t^\dagger$ to our core calculus in a call-by-value setting. Fixpoints for expressions `fix x.e` allows us to write recursive programs producing effects [32]. Variables `x` is now overloaded to be both term variables and expression variables, and thus typing contexts Γ are extended to handle typing for expression variables $\Gamma, x{:}t!\epsilon$.

Pointed types are yet more monads that keep track of possible divergence of the program [21]. The unit `lift m` injects the term `m` into the monad, while the sequence operator $\texttt{seq}\ x = m_1\ \texttt{in}\ m_2$ ensures the termination of first term before evaluating the second one:

$$\begin{array}{rcl} \Gamma & ::= & \ldots \mid \Gamma, x{:}t!\epsilon \\ \gamma & ::= & \ldots \mid \gamma, x \mapsto u \\ t & ::= & \ldots \mid t^\dagger \\ \textcircled{S} & ::= & \ldots \mid \oplus^\dagger \end{array}$$

$$\begin{array}{rcl} m & ::= & \ldots \mid \texttt{fix}\ m \mid \texttt{lift}\ m \mid \texttt{seq}\ x = m\ \texttt{in}\ m \\ e & ::= & \ldots \mid x \mid \texttt{fix}\ x{:}t!\epsilon.e \\ v & ::= & \ldots \mid \texttt{lift}\ v \\ E & ::= & \ldots \mid \texttt{fix}\ E \mid \texttt{lift}\ E \mid \texttt{seq}\ x = E\ \texttt{in}\ m \end{array}$$

$$\frac{\Delta;\ \Gamma \vdash m : t \to t \quad \Delta \vdash t \gg \dagger}{\Delta;\ \Gamma \vdash \texttt{fix}\ m : t} \quad \text{(T-Fix1)}$$

$$\frac{x{:}t!\epsilon \in \Gamma}{\Delta;\ \Gamma \vdash x : t!\epsilon} \quad \text{(T-Var2)}$$

$$\frac{\Delta;\ \Gamma, x{:}t!\epsilon \vdash e : t!\epsilon \quad \Delta \vdash t \gg \dagger}{\Delta;\ \Gamma \vdash \texttt{fix}\ x{:}t!\epsilon.\ e : t!\epsilon} \quad \text{(T-Fix2)}$$

$$\frac{\Delta;\ \Gamma \vdash m : t}{\Delta;\ \Gamma \vdash \texttt{lift}\ m : t^\dagger} \quad \text{(T-Lift)}$$

$$\frac{\Delta;\ \Gamma \vdash m_1 : t_1^\dagger \quad \Delta;\ \Gamma, x{:}t_1 \vdash m_2 : t_2 \quad \Delta \vdash t_2 \gg \dagger}{\Delta;\ \Gamma \vdash \texttt{seq}\ x = m_1\ \texttt{in}\ m_2 : t_2} \quad \text{(T-Seq)}$$

$$\texttt{fix}\ (\lambda x{:}t.m) \longrightarrow m\{\texttt{fix}\ (\lambda x{:}t.m)/x\} \quad \text{(E-Fix1)}$$

$$\texttt{fix}\ x{:}t.e \stackrel{\top}{\longrightarrow} e\{\texttt{fix}\ x{:}t.e/x\} \quad \text{(E-Fix2)}$$

$$\texttt{seq}\ x = \texttt{lift}\ v\ \texttt{in}\ m_2 \longrightarrow m_2\{v/x\} \quad \text{(E-Seq)}$$

The only new judgement is pointed protection: $\Delta \vdash t \gg \dagger$, which is defined similarly to the label protection $\Delta \vdash t \gg \ell$:

$$\Delta \vdash t^\dagger \gg \dagger \quad \text{(D-Div)}$$

$$\frac{\Delta \vdash t_2 \gg \dagger}{\Delta \vdash t_1 \to t_2 \gg \dagger} \quad \text{(D-Fun)}$$

Example 9. *The following expression* ω_L *of type* $\texttt{<>}^\dagger{:}L$ *will produce an infinite sequence of outputs at* `L`*:*

$$\omega_L = \texttt{fix}\ x{:}\texttt{<>}^\dagger!\epsilon.\ \texttt{run}\ y = (\texttt{return}\ \texttt{<>})!L\ \texttt{in}\ x$$

$$\begin{array}{rl} & \omega_L \\ \stackrel{\top}{\longrightarrow} & \texttt{run}\ y = (\texttt{return}\ \texttt{<>})!L\ \texttt{in}\ \omega_L \\ \stackrel{L}{\longrightarrow} & \omega_L\{\texttt{<>}/y\} \\ = & \omega_L \\ \stackrel{\top}{\longrightarrow} & \texttt{run}\ y = (\texttt{return}\ \texttt{<>})!L\ \texttt{in}\ \omega_L \\ \stackrel{L}{\longrightarrow} & \omega_L\{\texttt{<>}/y\} \\ \ldots & \end{array}$$

The label protection rule for pointed types (see below) allows a choice between *strong noninterference* and

weak noninterference, which determines whether the observer model is termination-sensitive. For both versions of noninterference, two terms are equivalent if they halt at equivalent values, or they both diverge. If one term halts while the other does not, the two terms are equivalent under weak noninterference, but not strong noninterference.

Therefore, strong noninterference is termination-sensitive and implies weak noninterference, which is termination-insensitive. A pointed type does not protect any label at all under strong noninterference; weak noninterference, on the other hand, permits the following label protection rule:

$$\frac{\Delta \vdash \mathtt{t} \gg \ell}{\Delta \vdash \mathtt{t}^{\dagger} \gg \ell} \quad \text{(P-Weak)}$$

According to the discussion above, we add the following rules for the value and the term equivalences. The predicate $\longrightarrow^{\omega}$ is the omega-closure of $\longrightarrow$, meaning that the program diverges and goes into an infinite loop.

$$\frac{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}}{\mathtt{lift}\ \mathtt{v}_1 \sim_\zeta \mathtt{lift}\ \mathtt{v}_2 : \mathtt{t}} \quad \text{(R-Lift)}$$

$$\frac{\mathtt{m}_1 \longrightarrow^{\omega} \quad \mathtt{m}_2 \longrightarrow^{\omega}}{\mathtt{m}_1 \approx_\zeta \mathtt{m}_2 : \mathtt{t}} \quad \text{(R-Strong1)}$$

$$\frac{\mathtt{m}_1 \longrightarrow^{\omega}}{\mathtt{m}_1 \approx_\zeta \mathtt{m}_2 : \mathtt{t}} \quad \text{(R-Weak1)}$$

$$\frac{\mathtt{m}_2 \longrightarrow^{\omega}}{\mathtt{m}_1 \approx_\zeta \mathtt{m}_2 : \mathtt{t}} \quad \text{(R-Weak2)}$$

Similarly, we add the rules for effectful values and expressions. The predicate $\xrightarrow{\not\preceq\zeta}{}^{\omega}$ is the omega-closure of $\xrightarrow{\not\preceq\zeta}$ (which is defined in Section 2.3), meaning that the program diverges and goes into an infinite loop that produces effects not visible to the observer at ζ.

$$\frac{\mathtt{e}_1 \xrightarrow{\not\preceq\zeta}{}^{\omega} \quad \mathtt{e}_2 \xrightarrow{\not\preceq\zeta}{}^{\omega}}{\mathtt{e}_1 \approx_\zeta \mathtt{e}_2 : \mathtt{t}!\epsilon} \quad \text{(R-Strong2)}$$

$$\frac{\mathtt{e}_1 \xrightarrow{\not\preceq\zeta}{}^{\omega}}{\mathtt{e}_1 \approx_\zeta \mathtt{e}_2 : \mathtt{t}!\epsilon} \quad \text{(R-Weak3)}$$

$$\frac{\mathtt{e}_2 \xrightarrow{\not\preceq\zeta}{}^{\omega}}{\mathtt{e}_1 \approx_\zeta \mathtt{e}_2 : \mathtt{t}!\epsilon} \quad \text{(R-Weak4)}$$

Since our language with fixpoints are no longer normalizing, the rules R-Term in Section 2.1 and R-Exp in Section 2.3 are not well-founded. Instead, we interpret them coinductively and treat $\approx_\zeta$ as the largest relation satisfying those rules.

Theorem 10 (Noninterference with fixpoints).

1. *Strong noninterference for terms: Theorem 4 with R-Strong1*
2. *Strong noninterference for expressions: Theorem 8 with R-Strong2*
3. *Weak noninterference for terms: Theorem 4 with P-Weak, R-Weak1 and R-Weak2*
4. *Weak noninterference for expressions: Theorem 8 with P-Weak, R-Weak3 and R-Weak4*

Proof sketch. The idea is to strengthen the coinductive hypothesis by defining another equivalence $\dot{\approx}_\zeta$ that satisfies the same set of rules defined above but also relates diverging terms and is closed under related substitutions of closed values. Since $\approx_\zeta$ is the largest relation satisfying these equivalence rules by definition, and $\dot{\approx}_\zeta \supseteq \approx_\zeta$ by construction, it follows that $\dot{\approx}_\zeta = \approx_\zeta$. This proof is similar to bisimulation proofs in process calculi but our language here is deterministic.

The key step is finding the appropriate strengthening of related substitutions; for instance we must relate term fixpoints as follows (and similarly for expression fixpoints):

$$\frac{\gamma_1 \dot{\sim}_\zeta \gamma_2 : \Gamma}{\gamma_1, \mathtt{x} \mapsto \gamma_1(\mathtt{fix}\ \lambda \mathtt{x{:}t.m}) \dot{\sim}_\zeta \gamma_2, \mathtt{x} \mapsto \gamma_2(\mathtt{fix}\ \lambda \mathtt{x{:}t.m}) : \Gamma, \mathtt{x{:}t}}$$

□

3 Decentralized label calculus

Having established the security property of our core calculus, we now investigate ways of extending the policy sublanguage to make security types more flexible. The key challenge is extending in a way that reuses the type machinery already present in the core.

This section shows how to integrate the decentralized label model by Myers and Liskov [35, 36] into our core label calculus. Decentralized labels allow different *principals* to specify finer-grained security policies such as *confidentiality* and *integrity*.

Combined with *run-time types*, the decentralized label calculus permits a connection between compile-time dependency analyses and the run-time public-key infrastructures. The benefit is twofold: (1) security policies can now be specified in term of information not known at compile time, such as the run-time identity of the users or the access permission of the file system; (2) more importantly, certificates can be used to regulate *declassification* and justify a conditioned version of the noninterference theorem.

3.1 Confidentiality and integrity

Confidentiality policies specify which principals allow which other principals to *read* the data; integrity policies specify which principals *trust* the data [26]. These

policy constructors, combined with the delegation relation over principals, provide a finer-grained control of security than the abstract label constants in the last section.

To model these policies, we treat principals $\mathtt{p}$ as abstract types and treat principal delegation $\mathtt{p}_1 \preceq \mathtt{p}_2$ as subtyping. That is, $\mathtt{p}_1$ is a subtype of $\mathtt{p}_2$ whenever $\mathtt{p}_1$ *delegates to* $\mathtt{p}_2$, or $\mathtt{p}_2$ is *acting for* $\mathtt{p}_1$. We also introduce two new label constructors, `R` (read) and `T` (trust), for confidentiality and integrity:

$$\begin{array}{rcl} \mathtt{p} & \equiv & \mathtt{t} \\ \ell & ::= & \ldots \mid \mathtt{R\ p\ p} \mid \mathtt{T\ p} \end{array}$$

The label $\mathtt{R\ p_1\ p_2}$ specifies the policy that a data is owned by $\mathtt{p}_1$ and that $\mathtt{p}_1$ allows $\mathtt{p}_2$ to read the data, while the label $\mathtt{T\ p}$ specifies the policy that the data is trusted by $\mathtt{p}$. As motivated in Section 2.1, intersection and union types can be used to represent sets of principals such as multiple owners, readers, and trusters.

To see why both intersection and union types are needed, let us first explain the subtyping rules of these policy constructors. For example, assume $\mathtt{p}_1$ delegates to $\mathtt{p}_2$. Then, any data owned by $\mathtt{p}_1$ is also owned by $\mathtt{p}_2$. Similarly, any data readable by $\mathtt{p}_1$ is also readable by $\mathtt{p}_2$. On the other hand, if $\mathtt{p}_1$ trusts some data, it does not necessarily mean that $\mathtt{p}_2$ trusts the data; but, if $\mathtt{p}_2$ trusts the data, $\mathtt{p}_1$ trusts it too. In short:

$$\textcircled{\scriptsize S} \ ::= \ \ldots \mid \mathtt{R} \oplus \oplus \mid \mathtt{T} \ominus$$

Because these two policy constructors have different polarities in subtyping, allowing both intersection and union types gives a natural interpretation of a principal set for confidentiality and integrity:

$$\begin{array}{rcl} \mathtt{R\ [p_1,p_2,\ldots,p_n]\ p} & = & \mathtt{R\ (p_1 \wedge p_2 \wedge \ldots \wedge p_n)\ p} \\ \mathtt{R\ p\ [p_1,p_2,\ldots,p_n]} & = & \mathtt{R\ p\ (p_1 \wedge p_2 \wedge \ldots \wedge p_n)} \\ \mathtt{T\ [p_1,p_2,\ldots,p_n]} & = & \mathtt{T\ (p_1 \vee p_2 \vee \ldots \vee p_n)} \end{array}$$

The subtyping relation above also naturally gives rise to the following default policy: data is owned, readable, and trusted by every principal; hence, putting an additional label on a data restricts access to the data and we can define a compound label as follows:

$$\mathtt{t\{\ell_1,\ldots,\ell_n\}} \ = \ \mathtt{t\{\ell_1\}\ldots\{\ell_n\}}$$

Example 11. *The following data has two security policies. The first one is a confidentiality policy saying that the data is owned by* $\mathtt{p}_1$ *and that* $\mathtt{p}_1$ *allows* $\mathtt{p}_2$ *or* $\mathtt{p}_3$ *to read the data. The second one is an integrity policy saying that both* $\mathtt{p}_1$ *and* $\mathtt{p}_2$ *trust the data.*

$$\mathtt{true\{R\ p_1\ [p_2,p_3],T\ [p_1,p_2]\}}$$

3.2 Delegation as extensible subtyping

The rest of the section discusses various downgrading mechanisms that intentionally leak information [56]. These mechanisms include:

1. *declassifying* some data to a lower label,
2. a principal *delegating* to other principals,
3. a principal *declassifying* some data to other principals for reading, and
4. a principal *endorsing* the integrity of some data.

The decentralized label model is essential in the last three mechanisms because each of those downgrading concerns a particular *principal*. In Section 3.4 we will see how a public key, which represents the concerned principal, can be used to verify a digital certificate in order to establish the *authority* for downgrading.

Here we start with a minimal extension to our calculus to study *delegation*, the simplest and coarsest of these three mechanisms, and show *extensible subtyping* can model delegation. The motivation is that delegation for a principal can be made *implicit* if the principal *explicitly* introduces the authority of such delegation in the program context [49]. This contrasts with the usual coercion approach that uses explicit constructs like `declassify m to` ℓ and `endorse p in m` for declassification and endorsement [35, 36]. Both approaches ensure that the authority of the concerned principal is granted before declassification. Our implicit approach allows a simple formulation of certificate-based declassification in Section 3.4.

We extend the type context Δ to keep track of the set of authority during typing. For now the only possible authority is $\mathtt{p}_1 \lhd \mathtt{p}_2$ for $\mathtt{p}_1$ delegating to $\mathtt{p}_2$. The following rule allows *extensible subtyping* for modeling delegation:

$$\frac{\mathtt{p}_1 \lhd \mathtt{p}_2 \in \Delta}{\Delta \vdash \mathtt{p}_1 \preceq \mathtt{p}_2} \quad \text{(S-Del)}$$

The term $\mathtt{let\ p_1 \lhd p_2\ in\ m}$ introduces a delegation from $\mathtt{p}_1$ to $\mathtt{p}_2$, and we assign such a term the type $\mathtt{t\ \%\ p_1 \lhd p_2}$ if $\mathtt{m}$ has the type $\mathtt{t}$. This construct, together with the term $\mathtt{pass\ x = m\ in\ m}$ for sequencing, forms a special monad for *authority*:

$$\begin{array}{rcl} \Delta & ::= & \ldots \mid \Delta, \mathtt{p} \lhd \mathtt{p} \\ \mathtt{t} & ::= & \ldots \mid \mathtt{t\ \%\ p} \lhd \mathtt{p} \\ \textcircled{\scriptsize S} & ::= & \ldots \mid \ \oplus\ \mathtt{\%}\ \ominus \lhd \oplus \\ \mathtt{m} & ::= & \ldots \mid \mathtt{let\ p} \lhd \mathtt{p\ in\ m} \mid \mathtt{pass\ x = m\ in\ m} \end{array}$$

Both the typing and evaluation rules are standard for monads, except that we extend the type context with the authority $\mathtt{p}_1 \lhd \mathtt{p}_2$ in T-Let:

$$\frac{\Delta, \mathtt{p}_1 \lhd \mathtt{p}_2;\ \Gamma \vdash \mathtt{m} : \mathtt{t} \quad \Delta \vdash \mathtt{p}_1 :: \mathtt{P} \quad \Delta \vdash \mathtt{p}_2 :: \mathtt{P}}{\Delta;\ \Gamma \vdash \mathtt{let\ p_1 \lhd p_2\ in\ m} : \mathtt{t\ \%\ p_1 \lhd p_2}} \quad \text{(T-Let)}$$

$$\frac{\begin{array}{c}\Delta;\ \Gamma \vdash \mathtt{m_1} : \mathtt{t_1\ \%\ p_1 \lhd p_2} \\ \Delta, \mathtt{p}_1 \lhd \mathtt{p}_2;\ \Gamma, \mathtt{x}{:}\mathtt{t}_1 \vdash \mathtt{m}_2 : \mathtt{t}_2\end{array}}{\Delta;\ \Gamma \vdash \mathtt{pass\ x = m_1\ in\ m_2} : \mathtt{t_2\ \%\ p_1 \lhd p_2}} \quad \text{(T-Pass)}$$

$$\Delta \vdash \mathtt{t} \preceq \mathtt{t\ \%\ p_1 \lhd p_2} \quad \text{(S-Auth)}$$

$$\begin{array}{rcl} \mathtt{v} & ::= & \ldots \mid \mathtt{let\ p} \lhd \mathtt{p\ in\ v} \\ \mathtt{E} & ::= & \ldots \mid \mathtt{let\ p} \lhd \mathtt{p\ in\ E} \mid \mathtt{pass\ x = E\ in\ e} \end{array}$$

$$\mathtt{pass\ x = (let\ p_1 \lhd p_2\ in\ v)\ in\ m} \longrightarrow \mathtt{let\ p_1 \lhd p_2\ in\ m\{v/x\}} \quad \text{(E-Pass)}$$

It is known that the noninterference theorem does not hold in the presence of downgrading [45]. Yet, it is intuitive that if the program does not use any downgrading, the program should still be secure. In fact, a slightly stronger statement holds: if no one delegates to a principal who transitively delegates to the observer, the program is still secure.

The following modified version of the noninterference theorem formally captures the intuition above. We write $\Delta = \Delta_\alpha, \Delta_\lhd$ to separate out the bindings and the authority. Also, we write $\mathtt{t} \Rightarrow \mathtt{t}_0 \,\%\, \Delta$ to collect all required authority in the value positions of the type, similar to the label protection rule $\Delta \vdash \ell \gg \mathtt{p}$.

$$\frac{\mathtt{t} \Rightarrow \mathtt{t}_0 \,\%\, \Delta}{\mathtt{t} \,\%\, \mathtt{p}_1 \lhd \mathtt{p}_2 \Rightarrow \Delta, \mathtt{p}_1 \lhd \mathtt{p}_2} \quad \text{(M-Auth)}$$

$$\frac{\mathtt{t}_2 \Rightarrow \mathtt{t} \,\%\, \Delta}{\mathtt{t}_1 \to \mathtt{t}_2 \Rightarrow (\mathtt{t}_1 \to \mathtt{t}) \,\%\, \Delta} \quad \text{(M-Fun)}$$

$$\frac{\mathtt{t}_2 \Rightarrow \mathtt{t} \,\%\, \Delta}{\forall \alpha \preceq \mathtt{t}_1.\mathtt{t}_2 \Rightarrow (\forall \alpha \preceq \mathtt{t}_1.\mathtt{t}) \,\%\, \Delta} \quad \text{(M-Poly)}$$

At last, the rule for related values at the new type is:

$$\frac{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}}{\begin{array}{l}\mathtt{let\ p_1 \preceq p_2\ in\ v_1} \\ \sim_\zeta \mathtt{let\ p_1 \preceq p_2\ in\ v_2 : t \,\%\, p_1 \preceq p_2}\end{array}} \quad \text{(R-Auth)}$$

because, from the condition of the theorem, we know that no downgrading that is visible to the observer has happened.

Theorem 12 (Conditioned noninterference). *Suppose* $\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t}$*, where* $\Delta = \Delta_\alpha, \Delta_\lhd$ *and* $\mathtt{t} \Rightarrow \mathtt{t}_0 \,\%\, \Delta_0$*, and* $\delta \models \Delta_\alpha$ *and* $\gamma_1 \sim_\zeta \gamma_2 : \delta(\Gamma)$*. If* $\Delta_0 \not\vdash \mathtt{p} \preceq \zeta$ *for all* $\mathtt{p} \in \mathtt{dom}(\Delta_\alpha)$ *such that* $\Delta \not\vdash \mathtt{p} \preceq \zeta$*, then* $\delta\gamma_1(\mathtt{m}) \approx_\zeta \delta\gamma_2(\mathtt{m}) : \delta(\mathtt{t})$*.*

Proof. By induction on the typing derivation. Case T-Fun for functions: We are given $\Delta;\ \Gamma \vdash \lambda \mathtt{x{:}t.m} : \mathtt{t}_1 \to \mathtt{t}_2$. By inversion, we have $\Delta;\ \Gamma, \mathtt{x} : \mathtt{t}_1 \vdash \mathtt{m} : \mathtt{t}_2$ (*1). By inversion of M-Fun, we have $\mathtt{t}_2 \Rightarrow \mathtt{t}_3 \,\%\, \Delta_0$ (*2) for the same Δ_0 as in $\mathtt{t} = \mathtt{t}_1 \to \mathtt{t}_2 \Rightarrow \mathtt{t}_0 \,\%\, \Delta_0$. Assume $\mathtt{v}_3 \sim_\zeta \mathtt{v}_4 : \delta(\mathtt{t}_1)$. We then extend the term substitutions as

$$\begin{array}{rcl} \gamma_1' & = & \gamma_1, \mathtt{x} \mapsto \mathtt{v}_3 \\ \gamma_2' & = & \gamma_2, \mathtt{x} \mapsto \mathtt{v}_4 \end{array}$$

such that $\gamma_1' \sim_\zeta \gamma_2' : \delta(\Gamma, \mathtt{x} : \mathtt{t}_1)$ (*3). By induction hypothesis with (*1,*2,*3), we have

$$\delta\gamma_1'(\mathtt{m}) \approx_\zeta \delta\gamma_2'(\mathtt{m}) : \delta(\mathtt{t}_2)$$

which, by R-Term, means that $\delta\gamma_1(\mathtt{m})\{\mathtt{v}_3/\mathtt{x}\} \approx_\zeta \delta\gamma_2(\mathtt{m})\{\mathtt{v}_4/\mathtt{x}\} : \delta(\mathtt{t}_2)$. By R-Term again, we have

$$\delta\gamma_1(\lambda \mathtt{x{:}t.m})\ \mathtt{v}_3 \approx_\zeta \delta\gamma_2(\lambda \mathtt{x{:}t.m})\ \mathtt{v}_4 : \delta(\mathtt{t}_2)$$

Therefore, by R-Fun, we conclude that $\delta\gamma_1(\lambda \mathtt{x{:}t.m}) \approx_\zeta \delta\gamma_2(\lambda \mathtt{x{:}t.m}) : \delta(\mathtt{t}_1 \to \mathtt{t}_2)$. □

As the proof shows, this conditioned version is only a slight generalization of the standard noninterference theorem. In Section 3.4, however, we will show how combining this theorem with ideas from public-key infrastructures justifies certificate-based declassification.

3.3 Public keys and certificates

Public-key infrastructures provide public keys and digital certificates for distributed access control. Our motivation here is to connect the type system with the security infrastructure such that a delegation certificate verified with a principal's public key can justify the information leaks due to delegation.

In our previous work [49], we presented the language λ_{RP} for specifying security policies with run-time principals. The type system uses *singleton types*, in combination with bounded polymorphism, to represent run-time principals and an abstract type to represent certificates.

Effectively, λ_{RP} models public keys and certificate verifications of public-key infrastructures in a sound type system. Since singleton types contain the same amount of information at the type level as at the term level [3], the type system can precisely analyze the authority required for delegation.

Allowing such run-time principals gives programmers more flexibility in specifying security policies. Combined with existential types, programmers can determine the run-time user identity of the system (`getuid`) or principals during authentication [24] but specify static policies parameterized by such principals. The type system enforces that such policies interact in a sound way with the rest of static analysis. Since principals, labels, and privileges are conflated as abstract types in our type system, the singleton types also allow the policies themselves to be dynamically determined at run time [60]. For example, access permissions from the file system (`fstat`) can be used to constrain the information flow of data read from the file.

We recap our previous work on run-time principals [49] here to set up the machinery necessary to prove the conditioned noninterference theorem in the next subsection:

$$\begin{array}{rcl} \mathtt{t} & ::= & \ldots \mid \mathtt{'p} \mid \mathtt{cert} \\ \textcircled{\scriptsize S} & ::= & \ldots \mid \mathtt{'}\odot \\ \mathtt{m} & ::= & \ldots \mid \mathtt{'p} \mid \mathtt{'p} \lhd \mathtt{'p} \mid \mathtt{if\ (m} \Rightarrow \mathtt{m} \lhd \mathtt{m)\ m\ m} \end{array}$$

The term `'p` represents the public key of the principal `p` and has the singleton type `'p`, carrying the most

precise information about the term in the type system. On the other hand, a digital certificate $\texttt{'p}_1 \triangleleft \texttt{'p}_2$ represents $\texttt{p}_1$ delegating to $\texttt{p}_2$ and has an abstract type `cert` that does not reveal any information at all at the type level. The reason is that we do not trust the validity of the certificate until we validate it with cryptographic verifications. Such verification is modeled with the term $\texttt{if } (\texttt{m}_1 \Rightarrow \texttt{m}_2 \triangleleft \texttt{m}_3)\ \texttt{m}_4\ \texttt{m}_5$ where $\texttt{m}_1$ is a certificate, and $\texttt{m}_2$ and $\texttt{m}_3$ are public keys representing the concerned principals, and the term takes branch $\texttt{m}_4$ or $\texttt{m}_5$ depending on the verification result. Note that a singleton type must be invariant in subtyping for a sound type system. The label protection rule for $\texttt{t \% p}_1 \preceq \texttt{p}_2$ will be shown in the next subsection.

The following typing and evaluation rules summarize our discussion:

$$\Delta;\ \Gamma \vdash \texttt{'p} : \texttt{'p} \qquad \text{(T-Sin)}$$

$$\Delta;\ \Gamma \vdash \texttt{'p}_1 \triangleleft \texttt{'p}_2 : \texttt{cert} \qquad \text{(T-Cert)}$$

$$\frac{\begin{array}{l}\Delta;\ \Gamma \vdash \texttt{m}_1 : \texttt{cert} \quad \Delta;\ \Gamma \vdash \texttt{m}_2 : \texttt{'p}_1 \\ \Delta;\ \Gamma \vdash \texttt{m}_3 : \texttt{'p}_2 \quad \Delta;\ \Gamma \vdash \texttt{m}_5 : \texttt{t} \\ \Delta, \texttt{p}_1 \triangleleft \texttt{p}_2;\ \Gamma \vdash \texttt{m}_4 : \texttt{t}\end{array}}{\Delta;\ \Gamma \vdash \texttt{if } (\texttt{m}_1 \Rightarrow \texttt{m}_2 \triangleleft \texttt{m}_3)\ \texttt{m}_4\ \texttt{m}_5 : \texttt{t \% p}_1 \triangleleft \texttt{p}_2} \qquad \text{(T-If)}$$

$$\frac{\vdash \texttt{'p}_1 \triangleleft \texttt{'p}_2 \Rightarrow \texttt{'p}_3 \triangleleft \texttt{'p}_4}{\begin{array}{l}\texttt{if } (\texttt{'p}_1 \triangleleft \texttt{'p}_2 \Rightarrow \texttt{'p}_3 \triangleleft \texttt{'p}_4)\ \texttt{m}_1\ \texttt{m}_2 \\ \quad \longrightarrow \texttt{let p}_1 \triangleleft \texttt{p}_2 \texttt{ in m}_1\end{array}} \qquad \text{(E-If1)}$$

$$\frac{\nvdash \texttt{'p}_1 \triangleleft \texttt{'p}_2 \Rightarrow \texttt{'p}_3 \triangleleft \texttt{'p}_4}{\texttt{if } (\texttt{'p}_1 \triangleleft \texttt{'p}_2 \Rightarrow \texttt{'p}_3 \triangleleft \texttt{'p}_4)\ \texttt{m}_1\ \texttt{m}_2 \longrightarrow \texttt{m}_2} \qquad \text{(E-If2)}$$

There exists a direct mapping from the language constructs ($\texttt{'p}$, $\texttt{'p} \triangleleft \texttt{'p}$, and $\vdash \texttt{'p}_1 \triangleleft \texttt{'p}_2 \Rightarrow \texttt{'p}_3 \triangleleft \texttt{'p}_4$) to the mechanisms of public-key infrastructures (public keys, certificate signed by the private key of the principal, and cryptographic verification using the public key of the principal) [49]. A public-key infrastructure is just one possible implementation that supports distributed access control. Our previous work [49] carries out the design and the proof of run-time principals in an abstract setting and provides constructs for testing delegation and acquiring certificates, which we do not explain here.

3.4 Robust declassification and endorsement

Finally we refine delegation to allow downgrading for each policy constructor: declassification $\texttt{dcls p}$ for confidentiality policy $\texttt{R p p}$, and endorsement `endr` for integrity policy $\texttt{T p}$. As mentioned in Section 2, we regard these authority as abstract types as well:

$$\begin{array}{rcl}\texttt{j} & \equiv & \texttt{t} \\ \texttt{j} & ::= & \ldots \mid \texttt{dcls p} \mid \texttt{endr} \\ \textcircled{S} & ::= & \ldots \mid \texttt{dcls} \oplus\end{array}$$

One appealing reason of modeling privileges as abstract types is that we can integrate the authority in the language simply by a slight modification of their corresponding subtyping rule of the policy constructors:

$$\Delta \vdash \texttt{p} \preceq \texttt{dcls} \top \qquad \text{(S-Dcls)}$$

$$\frac{\begin{array}{l}\Delta \vdash \texttt{p}_1 \preceq \texttt{p}_3 \\ \Delta \vdash \texttt{p} \wedge \texttt{p}_2 \preceq \texttt{p}_4 \quad \Delta \vdash \texttt{p}_1 \preceq \texttt{dcls p}\end{array}}{\Delta \vdash \texttt{R p}_1\ \texttt{p}_2 \preceq \texttt{R p}_3\ \texttt{p}_4} \qquad \text{(S-Read')}$$

$$\frac{\Delta \vdash \texttt{p} \preceq \texttt{endr} \quad \Delta \vdash \texttt{p}_2 \preceq \texttt{p} \vee \texttt{p}_1}{\Delta \vdash \texttt{T p}_1 \preceq \texttt{T p}_2} \qquad \text{(S-Trust')}$$

This modification matches our intuition how each downgrading mechanism corresponds to relaxing access control for each kind of policy. Here we treat $\texttt{dcls} \top = \top$ in the type system and allow subtyping between the principal kind `P` and the privilege kind `J`.

Another reason of treating privileges as abstract types is that we can reuse all the language constructs we have developed so far for types and apply them to privileges: polymorphism, subtyping, and run-time types. Most importantly, we can interpret the certificate $\texttt{'p}_1 \triangleleft \texttt{'(dcls p}_2\texttt{)}$ as the authority granted by principal $\texttt{p}_1$ for the program to declassify data by adding $\texttt{p}_2$ as a reader, and, similarly, we can interpret $\texttt{'p} \triangleleft \texttt{'endr}$ as the authority granted by principal `p` to endorse the integrity of the data.

As a pleasant bonus of monadic analysis, checking the *robustness condition* of downgrading reduces to adding one condition in the protection rule $\Delta \vdash \texttt{t} \gg \ell$ in Section 2.1. In particular, robust declassification says that the program context of declassification should be trusted by the owner of the data [56]. The following rule for label protection generalizes the condition to any downgrading mechanism:

$$\frac{\Delta \vdash \texttt{t} \gg \texttt{T p} \quad \Delta \vdash \texttt{p}_1 \preceq \texttt{p}}{\Delta \vdash \texttt{t \% p}_1 \triangleleft \texttt{p}_2 \gg \texttt{T p}} \qquad \text{(P-Auth)}$$

By connecting our language semantics to public-key infrastructures, we hope to justify our intuition behind certificate-based declassification: if no certificate is issued to used for the authority of downgrading, the program must still be secure; otherwise, if the program leaks information to the observer, then *some* principal must be responsible for leaking such information by signing a certificate for delegation or declassification. We rely such a justification on the following corollary of *certified* noninterference:

Corollary 13 (Certified noninterference). *Suppose* $\Delta;\ \Gamma \vdash \texttt{m} : \texttt{t}$, *where* $\Delta = \Delta_\alpha, \Delta_\triangleleft$ *and* $\texttt{t} \Rightarrow \texttt{t}_0\ \texttt{\%}\ \Delta_0$, *and* $\delta \models \Delta_\alpha$ *and* $\gamma_1 \sim_\zeta \gamma_2 : \delta(\Gamma)$. *If* $\delta\gamma_1(\texttt{m}) \not\approx_\zeta \delta\gamma_2(\texttt{m}) : \delta(\texttt{t})$, *then* $\texttt{t} = \texttt{t}_0\ \texttt{\%}\ \Delta_0$ *and* $\Delta_0 \vdash \texttt{p} \preceq \zeta$ *for some* `p` *that satisfies* $\Delta \nvdash \texttt{p} \preceq \zeta$.

Proof. By the converse of Theorem 12, extended with singletons and certificates. □

```
        Δ  =  alice, atm, bank, prt, deposit, withdraw

     login  :  <> → <∃user. 'user, cert>{R atm atm}
   request  :  ∀agent, user.<'agent, 'user, cert, cert>{R bank bank}
                   → int{R agent agent, T agent}![agent, bank]
    listen  :  <> → (∃agent, user. <'agent, 'user, cert, cert, (int{R agent agent} → <>![agent, bank])>)
                   {R bank bank, T bank}!agent
     print  :  int{R atm prt} → <>
       get  :  ∀user. 'user → int{R [user, bank] bank}
       set  :  ∀user. 'user → int{R [user, bank] bank} → <>
```

```
return
if (acquire 'atm ◁ '(dcls bank))
  ⇒ 'atm ◁ '(dcls bank) then
  bind x = login <> in
  let <y, cdel> = x in
  open (user, userid) = y in
  let creq = acquire userid ◁ withdraw in
  let msg = <'atm, userid, cdel, creq> in
  (run result = request [atm, user] msg in
    return bind balance = result in
    if (acquire 'atm ◁ '(dcls prt))
      ⇒ 'atm ◁ '(dcls prt) then
      print balance
    else <>)![atm, bank]
else error "insecure network"
```

```
run result = listen <> in
return bind x0 = result, x = x0 in
open (agent, user, y) = x in
if (acquire 'bank ◁ '(dcls user))
  ⇒ 'bank ◁ '(dcls user) then
  let <agentid, userid, cdel, creq, reply> = y in
  if cdel ⇒ userid ◁ 'agent then
    if creq ⇒ userid ◁ 'withdraw then
      let old = get [user] userid in
      let balance = bind x = old in x − 100 in
      let y = set [user] userid balance in
      (run u = reply balance in return <>)![agent, bank]
    else <>
  else error "insecure atm"
else error "insecure network"
```

Figure 1: A distributed banking example: ATM's code (left) and bank's code (right)

3.5 Implementation and proofs

We have written a prototype interpreter for our full language in OCaml [25]. Figure 1 shows a distributed banking example, which is taken from our previous work [49] but rewritten with monadic labels and effects and type-checked with the interpreter.

The example models the banking service of requesting money withdraw from the customer's account over a secure network. The action involves four principals: a bank customer `alice`, an ATM machine `atm`, the bank `bank`, and the printer terminal `prt`. Abstract privileges like `deposit` and `withdraw` represents different banking services.

We are using a construct which is explained in our previous work [49] but not here: `acquire` $\mathtt{m}_1 \triangleleft \mathtt{m}_2$ where $\mathtt{m}_1$ represents a run-time principal and $\mathtt{m}_2$ represents a run-time privilege. The construct models different ways of certification acquisitions such as preinstalled certificates, system calls, or even prompting users at the terminal.

The ATM's code starts by checking the security of the network. We use the certificate `'atm`$\triangleleft$`'(dcls bank)` to represent the trust of the ATM on the network such that the ATM allows declassification to the bank. Then, the customer `alice` enters the bank card and types in the password to login the system, revealing her own identity (`userid`) and delegating to the ATM for bank services (`cdel`). After that, the customer selects the service of withdrawing money from the terminal menu and the ATM packs the request message to the bank with its own identity, the customer's identity, the delegation certificate, and the request certificate. After the withdrawal, the ATM prompts if the customer wants to declassify her own balance to the printer terminal.

On the server's side, the bank checks the certificates to validate the delegation and the request. The bank can potentially store these certificates for auditing purposes later. The function `listen` also returns an authenticated channel `reply` for the bank to send the account balance back to the ATM. For brevity, we model only the side effects of network transmission, where `atm` and `bank` can leak information simply by sending to or receive from the network.

Besides the interpreter and examples, we also have the proofs for the soundness theorem and the corresponding noninterference theorems for the full language in the appendix

Currently, we are formalizing our language and the soundness proof in a logical framework called Twelf [37]. We bypass the higher-order abstract syntax of Twelf and encode variables using de Bruijn index. Doing this

gives us the control over the environment and the substitutions so that the typing and evaluation are closely matched with the presentation here. We have also developed a tool to visualize typing rules in Twelf as inference rules and theorem proofs in Twelf as proof derivation trees for reasoning of proof cases. One exciting future work is to prove noninterference in the logical framework; however, it seems that logical relations cannot be directly represented in Twelf [2].

We are writing larger examples in our language interpreter to gain more experience of monadic secure programming. Formalizing the full language semantics and security theorems in a logical framework is also one of our long-term goals of building a rigid foundation for security languages.

4 Related work

Security-typed languages The survey by Sabelfeld and Myers [45] on language-based information-flow security is an excellent introduction to the field. Our work builds on a long line of research for designing security-typed languages [51, 20, 1, 34, 42, 59, 43, 48, 4, 5]. Both Jif [34] and FlowCAML [43] have a comprehensive list of features for large-scale secure programming. Jif, based on the popular language Java, brings information-flow type systems with object-oriented design to mainstream programmers. Using dynamic classes, Jif also permits some form of run-time principals and authority for specifying dynamic policies. On the other hand, FlowCAML, based on the well-studied functional language ML, employs a constraint-based type system HM(X) to allow information flow inference.

This paper instead focuses on a smaller set of interesting features with the goal of a modular design. We emphasize the reuse of standard type constructs such as polymorphism and subtyping, and draw the connection to public-key infrastructures through the decentralized label model [35, 36] and singleton types [13, 49]. Chothia et al. also use public-key infrastructures to model typed cryptographic operations for distributed access control [10]. Type systems based on bounded quantifications, intersection and union types for precise specification and type refinement have been well-studied [9, 39, 40, 14, 8, 6, 55, 7, 15, 38, 16].

Monadic styles Monads are the key in the presentation of this paper, separating language features and making proofs modular. Since the introduction in the context of programming languages by Moggi [31] and their popularization by Wadler [46, 53], monads have become an established technique for reasoning and programming [17, 27, 46, 30, 23, 47, 18, 12]. Crary et al. share the same insight as we do to use monads for analyzing effects in information flow security; they focus on providing reference cells and proving noninterference with respect to equivalent heaps [12].

Noninterference Abadi et al. proved a noninterference theorem for DCC using a per semantics model [1]. Pottier and Simonet introduced a new proof technique [43] such that proving noninterference amounts to proving subject reduction for an extended operational semantics. Their lifting rules for reduction of the special pair construct are similar to our E-Pass rule in Section 3.2. We prefer syntactic proofs for noninterference with logical relations [56, 49], as this approach does not require a semantics model or modification to the calculus. Our previous work draws a connection between DCC and System F such that the standard parametricity theorem implies noninterference [50]. Hence, noninterference in the presence of computational effects [12] is closely related to parametricity with effects [11] or sequencing [22].

Declassification *Selective declassification* [42], *robust declassification* [58, 56, 57, 33], and *delimited release* [44] are proposed to allow downgrading that can be externally justified, yet still respect other constraints such as the authority of the concerned principal [56]. It is recognized that standard noninterference does not hold in the presence of declassification and it has been a challenging research problem to formulate and prove *any* variant of noninterference with declassification.

5 Conclusion

We have presented the design of a programming language that supports information-flow security policies and certificate-based declassification. We start with a base calculus with polymorphism and subtyping in order to express rich security policies. Different monads allow us to add interesting language features such as effects, fixpoints, decentralized policies and extensible subtyping in an incremental fashion. Such a monadic principle of language design makes the presentation of typing and evaluation rules, as well as the proofs, modular and easy to follow.

References

[1] Martin Abadi, Anindya Banerjee, Nevin Heintze, and Jon G. Riecke. A Core Calculus of Dependency. In *ACM Symposium on Principles of Programming Languages*, 1999.

[2] Andreas Abel. Weak Normalization for the Simply-Typed Lambda-Calculus in Twelf. In *International*

Workshop on Logical Frameworks and Meta-Languages, 2004.

[3] David Aspinall. Subtyping with Singleton Types. In *Computer Science Logic*, 1994.

[4] Anindya Banerjee and David A. Naumann. Secure Information Flow and Pointer Confinement in a Java-like Language. In *Computer Security Foundations Workshop*, 2002.

[5] Anindya Banerjee and David A. Naumann. Using Access Control for Secure Information Flow in a Java-like Language. In *Computer Security Foundations Workshop*, 2003.

[6] Franco Barbanera, Mariangiola Dezani-Ciancaglini, and Ugo de'Liguoro. Intersection and Union Types: Syntax and Semantics. *Information and Computation*, 119, 1995.

[7] Antonio Bucciarelli, Silvia De Lorenzis, Adolfo Piperno, and Ivano Salvo. Some Computational Properties of Intersection Types. In *IEEE Symposium on Logic in Computer Science*, 1999.

[8] Luca Cardelli, Simone Martini, John C. Mitchell, and Andre Scedrov. An extension of System F with subtyping. *Information and Computation*, 109(1), 1994. f-sub.

[9] Luca Cardelli and Peter Wegner. On understanding types, data abstraction, and polymorphism. *Computing Surveys*, 17(4), 1985. bounded f-sub.

[10] Tom Chothia, Dominic Duggan, and Jan Vitek. Type-Based Distributed Access Control. In *Computer Security Foundations Workshop*, 2003.

[11] Karl Crary. A Simple Proof Technique for Certain Parametricity Results. In *ACM International Conference on Functional Programming*, 1999.

[12] Karl Crary, Aleksey Kliger, and Frank Pfenning. A monadic analysis of information flow security with mutable state. In *Foundations of Computer Security Workshop*, 2004.

[13] Karl Crary, Stephanie Weirich, and J. Gregory Morrisett. Intensional Polymorphism in Type-Erasure Semantics. In *ACM International Conference on Functional Programming*, 1998.

[14] Pierre-Louis Curien and Giorgio Ghelli. Coherence of subsumption, minimum typing and type-checking in Fsub. *Mathematical Structures in Computer Science*, 1992.

[15] Rowan Davies and Frank Pfenning. Intersection types and computational effects. In *ACM International Conference on Functional Programming*, 2000.

[16] Joshua Dunfield and Frank Pfenning. Type Assignment for Intersections and Unions in Call-by-Value Languages. In *International Conference on Foundations of Software Science and Computation Structures*, 2003.

[17] Andrzej Filinski. Representing Monads. In *ACM Symposium on Principles of Programming Languages*, 1994.

[18] Matthew Fluet and Greg Morrisett. Monadic Regions. In *ACM International Conference on Functional Programming*, 2004.

[19] Joseph A. Goguen and Jose Meseguer. Security Policies and Security Models. In *IEEE Symposium on Security and Privacy*, 1982.

[20] Nevin Heintze and Jon G. Riecke. The SLam Calculus: Programming with Secrecy and Integrity. In *ACM Symposium on Principles of Programming Languages*, 1998.

[21] Brian T. Howard. Inductive, Coinductive, and Pointed Types. In *ACM International Conference on Functional Programming*, 1996.

[22] Patricia Johann and Janis Voigtlaender. Free Theorems in the Presence of seq. In *ACM Symposium on Principles of Programming Languages*, 2004.

[23] Richard B. Kieburtz. Taming Effects with Monadic Typing. In *ACM International Conference on Functional Programming*, 1998.

[24] Butler Lampson, Martín Abadi, Michael Burrows, and Edward Wobber. Authentication in distributed systems: Theory and practice. In *ACM Symposium on Operating Systems Principles*, pages 165–182, October 1991. *Operating System Review*, 253(5).

[25] Xavier Leroy. The OCaml Programming Language. `http://caml.inria.fr`.

[26] Peng Li, Yun Mao, and Steve Zdancewic. Information integrity policies. In *Proceedings of the Workshop on Formal Aspects in Security & Trust (FAST)*, September 2003.

[27] Sheng Liang, Paul Hudak, and Mark P. Jones. Monad Transformers and Modular Interpreters. In *ACM Symposium on Principles of Programming Languages*, 1995.

[28] Ian A. Mason and Carolyn L. Talcott. Axiomatizing Operational Equivalence in the Presence of Side Effects. In *IEEE Symposium on Logic in Computer Science*, 1989.

[29] Daryl McCullough. Noninterference and the Composability of Security Properties. In *IEEE Symposium on Security and Privacy*, pages 177–186, May 1988.

[30] E. Moggi and F. Palumbo. Monadic encapsulation of effects: A revised approach, 1999.

[31] Eugenio Moggi. Computational Lambda-Calculus and Monads. In *IEEE Symposium on Logic in Computer Science*, 1989.

[32] Eugenio Moggi and Amr Sabry. An Abstract Monadic Semantics for Value Recursion. In *Fixed Points in Computer Science*, 2003.

[33] Andrew Myers, Andrei Sabelfeld, and Steve Zdancewic. Enforcing Robust Declassification. In *Computer Security Foundations Workshop*, 2004.

[34] Andrew C. Myers. JFlow: Practical Mostly-Static Information Flow Control. In *ACM Symposium on Principles of Programming Languages*, 1999.

[35] Andrew C. Myers and Barbara Liskov. A Decentralized Model for Information Flow Control. In *ACM Symposium on Operating Systems Principles*, 1997.

[36] Andrew C. Myers and Barbara Liskov. Complete, Safe Information Flow with Decentralized Labels. In *IEEE Symposium on Security and Privacy*, 1998.

[37] Frank Pfenning and Carsten Schurmann. The Twelf Project. `http://www.twelf.org`.

[38] Benjamin Pierce. *Types and Programming Languages*. MIT Press, 2002.

[39] Benjamin C. Pierce. *Programming with Intersection Types and Bounded Polymorphism*. PhD thesis, Carnegie Mellon University, 1991.

[40] Benjamin C. Pierce. Programming with Intersection Types, Union Types, and Polymorphism. Technical Report CMU-CS-91-106, Carnegie Mellon University, 1991.

[41] Andrew Pitts. Existential Types: Logical Relations and Operational Equivalence. In *International Colloquium on Automata, Languages and Programming*, 1998.

[42] Francois Pottier and Sylvain Conchon. Information flow inference for free. In *ACM International Conference on Functional Programming*, 2000.

[43] Francois Pottier and Vincent Simonet. Information flow inference for ML. In *ACM Symposium on Principles of Programming Languages*, 2002.

[44] Andrei Sabelfeld and Andrew C. Myers. A Model for Delimited Release. In *International Symposium on Software Security*, 2003.

[45] Andrei Sabelfeld and Andrew C. Myers. Language-Based Information-Flow Security. *IEEE Journal on Selected Areas in Communications*, 21(1), 2003.

[46] Amr Sabry and Philip Wadler. A Reflection on Call-by-Value. In *ACM International Conference on Functional Programming*, 1996.

[47] Miley Semmelroth and Amr Sabry. Monadic Encapsulation in ML. In *ACM International Conference on Functional Programming*, 1999.

[48] Vincent Simonet. Fine-Grained Information Flow Analysis for a Lambda Calculus with Sum Types. In *Computer Security Foundations Workshop*, 2002.

[49] Stephen Tse and Steve Zdancewic. Run-time Principals in Information-flow Type Systems. In *IEEE Symposium on Security and Privacy*, 2004.

[50] Stephen Tse and Steve Zdancewic. Translating Dependency into Parametricity. In *ACM International Conference on Functional Programming*, 2004.

[51] Dennis Volpano and Geoffrey Smith. A type-based approach to program security. In *Proceedings of TAPSOFT '97, Colloquium on Formal Approaches to Software Engineering*, Lille, France, April 1997.

[52] Philip Wadler. Theorems for Free! In *Functional Programming Languages and Computer Architecture*, 1989.

[53] Philip Wadler. The Marriage of Effects and Monads. In *ACM International Conference on Functional Programming*, 1998.

[54] Andrew K. Wright and Matthias Felleisen. A Syntactic Approach to Type Soundness. *Information and Computation*, 115(1), 1994.

[55] Hirofumi Yokouchi. Completeness of Type Assignment Systems with Intersection, Union, and Type Quantifiers. In *IEEE Symposium on Logic in Computer Science*, 1998.

[56] Steve Zdancewic. *Programming Languages for Information Security*. PhD thesis, Cornell University, 1997.

[57] Steve Zdancewic. A type system for robust declassification. In *Proceedings of the Nineteenth Conference on the Mathematical Foundations of Programming Semantics*, March 2003.

[58] Steve Zdancewic and Andrew C. Myers. Robust Declassification. In *Computer Security Foundations Workshop*, 2001.

[59] Steve Zdancewic and Andrew C. Myers. Secure Information Flow and CPS. In *European Symposium on Programming*, 2001.

[60] Lantian Zheng and Andrew C. Myers. Dynamic Security Labels and Noninterference. Technical Report 2004-1924, Cornell University Computing and Information Science, 2004.

Contents

This appendix contains the full syntax, semantics and proofs of the language. Except the logical equivalence and noninterference theorem in Appendix E, all rules and proofs are mechanically generated by its formalization `apollo.elf` in Twelf, using the utility `lf2tex` (see `http://www.cis.upenn.edu/~stse/lf2tex`). The formalization is not complete: variable operations are abstract, no proofs for substitutions, function totalities, inversions, or canonical forms; yet it should still serves as a good outline to the full proof.

There are two *special* lemmas in the mechanical proof that should be mentioned: `psst` and `stinv` (page 43). We prefer the declarative style of subtyping and typing rules but still use Twelf to do *mode checking* for all rules except the subsumption rule for terms (`tyx-sub` on page 26). Hence we need to externally justify the use of subsumption with `psst` (page 43)in the preservation proof `ps-if5` (page 52). The other special lemma `stinv` is asserting that the canonical form of the typing derivation for `run x = (return v)!ϵ in m` involves the use the subsumption for expressions for terms (`tyx-sub` on page 26). We need such inversion of subtyping in the preservation proof `eps-run3` on page 54.

A Syntax

A.1 Kinds

$$\boxed{\texttt{k} ::= \cdots} \qquad \boxed{\text{k}}$$

$$\texttt{k} ::= \texttt{T} \qquad \text{(kt)}$$

$$\texttt{k} ::= \texttt{L} \qquad \text{(kl)}$$

$$\texttt{k} ::= \texttt{P} \qquad \text{(kp)}$$

$$\texttt{k} ::= \texttt{J} \qquad \text{(kj)}$$

$$\texttt{k} ::= \texttt{PJ} \qquad \text{(kpj)}$$

A.2 Variables

$$\boxed{\texttt{x} ::= \cdots} \qquad \boxed{\text{x}}$$

A.3 Types

$$\boxed{\texttt{t} ::= \cdots} \qquad \boxed{\text{t}}$$

$$\boxed{\ell \equiv \texttt{t}} \qquad \boxed{\text{l}}$$

$$\boxed{\texttt{p} \equiv \texttt{t}} \qquad \boxed{\text{p}}$$

$$\boxed{\texttt{j} \equiv \texttt{t}} \qquad \boxed{\text{j}}$$

$$\boxed{\epsilon \equiv \ell} \qquad \boxed{\text{q}}$$

$$\texttt{t} ::= \texttt{<>} \qquad \text{(tunit)}$$

$$\texttt{t} ::= \texttt{<t,t>} \qquad \text{(tprod)}$$

$$\texttt{t} ::= \texttt{t} + \texttt{t} \qquad \text{(tsum)}$$

$$\texttt{t} ::= \texttt{t} \to \texttt{t} \qquad \text{(tfun)}$$

$$\texttt{t} ::= \top \qquad \text{(ttop)}$$

$$\texttt{t} ::= \bot \qquad \text{(tbot)}$$

$$\texttt{t} ::= \texttt{x} \qquad \text{(tvar)}$$

$$\texttt{t} ::= \forall \alpha \preceq \texttt{t}.\, \texttt{t} \qquad \text{(tall)}$$

$$\texttt{t} ::= \exists \alpha \preceq \texttt{t}.\, \texttt{t} \qquad \text{(tsome)}$$

$$\texttt{t} ::= \texttt{t} \wedge \texttt{t} \qquad \text{(tinter)}$$

$$\texttt{t} ::= \texttt{t} \vee \texttt{t} \qquad \text{(tunion)}$$

$$\texttt{t} ::= \texttt{t}\{\ell\} \qquad \text{(tlab)}$$

$$\texttt{t} ::= \texttt{t ! } \epsilon \qquad \text{(teff)}$$

$$\texttt{t} ::= \texttt{t}^{\dagger} \qquad \text{(tpot)}$$

$$\ell ::= \texttt{R p p} \qquad \text{(tread)}$$

$$\ell ::= \texttt{T p} \qquad \text{(ttrust)}$$

$$\texttt{t} ::= \texttt{t \% p} \triangleleft \texttt{p} \qquad \text{(tauth)}$$

$$\texttt{t} ::= \texttt{'p} \qquad \text{(tsin)}$$

$$\texttt{t} ::= \texttt{cert} \qquad \text{(tcert)}$$

$$\texttt{t} ::= \texttt{dcls p} \qquad \text{(tdcls)}$$

$$\texttt{t} ::= \texttt{endr} \qquad \text{(tendr)}$$

A.4 Terms

$$\boxed{\texttt{m} ::= \cdots} \qquad \boxed{\text{m}}$$

$$\boxed{\texttt{e} ::= \cdots} \qquad \boxed{\text{e}}$$

$$\texttt{m} ::= \texttt{<>} \qquad \text{(unit)}$$

$$\texttt{m} ::= \texttt{x} \qquad \text{(var)}$$

$$\texttt{m} ::= \texttt{<m,m>} \qquad \text{(prod)}$$

$$\texttt{m} ::= \texttt{prl m} \qquad \text{(prl)}$$

$$\texttt{m} ::= \texttt{prr m} \qquad \text{(prr)}$$

$$\texttt{m} ::= \texttt{inl m as t} \qquad \text{(inl)}$$

$$\texttt{m} ::= \texttt{inr m as t} \qquad \text{(inr)}$$

$$\texttt{m} ::= \texttt{case m m m} \qquad \text{(case)}$$

$$\texttt{m} ::= \lambda\texttt{x:t.m} \qquad \text{(fun)}$$

$$\texttt{m} ::= \texttt{m m} \qquad \text{(app)}$$

$$\texttt{m} ::= \Lambda\alpha \preceq \texttt{t. m} \qquad \text{(poly)}$$

$$\texttt{m} ::= \texttt{m [t]} \qquad \text{(inst)}$$

$$\texttt{m} ::= \texttt{pack (t,m) as t} \qquad \text{(pack)}$$

$$\texttt{m} ::= \texttt{open } (\alpha,\texttt{x}) = \texttt{m in m} \qquad \text{(open)}$$

$$\texttt{m} ::= \texttt{m}\{\ell\} \qquad \text{(lab)}$$

$$\texttt{m} ::= \texttt{bind x} = \texttt{m in m} \qquad \text{(bind)}$$

$$\texttt{m} ::= \texttt{e ! } \epsilon \qquad \text{(eff)}$$

$$\texttt{m} ::= \texttt{fix m} \qquad \text{(fix)}$$

$$\texttt{m} ::= \texttt{lift m} \qquad \text{(lift)}$$

$$\texttt{m} ::= \texttt{seq x} = \texttt{m in m} \qquad \text{(seq)}$$

$$\texttt{m} ::= \texttt{let p} \lhd \texttt{p in m} \qquad \text{(let)}$$

$$\texttt{m} ::= \texttt{pass x} = \texttt{m in m} \qquad \text{(pass)}$$

$$\texttt{m} ::= \texttt{'p} \qquad \text{(sin)}$$

$$\texttt{m} ::= \texttt{'p} \lhd \texttt{'p} \qquad \text{(cert)}$$

$$\texttt{m} ::= \texttt{if } (\texttt{m} \Rightarrow \texttt{m} \lhd \texttt{m})\ \texttt{m m} \qquad \text{(if)}$$

A.5 Expressions

$$\texttt{e} ::= \texttt{ret m} \qquad \text{(ret)}$$

$$\mathtt{e} ::= \mathtt{run}\ \mathtt{x} = \mathtt{m}\ \mathtt{in}\ \mathtt{e} \tag{run}$$

$$\mathtt{e} ::= \mathtt{x} \tag{evar}$$

$$\mathtt{e} ::= \mathtt{fix}\ \mathtt{x}{:}\mathtt{t}\,!\,\epsilon.\ \mathtt{e} \tag{efix}$$

A.6 Contexts

$$\boxed{\Gamma ::= \cdots} \qquad \boxed{\text{g}}$$

$$\Gamma ::= \cdot \tag{gn}$$

$$\Gamma ::= \Gamma, \mathtt{x}{:}\mathtt{t} \tag{gt}$$

$$\Gamma ::= \Gamma, \mathtt{x}{:}\mathtt{t}\,!\,\epsilon \tag{gq}$$

A.7 Lattices

$$\boxed{\Delta ::= \cdots} \qquad \boxed{\text{d}}$$

$$\Delta ::= \cdot \tag{dn}$$

$$\Delta ::= \Delta, \alpha \preceq \mathtt{t} \tag{dt}$$

$$\Delta ::= \Delta, \mathtt{p} \lhd \mathtt{p} \tag{dp}$$

B Static semantics

B.1 Operations

$$\boxed{\mathtt{x} : \mathtt{t} \in \Gamma} \qquad \text{gtmem}$$

$$\boxed{\mathtt{x} : \mathtt{t}\,!\,\epsilon \in \Gamma} \qquad \text{gqmem}$$

$$\boxed{\mathtt{x} \preceq \mathtt{t} \in \Delta} \qquad \text{dtmem}$$

$$\boxed{\mathtt{p} \lhd \mathtt{p} \in \Delta} \qquad \text{dpmem}$$

$$\boxed{\mathtt{m}\{\mathtt{m}/\mathtt{x}\} = \mathtt{m}} \qquad \text{mmsub}$$

$$\boxed{\mathtt{e}\{\mathtt{m}/\mathtt{x}\} = \mathtt{e}} \qquad \text{emsub}$$

$$\boxed{\mathtt{e}\{\mathtt{e}/\mathtt{x}\} = \mathtt{e}} \qquad \text{eesub}$$

$$\boxed{\mathtt{m}\{\mathtt{t}/\alpha\} = \mathtt{m}} \qquad \text{mtsub}$$

$$\boxed{\mathtt{t}\{\mathtt{t}/\alpha\} = \mathtt{t}} \qquad \text{ttsub}$$

$$\boxed{\alpha \notin \mathtt{tfv}(\Gamma)} \qquad \text{gindep}$$

$$\boxed{\alpha \notin \mathtt{tfv}(\mathtt{t})} \qquad \text{tindep}$$

B.2 Kinding

$$\boxed{\Delta \vdash \mathtt{t} :: \mathtt{k}} \qquad \text{kd}$$

$$\Delta \vdash \mathtt{<>} :: \mathtt{T} \qquad \text{(kd-unit)}$$

$$\Delta \vdash \mathtt{<}\mathtt{t}_1\mathtt{,}\mathtt{t}_2\mathtt{>} :: \mathtt{T} \qquad \text{(kd-prod)}$$

$$\Delta \vdash \mathtt{t}_1 + \mathtt{t}_2 :: \mathtt{T} \qquad \text{(kd-sum)}$$

$$\Delta \vdash \mathtt{t}_1 \to \mathtt{t}_2 :: \mathtt{T} \qquad \text{(kd-fun)}$$

$$\Delta \vdash \top :: \mathtt{T} \qquad \text{(kd-topt)}$$

$$\Delta \vdash \top :: \mathtt{L} \qquad \text{(kd-topl)}$$

$$\Delta \vdash \top :: \mathtt{P} \qquad \text{(kd-topp)}$$

$$\Delta \vdash \top :: \mathtt{J} \qquad \text{(kd-topj)}$$

$$\Delta \vdash \bot :: \mathtt{T} \qquad \text{(kd-bott)}$$

$$\Delta \vdash \bot :: \mathtt{L} \qquad \text{(kd-botl)}$$

$$\Delta \vdash \bot :: \mathtt{P} \qquad \text{(kd-botp)}$$

$$\Delta \vdash \bot :: \mathtt{J} \qquad \text{(kd-botj)}$$

$$\frac{\Delta, \alpha \preceq \mathtt{t}_1 \vdash \mathtt{t}_2 :: \mathtt{T}}{\Delta \vdash \forall \alpha \preceq \mathtt{t}_1 \,.\, \mathtt{t}_2 :: \mathtt{T}} \qquad \text{(kd-all)}$$

$$\frac{\Delta, \alpha \preceq \mathtt{t}_1 \vdash \mathtt{t}_2 :: \mathtt{T}}{\Delta \vdash \exists \alpha \preceq \mathtt{t}_1 \,.\, \mathtt{t}_2 :: \mathtt{T}} \qquad \text{(kd-some)}$$

$$\frac{\Delta \vdash \mathtt{t}_1 :: \mathtt{k} \quad \Delta \vdash \mathtt{t}_2 :: \mathtt{k}}{\Delta \vdash \mathtt{t}_1 \wedge \mathtt{t}_2 :: \mathtt{k}} \qquad \text{(kd-inter)}$$

$$\frac{\Delta \vdash \mathtt{t}_1 :: \mathtt{k} \quad \Delta \vdash \mathtt{t}_2 :: \mathtt{k}}{\Delta \vdash \mathtt{t}_1 \vee \mathtt{t}_2 :: \mathtt{k}} \quad \text{(kd-union)}$$

$$\frac{\Delta \vdash \mathtt{t} :: \mathtt{T} \quad \Delta \vdash \ell :: \mathtt{L}}{\Delta \vdash \mathtt{t}\{\ell\} :: \mathtt{T}} \quad \text{(kd-lab)}$$

$$\frac{\Delta \vdash \mathtt{t} :: \mathtt{T} \quad \Delta \vdash \epsilon :: \mathtt{L}}{\Delta \vdash \mathtt{t} \; ! \; \epsilon :: \mathtt{T}} \quad \text{(kd-eff)}$$

$$\frac{\Delta \vdash \mathtt{t} :: \mathtt{T}}{\Delta \vdash \mathtt{t}^{\dagger} :: \mathtt{T}} \quad \text{(kd-pot)}$$

$$\frac{\Delta \vdash \mathtt{p}_1 :: \mathtt{P} \quad \Delta \vdash \mathtt{p}_2 :: \mathtt{P}}{\Delta \vdash \mathtt{R} \; \mathtt{p}_1 \; \mathtt{p}_2 :: \mathtt{L}} \quad \text{(kd-read)}$$

$$\frac{\Delta \vdash \mathtt{p} :: \mathtt{P}}{\Delta \vdash \mathtt{T} \; \mathtt{p} :: \mathtt{L}} \quad \text{(kd-trust)}$$

$$\frac{\Delta \vdash \mathtt{t} :: \mathtt{T} \quad \Delta \vdash \mathtt{p}_1 :: \mathtt{P} \quad \Delta \vdash \mathtt{p}_2 :: \mathtt{PJ}}{\Delta \vdash \mathtt{t} \; \% \; \mathtt{p}_1 \lhd \mathtt{p}_2 :: \mathtt{T}} \quad \text{(kd-auth)}$$

$$\frac{\Delta \vdash \mathtt{t} :: \mathtt{k}}{\Delta \vdash {}'\mathtt{t} :: \mathtt{T}} \quad \text{(kd-sin)}$$

$$\Delta \vdash \mathtt{cert} :: \mathtt{T} \quad \text{(kd-cert)}$$

$$\frac{\Delta \vdash \mathtt{p} :: \mathtt{P}}{\Delta \vdash \mathtt{dcls} \; \mathtt{p} :: \mathtt{J}} \quad \text{(kd-dcls)}$$

$$\Delta \vdash \mathtt{endr} :: \mathtt{J} \quad \text{(kd-endr)}$$

$$\frac{\mathtt{x} \preceq \mathtt{t} \in \Delta \quad \Delta \vdash \mathtt{t} :: \mathtt{k}}{\Delta \vdash \mathtt{x} :: \mathtt{k}} \quad \text{(kd-var)}$$

$$\frac{\Delta \vdash \mathtt{t} :: \mathtt{P}}{\Delta \vdash \mathtt{t} :: \mathtt{PJ}} \quad \text{(kd-pjp)}$$

$$\frac{\Delta \vdash \mathtt{t} :: \mathtt{J}}{\Delta \vdash \mathtt{t} :: \mathtt{PJ}} \quad \text{(kd-pjj)}$$

B.3 Subtyping

$$\boxed{\Delta \vdash \mathtt{t} \preceq \mathtt{t}} \quad \boxed{\text{st}}$$

$$\boxed{\Delta \nvdash \mathtt{t} \preceq \mathtt{t}} \quad \boxed{\text{nst}}$$

$$\Delta \vdash \mathtt{<>} \preceq \mathtt{<>} \quad \text{(st-unit)}$$

$$\frac{\Delta \vdash \mathtt{t}_1 \preceq \mathtt{t}_3 \quad \Delta \vdash \mathtt{t}_2 \preceq \mathtt{t}_4}{\Delta \vdash \mathtt{<t_1, t_2>} \preceq \mathtt{<t_3, t_4>}} \quad \text{(st-prod)}$$

$$\frac{\Delta \vdash \mathtt{t}_1 \preceq \mathtt{t}_3 \quad \Delta \vdash \mathtt{t}_2 \preceq \mathtt{t}_4}{\Delta \vdash \mathtt{t}_1 + \mathtt{t}_2 \preceq \mathtt{t}_3 + \mathtt{t}_4} \quad \text{(st-sum)}$$

$$\Delta \vdash \mathtt{t} \preceq \top \quad \text{(st-top)}$$

$$\Delta \vdash \bot \preceq \mathtt{t} \quad \text{(st-bot)}$$

$$\Delta \vdash \mathtt{x} \preceq \mathtt{x} \quad \text{(st-var)}$$

$$\frac{\Delta, \alpha \preceq \mathtt{t} \vdash \mathtt{t}_1 \preceq \mathtt{t}_2}{\Delta \vdash \forall \alpha \preceq \mathtt{t}.\, \mathtt{t}_1 \preceq \forall \alpha \preceq \mathtt{t}.\, \mathtt{t}_2} \quad \text{(st-all)}$$

$$\frac{\Delta, \alpha \preceq \mathtt{t} \vdash \mathtt{t}_1 \preceq \mathtt{t}_2}{\Delta \vdash \exists \alpha \preceq \mathtt{t}.\, \mathtt{t}_1 \preceq \exists \alpha \preceq \mathtt{t}.\, \mathtt{t}_2} \quad \text{(st-some)}$$

$$\frac{\Delta \vdash \mathtt{t}_1 \preceq \mathtt{t}}{\Delta \vdash \mathtt{t}_1 \wedge \mathtt{t}_2 \preceq \mathtt{t}} \quad \text{(st-inter1)}$$

$$\frac{\Delta \vdash \mathtt{t}_2 \preceq \mathtt{t}}{\Delta \vdash \mathtt{t}_1 \wedge \mathtt{t}_2 \preceq \mathtt{t}} \quad \text{(st-inter2)}$$

$$\frac{\Delta \vdash \mathtt{t} \preceq \mathtt{t}_1 \quad \Delta \vdash \mathtt{t} \preceq \mathtt{t}_2}{\Delta \vdash \mathtt{t} \preceq \mathtt{t}_1 \wedge \mathtt{t}_2} \quad \text{(st-inter3)}$$

$$\frac{\Delta \vdash \mathtt{t} \preceq \mathtt{t}_1}{\Delta \vdash \mathtt{t} \preceq \mathtt{t}_1 \vee \mathtt{t}_2} \quad \text{(st-union1)}$$

$$\frac{\Delta \vdash \mathtt{t} \preceq \mathtt{t}_2}{\Delta \vdash \mathtt{t} \preceq \mathtt{t}_1 \vee \mathtt{t}_2} \quad \text{(st-union2)}$$

$$\frac{\Delta \vdash \mathtt{t}_1 \preceq \mathtt{t} \quad \Delta \vdash \mathtt{t}_2 \preceq \mathtt{t}}{\Delta \vdash \mathtt{t}_1 \vee \mathtt{t}_2 \preceq \mathtt{t}} \quad \text{(st-union3)}$$

$$\frac{\Delta \vdash \mathtt{t}_1 \preceq \mathtt{t}_2 \quad \Delta \vdash \ell_1 \preceq \ell_2}{\Delta \vdash \mathtt{t}_1\{\ell_1\} \preceq \mathtt{t}_2\{\ell_2\}} \quad \text{(st-lab)}$$

$$\frac{\Delta \vdash \mathtt{t}_1 \preceq \mathtt{t}_2}{\Delta \vdash \mathtt{t}_1^\dagger \preceq \mathtt{t}_2^\dagger} \quad \text{(st-pot)}$$

$$\frac{\Delta \vdash \mathtt{p}_1 \preceq \mathtt{p}_3 \quad \Delta \vdash \mathtt{p}_2 \preceq \mathtt{p}_4}{\Delta \vdash \mathtt{R}\ \mathtt{p}_1\ \mathtt{p}_2 \preceq \mathtt{R}\ \mathtt{p}_3\ \mathtt{p}_4} \quad \text{(st-read)}$$

$$\Delta \vdash {'\mathtt{t}} \preceq {'\mathtt{t}} \quad \text{(st-sin)}$$

$$\Delta \vdash \mathtt{cert} \preceq \mathtt{cert} \quad \text{(st-cert)}$$

$$\frac{\Delta \vdash \mathtt{t}_1 \preceq \mathtt{t}_2}{\Delta \vdash \mathtt{dcls}\ \mathtt{t}_1 \preceq \mathtt{dcls}\ \mathtt{t}_2} \quad \text{(st-dcls1)}$$

$$\Delta \vdash \mathtt{p} \preceq \mathtt{dcls}\ \top \quad \text{(st-dcls2)}$$

$$\Delta \vdash \mathtt{endr} \preceq \mathtt{endr} \quad \text{(st-endr)}$$

$$\Delta \vdash \mathtt{t} \preceq \mathtt{t}\ \%\ \mathtt{p}_1 \triangleleft \mathtt{p}_2 \quad \text{(st-auth2)}$$

$$\frac{\Delta \vdash \mathtt{t}_3 \preceq \mathtt{t}_1 \quad \Delta \vdash \mathtt{t}_2 \preceq \mathtt{t}_4}{\Delta \vdash \mathtt{t}_1 \to \mathtt{t}_2 \preceq \mathtt{t}_3 \to \mathtt{t}_4} \quad \text{(st-fun)}$$

$$\frac{\Delta \vdash \mathtt{t}_1 \preceq \mathtt{t}_2 \quad \Delta \vdash \epsilon_2 \preceq \epsilon_1}{\Delta \vdash \mathtt{t}_1\ !\ \epsilon_1 \preceq \mathtt{t}_2\ !\ \epsilon_2} \quad \text{(st-eff)}$$

$$\frac{\Delta \vdash \mathtt{p}_1 \preceq \mathtt{p}_3 \quad \Delta \vdash \mathtt{p}_1 \preceq \mathtt{dcls}\ \mathtt{p} \quad \Delta \vdash \mathtt{p} \wedge \mathtt{p}_2 \preceq \mathtt{p}_4}{\Delta \vdash \mathtt{R}\ \mathtt{p}_1\ \mathtt{p}_2 \preceq \mathtt{R}\ \mathtt{p}_3\ \mathtt{p}_4} \quad \text{(st-read2)}$$

$$\frac{\Delta \vdash \mathtt{p}_2 \preceq \mathtt{p}_1}{\Delta \vdash \mathtt{T}\ \mathtt{p}_1 \preceq \mathtt{T}\ \mathtt{p}_2} \quad \text{(st-trust)}$$

$$\frac{\Delta \vdash \mathtt{p} \preceq \mathtt{endr} \quad \Delta \vdash \mathtt{p}_2 \preceq \mathtt{p} \vee \mathtt{p}_1}{\Delta \vdash \mathtt{T}\ \mathtt{p}_1 \preceq \mathtt{T}\ \mathtt{p}_2} \quad \text{(st-trust2)}$$

$$\frac{\Delta \vdash \mathtt{t}_1 \preceq \mathtt{t}_2 \quad \Delta \vdash \mathtt{p}_3 \preceq \mathtt{p}_1 \quad \Delta \vdash \mathtt{p}_2 \preceq \mathtt{p}_4}{\Delta \vdash \mathtt{t}_1\ \%\ \mathtt{p}_1 \triangleleft \mathtt{p}_2 \preceq \mathtt{t}_2\ \%\ \mathtt{p}_3 \triangleleft \mathtt{p}_4} \quad \text{(st-auth)}$$

$$\frac{\mathtt{p}_1 \triangleleft \mathtt{p}_2 \in \Delta}{\Delta \vdash \mathtt{p}_1 \preceq \mathtt{p}_2} \quad \text{(st-del)}$$

B.4 Protections

$$\boxed{\Delta \vdash \mathtt{t} \gg \ell} \quad \boxed{\text{plab}}$$

$$\Delta \vdash \texttt{<>} \gg \ell \qquad \text{(plab-unit)}$$

$$\frac{\Delta \vdash \mathtt{t}_2 \gg \ell \quad \Delta \vdash \mathtt{t}_1 \gg \ell}{\Delta \vdash \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>} \gg \ell} \qquad \text{(plab-prod)}$$

$$\frac{\Delta \vdash \mathtt{t}_2 \gg \ell}{\Delta \vdash \mathtt{t}_1 \to \mathtt{t}_2 \gg \ell} \qquad \text{(plab-fun)}$$

$$\Delta \vdash \top \gg \ell \qquad \text{(plab-top)}$$

$$\frac{\Delta, \alpha \preceq \mathtt{t}_1 \vdash \mathtt{t}_2 \gg \ell}{\Delta \vdash \forall \alpha \preceq \mathtt{t}_1 \texttt{.}\ \mathtt{t}_2 \gg \ell} \qquad \text{(plab-all)}$$

$$\frac{\Delta, \alpha \preceq \mathtt{t}_2 \vdash \mathtt{t}_2 \gg \ell}{\Delta \vdash \exists \alpha \preceq \mathtt{t}_1 \texttt{.}\ \mathtt{t}_2 \gg \ell} \qquad \text{(plab-some)}$$

$$\frac{\Delta \vdash \ell_2 \preceq \ell_1}{\Delta \vdash \mathtt{t}\{\ell_1\} \gg \ell_2} \qquad \text{(plab-lab1)}$$

$$\frac{\Delta \not\vdash \ell_2 \preceq \ell_1 \quad \Delta \vdash \mathtt{t} \gg \ell_2}{\Delta \vdash \mathtt{t}\{\ell_1\} \gg \ell_2} \qquad \text{(plab-lab2)}$$

$$\frac{\Delta \vdash \mathtt{t} \gg \ell \quad \Delta \vdash \ell \preceq \epsilon}{\Delta \vdash \mathtt{t}\ \texttt{!}\ \epsilon \gg \ell} \qquad \text{(plab-eff)}$$

$$\frac{\Delta \vdash \mathtt{t} \gg \ell}{\Delta \vdash \mathtt{t}^\dagger \gg \ell} \qquad \text{(plab-pot)}$$

$$\frac{\Delta \vdash \mathtt{t} \gg \mathtt{T}\ \mathtt{p} \quad \Delta \vdash \mathtt{p}_1 \preceq \mathtt{p}}{\Delta \vdash \mathtt{t}\ \texttt{\%}\ \mathtt{p}_1 \lhd \mathtt{p}_2 \gg \mathtt{T}\ \mathtt{p}} \qquad \text{(plab-auth)}$$

$$\Delta \vdash \texttt{'}\mathtt{t} \gg \ell \qquad \text{(plab-sin)}$$

$$\Delta \vdash \texttt{cert} \gg \ell \qquad \text{(plab-cert)}$$

$$\boxed{\Delta \vdash \mathtt{t} \gg \dagger} \qquad \boxed{\text{ppot}}$$

$$\frac{\Delta \vdash \mathtt{t}_1 \gg \dagger \quad \Delta \vdash \mathtt{t}_2 \gg \dagger}{\Delta \vdash \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>} \gg \dagger} \qquad \text{(ppot-prod)}$$

$$\frac{\Delta \vdash \mathtt{t}_1 \gg \dagger \quad \Delta \vdash \mathtt{t}_2 \gg \dagger}{\Delta \vdash \mathtt{t}_1 + \mathtt{t}_2 \gg \dagger} \qquad \text{(ppot-sum)}$$

$$\frac{\Delta \vdash \mathtt{t}_2 \gg \dagger}{\Delta \vdash \mathtt{t}_1 \to \mathtt{t}_2 \gg \dagger} \qquad \text{(ppot-fun)}$$

$$\frac{\Delta, \alpha \preceq \mathtt{t}_1 \vdash \mathtt{t}_2 \gg \dagger}{\Delta \vdash \forall \alpha \preceq \mathtt{t}_1 \texttt{.}\ \mathtt{t}_2 \gg \dagger} \qquad \text{(ppot-all)}$$

$$\frac{\Delta, \alpha \preceq \mathtt{t}_1 \vdash \mathtt{t}_2 \gg \dagger}{\Delta \vdash \exists \alpha \preceq \mathtt{t}_1 \texttt{.}\ \mathtt{t}_2 \gg \dagger} \qquad \text{(ppot-some)}$$

$$\frac{\Delta \vdash \mathtt{t} \gg \dagger}{\Delta \vdash \mathtt{t}\{\ell\} \gg \dagger} \qquad \text{(ppot-lab)}$$

$$\frac{\Delta \vdash \mathtt{t} \gg \dagger}{\Delta \vdash \mathtt{t}\ \texttt{!}\ \epsilon \gg \dagger} \qquad \text{(ppot-eff)}$$

$$\Delta \vdash \mathtt{t}^\dagger \gg \dagger \qquad \text{(ppot-pot)}$$

$$\frac{\Delta \vdash \mathtt{t} \gg \dagger}{\Delta \vdash \mathtt{t}\ \texttt{\%}\ \mathtt{p}_1 \lhd \mathtt{p}_2 \gg \dagger} \qquad \text{(ppot-auth)}$$

B.5 Term typings

$\boxed{\Delta;\Gamma \vdash \mathtt{m} : \mathtt{t}}$ ty

$\boxed{\Delta;\Gamma \vdash \mathtt{e} : \mathtt{t} \mathbin{!} \epsilon}$ ety

$$\Delta;\Gamma \vdash \mathtt{<>} : \mathtt{<>} \tag{ty-unit}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{t}_1 \quad \Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{t}_2}{\Delta;\Gamma \vdash \mathtt{<m_1,m_2>} : \mathtt{<t_1,t_2>}} \tag{ty-prod}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m} : \mathtt{<t_1,t_2>}}{\Delta;\Gamma \vdash \mathtt{prl\ m} : \mathtt{t}_1} \tag{ty-prl}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m} : \mathtt{<t_1,t_2>}}{\Delta;\Gamma \vdash \mathtt{prr\ m} : \mathtt{t}_2} \tag{ty-prr}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m} : \mathtt{t}_1 \quad \Delta \vdash \mathtt{t}_1 + \mathtt{t}_2 :: \mathtt{T}}{\Delta;\Gamma \vdash \mathtt{inl\ m\ as\ t_1 + t_2} : \mathtt{t}_1 + \mathtt{t}_2} \tag{ty-inl}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m} : \mathtt{t}_2 \quad \Delta \vdash \mathtt{t}_1 + \mathtt{t}_2 :: \mathtt{T}}{\Delta;\Gamma \vdash \mathtt{inr\ m\ as\ t_1 + t_2} : \mathtt{t}_1 + \mathtt{t}_2} \tag{ty-inr}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m} : \mathtt{t}_1 + \mathtt{t}_2 \quad \Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{t}_1 \to \mathtt{t} \quad \Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{t}_2 \to \mathtt{t}}{\Delta;\Gamma \vdash \mathtt{case\ m\ m_1\ m_2} : \mathtt{t}} \tag{ty-case}$$

$$\frac{\mathtt{x} : \mathtt{t} \in \Gamma}{\Delta;\Gamma \vdash \mathtt{x} : \mathtt{t}} \tag{ty-var}$$

$$\frac{\Delta;\Gamma,\mathtt{x}:\mathtt{t}_1 \vdash \mathtt{m} : \mathtt{t}_2 \quad \Delta \vdash \mathtt{t}_1 :: \mathtt{T}}{\Delta;\Gamma \vdash \lambda \mathtt{x}:\mathtt{t}_1.\mathtt{m} : \mathtt{t}_1 \to \mathtt{t}_2} \tag{ty-fun}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{t}_1 \to \mathtt{t}_2 \quad \Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{t}_1}{\Delta;\Gamma \vdash \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_2} \tag{ty-app}$$

$$\frac{\Delta,\alpha \preceq \mathtt{t}_1;\Gamma \vdash \mathtt{m} : \mathtt{t}_2 \quad \Delta \vdash \mathtt{t}_1 :: \mathtt{k} \quad \alpha \notin \mathtt{tfv}(\Gamma)}{\Delta;\Gamma \vdash \Lambda\alpha \preceq \mathtt{t}_1.\,\mathtt{m} : \forall \alpha \preceq \mathtt{t}_1.\,\mathtt{t}_2} \tag{ty-poly}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m} : \forall \alpha \preceq \mathtt{t}_1.\,\mathtt{t}_2 \quad \Delta \vdash \mathtt{t}_1 :: \mathtt{k} \quad \Delta \vdash \mathtt{t}_3 :: \mathtt{k} \quad \Delta \vdash \mathtt{t}_3 \preceq \mathtt{t}_1 \quad \mathtt{t}_2\{\mathtt{t}_3/\alpha\} = \mathtt{t}_4}{\Delta;\Gamma \vdash \mathtt{m}\ [\mathtt{t}_3] : \mathtt{t}_4} \tag{ty-inst}$$

$$\frac{\Delta \vdash \mathtt{t} :: \mathtt{k} \quad \Delta \vdash \mathtt{t}_1 :: \mathtt{k} \quad \Delta \vdash \mathtt{t}_2 :: \mathtt{T} \quad \Delta \vdash \mathtt{t} \preceq \mathtt{t}_1 \quad \mathtt{t}_2\{\mathtt{t}/\alpha\} = \mathtt{t}_3 \quad \Delta;\Gamma \vdash \mathtt{m} : \mathtt{t}_3}{\Delta;\Gamma \vdash \mathtt{pack\ (t,m)\ as\ } \exists \alpha \preceq \mathtt{t}_1.\,\mathtt{t}_2 : \exists \alpha \preceq \mathtt{t}_1.\,\mathtt{t}_2} \tag{ty-pack}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m}_1 : \exists \alpha \preceq \mathtt{t}_1.\,\mathtt{t}_2 \quad \Delta,\alpha \preceq \mathtt{t}_1;\Gamma,\mathtt{x}:\mathtt{t}_2 \vdash \mathtt{m}_2 : \mathtt{t} \quad \alpha \notin \mathtt{tfv}(\Gamma) \quad \alpha \notin \mathtt{tfv(t)}}{\Delta;\Gamma \vdash \mathtt{open\ } (\alpha,\mathtt{x}) = \mathtt{m}_1 \mathtt{\ in\ m}_2 : \mathtt{t}} \tag{ty-open}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m} : \mathtt{t} \quad \Delta \vdash \ell :: \mathtt{L}}{\Delta;\Gamma \vdash \mathtt{m}\{\ell\} : \mathtt{t}\{\ell\}} \tag{ty-lab}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{t}_1\{\ell\} \quad \Delta;\Gamma,\mathtt{x}:\mathtt{t}_1 \vdash \mathtt{m}_2 : \mathtt{t}_2 \quad \Delta \vdash \mathtt{t}_2 \gg \ell}{\Delta;\Gamma \vdash \mathtt{bind\ x} = \mathtt{m}_1 \mathtt{\ in\ m}_2 : \mathtt{t}_2} \tag{ty-bind}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{e} : \mathtt{t} \mathbin{!} \epsilon \quad \Delta \vdash \epsilon :: \mathtt{L}}{\Delta;\Gamma \vdash \mathtt{e} \mathbin{!} \epsilon : \mathtt{t} \mathbin{!} \epsilon} \tag{ty-eff}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m} : \mathtt{t} \to \mathtt{t} \quad \Delta \vdash \mathtt{t} \gg \dagger}{\Delta;\Gamma \vdash \mathtt{fix\ m} : \mathtt{t}} \tag{ty-fix}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m} : \mathtt{t}}{\Delta;\Gamma \vdash \mathtt{lift\ m} : \mathtt{t}^\dagger} \tag{ty-lift}$$

$$\frac{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{t}_1^\dagger \quad \Delta;\Gamma,\mathtt{x}:\mathtt{t}_1 \vdash \mathtt{m}_2 : \mathtt{t}_2 \quad \Delta \vdash \mathtt{t}_2 \gg \dagger}{\Delta;\Gamma \vdash \mathtt{seq\ x} = \mathtt{m}_1 \mathtt{\ in\ m}_2 : \mathtt{t}_2} \tag{ty-seq}$$

$$\frac{\Delta, \mathtt{p}_1 \lhd \mathtt{p}_2; \Gamma \vdash \mathtt{m} : \mathtt{t} \quad \Delta \vdash \mathtt{p}_1 :: \mathtt{P} \quad \Delta \vdash \mathtt{p}_2 :: \mathtt{PJ}}{\Delta; \Gamma \vdash \mathtt{let}\ \mathtt{p}_1 \lhd \mathtt{p}_2\ \mathtt{in}\ \mathtt{m} : \mathtt{t}\ \%\ \mathtt{p}_1 \lhd \mathtt{p}_2} \quad \text{(ty-let)}$$

$$\frac{\Delta; \Gamma \vdash \mathtt{m}_1 : \mathtt{t}_1\ \%\ \mathtt{p}_1 \lhd \mathtt{p}_2 \quad \Delta, \mathtt{p}_1 \lhd \mathtt{p}_2; \Gamma, \mathtt{x}{:}\mathtt{t}_1 \vdash \mathtt{m}_2 : \mathtt{t}_2}{\Delta; \Gamma \vdash \mathtt{pass}\ \mathtt{x} = \mathtt{m}_1\ \mathtt{in}\ \mathtt{m}_2 : \mathtt{t}_2\ \%\ \mathtt{p}_1 \lhd \mathtt{p}_2} \quad \text{(ty-pass)}$$

$$\frac{\Delta \vdash \mathtt{p} :: \mathtt{k}}{\Delta; \Gamma \vdash \mathtt{'p} : \mathtt{'p}} \quad \text{(ty-sin)}$$

$$\frac{\Delta \vdash \mathtt{p}_1 :: \mathtt{P} \quad \Delta \vdash \mathtt{p}_2 :: \mathtt{PJ}}{\Delta; \Gamma \vdash \mathtt{'p}_1 \lhd \mathtt{'p}_2 : \mathtt{cert}} \quad \text{(ty-cert)}$$

$$\frac{\Delta; \Gamma \vdash \mathtt{m}_1 : \mathtt{cert} \quad \Delta; \Gamma \vdash \mathtt{m}_2 : \mathtt{'p}_1 \quad \Delta; \Gamma \vdash \mathtt{m}_3 : \mathtt{'p}_2 \quad \Delta, \mathtt{p}_1 \lhd \mathtt{p}_2; \Gamma \vdash \mathtt{m}_4 : \mathtt{t} \quad \Delta; \Gamma \vdash \mathtt{m}_5 : \mathtt{t} \quad \Delta \vdash \mathtt{p}_1 :: \mathtt{P} \quad \Delta \vdash \mathtt{p}_2 :: \mathtt{PJ}}{\Delta; \Gamma \vdash \mathtt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_2 \lhd \mathtt{m}_3)\ \mathtt{m}_4\ \mathtt{m}_5 : \mathtt{t}\ \%\ \mathtt{p}_1 \lhd \mathtt{p}_2} \quad \text{(ty-if)}$$

$$\frac{\Delta; \Gamma \vdash \mathtt{m} : \mathtt{t}_1 \quad \Delta \vdash \mathtt{t}_1 \preceq \mathtt{t}_2}{\Delta; \Gamma \vdash \mathtt{m} : \mathtt{t}_2} \quad \text{(tyx-sub)}$$

B.6 Expression typings

$$\frac{\Delta; \Gamma \vdash \mathtt{m} : \mathtt{t}}{\Delta; \Gamma \vdash \mathtt{ret}\ \mathtt{m} : \mathtt{t}\ !\ \top} \quad \text{(ety-ret)}$$

$$\frac{\Delta; \Gamma \vdash \mathtt{m} : \mathtt{t}_1\ !\ \epsilon \quad \Delta; \Gamma, \mathtt{x}{:}\mathtt{t}_1 \vdash \mathtt{e} : \mathtt{t}_2\ !\ \epsilon}{\Delta; \Gamma \vdash \mathtt{run}\ \mathtt{x} = \mathtt{m}\ \mathtt{in}\ \mathtt{e} : \mathtt{t}_2\ !\ \epsilon} \quad \text{(ety-run)}$$

$$\frac{\mathtt{x} : \mathtt{t}!\epsilon \in \Gamma}{\Delta; \Gamma \vdash \mathtt{x} : \mathtt{t}\ !\ \epsilon} \quad \text{(ety-var)}$$

$$\frac{\Delta; \Gamma, \mathtt{x}{:}\mathtt{t}!\epsilon \vdash \mathtt{e} : \mathtt{t}\ !\ \epsilon \quad \Delta \vdash \mathtt{t} \gg \dagger \quad \Delta \vdash \epsilon :: \mathtt{L}}{\Delta; \Gamma \vdash \mathtt{fix}\ \mathtt{x}{:}\mathtt{t}!\epsilon.\ \mathtt{e} : \mathtt{t}\ !\ \epsilon} \quad \text{(ety-fix)}$$

$$\frac{\Delta; \Gamma \vdash \mathtt{e} : \mathtt{t}_1\ !\ \epsilon_1 \quad \Delta \vdash \mathtt{t}_1 \preceq \mathtt{t}_2 \quad \Delta \vdash \epsilon_2 \preceq \epsilon_1}{\Delta; \Gamma \vdash \mathtt{e} : \mathtt{t}_2\ !\ \epsilon_2} \quad \text{(etyx-sub)}$$

C Dynamic semantics

C.1 Values

$$\boxed{\texttt{val m}} \qquad \boxed{\text{val}}$$

$$\boxed{\texttt{val e}} \qquad \boxed{\text{uval}}$$

$$\texttt{val <>} \qquad \text{(val-unit)}$$

$$\frac{\texttt{val } m_1 \quad \texttt{val } m_2}{\texttt{val <}m_1\texttt{,}m_2\texttt{>}} \qquad \text{(val-prod)}$$

$$\frac{\texttt{val m}}{\texttt{val inl m as t}} \qquad \text{(val-inl)}$$

$$\frac{\texttt{val m}}{\texttt{val inr m as t}} \qquad \text{(val-inr)}$$

$$\texttt{val } \lambda\texttt{x:t.m} \qquad \text{(val-fun)}$$

$$\texttt{val } \Lambda\alpha \preceq \texttt{t. m} \qquad \text{(val-poly)}$$

$$\frac{\texttt{val m}}{\texttt{val pack (}t_1\texttt{,m) as }t_2} \qquad \text{(val-pack)}$$

$$\frac{\texttt{val m}}{\texttt{val m}\{\ell\}} \qquad \text{(val-lab)}$$

$$\texttt{val m ! } \epsilon \qquad \text{(val-eff)}$$

$$\frac{\texttt{val m}}{\texttt{val lift m}} \qquad \text{(val-lift)}$$

$$\frac{\texttt{val m}}{\texttt{val let } p_1 \lhd p_2 \texttt{ in m}} \qquad \text{(val-let)}$$

$$\texttt{val } '\texttt{p} \qquad \text{(val-sin)}$$

$$\texttt{val } '\texttt{p}_1 \lhd '\texttt{p}_2 \qquad \text{(val-cert)}$$

$$\frac{\texttt{val m}}{\texttt{val ret m}} \qquad \text{(uval-ret)}$$

C.2 Verifications

$$\boxed{\vdash '\texttt{p} \lhd '\texttt{p} \Rightarrow '\texttt{p} \lhd '\texttt{p}} \qquad \boxed{\text{ve}}$$

$$\boxed{\nvdash '\texttt{p} \lhd '\texttt{p} \Rightarrow '\texttt{p} \lhd '\texttt{p}} \qquad \boxed{\text{nve}}$$

C.3 Term evaluations

$$\boxed{\texttt{m} \longrightarrow \texttt{m}} \qquad \boxed{\text{ev}}$$

$$\frac{m_1 \longrightarrow m_3}{\texttt{<}m_1\texttt{,}m_2\texttt{>} \longrightarrow \texttt{<}m_3\texttt{,}m_2\texttt{>}} \qquad \text{(ev-prod1)}$$

$$\frac{\texttt{val } m_1 \quad m_2 \longrightarrow m_3}{\texttt{<}m_1\texttt{,}m_2\texttt{>} \longrightarrow \texttt{<}m_2\texttt{,}m_3\texttt{>}} \qquad \text{(ev-prod2)}$$

$$\frac{m_1 \longrightarrow m_2}{\texttt{prl } m_1 \longrightarrow \texttt{prl } m_2} \qquad \text{(ev-prl1)}$$

$$\frac{\texttt{val } m_1 \quad \texttt{val } m_2}{\texttt{prl <}m_1\texttt{,}m_2\texttt{>} \longrightarrow m_1} \qquad \text{(ev-prl2)}$$

$$\frac{m_1 \longrightarrow m_2}{\texttt{prr } m_1 \longrightarrow \texttt{prr } m_2} \qquad \text{(ev-prr1)}$$

$$\frac{\texttt{val}\ \texttt{m}_1 \quad \texttt{val}\ \texttt{m}_2}{\texttt{prr}\ \texttt{<m}_1\texttt{,m}_2\texttt{>} \longrightarrow \texttt{m}_2} \tag{ev-prr2}$$

$$\frac{\texttt{m}_1 \longrightarrow \texttt{m}_2}{\texttt{inl}\ \texttt{m}_1\ \texttt{as}\ \texttt{t} \longrightarrow \texttt{inl}\ \texttt{m}_2\ \texttt{as}\ \texttt{t}} \tag{ev-inl}$$

$$\frac{\texttt{m}_1 \longrightarrow \texttt{m}_2}{\texttt{inr}\ \texttt{m}_1\ \texttt{as}\ \texttt{t} \longrightarrow \texttt{inr}\ \texttt{m}_2\ \texttt{as}\ \texttt{t}} \tag{ev-inr}$$

$$\frac{\texttt{m} \longrightarrow \texttt{m}_3}{\texttt{case}\ \texttt{m}\ \texttt{m}_1\ \texttt{m}_2 \longrightarrow \texttt{case}\ \texttt{m}_3\ \texttt{m}_1\ \texttt{m}_2} \tag{ev-case1}$$

$$\texttt{case inl m as t m}_1\ \texttt{m}_2 \longrightarrow \texttt{m}_1\ \texttt{m} \tag{ev-case2}$$

$$\texttt{case inr m as t m}_1\ \texttt{m}_2 \longrightarrow \texttt{m}_2\ \texttt{m} \tag{ev-case3}$$

$$\frac{\texttt{m}_1 \longrightarrow \texttt{m}_3}{\texttt{m}_1\ \texttt{m}_2 \longrightarrow \texttt{m}_3\ \texttt{m}_2} \tag{ev-app1}$$

$$\frac{\texttt{val}\ \texttt{m}_1 \quad \texttt{m}_2 \longrightarrow \texttt{m}_3}{\texttt{m}_1\ \texttt{m}_2 \longrightarrow \texttt{m}_1\ \texttt{m}_3} \tag{ev-app2}$$

$$\frac{\texttt{val}\ \texttt{m}_2 \quad \texttt{m}_1\{\texttt{m}_2/\texttt{x}\} = \texttt{m}_3}{(\lambda\texttt{x:t.m}_1)\ \texttt{m}_2 \longrightarrow \texttt{m}_3} \tag{ev-app3}$$

$$\frac{\texttt{m}_1 \longrightarrow \texttt{m}_2}{\texttt{m}_1\ \texttt{[t]} \longrightarrow \texttt{m}_2\ \texttt{[t]}} \tag{ev-inst1}$$

$$\frac{\texttt{m}_1\{\texttt{t}_2/\alpha\} = \texttt{m}_2}{(\Lambda\alpha \preceq \texttt{t}_1\,.\,\texttt{m}_1)\ \texttt{[t}_2\texttt{]} \longrightarrow \texttt{m}_2} \tag{ev-inst2}$$

$$\frac{\texttt{m}_1 \longrightarrow \texttt{m}_2}{\texttt{pack (t}_1\texttt{,m}_1\texttt{) as t}_2 \longrightarrow \texttt{pack (t}_1\texttt{,m}_2\texttt{) as t}_2} \tag{ev-pack}$$

$$\frac{\texttt{m}_1 \longrightarrow \texttt{m}_3}{\texttt{open}\ (\alpha,\texttt{x}) = \texttt{m}_1\ \texttt{in}\ \texttt{m}_2 \longrightarrow \texttt{open}\ (\alpha,\texttt{x}) = \texttt{m}_3\ \texttt{in}\ \texttt{m}_2} \tag{ev-open1}$$

$$\frac{\texttt{val}\ \texttt{m}_1 \quad \texttt{m}_2\{\texttt{t}_1/\alpha\} = \texttt{m}_3 \quad \texttt{m}_3\{\texttt{m}_1/\texttt{x}\} = \texttt{m}_4}{\texttt{open}\ (\alpha,\texttt{x}) = \texttt{pack (t}_1\texttt{,m}_1\texttt{) as t}_2\ \texttt{in}\ \texttt{m}_2 \longrightarrow \texttt{m}_4} \tag{ev-open2}$$

$$\frac{\texttt{m}_1 \longrightarrow \texttt{m}_2}{\texttt{m}_1\{\ell\} \longrightarrow \texttt{m}_2\{\ell\}} \tag{ev-lab}$$

$$\frac{\texttt{m}_1 \longrightarrow \texttt{m}_3}{\texttt{bind x} = \texttt{m}_1\ \texttt{in}\ \texttt{m}_2 \longrightarrow \texttt{bind x} = \texttt{m}_3\ \texttt{in}\ \texttt{m}_2} \tag{ev-bind1}$$

$$\frac{\texttt{val}\ \texttt{m}_1 \quad \texttt{m}_2\{\texttt{m}_1/\texttt{x}\} = \texttt{m}_3}{\texttt{bind x} = \texttt{m}_1\{\ell\}\ \texttt{in}\ \texttt{m}_2 \longrightarrow \texttt{m}_3} \tag{ev-bind2}$$

$$\frac{\texttt{m}_1\{\texttt{fix}\ \lambda\texttt{x:t.m}_1/\texttt{x}\} = \texttt{m}_2}{\texttt{fix}\ \lambda\texttt{x:t.m}_1 \longrightarrow \texttt{m}_2} \tag{ev-fix}$$

$$\frac{\texttt{m}_1 \longrightarrow \texttt{m}_2}{\texttt{lift}\ \texttt{m}_1 \longrightarrow \texttt{lift}\ \texttt{m}_2} \tag{ev-lift}$$

$$\frac{\texttt{m}_1 \longrightarrow \texttt{m}_3}{\texttt{seq x} = \texttt{m}_1\ \texttt{in}\ \texttt{m}_2 \longrightarrow \texttt{seq x} = \texttt{m}_3\ \texttt{in}\ \texttt{m}_2} \tag{ev-seq1}$$

$$\frac{\texttt{val}\ \texttt{m}_1 \quad \texttt{m}_2\{\texttt{m}_1/\texttt{x}\} = \texttt{m}_3}{\texttt{seq x} = \texttt{lift}\ \texttt{m}_1\ \texttt{in}\ \texttt{m}_2 \longrightarrow \texttt{m}_3} \tag{ev-seq2}$$

$$\frac{\texttt{m}_1 \longrightarrow \texttt{m}_2}{\texttt{let}\ \texttt{p}_1 \lhd \texttt{p}_2\ \texttt{in}\ \texttt{m}_1 \longrightarrow \texttt{let}\ \texttt{p}_1 \lhd \texttt{p}_2\ \texttt{in}\ \texttt{m}_2} \tag{ev-let}$$

$$\frac{\texttt{m}_1 \longrightarrow \texttt{m}_3}{\texttt{pass x} = \texttt{m}_1\ \texttt{in}\ \texttt{m}_2 \longrightarrow \texttt{pass x} = \texttt{m}_3\ \texttt{in}\ \texttt{m}_2} \tag{ev-pass1}$$

$$\frac{\texttt{val}\ \texttt{m}_1 \quad \texttt{m}_2\{\texttt{m}_1/\texttt{x}\} = \texttt{m}_3}{\texttt{pass x} = \texttt{let}\ \texttt{p}_1 \lhd \texttt{p}_2\ \texttt{in}\ \texttt{m}_1\ \texttt{in}\ \texttt{m}_2 \longrightarrow \texttt{let}\ \texttt{p}_1 \lhd \texttt{p}_2\ \texttt{in}\ \texttt{m}_3} \tag{ev-pass2}$$

$$\frac{\mathtt{m}_1 \longrightarrow \mathtt{m}_6}{\mathtt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_2 \lhd \mathtt{m}_3)\ \mathtt{m}_4\ \mathtt{m}_5 \longrightarrow \mathtt{if}\ (\mathtt{m}_6 \Rightarrow \mathtt{m}_2 \lhd \mathtt{m}_3)\ \mathtt{m}_4\ \mathtt{m}_5} \quad \text{(ev-if1)}$$

$$\frac{\mathtt{val}\ \mathtt{m}_1 \quad \mathtt{m}_2 \longrightarrow \mathtt{m}_6}{\mathtt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_2 \lhd \mathtt{m}_3)\ \mathtt{m}_4\ \mathtt{m}_5 \longrightarrow \mathtt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_6 \lhd \mathtt{m}_3)\ \mathtt{m}_4\ \mathtt{m}_5} \quad \text{(ev-if2)}$$

$$\frac{\mathtt{val}\ \mathtt{m}_1 \quad \mathtt{val}\ \mathtt{m}_2 \quad \mathtt{m}_3 \longrightarrow \mathtt{m}_6}{\mathtt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_2 \lhd \mathtt{m}_3)\ \mathtt{m}_4\ \mathtt{m}_5 \longrightarrow \mathtt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_2 \lhd \mathtt{m}_6)\ \mathtt{m}_4\ \mathtt{m}_5} \quad \text{(ev-if3)}$$

$$\frac{\vdash\ '\mathtt{p}_1 \lhd\ '\mathtt{p}_2 \Rightarrow\ '\mathtt{p}_3 \lhd\ '\mathtt{p}_4}{\mathtt{if}\ (\prime\mathtt{p}_1 \Rightarrow \prime\mathtt{p}_2 \lhd\ '\mathtt{p}_3\ \lhd\ '\mathtt{p}_4)\ \mathtt{m}_1\ \mathtt{m}_2 \longrightarrow \mathtt{let}\ \mathtt{p}_1 \lhd \mathtt{p}_2\ \mathtt{in}\ \mathtt{m}_1} \quad \text{(ev-if4)}$$

$$\frac{\not\vdash\ '\mathtt{p}_1 \lhd\ '\mathtt{p}_2 \Rightarrow\ '\mathtt{p}_3 \lhd\ '\mathtt{p}_4}{\mathtt{if}\ (\prime\mathtt{p}_1 \Rightarrow \prime\mathtt{p}_2 \lhd\ '\mathtt{p}_3\ \lhd\ '\mathtt{p}_4)\ \mathtt{m}_1\ \mathtt{m}_2 \longrightarrow \mathtt{m}_2} \quad \text{(ev-if5)}$$

C.4 Expression evaluations

$$\boxed{\mathtt{e} \xrightarrow{\epsilon} \mathtt{e}} \qquad \boxed{\text{eev}}$$

$$\frac{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}{\mathtt{ret}\ \mathtt{m}_1 \xrightarrow{\top} \mathtt{ret}\ \mathtt{m}_2} \quad \text{(eev-ret)}$$

$$\frac{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}{\mathtt{run}\ \mathtt{x} = \mathtt{m}_1\ \mathtt{in}\ \mathtt{e} \xrightarrow{\top} \mathtt{run}\ \mathtt{x} = \mathtt{m}_2\ \mathtt{in}\ \mathtt{e}} \quad \text{(eev-run1)}$$

$$\frac{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}{\mathtt{run}\ \mathtt{x} = \mathtt{ret}\ \mathtt{m}_1\ !\ \epsilon\ \mathtt{in}\ \mathtt{e}_2 \xrightarrow{\top} \mathtt{run}\ \mathtt{x} = \mathtt{ret}\ \mathtt{m}_2\ !\ \epsilon\ \mathtt{in}\ \mathtt{e}_2} \quad \text{(eev-run2)}$$

$$\frac{\mathtt{val}\ \mathtt{m} \quad \mathtt{e}_1\{\mathtt{m}/\mathtt{x}\} = \mathtt{e}_2}{\mathtt{run}\ \mathtt{x} = \mathtt{ret}\ \mathtt{m}\ !\ \epsilon\ \mathtt{in}\ \mathtt{e}_1 \xrightarrow{\epsilon} \mathtt{e}_2} \quad \text{(eev-run3)}$$

$$\frac{\mathtt{e}_1\{\mathtt{fix}\ \mathtt{x}{:}\mathtt{t}\,!\,\epsilon.\ \mathtt{e}_1\,/\mathtt{x}\} = \mathtt{e}_2}{\mathtt{fix}\ \mathtt{x}{:}\mathtt{t}\,!\,\epsilon.\ \mathtt{e}_1 \xrightarrow{\top} \mathtt{e}_2} \quad \text{(eev-fix)}$$

D Soundness

D.1 Evaluation or value

$$\boxed{\texttt{evval m}} \qquad \boxed{\text{evval}}$$

$$\frac{\texttt{m}_1 \longrightarrow \texttt{m}_2}{\texttt{evval m}_1} \qquad \text{(evval-ev)}$$

$$\frac{\texttt{val m}}{\texttt{evval m}} \qquad \text{(evval-val)}$$

$$\boxed{\texttt{evval e}} \qquad \boxed{\text{eevuval}}$$

$$\frac{\texttt{e}_1 \xrightarrow{\epsilon} \texttt{e}_2}{\texttt{evval e}_1} \qquad \text{(eevuval-eev)}$$

$$\frac{\texttt{val e}}{\texttt{evval e}} \qquad \text{(eevuval-uval)}$$

D.2 Function totality

$$\boxed{\frac{}{\texttt{m}_1\{\texttt{m}_2/\texttt{x}\} = \texttt{m}_3}} \qquad \boxed{\text{subx}}$$

$$\boxed{\frac{}{\texttt{m}_1\{\texttt{t}/\alpha\} = \texttt{m}_2}} \qquad \boxed{\text{mtsubx}}$$

$$\boxed{\frac{}{\texttt{e}_1\{\texttt{m}/\texttt{x}\} = \texttt{e}_2}} \qquad \boxed{\text{emsubx}}$$

$$\boxed{\frac{}{\texttt{e}_1\{\texttt{e}/\texttt{x}\} = \texttt{e}_2}} \qquad \boxed{\text{eesubx}}$$

$$\boxed{\vdash^? \texttt{'p} \lhd \texttt{'p} \Rightarrow \texttt{'p} \lhd \texttt{'p}} \qquad \boxed{\text{venve}}$$

$$\frac{\vdash \texttt{'p}_1 \lhd \texttt{'p}_2 \Rightarrow \texttt{'p}_3 \lhd \texttt{'p}_4}{\vdash^? \texttt{'p}_1 \lhd \texttt{'p}_2 \Rightarrow \texttt{'p}_3 \lhd \texttt{'p}_4} \qquad \text{(venve-ve)}$$

$$\frac{\nvdash \texttt{'p}_1 \lhd \texttt{'p}_2 \Rightarrow \texttt{'p}_3 \lhd \texttt{'p}_4}{\vdash^? \texttt{'p}_1 \lhd \texttt{'p}_2 \Rightarrow \texttt{'p}_3 \lhd \texttt{'p}_4} \qquad \text{(venve-nve)}$$

$$\boxed{\frac{}{\vdash^? \texttt{'p}_1 \lhd \texttt{'p}_2 \Rightarrow \texttt{'p}_3 \lhd \texttt{'p}_4}} \qquad \boxed{\text{vex}}$$

D.3 Term progress

$$\boxed{\frac{\Delta;\cdot \vdash \texttt{m} : \texttt{t}}{\texttt{evval m}}} \qquad \boxed{\text{pg}}$$

$$\frac{\dfrac{\Delta;\cdot \vdash \texttt{<>} : \texttt{<>}}{\texttt{val <>}}\ \text{val-unit}}{\texttt{evval <>}}\ \text{evval-val} \qquad \text{(pg-unit)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_3\texttt{>} : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}{\Delta;\cdot \vdash \mathtt{m}_3 : \mathtt{t}_2}\downarrow\text{ty-prod}}{\vdots}}{\dfrac{\Delta;\cdot \vdash \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_3\texttt{>} : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}{\Delta;\cdot \vdash \mathtt{m}_1 : \mathtt{t}_1}\downarrow\text{ty-prod}}\text{pg}}{\dfrac{\texttt{evval}\ \mathtt{m}_1}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\downarrow\text{evval-ev}}}{\texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_3\texttt{>} \longrightarrow \texttt{<}\mathtt{m}_2\texttt{,}\mathtt{m}_3\texttt{>}}\text{ev-prod1}}{\texttt{evval <}\mathtt{m}_1\texttt{,}\mathtt{m}_3\texttt{>}}\text{evval-ev}$$

(pg-prod1)

$$\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{<}\mathtt{m}_3\texttt{,}\mathtt{m}_1\texttt{>} : \texttt{<}\mathtt{t}_2\texttt{,}\mathtt{t}_1\texttt{>}}{\Delta;\cdot \vdash \mathtt{m}_3 : \mathtt{t}_2}\downarrow\text{ty-prod}}{\dfrac{\texttt{evval}\ \mathtt{m}_3}{\texttt{val}\ \mathtt{m}_3}\downarrow\text{evval-val}}\text{pg} \quad \dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{<}\mathtt{m}_3\texttt{,}\mathtt{m}_1\texttt{>} : \texttt{<}\mathtt{t}_2\texttt{,}\mathtt{t}_1\texttt{>}}{\Delta;\cdot \vdash \mathtt{m}_1 : \mathtt{t}_1}\downarrow\text{ty-prod}}{\dfrac{\texttt{evval}\ \mathtt{m}_1}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\downarrow\text{evval-ev}}\text{pg}}{\texttt{<}\mathtt{m}_3\texttt{,}\mathtt{m}_1\texttt{>} \longrightarrow \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>}}\text{ev-prod2}}{\texttt{evval <}\mathtt{m}_3\texttt{,}\mathtt{m}_1\texttt{>}}\text{evval-ev}$$

(pg-prod2)

$$\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{<}\mathtt{m}_2\texttt{,}\mathtt{m}_1\texttt{>} : \texttt{<}\mathtt{t}_2\texttt{,}\mathtt{t}_1\texttt{>}}{\Delta;\cdot \vdash \mathtt{m}_2 : \mathtt{t}_2}\downarrow\text{ty-prod}}{\dfrac{\texttt{evval}\ \mathtt{m}_2}{\texttt{val}\ \mathtt{m}_2}\downarrow\text{evval-val}}\text{pg} \quad \dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{<}\mathtt{m}_2\texttt{,}\mathtt{m}_1\texttt{>} : \texttt{<}\mathtt{t}_2\texttt{,}\mathtt{t}_1\texttt{>}}{\Delta;\cdot \vdash \mathtt{m}_1 : \mathtt{t}_1}\downarrow\text{ty-prod}}{\dfrac{\texttt{evval}\ \mathtt{m}_1}{\texttt{val}\ \mathtt{m}_1}\downarrow\text{evval-val}}\text{pg}}{\texttt{val <}\mathtt{m}_2\texttt{,}\mathtt{m}_1\texttt{>}}\text{val-prod}}{\texttt{evval <}\mathtt{m}_2\texttt{,}\mathtt{m}_1\texttt{>}}\text{evval-val}$$

(pg-prod3)

$$\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{prl}\ \mathtt{m}_1 : \mathtt{t}_1}{\Delta;\cdot \vdash \mathtt{m}_1 : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}\downarrow\text{ty-prl}}{\dfrac{\texttt{evval}\ \mathtt{m}_1}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\downarrow\text{evval-ev}}\text{pg}}{\texttt{prl}\ \mathtt{m}_1 \longrightarrow \texttt{prl}\ \mathtt{m}_2}\text{ev-prl1}}{\texttt{evval prl}\ \mathtt{m}_1}\text{evval-ev}$$

(pg-prl1)

$$\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{prl <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \mathtt{t}_1}{\Delta;\cdot \vdash \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}\downarrow\text{ty-prl}}{\dfrac{\texttt{evval <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>}}{\texttt{val <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>}}\downarrow\text{evval-val}}\text{pg} \quad \dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{prl <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \mathtt{t}_1}{\Delta;\cdot \vdash \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}\downarrow\text{ty-prl}}{\dfrac{\texttt{evval <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>}}{\texttt{val <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>}}\downarrow\text{evval-val}}\text{pg}}{\texttt{val}\ \mathtt{m}_2}\downarrow\text{val-prod}}{\texttt{val}\ \mathtt{m}_1}\downarrow\text{val-prod}}{\texttt{prl <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} \longrightarrow \mathtt{m}_1}\text{ev-prl2}}{\texttt{evval prl <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>}}\text{evval-ev}$$

(pg-prl2)

$$\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{prr}\ \mathtt{m}_1 : \mathtt{t}_2}{\Delta;\cdot \vdash \mathtt{m}_1 : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}\downarrow\text{ty-prr}}{\dfrac{\texttt{evval}\ \mathtt{m}_1}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\downarrow\text{evval-ev}}\text{pg}}{\texttt{prr}\ \mathtt{m}_1 \longrightarrow \texttt{prr}\ \mathtt{m}_2}\text{ev-prr1}}{\texttt{evval prr}\ \mathtt{m}_1}\text{evval-ev}$$

(pg-prr1)

$$\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{prr <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \mathtt{t}_2}{\Delta;\cdot \vdash \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}\downarrow\text{ty-prr}}{\dfrac{\texttt{evval <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>}}{\texttt{val <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>}}\downarrow\text{evval-val}}\text{pg} \quad \dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{prr <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \mathtt{t}_2}{\Delta;\cdot \vdash \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}\downarrow\text{ty-prr}}{\dfrac{\texttt{evval <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>}}{\texttt{val <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>}}\downarrow\text{evval-val}}\text{pg}}{\texttt{val}\ \mathtt{m}_2}\downarrow\text{val-prod}}{\texttt{val}\ \mathtt{m}_1}\downarrow\text{val-prod}}{\texttt{prr <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} \longrightarrow \mathtt{m}_2}\text{ev-prr2}}{\texttt{evval prr <}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>}}\text{evval-ev}$$

(pg-prr2)

$$\Delta;\cdot \vdash \lambda x{:}t_1.m : t_1 \to t_2 \quad \dfrac{\dfrac{\Delta;\cdot \vdash \lambda x{:}t_1.m : t_1 \to t_2}{\Delta \vdash t_1 :: T}\downarrow\text{ty-fun} \quad \dfrac{\Delta;\cdot \vdash \lambda x{:}t_1.m : t_1 \to t_2}{\Delta;\cdot, x{:}t_1 \vdash m : t_2}\downarrow\text{ty-fun}}{\vdots}$$
$$\dfrac{\dfrac{}{\texttt{val}\ \lambda x{:}t_1.m}\ \text{val-fun}}{\texttt{evval}\ \lambda x{:}t_1.m}\ \text{evval-val} \qquad \text{(pg-fun)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash m_1\ m_3 : t_2}{\Delta;\cdot \vdash m_3 : t_1}\downarrow\text{ty-app}}{\vdots}}{\dfrac{\Delta;\cdot \vdash m_1\ m_3 : t_2}{\Delta;\cdot \vdash m_1 : t_1 \to t_2}\downarrow\text{ty-app}}\ \text{pg}}{\dfrac{\texttt{evval}\ m_1}{m_1 \longrightarrow m_2}\downarrow\text{evval-ev}}}{\dfrac{m_1\ m_3 \longrightarrow m_2\ m_3}{\texttt{evval}\ m_1\ m_3}\ \text{evval-ev}}\ \text{ev-app1}$$
(pg-app1)

$$\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash m_3\ m_1 : t_2}{\Delta;\cdot \vdash m_3 : t_1 \to t_2}\downarrow\text{ty-app}}{\dfrac{\texttt{evval}\ m_3}{\texttt{val}\ m_3}\downarrow\text{evval-val}}\ \text{pg} \quad \dfrac{\dfrac{\Delta;\cdot \vdash m_3\ m_1 : t_2}{\Delta;\cdot \vdash m_1 : t_1}\downarrow\text{ty-app}}{\dfrac{\texttt{evval}\ m_1}{m_1 \longrightarrow m_2}\downarrow\text{evval-ev}}\ \text{pg}}{\dfrac{m_3\ m_1 \longrightarrow m_3\ m_2}{\texttt{evval}\ m_3\ m_1}\ \text{evval-ev}}\ \text{ev-app2}$$
(pg-app2)

$$\dfrac{\Delta;\cdot \vdash (\lambda x{:}t_1.m_2)\ m_1 : t_2}{\Delta;\cdot \vdash \lambda x{:}t_1.m_2 : t_1 \to t_2}\downarrow\text{ty-app} \quad \dfrac{\dfrac{\Delta;\cdot \vdash (\lambda x{:}t_1.m_2)\ m_1 : t_2}{\Delta;\cdot \vdash \lambda x{:}t_1.m_2 : t_1 \to t_2}\downarrow\text{ty-app}}{\Delta \vdash t_1 :: T}\downarrow\text{ty-fun} \quad \dfrac{\dfrac{\Delta;\cdot \vdash (\lambda x{:}t_1.m_2)\ m_1 : t_2}{\Delta;\cdot \vdash \lambda x{:}t_1.m_2 : t_1 \to t_2}\downarrow\text{ty-app}}{\Delta;\cdot, x{:}t_1 \vdash m_2 : t_2}\downarrow\text{ty-fun}$$

- $\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash (\lambda x{:}t_1.m_2)\ m_1 : t_2}{\vdots}}{\dfrac{\Delta;\cdot \vdash m_1 : t_1}{\texttt{evval}\ m_1}\ \text{pg}}}{\texttt{val}\ m_1}\downarrow\text{evval-val}$
- $\dfrac{}{m_2\{m_1/x\} = m_3}\ \text{subx}$

$$\dfrac{}{\dfrac{(\lambda x{:}t_1.m_2)\ m_1 \longrightarrow m_3}{\texttt{evval}\ (\lambda x{:}t_1.m_2)\ m_1}\ \text{evval-ev}}\ \text{ev-app3}$$
(pg-app3)

- $\Delta;\cdot \vdash \Lambda\alpha \preceq t_1.\, m : \forall \alpha \preceq t_1.\, t_2$
- $\dfrac{\Delta;\cdot \vdash \Lambda\alpha \preceq t_1.\, m : \forall \alpha \preceq t_1.\, t_2}{\alpha \notin \texttt{tfv}(\cdot)}\downarrow\text{ty-poly}$
- $\dfrac{\Delta;\cdot \vdash \Lambda\alpha \preceq t_1.\, m : \forall \alpha \preceq t_1.\, t_2}{\Delta \vdash t_1 :: k}\downarrow\text{ty-poly}$
- $\dfrac{\Delta;\cdot \vdash \Lambda\alpha \preceq t_1.\, m : \forall \alpha \preceq t_1.\, t_2}{\Delta, \alpha \preceq t_1;\cdot \vdash m : t_2}\downarrow\text{ty-poly}$

$$\dfrac{\dfrac{\dfrac{}{\texttt{val}\ \Lambda\alpha \preceq t_1.\, m}\ \text{val-poly}}{\texttt{evval}\ \Lambda\alpha \preceq t_1.\, m}\ \text{evval-val}}{\vdots}$$
(pg-poly)

- $$\frac{\Delta; \cdot \vdash \mathtt{m_1\ [t_3]} : \mathtt{t_4}}{\mathtt{t_2}\{\mathtt{t_3}/\alpha\} = \mathtt{t_4}}\ \downarrow\text{ty-inst}$$
- $$\frac{\Delta; \cdot \vdash \mathtt{m_1\ [t_3]} : \mathtt{t_4}}{\Delta \vdash \mathtt{t_3} \preceq \mathtt{t_1}}\ \downarrow\text{ty-inst}$$
- $$\frac{\Delta; \cdot \vdash \mathtt{m_1\ [t_3]} : \mathtt{t_4}}{\Delta \vdash \mathtt{t_3} :: \mathtt{k}}\ \downarrow\text{ty-inst}$$
- $$\frac{\Delta; \cdot \vdash \mathtt{m_1\ [t_3]} : \mathtt{t_4}}{\Delta \vdash \mathtt{t_1} :: \mathtt{k}}\ \downarrow\text{ty-inst}$$

$$\vdots$$

$$\cfrac{\cfrac{\cfrac{\cfrac{\Delta; \cdot \vdash \mathtt{m_1\ [t_3]} : \mathtt{t_4}}{\Delta; \cdot \vdash \mathtt{m_1} : \forall \alpha \preceq \mathtt{t_1}.\, \mathtt{t_2}}\ \downarrow\text{ty-inst}}{\mathtt{evval\ m_1}}\ \text{pg}}{\mathtt{m_1} \longrightarrow \mathtt{m_2}}\ \downarrow\text{evval-ev}}{\cfrac{\mathtt{m_1\ [t_3]} \longrightarrow \mathtt{m_2\ [t_3]}}{\mathtt{evval\ m_1\ [t_3]}}\ \text{evval-ev}}\ \text{ev-inst1} \qquad \text{(pg-inst1)}$$

- $\Delta; \cdot \vdash (\Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1})\ [\mathtt{t_1}] : \mathtt{t_3}$
- $$\frac{\Delta; \cdot \vdash (\Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1})\ [\mathtt{t_1}] : \mathtt{t_3}}{\mathtt{t_4}\{\mathtt{t_1}/\alpha\} = \mathtt{t_3}}\ \downarrow\text{ty-inst}$$
- $$\frac{\Delta; \cdot \vdash (\Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1})\ [\mathtt{t_1}] : \mathtt{t_3}}{\Delta \vdash \mathtt{t_1} \preceq \mathtt{t_2}}\ \downarrow\text{ty-inst}$$
- $$\frac{\Delta; \cdot \vdash (\Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1})\ [\mathtt{t_1}] : \mathtt{t_3}}{\Delta \vdash \mathtt{t_1} :: \mathtt{k_1}}\ \downarrow\text{ty-inst}$$
- $$\frac{\Delta; \cdot \vdash (\Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1})\ [\mathtt{t_1}] : \mathtt{t_3}}{\Delta \vdash \mathtt{t_2} :: \mathtt{k_1}}\ \downarrow\text{ty-inst}$$
- $$\frac{\Delta; \cdot \vdash (\Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1})\ [\mathtt{t_1}] : \mathtt{t_3}}{\Delta; \cdot \vdash \Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1} : \forall \alpha \preceq \mathtt{t_2}.\, \mathtt{t_4}}\ \downarrow\text{ty-inst}$$
- $$\cfrac{\cfrac{\Delta; \cdot \vdash (\Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1})\ [\mathtt{t_1}] : \mathtt{t_3}}{\Delta; \cdot \vdash \Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1} : \forall \alpha \preceq \mathtt{t_2}.\, \mathtt{t_4}}\ \downarrow\text{ty-inst}}{\alpha \notin \mathtt{tfv}(\cdot)}\ \downarrow\text{ty-poly}$$
- $$\cfrac{\cfrac{\Delta; \cdot \vdash (\Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1})\ [\mathtt{t_1}] : \mathtt{t_3}}{\Delta; \cdot \vdash \Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1} : \forall \alpha \preceq \mathtt{t_2}.\, \mathtt{t_4}}\ \downarrow\text{ty-inst}}{\Delta \vdash \mathtt{t_2} :: \mathtt{k_2}}\ \downarrow\text{ty-poly}$$
- $$\cfrac{\cfrac{\Delta; \cdot \vdash (\Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1})\ [\mathtt{t_1}] : \mathtt{t_3}}{\Delta; \cdot \vdash \Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1} : \forall \alpha \preceq \mathtt{t_2}.\, \mathtt{t_4}}\ \downarrow\text{ty-inst}}{\Delta, \alpha \preceq \mathtt{t_2}; \cdot \vdash \mathtt{m_1} : \mathtt{t_4}}\ \downarrow\text{ty-poly}$$

$$\vdots$$

$$\cfrac{\cfrac{\cfrac{}{\mathtt{m_1}\{\mathtt{t_1}/\alpha\} = \mathtt{m_2}}\ \text{mtsubx}}{(\Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1})\ [\mathtt{t_1}] \longrightarrow \mathtt{m_2}}\ \text{ev-inst2}}{\mathtt{evval}\ (\Lambda \alpha \preceq \mathtt{t_2}.\, \mathtt{m_1})\ [\mathtt{t_1}]}\ \text{evval-ev} \qquad \text{(pg-inst2)}$$

- $$\dfrac{\Delta;\cdot\vdash \texttt{pack (t}_2\texttt{,m}_1\texttt{) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4 : \exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}{\texttt{t}_4\{\texttt{t}_2/\alpha\} = \texttt{t}_1}\ \downarrow\text{ty-pack}$$
- $$\dfrac{\Delta;\cdot\vdash \texttt{pack (t}_2\texttt{,m}_1\texttt{) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4 : \exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}{\Delta\vdash \texttt{t}_2 \preceq \texttt{t}_3}\ \downarrow\text{ty-pack}$$
- $$\dfrac{\Delta;\cdot\vdash \texttt{pack (t}_2\texttt{,m}_1\texttt{) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4 : \exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}{\Delta\vdash \texttt{t}_4 :: \texttt{T}}\ \downarrow\text{ty-pack}$$
- $$\dfrac{\Delta;\cdot\vdash \texttt{pack (t}_2\texttt{,m}_1\texttt{) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4 : \exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}{\Delta\vdash \texttt{t}_3 :: \texttt{k}}\ \downarrow\text{ty-pack}$$
- $$\dfrac{\Delta;\cdot\vdash \texttt{pack (t}_2\texttt{,m}_1\texttt{) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4 : \exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}{\Delta\vdash \texttt{t}_2 :: \texttt{k}}\ \downarrow\text{ty-pack}$$

$$\vdots$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot\vdash \texttt{pack (t}_2\texttt{,m}_1\texttt{) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4 : \exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}{\Delta;\cdot\vdash \texttt{m}_1 : \texttt{t}_1}\ \downarrow\text{ty-pack}}{\texttt{evval m}_1}\ \text{pg}}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \downarrow\text{evval-ev}}{\texttt{pack (t}_2\texttt{,m}_1\texttt{) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4 \longrightarrow \texttt{pack (t}_2\texttt{,m}_2\texttt{) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}\ \text{ev-pack}}{\texttt{evval pack (t}_2\texttt{,m}_1\texttt{) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}\ \text{evval-ev} \tag{pg-pack1}$$

- $$\dfrac{\Delta;\cdot\vdash \texttt{pack (t}_2\texttt{,m) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4 : \exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}{\texttt{t}_4\{\texttt{t}_2/\alpha\} = \texttt{t}_1}\ \downarrow\text{ty-pack}$$
- $$\dfrac{\Delta;\cdot\vdash \texttt{pack (t}_2\texttt{,m) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4 : \exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}{\Delta\vdash \texttt{t}_2 \preceq \texttt{t}_3}\ \downarrow\text{ty-pack}$$
- $$\dfrac{\Delta;\cdot\vdash \texttt{pack (t}_2\texttt{,m) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4 : \exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}{\Delta\vdash \texttt{t}_4 :: \texttt{T}}\ \downarrow\text{ty-pack}$$
- $$\dfrac{\Delta;\cdot\vdash \texttt{pack (t}_2\texttt{,m) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4 : \exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}{\Delta\vdash \texttt{t}_3 :: \texttt{k}}\ \downarrow\text{ty-pack}$$
- $$\dfrac{\Delta;\cdot\vdash \texttt{pack (t}_2\texttt{,m) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4 : \exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}{\Delta\vdash \texttt{t}_2 :: \texttt{k}}\ \downarrow\text{ty-pack}$$

$$\vdots$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot\vdash \texttt{pack (t}_2\texttt{,m) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4 : \exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}{\Delta;\cdot\vdash \texttt{m} : \texttt{t}_1}\ \downarrow\text{ty-pack}}{\texttt{evval m}}\ \text{pg}}{\texttt{val m}}\ \downarrow\text{evval-val}}{\texttt{val pack (t}_2\texttt{,m) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}\ \text{val-pack}}{\texttt{evval pack (t}_2\texttt{,m) as }\exists\alpha\preceq\texttt{t}_3\texttt{. t}_4}\ \text{evval-val} \tag{pg-pack2}$$

- $$\dfrac{\Delta;\cdot\vdash \texttt{open (}\alpha\texttt{,x) = m}_1\texttt{ in m}_3 : \texttt{t}_3}{\alpha\notin\texttt{tfv(t}_3\texttt{)}}\ \downarrow\text{ty-open}$$
- $$\dfrac{\Delta;\cdot\vdash \texttt{open (}\alpha\texttt{,x) = m}_1\texttt{ in m}_3 : \texttt{t}_3}{\alpha\notin\texttt{tfv(}\cdot\texttt{)}}\ \downarrow\text{ty-open}$$
- $$\dfrac{\Delta;\cdot\vdash \texttt{open (}\alpha\texttt{,x) = m}_1\texttt{ in m}_3 : \texttt{t}_3}{\Delta,\alpha\preceq\texttt{t}_1;\cdot,\texttt{x:t}_2\vdash \texttt{m}_3 : \texttt{t}_3}\ \downarrow\text{ty-open}$$

$$\vdots$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot\vdash \texttt{open (}\alpha\texttt{,x) = m}_1\texttt{ in m}_3 : \texttt{t}_3}{\Delta;\cdot\vdash \texttt{m}_1 : \exists\alpha\preceq\texttt{t}_1\texttt{. t}_2}\ \downarrow\text{ty-open}}{\texttt{evval m}_1}\ \text{pg}}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \downarrow\text{evval-ev}}{\texttt{open (}\alpha\texttt{,x) = m}_1\texttt{ in m}_3 \longrightarrow \texttt{open (}\alpha\texttt{,x) = m}_2\texttt{ in m}_3}\ \text{ev-open1}}{\texttt{evval open (}\alpha\texttt{,x) = m}_1\texttt{ in m}_3}\ \text{evval-ev} \tag{pg-open1}$$

- $$\frac{\Delta;\cdot \vdash \texttt{open }(\alpha,\texttt{x}) = \texttt{pack }(\texttt{t}_1,\texttt{m}_2)\texttt{ as t}_2\texttt{ in m}_4 : \texttt{t}_5}{\alpha \notin \texttt{tfv}(\texttt{t}_5)}\ \downarrow\text{ty-open}$$
- $$\frac{\Delta;\cdot \vdash \texttt{open }(\alpha,\texttt{x}) = \texttt{pack }(\texttt{t}_1,\texttt{m}_2)\texttt{ as t}_2\texttt{ in m}_4 : \texttt{t}_5}{\alpha \notin \texttt{tfv}(\cdot)}\ \downarrow\text{ty-open}$$
- $$\frac{\Delta;\cdot \vdash \texttt{open }(\alpha,\texttt{x}) = \texttt{pack }(\texttt{t}_1,\texttt{m}_2)\texttt{ as t}_2\texttt{ in m}_4 : \texttt{t}_5}{\Delta,\alpha \preceq \texttt{t}_3;\cdot,\texttt{x}{:}\texttt{t}_4 \vdash \texttt{m}_4 : \texttt{t}_5}\ \downarrow\text{ty-open}$$

$$\vdots$$

$$\frac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{open }(\alpha,\texttt{x}) = \texttt{pack }(\texttt{t}_1,\texttt{m}_2)\texttt{ as t}_2\texttt{ in m}_4 : \texttt{t}_5}{\Delta;\cdot \vdash \texttt{pack }(\texttt{t}_1,\texttt{m}_2)\texttt{ as t}_2 : \exists\alpha \preceq \texttt{t}_3\,.\,\texttt{t}_4}\ \downarrow\text{ty-open}}{\texttt{evval pack }(\texttt{t}_1,\texttt{m}_2)\texttt{ as t}_2}\ \text{pg}}{\texttt{val pack }(\texttt{t}_1,\texttt{m}_2)\texttt{ as t}_2}\ \downarrow\text{evval-val}}{\texttt{val m}_2}\ \downarrow\text{val-pack} \quad \dfrac{}{\texttt{m}_4\{\texttt{t}_1/\alpha\} = \texttt{m}_1}\ \text{mtsubx} \quad \dfrac{}{\texttt{m}_1\{\texttt{m}_2/\texttt{x}\} = \texttt{m}_3}\ \text{subx}}{\dfrac{\texttt{open }(\alpha,\texttt{x}) = \texttt{pack }(\texttt{t}_1,\texttt{m}_2)\texttt{ as t}_2\texttt{ in m}_4 \longrightarrow \texttt{m}_3}{\texttt{evval open }(\alpha,\texttt{x}) = \texttt{pack }(\texttt{t}_1,\texttt{m}_2)\texttt{ as t}_2\texttt{ in m}_4}\ \text{evval-ev}}\ \text{ev-open2} \qquad \text{(pg-open2)}$$

$$\frac{\Delta;\cdot \vdash \texttt{m}_1\{\texttt{t}_2\} : \texttt{t}_1\{\texttt{t}_2\}}{\Delta \vdash \texttt{t}_2 :: \texttt{L}}\ \downarrow\text{ty-lab}$$

$$\vdots$$

$$\frac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{m}_1\{\texttt{t}_2\} : \texttt{t}_1\{\texttt{t}_2\}}{\Delta;\cdot \vdash \texttt{m}_1 : \texttt{t}_1}\ \downarrow\text{ty-lab}}{\texttt{evval m}_1}\ \text{pg}}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \downarrow\text{evval-ev}}{\dfrac{\texttt{m}_1\{\texttt{t}_2\} \longrightarrow \texttt{m}_2\{\texttt{t}_2\}}{\texttt{evval m}_1\{\texttt{t}_2\}}\ \text{evval-ev}}\ \text{ev-lab} \qquad \text{(pg-lab1)}$$

$$\frac{\Delta;\cdot \vdash \texttt{m}\{\texttt{t}_2\} : \texttt{t}_1\{\texttt{t}_2\}}{\Delta \vdash \texttt{t}_2 :: \texttt{L}}\ \downarrow\text{ty-lab}$$

$$\vdots$$

$$\frac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{m}\{\texttt{t}_2\} : \texttt{t}_1\{\texttt{t}_2\}}{\Delta;\cdot \vdash \texttt{m} : \texttt{t}_1}\ \downarrow\text{ty-lab}}{\texttt{evval m}}\ \text{pg}}{\texttt{val m}}\ \downarrow\text{evval-val}}{\dfrac{\texttt{val m}\{\texttt{t}_2\}}{\texttt{evval m}\{\texttt{t}_2\}}\ \text{evval-val}}\ \text{val-lab} \qquad \text{(pg-lab2)}$$

$$\frac{\Delta;\cdot \vdash \texttt{bind x} = \texttt{m}_1\texttt{ in m}_3 : \texttt{t}_3}{\Delta \vdash \texttt{t}_3 \gg \texttt{t}_2}\ \downarrow\text{ty-bind} \qquad \frac{\Delta;\cdot \vdash \texttt{bind x} = \texttt{m}_1\texttt{ in m}_3 : \texttt{t}_3}{\Delta;\cdot,\texttt{x}{:}\texttt{t}_1 \vdash \texttt{m}_3 : \texttt{t}_3}\ \downarrow\text{ty-bind}$$

$$\vdots$$

$$\frac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{bind x} = \texttt{m}_1\texttt{ in m}_3 : \texttt{t}_3}{\Delta;\cdot \vdash \texttt{m}_1 : \texttt{t}_1\{\texttt{t}_2\}}\ \downarrow\text{ty-bind}}{\texttt{evval m}_1}\ \text{pg}}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \downarrow\text{evval-ev}}{\dfrac{\texttt{bind x} = \texttt{m}_1\texttt{ in m}_3 \longrightarrow \texttt{bind x} = \texttt{m}_2\texttt{ in m}_3}{\texttt{evval bind x} = \texttt{m}_1\texttt{ in m}_3}\ \text{evval-ev}}\ \text{ev-bind1} \qquad \text{(pg-bind1)}$$

$$\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{bind x} = \texttt{m}_1\{\texttt{t}_1\}\ \texttt{in m}_2 : \texttt{t}_4}{\Delta \vdash \texttt{t}_4 \gg \texttt{t}_3}\downarrow\text{ty-bind} \quad \dfrac{\Delta;\cdot \vdash \texttt{bind x} = \texttt{m}_1\{\texttt{t}_1\}\ \texttt{in m}_2 : \texttt{t}_4}{\Delta;\cdot,\texttt{x:t}_2 \vdash \texttt{m}_2 : \texttt{t}_4}\downarrow\text{ty-bind}}{\Delta;\cdot \vdash \texttt{m}_1\{\texttt{t}_1\} : \texttt{t}_2\{\texttt{t}_3\}}\ \text{pg}$$

$$\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{bind x} = \texttt{m}_1\{\texttt{t}_1\}\ \texttt{in m}_2 : \texttt{t}_4}{\Delta;\cdot \vdash \texttt{m}_1\{\texttt{t}_1\} : \texttt{t}_2\{\texttt{t}_3\}}\ \text{pg}}{\texttt{evval m}_1\{\texttt{t}_1\}}\downarrow\text{evval-val}}{\texttt{val m}_1\{\texttt{t}_1\}}\downarrow\text{val-lab}$$

- $\dfrac{}{\texttt{m}_2\{\texttt{m}_1/\texttt{x}\} = \texttt{m}_3}\ \text{subx}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{bind x} = \texttt{m}_1\{\texttt{t}_1\}\ \texttt{in m}_2 : \texttt{t}_4}{\Delta;\cdot \vdash \texttt{m}_1\{\texttt{t}_1\} : \texttt{t}_2\{\texttt{t}_3\}}\ \text{pg}}{\texttt{evval m}_1\{\texttt{t}_1\}}\downarrow\text{evval-val}}{\texttt{val m}_1\{\texttt{t}_1\}}\downarrow\text{val-lab}}{\texttt{val m}_1}$$

- $\dfrac{}{\texttt{m}_2\{\texttt{m}_1/\texttt{x}\} = \texttt{m}_3}\ \text{subx}$

$$\dfrac{\dfrac{\texttt{bind x} = \texttt{m}_1\{\texttt{t}_1\}\ \texttt{in m}_2 \longrightarrow \texttt{m}_3}{\texttt{evval bind x} = \texttt{m}_1\{\texttt{t}_1\}\ \texttt{in m}_2}\ \text{evval-ev}}{\text{ev-bind2}} \tag{pg-bind2}$$

$$\Delta;\cdot \vdash \texttt{e ! t}_1 : \texttt{t}_2\ \texttt{!}\ \texttt{t}_1 \qquad \dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{e ! t}_1 : \texttt{t}_2\ \texttt{!}\ \texttt{t}_1}{\Delta \vdash \texttt{t}_1 :: \texttt{L}}\downarrow\text{ty-eff} \quad \dfrac{\Delta;\cdot \vdash \texttt{e ! t}_1 : \texttt{t}_2\ \texttt{!}\ \texttt{t}_1}{\Delta;\cdot \vdash \texttt{e} : \texttt{t}_2\ \texttt{!}\ \texttt{t}_1}\downarrow\text{ty-eff}}{\texttt{val e ! t}_1}\ \text{val-eff}}{\texttt{evval e ! t}_1}\ \text{evval-val} \tag{pg-eff}$$

$$\Delta;\cdot \vdash \texttt{fix } \lambda\texttt{x:t}_1.\texttt{m}_1 : \texttt{t}_2 \qquad \dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{fix } \lambda\texttt{x:t}_1.\texttt{m}_1 : \texttt{t}_2}{\Delta \vdash \texttt{t}_2 \gg \dagger}\downarrow\text{ty-fix} \quad \dfrac{\Delta;\cdot \vdash \texttt{fix } \lambda\texttt{x:t}_1.\texttt{m}_1 : \texttt{t}_2}{\Delta;\cdot \vdash \lambda\texttt{x:t}_1.\texttt{m}_1 : \texttt{t}_2 \to \texttt{t}_2}\downarrow\text{ty-fix}}{\texttt{m}_1\{\texttt{fix } \lambda\texttt{x:t}_1.\texttt{m}_1/\texttt{x}\} = \texttt{m}_2}\ \text{subx}}{\texttt{fix } \lambda\texttt{x:t}_1.\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \text{ev-fix}}{\texttt{evval fix } \lambda\texttt{x:t}_1.\texttt{m}_1}\ \text{evval-ev} \tag{pg-fix}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{lift m}_1 : \texttt{t}^\dagger}{\Delta;\cdot \vdash \texttt{m}_1 : \texttt{t}}\downarrow\text{ty-lift}}{\texttt{evval m}_1}\ \text{pg}}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\downarrow\text{evval-ev}}{\texttt{lift m}_1 \longrightarrow \texttt{lift m}_2}\ \text{ev-lift}}{\texttt{evval lift m}_1}\ \text{evval-ev} \tag{pg-lift1}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{lift m} : \texttt{t}^\dagger}{\Delta;\cdot \vdash \texttt{m} : \texttt{t}}\downarrow\text{ty-lift}}{\texttt{evval m}}\ \text{pg}}{\texttt{val m}}\downarrow\text{evval-val}}{\texttt{val lift m}}\ \text{val-lift}}{\texttt{evval lift m}}\ \text{evval-val} \tag{pg-lift2}$$

$$\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{seq x} = \texttt{m}_1\ \texttt{in m}_3 : \texttt{t}_2}{\Delta \vdash \texttt{t}_2 \gg \dagger}\downarrow\text{ty-seq} \quad \dfrac{\Delta;\cdot \vdash \texttt{seq x} = \texttt{m}_1\ \texttt{in m}_3 : \texttt{t}_2}{\Delta;\cdot,\texttt{x:t}_1 \vdash \texttt{m}_3 : \texttt{t}_2}\downarrow\text{ty-seq}}{\Delta;\cdot \vdash \texttt{m}_1 : \texttt{t}_1^\dagger}\ \text{pg}}{\texttt{evval m}_1}\downarrow\text{evval-ev}}{\texttt{seq x} = \texttt{m}_1\ \texttt{in m}_3 \longrightarrow \texttt{seq x} = \texttt{m}_2\ \texttt{in m}_3}\ \text{ev-seq1}}{\texttt{evval seq x} = \texttt{m}_1\ \texttt{in m}_3}\ \text{evval-ev} \tag{pg-seq1}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{seq x} = \texttt{lift m}_2 \texttt{ in m}_1 : \texttt{t}_2}{\Delta \vdash \texttt{t}_2 \gg \dagger}\downarrow\text{ty-seq} \quad \dfrac{\Delta;\cdot \vdash \texttt{seq x} = \texttt{lift m}_2 \texttt{ in m}_1 : \texttt{t}_2}{\Delta;\cdot,\texttt{x}:\texttt{t}_1 \vdash \texttt{m}_1 : \texttt{t}_2}\downarrow\text{ty-seq}}{\vdots}}{\Delta;\cdot \vdash \texttt{seq x} = \texttt{lift m}_2 \texttt{ in m}_1 : \texttt{t}_2}\downarrow\text{ty-seq}}{\Delta;\cdot \vdash \texttt{lift m}_2 : \texttt{t}_1^\dagger}\text{ pg}}{\texttt{evval lift m}_2}\downarrow\text{evval-val}}{\texttt{val lift m}_2}\downarrow\text{val-lift} \quad \dfrac{}{\texttt{m}_1\{\texttt{m}_2/\texttt{x}\} = \texttt{m}_3}\text{ subx}}{\texttt{seq x} = \texttt{lift m}_2 \texttt{ in m}_1 \longrightarrow \texttt{m}_3}\text{ ev-seq2}}{\texttt{evval seq x} = \texttt{lift m}_2 \texttt{ in m}_1}\text{ evval-ev} \tag{pg-seq2}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_1 : \texttt{t}_3 \,\%\, \texttt{t}_1 \lhd \texttt{t}_2}{\Delta \vdash \texttt{t}_2 :: \texttt{PJ}}\downarrow\text{ty-let} \quad \dfrac{\Delta;\cdot \vdash \texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_1 : \texttt{t}_3 \,\%\, \texttt{t}_1 \lhd \texttt{t}_2}{\Delta \vdash \texttt{t}_1 :: \texttt{P}}\downarrow\text{ty-let}}{\vdots}}{\Delta;\cdot \vdash \texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_1 : \texttt{t}_3 \,\%\, \texttt{t}_1 \lhd \texttt{t}_2}\downarrow\text{ty-let}}{\Delta,\texttt{t}_1 \lhd \texttt{t}_2;\cdot \vdash \texttt{m}_1 : \texttt{t}_3}\text{ pg}}{\texttt{evval m}_1}\downarrow\text{evval-ev}}{\texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_1 \longrightarrow \texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_2}\text{ ev-let}}{\texttt{evval let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_1}\text{ evval-ev} \tag{pg-let1}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m} : \texttt{t}_3 \,\%\, \texttt{t}_1 \lhd \texttt{t}_2}{\Delta \vdash \texttt{t}_2 :: \texttt{PJ}}\downarrow\text{ty-let} \quad \dfrac{\Delta;\cdot \vdash \texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m} : \texttt{t}_3 \,\%\, \texttt{t}_1 \lhd \texttt{t}_2}{\Delta \vdash \texttt{t}_1 :: \texttt{P}}\downarrow\text{ty-let}}{\vdots}}{\Delta;\cdot \vdash \texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m} : \texttt{t}_3 \,\%\, \texttt{t}_1 \lhd \texttt{t}_2}\downarrow\text{ty-let}}{\Delta,\texttt{t}_1 \lhd \texttt{t}_2;\cdot \vdash \texttt{m} : \texttt{t}_3}\text{ pg}}{\texttt{evval m}}\downarrow\text{evval-val}}{\texttt{val m}}\text{ val-let}}{\texttt{val let t}_1 \lhd \texttt{t}_2 \texttt{ in m}}\text{ evval-val} \tag{pg-let2}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{pass x} = \texttt{m}_1 \texttt{ in m}_3 : \texttt{t}_4 \,\%\, \texttt{t}_2 \lhd \texttt{t}_3}{\Delta,\texttt{t}_2 \lhd \texttt{t}_3;\cdot,\texttt{x}:\texttt{t}_1 \vdash \texttt{m}_3 : \texttt{t}_4}\downarrow\text{ty-pass}}{\vdots}}{\Delta;\cdot \vdash \texttt{pass x} = \texttt{m}_1 \texttt{ in m}_3 : \texttt{t}_4 \,\%\, \texttt{t}_2 \lhd \texttt{t}_3}\downarrow\text{ty-pass}}{\Delta;\cdot \vdash \texttt{m}_1 : \texttt{t}_1 \,\%\, \texttt{t}_2 \lhd \texttt{t}_3}\text{ pg}}{\texttt{evval m}_1}\downarrow\text{evval-ev}}{\texttt{pass x} = \texttt{m}_1 \texttt{ in m}_3 \longrightarrow \texttt{pass x} = \texttt{m}_2 \texttt{ in m}_3}\text{ ev-pass1}}{\texttt{evval pass x} = \texttt{m}_1 \texttt{ in m}_3}\text{ evval-ev} \tag{pg-pass1}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{pass x} = \texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_2 \texttt{ in m}_1 : \texttt{t}_6 \,\%\, \texttt{t}_4 \lhd \texttt{t}_5}{\Delta,\texttt{t}_4 \lhd \texttt{t}_5;\cdot,\texttt{x}:\texttt{t}_3 \vdash \texttt{m}_1 : \texttt{t}_6}\downarrow\text{ty-pass}}{\vdots}}{\Delta;\cdot \vdash \texttt{pass x} = \texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_2 \texttt{ in m}_1 : \texttt{t}_6 \,\%\, \texttt{t}_4 \lhd \texttt{t}_5}\downarrow\text{ty-pass}}{\Delta;\cdot \vdash \texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_2 : \texttt{t}_3 \,\%\, \texttt{t}_4 \lhd \texttt{t}_5}\text{ pg}}{\texttt{evval let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_2}\downarrow\text{evval-val}}{\texttt{val let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_2}\downarrow\text{val-let} \quad \dfrac{}{\texttt{m}_1\{\texttt{m}_2/\texttt{x}\} = \texttt{m}_3}\text{ subx}}{\texttt{pass x} = \texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_2 \texttt{ in m}_1 \longrightarrow \texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_3}\text{ ev-pass2}}{\texttt{evval pass x} = \texttt{let t}_1 \lhd \texttt{t}_2 \texttt{ in m}_2 \texttt{ in m}_1}\text{ evval-ev} \tag{pg-pass2}$$

$$\Delta;\cdot\vdash {}'\mathtt{t} : {}'\mathtt{t} \qquad \dfrac{\Delta;\cdot\vdash {}'\mathtt{t} : {}'\mathtt{t}}{\Delta\vdash \mathtt{t} :: \mathtt{k}}\ \downarrow\text{ty-sin}$$

$$\vdots$$

$$\dfrac{\dfrac{}{\mathtt{val}\ {}'\mathtt{t}}\ \text{val-sin}}{\mathtt{evval}\ {}'\mathtt{t}}\ \text{evval-val} \tag{pg-sin}$$

$$\Delta;\cdot\vdash {}'\mathtt{t_1} \lhd {}'\mathtt{t_2} : \mathtt{cert} \qquad \dfrac{\Delta;\cdot\vdash {}'\mathtt{t_1} \lhd {}'\mathtt{t_2} : \mathtt{cert}}{\Delta\vdash \mathtt{t_2} :: \mathtt{PJ}}\ \downarrow\text{ty-cert} \qquad \dfrac{\Delta;\cdot\vdash {}'\mathtt{t_1} \lhd {}'\mathtt{t_2} : \mathtt{cert}}{\Delta\vdash \mathtt{t_1} :: \mathtt{P}}\ \downarrow\text{ty-cert}$$

$$\vdots$$

$$\dfrac{\dfrac{}{\mathtt{val}\ {}'\mathtt{t_1} \lhd {}'\mathtt{t_2}}\ \text{val-cert}}{\mathtt{evval}\ {}'\mathtt{t_1} \lhd {}'\mathtt{t_2}}\ \text{evval-val} \tag{pg-cert}$$

- $\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_1} \Rightarrow \mathtt{m_3} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_1}\ \%\ \mathtt{t_2} \lhd \mathtt{t_3}}{\Delta\vdash \mathtt{t_3} :: \mathtt{PJ}}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_1} \Rightarrow \mathtt{m_3} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_1}\ \%\ \mathtt{t_2} \lhd \mathtt{t_3}}{\Delta\vdash \mathtt{t_2} :: \mathtt{P}}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_1} \Rightarrow \mathtt{m_3} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_1}\ \%\ \mathtt{t_2} \lhd \mathtt{t_3}}{\Delta;\cdot\vdash \mathtt{m_6} : \mathtt{t_1}}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_1} \Rightarrow \mathtt{m_3} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_1}\ \%\ \mathtt{t_2} \lhd \mathtt{t_3}}{\Delta, \mathtt{t_2} \lhd \mathtt{t_3};\cdot\vdash \mathtt{m_5} : \mathtt{t_1}}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_1} \Rightarrow \mathtt{m_3} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_1}\ \%\ \mathtt{t_2} \lhd \mathtt{t_3}}{\Delta;\cdot\vdash \mathtt{m_4} : {}'\mathtt{t_3}}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_1} \Rightarrow \mathtt{m_3} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_1}\ \%\ \mathtt{t_2} \lhd \mathtt{t_3}}{\Delta;\cdot\vdash \mathtt{m_3} : {}'\mathtt{t_2}}\ \downarrow\text{ty-if}$

$$\vdots$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_1} \Rightarrow \mathtt{m_3} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_1}\ \%\ \mathtt{t_2} \lhd \mathtt{t_3}}{\Delta;\cdot\vdash \mathtt{m_1} : \mathtt{cert}}\ \downarrow\text{ty-if}}{\mathtt{evval}\ \mathtt{m_1}}\ \text{pg}}{\mathtt{m_1} \longrightarrow \mathtt{m_2}}\ \downarrow\text{evval-ev}}{\mathtt{if}\ (\mathtt{m_1} \Rightarrow \mathtt{m_3} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} \longrightarrow \mathtt{if}\ (\mathtt{m_2} \Rightarrow \mathtt{m_3} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6}}\ \text{ev-if1}}{\mathtt{evval}\ \mathtt{if}\ (\mathtt{m_1} \Rightarrow \mathtt{m_3} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6}}\ \text{evval-ev} \tag{pg-if1}$$

- $\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_3} \Rightarrow \mathtt{m_1} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_2}\ \%\ \mathtt{t_1} \lhd \mathtt{t_3}}{\Delta\vdash \mathtt{t_3} :: \mathtt{PJ}}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_3} \Rightarrow \mathtt{m_1} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_2}\ \%\ \mathtt{t_1} \lhd \mathtt{t_3}}{\Delta\vdash \mathtt{t_1} :: \mathtt{P}}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_3} \Rightarrow \mathtt{m_1} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_2}\ \%\ \mathtt{t_1} \lhd \mathtt{t_3}}{\Delta;\cdot\vdash \mathtt{m_6} : \mathtt{t_2}}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_3} \Rightarrow \mathtt{m_1} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_2}\ \%\ \mathtt{t_1} \lhd \mathtt{t_3}}{\Delta, \mathtt{t_1} \lhd \mathtt{t_3};\cdot\vdash \mathtt{m_5} : \mathtt{t_2}}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_3} \Rightarrow \mathtt{m_1} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_2}\ \%\ \mathtt{t_1} \lhd \mathtt{t_3}}{\Delta;\cdot\vdash \mathtt{m_4} : {}'\mathtt{t_3}}\ \downarrow\text{ty-if}$

$$\vdots$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_3} \Rightarrow \mathtt{m_1} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_2}\ \%\ \mathtt{t_1} \lhd \mathtt{t_3}}{\Delta;\cdot\vdash \mathtt{m_3} : \mathtt{cert}}\ \downarrow\text{ty-if}}{\mathtt{evval}\ \mathtt{m_3}}\ \text{pg}}{\mathtt{val}\ \mathtt{m_3}}\ \downarrow\text{evval-val} \qquad \dfrac{\dfrac{\dfrac{\Delta;\cdot\vdash \mathtt{if}\ (\mathtt{m_3} \Rightarrow \mathtt{m_1} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} : \mathtt{t_2}\ \%\ \mathtt{t_1} \lhd \mathtt{t_3}}{\Delta;\cdot\vdash \mathtt{m_1} : {}'\mathtt{t_1}}\ \downarrow\text{ty-if}}{\mathtt{evval}\ \mathtt{m_1}}\ \text{pg}}{\mathtt{m_1} \longrightarrow \mathtt{m_2}}\ \downarrow\text{evval-ev}}{\mathtt{if}\ (\mathtt{m_3} \Rightarrow \mathtt{m_1} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6} \longrightarrow \mathtt{if}\ (\mathtt{m_3} \Rightarrow \mathtt{m_2} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6}}\ \text{ev-if2}}{\mathtt{evval}\ \mathtt{if}\ (\mathtt{m_3} \Rightarrow \mathtt{m_1} \lhd \mathtt{m_4})\ \mathtt{m_5}\ \mathtt{m_6}}\ \text{evval-ev} \tag{pg-if2}$$

$$\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\mathtt{m}_4 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_1)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_3\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_1}{\Delta \vdash \mathtt{t}_1 :: \mathtt{PJ}}\ \downarrow\text{ty-if} \quad \bullet \quad \dfrac{\Delta;\cdot \vdash \texttt{if}\ (\mathtt{m}_4 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_1)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_3\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_1}{\Delta \vdash \mathtt{t}_2 :: \mathtt{P}}\ \downarrow\text{ty-if} \quad \bullet \quad \dfrac{\Delta;\cdot \vdash \texttt{if}\ (\mathtt{m}_4 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_1)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_3\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_1}{\Delta;\cdot \vdash \mathtt{m}_6 : \mathtt{t}_3}\ \downarrow\text{ty-if} \quad \bullet \quad \dfrac{\Delta;\cdot \vdash \texttt{if}\ (\mathtt{m}_4 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_1)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_3\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_1}{\begin{array}{c}\Delta, \mathtt{t}_2 \lhd \mathtt{t}_1;\cdot \vdash \mathtt{m}_5 : \mathtt{t}_3 \\ \vdots \\ \dfrac{\Delta;\cdot \vdash \texttt{if}\ (\mathtt{m}_4 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_1)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_3\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_1}{\dfrac{\dfrac{\Delta;\cdot \vdash \mathtt{m}_4 : \mathtt{cert}}{\texttt{evval}\ \mathtt{m}_4}\ \text{pg}}{\texttt{val}\ \mathtt{m}_4}\ \downarrow\text{evval-val}}\ \downarrow\text{ty-if}\end{array}}\ \downarrow\text{ty-if} \quad \bullet \quad \dfrac{\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\mathtt{m}_4 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_1)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_3\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_1}{\dfrac{\dfrac{\Delta;\cdot \vdash \mathtt{m}_3 : {}'\mathtt{t}_2}{\texttt{evval}\ \mathtt{m}_3}\ \text{pg}}{\texttt{val}\ \mathtt{m}_3}\ \downarrow\text{evval-val}}\ \downarrow\text{ty-if} \quad \bullet \quad \dfrac{\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\mathtt{m}_4 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_1)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_3\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_1}{\dfrac{\dfrac{\Delta;\cdot \vdash \mathtt{m}_1 : {}'\mathtt{t}_1}{\texttt{evval}\ \mathtt{m}_1}\ \text{pg}}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\ \downarrow\text{evval-ev}}\ \downarrow\text{ty-if} \quad \bullet}{\dfrac{\texttt{if}\ (\mathtt{m}_4 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_1)\ \mathtt{m}_5\ \mathtt{m}_6 \longrightarrow \texttt{if}\ (\mathtt{m}_4 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_2)\ \mathtt{m}_5\ \mathtt{m}_6}{\texttt{evval if}\ (\mathtt{m}_4 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_1)\ \mathtt{m}_5\ \mathtt{m}_6}\ \text{evval-ev}}\ \text{ev-if3}$$

(pg-if3)

- $\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5$

- $\dfrac{\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5}{\Delta \vdash \mathtt{t}_5 :: \mathtt{PJ}}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5}{\Delta \vdash \mathtt{t}_6 :: \mathtt{P}}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5}{\Delta;\cdot \vdash \mathtt{m}_2 : \mathtt{t}_7}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5}{\Delta, \mathtt{t}_6 \lhd \mathtt{t}_5;\cdot \vdash \mathtt{m}_1 : \mathtt{t}_7}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5}{\Delta;\cdot \vdash '\mathtt{t}_3\ \lhd '\mathtt{t}_4 : '\mathtt{t}_5}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5}{\Delta;\cdot \vdash '\mathtt{t}_2 : '\mathtt{t}_6}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5}{\Delta;\cdot \vdash '\mathtt{t}_1 : \mathtt{cert}}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5}{\dfrac{\Delta;\cdot \vdash '\mathtt{t}_3\ \lhd '\mathtt{t}_4 : '\mathtt{t}_5}{\mathtt{evval}\ '\mathtt{t}_3\ \lhd '\mathtt{t}_4}\ \text{pg}}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5}{\dfrac{\dfrac{\Delta;\cdot \vdash '\mathtt{t}_3\ \lhd '\mathtt{t}_4 : '\mathtt{t}_5}{\mathtt{evval}\ '\mathtt{t}_3\ \lhd '\mathtt{t}_4}\ \text{pg}}{\mathtt{val}\ '\mathtt{t}_3\ \lhd '\mathtt{t}_4}\ \downarrow\text{evval-val}}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5}{\dfrac{\Delta;\cdot \vdash '\mathtt{t}_2 : '\mathtt{t}_6}{\mathtt{evval}\ '\mathtt{t}_2}\ \text{pg}}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5}{\dfrac{\dfrac{\Delta;\cdot \vdash '\mathtt{t}_2 : '\mathtt{t}_6}{\mathtt{evval}\ '\mathtt{t}_2}\ \text{pg}}{\mathtt{val}\ '\mathtt{t}_2}\ \downarrow\text{evval-val}}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5}{\dfrac{\Delta;\cdot \vdash '\mathtt{t}_1 : \mathtt{cert}}{\mathtt{evval}\ '\mathtt{t}_1}\ \text{pg}}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_7\ \%\ \mathtt{t}_6 \lhd \mathtt{t}_5}{\dfrac{\dfrac{\Delta;\cdot \vdash '\mathtt{t}_1 : \mathtt{cert}}{\mathtt{evval}\ '\mathtt{t}_1}\ \text{pg}}{\mathtt{val}\ '\mathtt{t}_1}\ \downarrow\text{evval-val}}\ \downarrow\text{ty-if}$

$$\dfrac{\dfrac{\dfrac{\dfrac{\vdots}{\vdash^{?}\ '\mathtt{t}_1 \lhd '\mathtt{t}_2 \Rightarrow '\mathtt{t}_3 \lhd '\mathtt{t}_4}\ \text{vex}}{\vdash\ '\mathtt{t}_1 \lhd '\mathtt{t}_2 \Rightarrow '\mathtt{t}_3 \lhd '\mathtt{t}_4}\ \downarrow\text{venve-ve}}{\mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 \longrightarrow \mathtt{let}\ \mathtt{t}_1 \lhd \mathtt{t}_2\ \mathtt{in}\ \mathtt{m}_1}\ \text{ev-if4}}{\mathtt{evval}\ \mathtt{if}\ ('\mathtt{t}_1 \Rightarrow '\mathtt{t}_2 \lhd '\mathtt{t}_3\ \lhd '\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2}\ \text{evval-ev} \qquad \text{(pg-if4)}$$

- $\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5$

- $\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5}{\Delta \vdash \texttt{t}_5 :: \texttt{PJ}}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5}{\Delta \vdash \texttt{t}_6 :: \texttt{P}}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5}{\Delta;\cdot \vdash \texttt{m}_2 : \texttt{t}_7}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5}{\Delta, \texttt{t}_6 \lhd \texttt{t}_5;\cdot \vdash \texttt{m}_1 : \texttt{t}_7}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5}{\Delta;\cdot \vdash \texttt{'t}_3\ \lhd \texttt{'t}_4 : \texttt{'t}_5}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5}{\Delta;\cdot \vdash \texttt{'t}_2 : \texttt{'t}_6}\ \downarrow\text{ty-if}$

- $\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5}{\Delta;\cdot \vdash \texttt{'t}_1 : \texttt{cert}}\ \downarrow\text{ty-if}$

- $\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5}{\Delta;\cdot \vdash \texttt{'t}_3\ \lhd \texttt{'t}_4 : \texttt{'t}_5}\ \downarrow\text{ty-if}}{\texttt{evval 't}_3\ \lhd \texttt{'t}_4}\ \text{pg}$

- $\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5}{\Delta;\cdot \vdash \texttt{'t}_3\ \lhd \texttt{'t}_4 : \texttt{'t}_5}\ \downarrow\text{ty-if}}{\texttt{evval 't}_3\ \lhd \texttt{'t}_4}\ \text{pg}}{\texttt{val 't}_3\ \lhd \texttt{'t}_4}\ \downarrow\text{evval-val}$

- $\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5}{\Delta;\cdot \vdash \texttt{'t}_2 : \texttt{'t}_6}\ \downarrow\text{ty-if}}{\texttt{evval 't}_2}\ \text{pg}$

- $\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5}{\Delta;\cdot \vdash \texttt{'t}_2 : \texttt{'t}_6}\ \downarrow\text{ty-if}}{\texttt{evval 't}_2}\ \text{pg}}{\texttt{val 't}_2}\ \downarrow\text{evval-val}$

- $\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5}{\Delta;\cdot \vdash \texttt{'t}_1 : \texttt{cert}}\ \downarrow\text{ty-if}}{\texttt{evval 't}_1}\ \text{pg}$

- $\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 : \texttt{t}_7\ \%\ \texttt{t}_6 \lhd \texttt{t}_5}{\Delta;\cdot \vdash \texttt{'t}_1 : \texttt{cert}}\ \downarrow\text{ty-if}}{\texttt{evval 't}_1}\ \text{pg}}{\texttt{val 't}_1}\ \downarrow\text{evval-val}}{\vdots}$

$$\dfrac{\dfrac{\dfrac{}{\vdash^{?} \texttt{'t}_1 \lhd \texttt{'t}_2 \Rightarrow \texttt{'t}_3 \lhd \texttt{'t}_4}\ \text{vex}}{\not\vdash \texttt{'t}_1 \lhd \texttt{'t}_2 \Rightarrow \texttt{'t}_3 \lhd \texttt{'t}_4}\ \downarrow\text{venve-nve}}{\texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 \longrightarrow \texttt{m}_2}\ \text{ev-if5}$$

$$\dfrac{\texttt{if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2 \longrightarrow \texttt{m}_2}{\texttt{evval if}\ (\texttt{'t}_1 \Rightarrow \texttt{'t}_2 \lhd \texttt{'t}_3\ \lhd \texttt{'t}_4)\ \texttt{m}_1\ \texttt{m}_2}\ \text{evval-ev}$$

(pg-if5)

D.4 Expression progress

$$\boxed{\dfrac{\Delta;\cdot \vdash \texttt{e} : \texttt{t}\ !\ \epsilon}{\texttt{evval e}}}$$

epg

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{ret}\ \texttt{m}_1 : \texttt{t}\ !\ \top}{\Delta;\cdot \vdash \texttt{m}_1 : \texttt{t}}\ \downarrow\text{ety-ret}}{\texttt{evval}\ \texttt{m}_1}\ \text{pg}}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \downarrow\text{evval-ev}}{\texttt{ret}\ \texttt{m}_1 \xrightarrow{\top} \texttt{ret}\ \texttt{m}_2}\ \text{eev-ret}}{\texttt{evval ret}\ \texttt{m}_1}\ \text{eevuval-eev} \qquad \text{(epg-ret1)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{ret}\ \texttt{m} : \texttt{t}\ !\ \top}{\Delta;\cdot \vdash \texttt{m} : \texttt{t}}\ \downarrow\text{ety-ret}}{\texttt{evval}\ \texttt{m}}\ \text{pg}}{\texttt{val}\ \texttt{m}}\ \downarrow\text{evval-val}}{\texttt{val ret}\ \texttt{m}}\ \text{uval-ret}}{\texttt{evval ret}\ \texttt{m}}\ \text{eevuval-uval} \qquad \text{(epg-ret2)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{run}\ \texttt{x} = \texttt{m}_1\ \texttt{in}\ \texttt{e} : \texttt{t}_3\ !\ \texttt{t}_2}{\Delta;\cdot,\texttt{x}:\texttt{t}_1 \vdash \texttt{e} : \texttt{t}_3\ !\ \texttt{t}_2}\ \downarrow\text{ety-run}}{\vdots}}{\Delta;\cdot \vdash \texttt{run}\ \texttt{x} = \texttt{m}_1\ \texttt{in}\ \texttt{e} : \texttt{t}_3\ !\ \texttt{t}_2}\ \downarrow\text{ety-run}}{\Delta;\cdot \vdash \texttt{m}_1 : \texttt{t}_1\ !\ \texttt{t}_2}\ \text{pg}}{\texttt{evval}\ \texttt{m}_1}}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \downarrow\text{evval-ev}}{\texttt{run}\ \texttt{x} = \texttt{m}_1\ \texttt{in}\ \texttt{e} \xrightarrow{\top} \texttt{run}\ \texttt{x} = \texttt{m}_2\ \texttt{in}\ \texttt{e}}\ \text{eev-run1}}{\texttt{evval run}\ \texttt{x} = \texttt{m}_1\ \texttt{in}\ \texttt{e}}\ \text{eevuval-eev} \qquad \text{(epg-run1)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{run}\ \texttt{x} = \texttt{ret}\ \texttt{m}_1\ !\ \top\ \texttt{in}\ \texttt{e} : \texttt{t}_2\ !\ \top}{\Delta;\cdot,\texttt{x}:\texttt{t}_1 \vdash \texttt{e} : \texttt{t}_2\ !\ \top}\ \downarrow\text{ety-run}}{\vdots}}{\Delta;\cdot \vdash \texttt{run}\ \texttt{x} = \texttt{ret}\ \texttt{m}_1\ !\ \top\ \texttt{in}\ \texttt{e} : \texttt{t}_2\ !\ \top}\ \downarrow\text{ety-run}}{\Delta;\cdot \vdash \texttt{ret}\ \texttt{m}_1\ !\ \top : \texttt{t}_1\ !\ \top}\ \downarrow\text{ty-eff}}{\Delta;\cdot \vdash \texttt{ret}\ \texttt{m}_1 : \texttt{t}_1\ !\ \top}\ \downarrow\text{ety-ret}}{\Delta;\cdot \vdash \texttt{m}_1 : \texttt{t}_1}\ \text{pg}}{\texttt{evval}\ \texttt{m}_1}}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \downarrow\text{evval-ev}}{\texttt{run}\ \texttt{x} = \texttt{ret}\ \texttt{m}_1\ !\ \top\ \texttt{in}\ \texttt{e} \xrightarrow{\top} \texttt{run}\ \texttt{x} = \texttt{ret}\ \texttt{m}_2\ !\ \top\ \texttt{in}\ \texttt{e}}\ \text{eev-run2}}{\texttt{evval run}\ \texttt{x} = \texttt{ret}\ \texttt{m}_1\ !\ \top\ \texttt{in}\ \texttt{e}}\ \text{eevuval-eev}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\cdot \vdash \texttt{run}\ \texttt{x} = \texttt{ret}\ \texttt{m}\ !\ \top\ \texttt{in}\ \texttt{e}_1 : \texttt{t}_2\ !\ \top}{\Delta;\cdot,\texttt{x}:\texttt{t}_1 \vdash \texttt{e}_1 : \texttt{t}_2\ !\ \top}\ \downarrow\text{ety-run}}{\vdots}}{\Delta;\cdot \vdash \texttt{run}\ \texttt{x} = \texttt{ret}\ \texttt{m}\ !\ \top\ \texttt{in}\ \texttt{e}_1 : \texttt{t}_2\ !\ \top}\ \downarrow\text{ety-run}}{\Delta;\cdot \vdash \texttt{ret}\ \texttt{m}\ !\ \top : \texttt{t}_1\ !\ \top}\ \downarrow\text{ty-eff}}{\Delta;\cdot \vdash \texttt{ret}\ \texttt{m} : \texttt{t}_1\ !\ \top}\ \downarrow\text{ety-ret}}{\Delta;\cdot \vdash \texttt{m} : \texttt{t}_1}\ \text{pg}}{\texttt{evval}\ \texttt{m}}\ \downarrow\text{evval-val}}{\texttt{val}\ \texttt{m}}}{\texttt{e}_1\{\texttt{m}/\texttt{x}\} = \texttt{e}_2}\ \text{emsubx}}{\texttt{run}\ \texttt{x} = \texttt{ret}\ \texttt{m}\ !\ \top\ \texttt{in}\ \texttt{e}_1 \xrightarrow{\top} \texttt{e}_2}\ \text{eev-run3}}{\texttt{evval run}\ \texttt{x} = \texttt{ret}\ \texttt{m}\ !\ \top\ \texttt{in}\ \texttt{e}_1}\ \text{eevuval-eev} \qquad \text{(epg-run3)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Delta;\cdot \vdash \texttt{fix x:t}_1\texttt{ !t}_2\texttt{. e}_1\texttt{ : t}_1\texttt{ ! t}_2}\bullet}{\Delta \vdash \texttt{t}_2 :: \texttt{L}}\downarrow\text{ety-fix}\bullet}{\Delta \vdash \texttt{t}_1 \gg \dagger}\downarrow\text{ety-fix}\bullet}{\Delta;\cdot,\texttt{x:t}_1\texttt{ !t}_2 \vdash \texttt{e}_1\texttt{ : t}_1\texttt{ ! t}_2}\downarrow\text{ety-fix}\bullet}{\vdots}}{\dfrac{\texttt{e}_1\{\texttt{fix x:t}_1\texttt{ !t}_2\texttt{. e}_1/\texttt{x}\} = \texttt{e}_2}{\dfrac{\texttt{fix x:t}_1\texttt{ !t}_2\texttt{. e}_1 \xrightarrow{\top} \texttt{e}_2}{\texttt{evval fix x:t}_1\texttt{ !t}_2\texttt{. e}_1}\text{ eevuval-eev}}\text{ eev-fix}}\text{ eesubx}$$

(epg-fix)

D.5 Lemmas

$$\boxed{\dfrac{\Delta;\Gamma,\texttt{x:t}_1 \vdash \texttt{m}_1\texttt{ : t}_2 \quad \Delta;\Gamma \vdash \texttt{m}_2\texttt{ : t}_1 \quad \texttt{m}_1\{\texttt{m}_2/\texttt{x}\} = \texttt{m}_3}{\Delta;\Gamma \vdash \texttt{m}_3\texttt{ : t}_2}}$$ pssub

$$\boxed{\dfrac{\Delta;\Gamma,\texttt{x:t}_1 \vdash \texttt{e}_1\texttt{ : t}_2\texttt{ ! }\epsilon \quad \Delta;\Gamma \vdash \texttt{m : t}_1 \quad \texttt{e}_1\{\texttt{m}/\texttt{x}\} = \texttt{e}_2}{\Delta;\Gamma \vdash \texttt{e}_2\texttt{ : t}_2\texttt{ ! }\epsilon}}$$ psemsub

$$\boxed{\dfrac{\Delta;\Gamma,\texttt{x:}\epsilon\texttt{!t}_1 \vdash \texttt{e}_1\texttt{ : t}_2\texttt{ ! }\epsilon \quad \Delta;\Gamma \vdash \texttt{e}_2\texttt{ : t}_1\texttt{ ! }\epsilon \quad \texttt{e}_1\{\texttt{e}_2/\texttt{x}\} = \texttt{e}_3}{\Delta;\Gamma \vdash \texttt{e}_3\texttt{ : t}_2\texttt{ ! }\epsilon}}$$ pseesub

$$\boxed{\dfrac{\Delta,\alpha \preceq \texttt{t}_1;\Gamma \vdash \texttt{m}_1\texttt{ : t}_2 \quad \Delta \vdash \texttt{t} \preceq \texttt{t}_1 \quad \alpha \notin \texttt{tfv}(\Gamma) \quad \texttt{m}_1\{\texttt{t}/\alpha\} = \texttt{m}_2 \quad \texttt{t}_2\{\texttt{t}/\alpha\} = \texttt{t}_3}{\Delta;\Gamma \vdash \texttt{m}_2\texttt{ : t}_3}}$$ psmtsub1

$$\boxed{\dfrac{\Delta,\alpha \preceq \texttt{t}_1;\Gamma,\texttt{x:t}_2 \vdash \texttt{m}_1\texttt{ : t}_3 \quad \Delta \vdash \texttt{t} \preceq \texttt{t}_1 \quad \alpha \notin \texttt{tfv}(\Gamma) \quad \texttt{t}_2\{\texttt{t}/\alpha\} = \texttt{t}_4 \quad \texttt{m}_1\{\texttt{t}/\alpha\} = \texttt{m}_2 \quad \alpha \notin \texttt{tfv}(\texttt{t}_3)}{\Delta;\Gamma,\texttt{x:t}_4 \vdash \texttt{m}_2\texttt{ : t}_3}}$$ psmtsub2

$$\boxed{\dfrac{\Delta;\Gamma \vdash \texttt{m : t}_1 \quad \Delta \vdash \texttt{t}_1 \preceq \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{m : t}_2}}$$ psst

$$\boxed{\dfrac{\Delta;\Gamma \vdash \texttt{ret m : t ! }\epsilon}{\Delta;\Gamma \vdash \texttt{ret m : t ! }\top}}$$ stinv

D.6 Term preservation

$$\boxed{\dfrac{\Delta;\Gamma \vdash \texttt{m}_1\texttt{ : t} \quad \texttt{m}_1 \longrightarrow \texttt{m}_2}{\Delta;\Gamma \vdash \texttt{m}_2\texttt{ : t}}}$$ ps

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{<m}_1\texttt{,m}_3\texttt{> : <t}_1\texttt{,t}_2\texttt{>}}{\Delta;\Gamma \vdash \texttt{m}_1\texttt{ : t}_1}\downarrow\text{ty-prod} \quad \dfrac{\texttt{<m}_1\texttt{,m}_3\texttt{>} \longrightarrow \texttt{<m}_2\texttt{,m}_3\texttt{>}}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\text{ ps}}{\Delta;\Gamma \vdash \texttt{m}_2\texttt{ : t}_1}\downarrow\text{ev-prod1} \quad \dfrac{\Delta;\Gamma \vdash \texttt{<m}_1\texttt{,m}_3\texttt{> : <t}_1\texttt{,t}_2\texttt{>}}{\Delta;\Gamma \vdash \texttt{m}_3\texttt{ : t}_2}\downarrow\text{ty-prod}$$
$$\Delta;\Gamma \vdash \texttt{<m}_2\texttt{,m}_3\texttt{> : <t}_1\texttt{,t}_2\texttt{>}\text{ ty-prod}$$

(ps-prod1)

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_1\texttt{>} : \texttt{<}\mathtt{t}_2\texttt{,}\mathtt{t}_1\texttt{>}}{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{t}_2}\downarrow\text{ty-prod} \qquad \dfrac{\dfrac{\dfrac{\texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_1\texttt{>} \longrightarrow \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>}}{\texttt{val}\ \mathtt{m}_1}\downarrow\text{ev-prod2}}{\vdots}}{\dfrac{\Delta;\Gamma \vdash \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_1\texttt{>} : \texttt{<}\mathtt{t}_2\texttt{,}\mathtt{t}_1\texttt{>}}{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{t}_1}\downarrow\text{ty-prod} \qquad \dfrac{\texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_1\texttt{>} \longrightarrow \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>}}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\text{ps}\downarrow\text{ev-prod2}}{\Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{t}_1}\text{ty-prod}}{\Delta;\Gamma \vdash \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \texttt{<}\mathtt{t}_2\texttt{,}\mathtt{t}_1\texttt{>}}\text{ty-prod}$$

(ps-prod2)

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{prl}\ \mathtt{m}_1 : \mathtt{t}_1}{\Delta;\Gamma \vdash \mathtt{m}_1 : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}\downarrow\text{ty-prl} \qquad \dfrac{\texttt{prl}\ \mathtt{m}_1 \longrightarrow \texttt{prl}\ \mathtt{m}_2}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\text{ps}\downarrow\text{ev-prl1}}{\dfrac{\Delta;\Gamma \vdash \mathtt{m}_2 : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}{\Delta;\Gamma \vdash \texttt{prl}\ \mathtt{m}_2 : \mathtt{t}_1}\text{ty-prl}}$$

(ps-prl1)

- $\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{prl}\ \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \mathtt{t}_1}{\Delta;\Gamma \vdash \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}\downarrow\text{ty-prl}}{\Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{t}_2}\downarrow\text{ty-prod}$
- $\texttt{prl}\ \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} \longrightarrow \mathtt{m}_1$
- $\dfrac{\texttt{prl}\ \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} \longrightarrow \mathtt{m}_1}{\texttt{val}\ \mathtt{m}_2}\downarrow\text{ev-prl2}$
- $\dfrac{\texttt{prl}\ \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} \longrightarrow \mathtt{m}_1}{\texttt{val}\ \mathtt{m}_1}\downarrow\text{ev-prl2}$

$$\vdots$$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{prl}\ \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \mathtt{t}_1}{\Delta;\Gamma \vdash \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}\downarrow\text{ty-prl}}{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{t}_1}\downarrow\text{ty-prod}$$

(ps-prl2)

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{prr}\ \mathtt{m}_1 : \mathtt{t}_2}{\Delta;\Gamma \vdash \mathtt{m}_1 : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}\downarrow\text{ty-prr} \qquad \dfrac{\texttt{prr}\ \mathtt{m}_1 \longrightarrow \texttt{prr}\ \mathtt{m}_2}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\text{ps}\downarrow\text{ev-prr1}}{\dfrac{\Delta;\Gamma \vdash \mathtt{m}_2 : \texttt{<}\mathtt{t}_1\texttt{,}\mathtt{t}_2\texttt{>}}{\Delta;\Gamma \vdash \texttt{prr}\ \mathtt{m}_2 : \mathtt{t}_2}\text{ty-prr}}$$

(ps-prr1)

- $\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{prr}\ \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \mathtt{t}_1}{\Delta;\Gamma \vdash \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \texttt{<}\mathtt{t}_2\texttt{,}\mathtt{t}_1\texttt{>}}\downarrow\text{ty-prr}}{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{t}_2}\downarrow\text{ty-prod}$
- $\texttt{prr}\ \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} \longrightarrow \mathtt{m}_2$
- $\dfrac{\texttt{prr}\ \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} \longrightarrow \mathtt{m}_2}{\texttt{val}\ \mathtt{m}_2}\downarrow\text{ev-prr2}$
- $\dfrac{\texttt{prr}\ \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} \longrightarrow \mathtt{m}_2}{\texttt{val}\ \mathtt{m}_1}\downarrow\text{ev-prr2}$

$$\vdots$$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{prr}\ \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \mathtt{t}_1}{\Delta;\Gamma \vdash \texttt{<}\mathtt{m}_1\texttt{,}\mathtt{m}_2\texttt{>} : \texttt{<}\mathtt{t}_2\texttt{,}\mathtt{t}_1\texttt{>}}\downarrow\text{ty-prr}}{\Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{t}_1}\downarrow\text{ty-prod}$$

(ps-prr2)

- $\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{inl}\ \mathtt{m}_1\ \texttt{as}\ \mathtt{t}_1 + \mathtt{t}_2 : \mathtt{t}_1 + \mathtt{t}_2}{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{t}_1}\downarrow\text{ty-inl} \qquad \dfrac{\texttt{inl}\ \mathtt{m}_1\ \texttt{as}\ \mathtt{t}_1 + \mathtt{t}_2 \longrightarrow \texttt{inl}\ \mathtt{m}_2\ \texttt{as}\ \mathtt{t}_1 + \mathtt{t}_2}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\text{ps}\downarrow\text{ev-inl}}{\Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{t}_1}$
- $\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{inl}\ \mathtt{m}_1\ \texttt{as}\ \mathtt{t}_1 + \mathtt{t}_2 : \mathtt{t}_1 + \mathtt{t}_2}{\Delta \vdash \mathtt{t}_1 + \mathtt{t}_2 :: \mathtt{T}}\downarrow\text{ty-inl}}{\Delta;\Gamma \vdash \texttt{inl}\ \mathtt{m}_2\ \texttt{as}\ \mathtt{t}_1 + \mathtt{t}_2 : \mathtt{t}_1 + \mathtt{t}_2}\text{ty-inl}$

(ps-inl)

- $$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{inr}\ m_1\ \texttt{as}\ t_2 + t_1 : t_2 + t_1}{\Delta;\Gamma \vdash m_1 : t_1}\ \downarrow\text{ty-inr} \quad \dfrac{\texttt{inr}\ m_1\ \texttt{as}\ t_2 + t_1 \longrightarrow \texttt{inr}\ m_2\ \texttt{as}\ t_2 + t_1}{m_1 \longrightarrow m_2}\ \downarrow\text{ev-inr}}{\Delta;\Gamma \vdash m_2 : t_1}\ \text{ps}$$

- $$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{inr}\ m_1\ \texttt{as}\ t_2 + t_1 : t_2 + t_1}{\Delta \vdash t_2 + t_1 :: \mathtt{T}}\ \downarrow\text{ty-inr}}{\Delta;\Gamma \vdash \texttt{inr}\ m_2\ \texttt{as}\ t_2 + t_1 : t_2 + t_1}\ \text{ty-inr}$$

(ps-inr)

- $$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{case}\ m_1\ m_3\ m_4 : t_3}{\Delta;\Gamma \vdash m_1 : t_1 + t_2}\ \downarrow\text{ty-case} \quad \dfrac{\texttt{case}\ m_1\ m_3\ m_4 \longrightarrow \texttt{case}\ m_2\ m_3\ m_4}{m_1 \longrightarrow m_2}\ \downarrow\text{ev-case1}}{\Delta;\Gamma \vdash m_2 : t_1 + t_2}\ \text{ps}$$

- $$\dfrac{\Delta;\Gamma \vdash \texttt{case}\ m_1\ m_3\ m_4 : t_3}{\Delta;\Gamma \vdash m_3 : t_1 \to t_3}\ \downarrow\text{ty-case}$$

- $$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{case}\ m_1\ m_3\ m_4 : t_3}{\Delta;\Gamma \vdash m_4 : t_2 \to t_3}\ \downarrow\text{ty-case}}{\Delta;\Gamma \vdash \texttt{case}\ m_2\ m_3\ m_4 : t_3}\ \text{ty-case}$$

(ps-case1)

- $$\dfrac{\Delta;\Gamma \vdash \texttt{case inl}\ m_1\ \texttt{as}\ t_1 + t_2\ m_2\ m_3 : t_3}{\Delta;\Gamma \vdash m_3 : t_2 \to t_3}\ \downarrow\text{ty-case}$$

- $$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{case inl}\ m_1\ \texttt{as}\ t_1 + t_2\ m_2\ m_3 : t_3}{\Delta;\Gamma \vdash \texttt{inl}\ m_1\ \texttt{as}\ t_1 + t_2 : t_1 + t_2}\ \downarrow\text{ty-case}}{\Delta \vdash t_1 + t_2 :: \mathtt{T}}\ \downarrow\text{ty-inl}$$

- $\texttt{case inl}\ m_1\ \texttt{as}\ t_1 + t_2\ m_2\ m_3 \longrightarrow m_2\ m_1$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{case inl}\ m_1\ \texttt{as}\ t_1 + t_2\ m_2\ m_3 : t_3}{\Delta;\Gamma \vdash m_2 : t_1 \to t_3}\ \downarrow\text{ty-case} \quad \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{case inl}\ m_1\ \texttt{as}\ t_1 + t_2\ m_2\ m_3 : t_3}{\Delta;\Gamma \vdash \texttt{inl}\ m_1\ \texttt{as}\ t_1 + t_2 : t_1 + t_2}\ \downarrow\text{ty-case}}{\Delta;\Gamma \vdash m_1 : t_1}\ \downarrow\text{ty-inl}}{\Delta;\Gamma \vdash m_2\ m_1 : t_3}\ \text{ty-app}$$

(ps-case2)

- $$\dfrac{\Delta;\Gamma \vdash \texttt{case inr}\ m_1\ \texttt{as}\ t_1 + t_2\ m_2\ m_3 : t_3}{\Delta;\Gamma \vdash m_2 : t_1 \to t_3}\ \downarrow\text{ty-case}$$

- $$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{case inr}\ m_1\ \texttt{as}\ t_1 + t_2\ m_2\ m_3 : t_3}{\Delta;\Gamma \vdash \texttt{inr}\ m_1\ \texttt{as}\ t_1 + t_2 : t_1 + t_2}\ \downarrow\text{ty-case}}{\Delta \vdash t_1 + t_2 :: \mathtt{T}}\ \downarrow\text{ty-inr}$$

- $\texttt{case inr}\ m_1\ \texttt{as}\ t_1 + t_2\ m_2\ m_3 \longrightarrow m_3\ m_1$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{case inr}\ m_1\ \texttt{as}\ t_1 + t_2\ m_2\ m_3 : t_3}{\Delta;\Gamma \vdash m_3 : t_2 \to t_3}\ \downarrow\text{ty-case} \quad \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{case inr}\ m_1\ \texttt{as}\ t_1 + t_2\ m_2\ m_3 : t_3}{\Delta;\Gamma \vdash \texttt{inr}\ m_1\ \texttt{as}\ t_1 + t_2 : t_1 + t_2}\ \downarrow\text{ty-case}}{\Delta;\Gamma \vdash m_1 : t_2}\ \downarrow\text{ty-inr}}{\Delta;\Gamma \vdash m_3\ m_1 : t_3}\ \text{ty-app}$$

(ps-case3)

$$\dfrac{\dfrac{\dfrac{\Delta;\Gamma \vdash m_1\ m_3 : t_2}{\Delta;\Gamma \vdash m_1 : t_1 \to t_2}\ \downarrow\text{ty-app} \quad \dfrac{m_1\ m_3 \longrightarrow m_2\ m_3}{m_1 \longrightarrow m_2}\ \downarrow\text{ev-app1}}{\Delta;\Gamma \vdash m_2 : t_1 \to t_2}\ \text{ps} \quad \dfrac{\Delta;\Gamma \vdash m_1\ m_3 : t_2}{\Delta;\Gamma \vdash m_3 : t_1}\ \downarrow\text{ty-app}}{\Delta;\Gamma \vdash m_2\ m_3 : t_2}\ \text{ty-app}$$

(ps-app1)

$$
\dfrac{
\dfrac{\Delta;\Gamma \vdash \mathtt{m}_3\ \mathtt{m}_1 : \mathtt{t}_2}{\Delta;\Gamma \vdash \mathtt{m}_3 : \mathtt{t}_1 \to \mathtt{t}_2}\ {\downarrow}\text{ty-app}
\qquad
\dfrac{
\dfrac{\begin{array}{c}\dfrac{\mathtt{m}_3\ \mathtt{m}_1 \longrightarrow \mathtt{m}_3\ \mathtt{m}_2}{\mathtt{val}\ \mathtt{m}_3}\ {\downarrow}\text{ev-app2} \\ \vdots \\ \Delta;\Gamma \vdash \mathtt{m}_3\ \mathtt{m}_1 : \mathtt{t}_2\end{array}}{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{t}_1}\ {\downarrow}\text{ty-app}
\quad
\dfrac{\mathtt{m}_3\ \mathtt{m}_1 \longrightarrow \mathtt{m}_3\ \mathtt{m}_2}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\ {\downarrow}\text{ev-app2}
}{\Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{t}_1}\ \text{ps}
}{\Delta;\Gamma \vdash \mathtt{m}_3\ \mathtt{m}_2 : \mathtt{t}_2}\ \text{ty-app}
\tag{ps-app2}
$$

$$
\begin{array}{l}
\begin{array}{c}
\dfrac{\dfrac{\Delta;\Gamma \vdash (\lambda \mathtt{x}{:}\mathtt{t}_1 . \mathtt{m}_1)\ \mathtt{m}_2 : \mathtt{t}_2}{\Delta;\Gamma \vdash \lambda \mathtt{x}{:}\mathtt{t}_1 . \mathtt{m}_1 : \mathtt{t}_1 \to \mathtt{t}_2}\ {\downarrow}\text{ty-app}}{\Delta \vdash \mathtt{t}_1 :: \mathtt{T}}\ {\downarrow}\text{ty-fun}
\quad
\dfrac{(\lambda \mathtt{x}{:}\mathtt{t}_1 . \mathtt{m}_1)\ \mathtt{m}_2 \longrightarrow \mathtt{m}_3}{\mathtt{val}\ \mathtt{m}_2}\ {\downarrow}\text{ev-app3} \\
\vdots
\end{array} \\
\dfrac{
\begin{array}{l}
\bullet\ \dfrac{\dfrac{\Delta;\Gamma \vdash (\lambda \mathtt{x}{:}\mathtt{t}_1 . \mathtt{m}_1)\ \mathtt{m}_2 : \mathtt{t}_2}{\Delta;\Gamma \vdash \lambda \mathtt{x}{:}\mathtt{t}_1 . \mathtt{m}_1 : \mathtt{t}_1 \to \mathtt{t}_2}\ {\downarrow}\text{ty-app}}{\Delta;\Gamma,\mathtt{x}{:}\mathtt{t}_1 \vdash \mathtt{m}_1 : \mathtt{t}_2}\ {\downarrow}\text{ty-fun} \\
\bullet\ \dfrac{\Delta;\Gamma \vdash (\lambda \mathtt{x}{:}\mathtt{t}_1 . \mathtt{m}_1)\ \mathtt{m}_2 : \mathtt{t}_2}{\Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{t}_1}\ {\downarrow}\text{ty-app} \\
\bullet\ \dfrac{(\lambda \mathtt{x}{:}\mathtt{t}_1 . \mathtt{m}_1)\ \mathtt{m}_2 \longrightarrow \mathtt{m}_3}{\mathtt{m}_1\{\mathtt{m}_2/\mathtt{x}\} = \mathtt{m}_3}\ {\downarrow}\text{ev-app3}
\end{array}
}{\Delta;\Gamma \vdash \mathtt{m}_3 : \mathtt{t}_2}\ \text{pssub}
\end{array}
\tag{ps-app3}
$$

$$
\dfrac{
\begin{array}{l}
\bullet\ \dfrac{\dfrac{\Delta;\Gamma \vdash \mathtt{m}_1\ [\mathtt{t}_3] : \mathtt{t}_4}{\Delta;\Gamma \vdash \mathtt{m}_1 : \forall \alpha \preceq \mathtt{t}_1 .\ \mathtt{t}_2}\ {\downarrow}\text{ty-inst} \quad \dfrac{\mathtt{m}_1\ [\mathtt{t}_3] \longrightarrow \mathtt{m}_2\ [\mathtt{t}_3]}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\ {\downarrow}\text{ev-inst1}}{\Delta;\Gamma \vdash \mathtt{m}_2 : \forall \alpha \preceq \mathtt{t}_1 .\ \mathtt{t}_2}\ \text{ps} \\
\bullet\ \dfrac{\Delta;\Gamma \vdash \mathtt{m}_1\ [\mathtt{t}_3] : \mathtt{t}_4}{\Delta \vdash \mathtt{t}_1 :: \mathtt{k}}\ {\downarrow}\text{ty-inst} \\
\bullet\ \dfrac{\Delta;\Gamma \vdash \mathtt{m}_1\ [\mathtt{t}_3] : \mathtt{t}_4}{\Delta \vdash \mathtt{t}_3 :: \mathtt{k}}\ {\downarrow}\text{ty-inst} \\
\bullet\ \dfrac{\Delta;\Gamma \vdash \mathtt{m}_1\ [\mathtt{t}_3] : \mathtt{t}_4}{\Delta \vdash \mathtt{t}_3 \preceq \mathtt{t}_1}\ {\downarrow}\text{ty-inst} \\
\bullet\ \dfrac{\Delta;\Gamma \vdash \mathtt{m}_1\ [\mathtt{t}_3] : \mathtt{t}_4}{\mathtt{t}_2\{\mathtt{t}_3/\alpha\} = \mathtt{t}_4}\ {\downarrow}\text{ty-inst}
\end{array}
}{\Delta;\Gamma \vdash \mathtt{m}_2\ [\mathtt{t}_3] : \mathtt{t}_4}\ \text{ty-inst}
\tag{ps-inst1}
$$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash (\Lambda\alpha \preceq \mathtt{t}_1\,.\,\mathtt{m}_1)\ [\mathtt{t}_3] : \mathtt{t}_4}{\Delta \vdash \mathtt{t}_3 :: \mathtt{k}_1}\downarrow\text{ty-inst} \quad \dfrac{\Delta;\Gamma \vdash (\Lambda\alpha \preceq \mathtt{t}_1\,.\,\mathtt{m}_1)\ [\mathtt{t}_3] : \mathtt{t}_4}{\Delta \vdash \mathtt{t}_1 :: \mathtt{k}_1}\downarrow\text{ty-inst} \quad \dfrac{\dfrac{\Delta;\Gamma \vdash (\Lambda\alpha \preceq \mathtt{t}_1\,.\,\mathtt{m}_1)\ [\mathtt{t}_3] : \mathtt{t}_4}{\Delta;\Gamma \vdash \Lambda\alpha \preceq \mathtt{t}_1\,.\,\mathtt{m}_1 : \forall\alpha \preceq \mathtt{t}_1\,.\,\mathtt{t}_2}\downarrow\text{ty-inst}}{\Delta \vdash \mathtt{t}_1 :: \mathtt{k}_2}\downarrow\text{ty-poly}}{\vdots}$$

- $\dfrac{\dfrac{\Delta;\Gamma \vdash (\Lambda\alpha \preceq \mathtt{t}_1\,.\,\mathtt{m}_1)\ [\mathtt{t}_3] : \mathtt{t}_4}{\Delta;\Gamma \vdash \Lambda\alpha \preceq \mathtt{t}_1\,.\,\mathtt{m}_1 : \forall\alpha \preceq \mathtt{t}_1\,.\,\mathtt{t}_2}\downarrow\text{ty-inst}}{\Delta, \alpha \preceq \mathtt{t}_1; \Gamma \vdash \mathtt{m}_1 : \mathtt{t}_2}\downarrow\text{ty-poly}$
- $\dfrac{\Delta;\Gamma \vdash (\Lambda\alpha \preceq \mathtt{t}_1\,.\,\mathtt{m}_1)\ [\mathtt{t}_3] : \mathtt{t}_4}{\Delta \vdash \mathtt{t}_3 \preceq \mathtt{t}_1}\downarrow\text{ty-inst}$
- $\dfrac{\dfrac{\Delta;\Gamma \vdash (\Lambda\alpha \preceq \mathtt{t}_1\,.\,\mathtt{m}_1)\ [\mathtt{t}_3] : \mathtt{t}_4}{\Delta;\Gamma \vdash \Lambda\alpha \preceq \mathtt{t}_1\,.\,\mathtt{m}_1 : \forall\alpha \preceq \mathtt{t}_1\,.\,\mathtt{t}_2}\downarrow\text{ty-inst}}{\alpha \notin \mathtt{tfv}(\Gamma)}\downarrow\text{ty-poly}$
- $\dfrac{(\Lambda\alpha \preceq \mathtt{t}_1\,.\,\mathtt{m}_1)\ [\mathtt{t}_3] \longrightarrow \mathtt{m}_2}{\mathtt{m}_1\{\mathtt{t}_3/\alpha\} = \mathtt{m}_2}\downarrow\text{ev-inst2}$
- $\dfrac{\dfrac{\Delta;\Gamma \vdash (\Lambda\alpha \preceq \mathtt{t}_1\,.\,\mathtt{m}_1)\ [\mathtt{t}_3] : \mathtt{t}_4}{\mathtt{t}_2\{\mathtt{t}_3/\alpha\} = \mathtt{t}_4}\downarrow\text{ty-inst}}{\Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{t}_4}\text{psmtsub1}$

(ps-inst2)

- $\dfrac{\Delta;\Gamma \vdash \mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_1)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4 : \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4}{\Delta \vdash \mathtt{t}_2 :: \mathtt{k}}\downarrow\text{ty-pack}$
- $\dfrac{\Delta;\Gamma \vdash \mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_1)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4 : \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4}{\Delta \vdash \mathtt{t}_3 :: \mathtt{k}}\downarrow\text{ty-pack}$
- $\dfrac{\Delta;\Gamma \vdash \mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_1)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4 : \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4}{\Delta \vdash \mathtt{t}_4 :: \mathtt{T}}\downarrow\text{ty-pack}$
- $\dfrac{\Delta;\Gamma \vdash \mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_1)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4 : \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4}{\Delta \vdash \mathtt{t}_2 \preceq \mathtt{t}_3}\downarrow\text{ty-pack}$
- $\dfrac{\Delta;\Gamma \vdash \mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_1)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4 : \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4}{\mathtt{t}_4\{\mathtt{t}_2/\alpha\} = \mathtt{t}_1}\downarrow\text{ty-pack}$
  - $\dfrac{\Delta;\Gamma \vdash \mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_1)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4 : \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4}{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{t}_1}\downarrow\text{ty-pack}$
  - $\dfrac{\mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_1)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4 \longrightarrow \mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_2)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\downarrow\text{ev-pack}$
  - $\dfrac{\dfrac{\mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_1)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4 \longrightarrow \mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_2)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\text{ps}}{\Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{t}_1}$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_1)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4 : \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4}{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{t}_1}\downarrow\text{ty-pack} \quad \dfrac{\mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_1)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4 \longrightarrow \mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_2)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\downarrow\text{ev-pack}}{\Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{t}_1}\text{ps}}{\Delta;\Gamma \vdash \mathtt{pack}\ (\mathtt{t}_2, \mathtt{m}_2)\ \mathtt{as}\ \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4 : \exists\alpha \preceq \mathtt{t}_3\,.\,\mathtt{t}_4}\text{ty-pack}$$

(ps-pack)

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \mathtt{open}\ (\alpha, \mathtt{x}) = \mathtt{m}_1\ \mathtt{in}\ \mathtt{m}_3 : \mathtt{t}_3}{\Delta;\Gamma \vdash \mathtt{m}_1 : \exists\alpha \preceq \mathtt{t}_1\,.\,\mathtt{t}_2}\downarrow\text{ty-open} \quad \dfrac{\mathtt{open}\ (\alpha, \mathtt{x}) = \mathtt{m}_1\ \mathtt{in}\ \mathtt{m}_3 \longrightarrow \mathtt{open}\ (\alpha, \mathtt{x}) = \mathtt{m}_2\ \mathtt{in}\ \mathtt{m}_3}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\text{ps}\downarrow\text{ev-open1}}{\Delta;\Gamma \vdash \mathtt{m}_2 : \exists\alpha \preceq \mathtt{t}_1\,.\,\mathtt{t}_2}$$

- $\dfrac{\Delta;\Gamma \vdash \mathtt{open}\ (\alpha, \mathtt{x}) = \mathtt{m}_1\ \mathtt{in}\ \mathtt{m}_3 : \mathtt{t}_3}{\Delta, \alpha \preceq \mathtt{t}_1; \Gamma, \mathtt{x}{:}\mathtt{t}_2 \vdash \mathtt{m}_3 : \mathtt{t}_3}\downarrow\text{ty-open}$
- $\dfrac{\Delta;\Gamma \vdash \mathtt{open}\ (\alpha, \mathtt{x}) = \mathtt{m}_1\ \mathtt{in}\ \mathtt{m}_3 : \mathtt{t}_3}{\alpha \notin \mathtt{tfv}(\Gamma)}\downarrow\text{ty-open}$
- $\dfrac{\dfrac{\Delta;\Gamma \vdash \mathtt{open}\ (\alpha, \mathtt{x}) = \mathtt{m}_1\ \mathtt{in}\ \mathtt{m}_3 : \mathtt{t}_3}{\alpha \notin \mathtt{tfv}(\mathtt{t}_3)}\downarrow\text{ty-open}}{\Delta;\Gamma \vdash \mathtt{open}\ (\alpha, \mathtt{x}) = \mathtt{m}_2\ \mathtt{in}\ \mathtt{m}_3 : \mathtt{t}_3}\text{ty-open}$

(ps-open1)

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{open}\ (\alpha,\texttt{x}) = \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4\ \texttt{in}\ \texttt{m}_4 : \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4 : \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4}\ \downarrow\text{ty-open}}{\Delta \vdash \texttt{t}_4 :: \texttt{T}}\ \downarrow\text{ty-pack}$$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{open}\ (\alpha,\texttt{x}) = \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4\ \texttt{in}\ \texttt{m}_4 : \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4 : \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4}\ \downarrow\text{ty-open}}{\Delta \vdash \texttt{t}_3 :: \texttt{k}}\ \downarrow\text{ty-pack}$$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{open}\ (\alpha,\texttt{x}) = \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4\ \texttt{in}\ \texttt{m}_4 : \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4 : \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4}\ \downarrow\text{ty-open}}{\Delta \vdash \texttt{t}_5 :: \texttt{k}}\ \downarrow\text{ty-pack}$$

$$\dfrac{\texttt{open}\ (\alpha,\texttt{x}) = \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4\ \texttt{in}\ \texttt{m}_4 \longrightarrow \texttt{m}_3}{\texttt{val}\ \texttt{m}_2}\ \downarrow\text{ev-open2}$$

$$\vdots$$

$$\dfrac{\Delta;\Gamma \vdash \texttt{open}\ (\alpha,\texttt{x}) = \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4\ \texttt{in}\ \texttt{m}_4 : \texttt{t}_2}{\Delta, \alpha \preceq \texttt{t}_3; \Gamma, \texttt{x}{:}\texttt{t}_4 \vdash \texttt{m}_4 : \texttt{t}_2}\ \downarrow\text{ty-open}$$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{open}\ (\alpha,\texttt{x}) = \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4\ \texttt{in}\ \texttt{m}_4 : \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4 : \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4}\ \downarrow\text{ty-open}}{\Delta \vdash \texttt{t}_5 \preceq \texttt{t}_3}\ \downarrow\text{ty-pack}$$

$$\dfrac{\Delta;\Gamma \vdash \texttt{open}\ (\alpha,\texttt{x}) = \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4\ \texttt{in}\ \texttt{m}_4 : \texttt{t}_2}{\alpha \notin \texttt{tfv}(\Gamma)}\ \downarrow\text{ty-open}$$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{open}\ (\alpha,\texttt{x}) = \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4\ \texttt{in}\ \texttt{m}_4 : \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4 : \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4}\ \downarrow\text{ty-open}}{\texttt{t}_4\{\texttt{t}_5/\alpha\} = \texttt{t}_1}\ \downarrow\text{ty-pack}$$

$$\dfrac{\texttt{open}\ (\alpha,\texttt{x}) = \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4\ \texttt{in}\ \texttt{m}_4 \longrightarrow \texttt{m}_3}{\texttt{m}_4\{\texttt{t}_5/\alpha\} = \texttt{m}_1}\ \downarrow\text{ev-open2}$$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{open}\ (\alpha,\texttt{x}) = \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4\ \texttt{in}\ \texttt{m}_4 : \texttt{t}_2}{\alpha \notin \texttt{tfv}(\texttt{t}_2)}\ \downarrow\text{ty-open}}{\Delta;\Gamma,\texttt{x}{:}\texttt{t}_1 \vdash \texttt{m}_1 : \texttt{t}_2}\ \text{psmtsub2}$$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{open}\ (\alpha,\texttt{x}) = \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4\ \texttt{in}\ \texttt{m}_4 : \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4 : \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4}\ \downarrow\text{ty-open}}{\Delta;\Gamma \vdash \texttt{m}_2 : \texttt{t}_1}\ \downarrow\text{ty-pack}$$

$$\dfrac{\dfrac{\texttt{open}\ (\alpha,\texttt{x}) = \texttt{pack}\ (\texttt{t}_5,\texttt{m}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_3.\ \texttt{t}_4\ \texttt{in}\ \texttt{m}_4 \longrightarrow \texttt{m}_3}{\texttt{m}_1\{\texttt{m}_2/\texttt{x}\} = \texttt{m}_3}\ \downarrow\text{ev-open2}}{\Delta;\Gamma \vdash \texttt{m}_3 : \texttt{t}_2}\ \text{pssub}$$

(ps-open2)

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{m}_1\{\texttt{t}_2\} : \texttt{t}_1\{\texttt{t}_2\}}{\Delta;\Gamma \vdash \texttt{m}_1 : \texttt{t}_1}\ \downarrow\text{ty-lab} \quad \dfrac{\texttt{m}_1\{\texttt{t}_2\} \longrightarrow \texttt{m}_2\{\texttt{t}_2\}}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \text{ps} \quad \downarrow\text{ev-lab} \quad \dfrac{\Delta;\Gamma \vdash \texttt{m}_1\{\texttt{t}_2\} : \texttt{t}_1\{\texttt{t}_2\}}{\Delta \vdash \texttt{t}_2 :: \texttt{L}}\ \downarrow\text{ty-lab}}{\Delta;\Gamma \vdash \texttt{m}_2 : \texttt{t}_1}\ \text{ty-lab}$$

$$\Delta;\Gamma \vdash \texttt{m}_2\{\texttt{t}_2\} : \texttt{t}_1\{\texttt{t}_2\}$$

(ps-lab)

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{bind}\ \texttt{x} = \texttt{m}_1\ \texttt{in}\ \texttt{m}_3 : \texttt{t}_3}{\Delta;\Gamma \vdash \texttt{m}_1 : \texttt{t}_1\{\texttt{t}_2\}}\ \downarrow\text{ty-bind} \quad \dfrac{\texttt{bind}\ \texttt{x} = \texttt{m}_1\ \texttt{in}\ \texttt{m}_3 \longrightarrow \texttt{bind}\ \texttt{x} = \texttt{m}_2\ \texttt{in}\ \texttt{m}_3}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \downarrow\text{ev-bind1}}{\Delta;\Gamma \vdash \texttt{m}_2 : \texttt{t}_1\{\texttt{t}_2\}}\ \text{ps}$$

$$\dfrac{\Delta;\Gamma \vdash \texttt{bind}\ \texttt{x} = \texttt{m}_1\ \texttt{in}\ \texttt{m}_3 : \texttt{t}_3}{\Delta;\Gamma,\texttt{x}{:}\texttt{t}_1 \vdash \texttt{m}_3 : \texttt{t}_3}\ \downarrow\text{ty-bind}$$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{bind}\ \texttt{x} = \texttt{m}_1\ \texttt{in}\ \texttt{m}_3 : \texttt{t}_3}{\Delta \vdash \texttt{t}_3 \gg \texttt{t}_2}\ \downarrow\text{ty-bind}}{\Delta;\Gamma \vdash \texttt{bind}\ \texttt{x} = \texttt{m}_2\ \texttt{in}\ \texttt{m}_3 : \texttt{t}_3}\ \text{ty-bind}$$

(ps-bind1)

$$
\begin{array}{l}
\bullet\ \dfrac{\Delta;\Gamma \vdash \texttt{bind x} = \texttt{m}_2\{\texttt{t}_3\}\ \texttt{in m}_1 : \texttt{t}_2}{\Delta \vdash \texttt{t}_2 \gg \texttt{t}_3}\ \downarrow\text{ty-bind} \\[2ex]
\bullet\ \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{bind x} = \texttt{m}_2\{\texttt{t}_3\}\ \texttt{in m}_1 : \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{m}_2\{\texttt{t}_3\} : \texttt{t}_1\{\texttt{t}_3\}}\ \downarrow\text{ty-bind}}{\Delta \vdash \texttt{t}_3 :: \texttt{L}}\ \downarrow\text{ty-lab} \\[2ex]
\bullet\ \dfrac{\texttt{bind x} = \texttt{m}_2\{\texttt{t}_3\}\ \texttt{in m}_1 \longrightarrow \texttt{m}_3}{\texttt{val m}_2}\ \downarrow\text{ev-bind2} \\[2ex]
\qquad\qquad\vdots \\[2ex]
\dfrac{\Delta;\Gamma \vdash \texttt{bind x} = \texttt{m}_2\{\texttt{t}_3\}\ \texttt{in m}_1 : \texttt{t}_2}{\Delta;\Gamma,\texttt{x:t}_1 \vdash \texttt{m}_1 : \texttt{t}_2}\ \downarrow\text{ty-bind} \\[2ex]
\bullet\ \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{bind x} = \texttt{m}_2\{\texttt{t}_3\}\ \texttt{in m}_1 : \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{m}_2\{\texttt{t}_3\} : \texttt{t}_1\{\texttt{t}_3\}}\ \downarrow\text{ty-bind}}{\Delta;\Gamma \vdash \texttt{m}_2 : \texttt{t}_1}\ \downarrow\text{ty-lab} \\[2ex]
\bullet\ \dfrac{\dfrac{\texttt{bind x} = \texttt{m}_2\{\texttt{t}_3\}\ \texttt{in m}_1 \longrightarrow \texttt{m}_3}{\texttt{m}_1\{\texttt{m}_2/\texttt{x}\} = \texttt{m}_3}\ \downarrow\text{ev-bind2}}{\Delta;\Gamma \vdash \texttt{m}_3 : \texttt{t}_2}\ \text{pssub}
\end{array}
\qquad \text{(ps-bind2)}
$$

$$
\begin{array}{l}
\bullet\ \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{fix}\ \lambda\texttt{x:t.m}_1 : \texttt{t}}{\Delta;\Gamma \vdash \lambda\texttt{x:t.m}_1 : \texttt{t} \to \texttt{t}}\ \downarrow\text{ty-fix}}{\Delta;\Gamma,\texttt{x:t} \vdash \texttt{m}_1 : \texttt{t}}\ \downarrow\text{ty-fun} \\[2ex]
\bullet\ \dfrac{\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{fix}\ \lambda\texttt{x:t.m}_1 : \texttt{t}}{\Delta;\Gamma \vdash \lambda\texttt{x:t.m}_1 : \texttt{t} \to \texttt{t}}\ \downarrow\text{ty-fix}}{\Delta;\Gamma,\texttt{x:t} \vdash \texttt{m}_1 : \texttt{t}}\ \downarrow\text{ty-fun} \quad \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{fix}\ \lambda\texttt{x:t.m}_1 : \texttt{t}}{\Delta;\Gamma \vdash \lambda\texttt{x:t.m}_1 : \texttt{t} \to \texttt{t}}\ \downarrow\text{ty-fix}}{\Delta \vdash \texttt{t} :: \texttt{T}}\ \downarrow\text{ty-fun}}{\Delta;\Gamma \vdash \lambda\texttt{x:t.m}_1 : \texttt{t} \to \texttt{t}}\ \text{ty-fun} \quad \dfrac{\Delta;\Gamma \vdash \texttt{fix}\ \lambda\texttt{x:t.m}_1 : \texttt{t}}{\Delta \vdash \texttt{t} \gg \dagger}\ \downarrow\text{ty-fix}}{\Delta;\Gamma \vdash \texttt{fix}\ \lambda\texttt{x:t.m}_1 : \texttt{t}}\ \text{ty-fix} \\[2ex]
\bullet\ \dfrac{\dfrac{\texttt{fix}\ \lambda\texttt{x:t.m}_1 \longrightarrow \texttt{m}_2}{\texttt{m}_1\{\texttt{fix}\ \lambda\texttt{x:t.m}_1/\texttt{x}\} = \texttt{m}_2}\ \downarrow\text{ev-fix}}{\Delta;\Gamma \vdash \texttt{m}_2 : \texttt{t}}\ \text{pssub}
\end{array}
\qquad \text{(ps-fix)}
$$

$$
\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{lift m}_1 : \texttt{t}^\dagger}{\Delta;\Gamma \vdash \texttt{m}_1 : \texttt{t}}\ \downarrow\text{ty-lift} \quad \dfrac{\texttt{lift m}_1 \longrightarrow \texttt{lift m}_2}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \text{ps}\ \downarrow\text{ev-lift}}{\dfrac{\Delta;\Gamma \vdash \texttt{m}_2 : \texttt{t}}{\Delta;\Gamma \vdash \texttt{lift m}_2 : \texttt{t}^\dagger}\ \text{ty-lift}}
\qquad \text{(ps-lift)}
$$

$$
\begin{array}{l}
\bullet\ \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{seq x} = \texttt{m}_1\ \texttt{in m}_3 : \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{m}_1 : \texttt{t}_1^\dagger}\ \downarrow\text{ty-seq} \quad \dfrac{\texttt{seq x} = \texttt{m}_1\ \texttt{in m}_3 \longrightarrow \texttt{seq x} = \texttt{m}_2\ \texttt{in m}_3}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \text{ps}\ \downarrow\text{ev-seq1}}{\Delta;\Gamma \vdash \texttt{m}_2 : \texttt{t}_1^\dagger} \\[2ex]
\bullet\ \dfrac{\Delta;\Gamma \vdash \texttt{seq x} = \texttt{m}_1\ \texttt{in m}_3 : \texttt{t}_2}{\Delta;\Gamma,\texttt{x:t}_1 \vdash \texttt{m}_3 : \texttt{t}_2}\ \downarrow\text{ty-seq} \\[2ex]
\bullet\ \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{seq x} = \texttt{m}_1\ \texttt{in m}_3 : \texttt{t}_2}{\Delta \vdash \texttt{t}_2 \gg \dagger}\ \downarrow\text{ty-seq}}{\Delta;\Gamma \vdash \texttt{seq x} = \texttt{m}_2\ \texttt{in m}_3 : \texttt{t}_2}\ \text{ty-seq}
\end{array}
\qquad \text{(ps-seq1)}
$$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{seq x} = \texttt{lift m}_2\ \texttt{in m}_1 : \texttt{t}_2}{\Delta \vdash \texttt{t}_2 \gg \dagger}\ \downarrow\text{ty-seq} \quad \dfrac{\texttt{seq x} = \texttt{lift m}_2\ \texttt{in m}_1 \longrightarrow \texttt{m}_3}{\texttt{val m}_2}\ \downarrow\text{ev-seq2}}{\begin{array}{l}\vdots \\ \bullet\ \dfrac{\Delta;\Gamma \vdash \texttt{seq x} = \texttt{lift m}_2\ \texttt{in m}_1 : \texttt{t}_2}{\Delta;\Gamma,\texttt{x:t}_1 \vdash \texttt{m}_1 : \texttt{t}_2}\ \downarrow\text{ty-seq} \\ \bullet\ \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{seq x} = \texttt{lift m}_2\ \texttt{in m}_1 : \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{lift m}_2 : \texttt{t}_1^{\dagger}}\ \downarrow\text{ty-seq}}{\Delta;\Gamma \vdash \texttt{m}_2 : \texttt{t}_1}\ \downarrow\text{ty-lift} \\ \bullet\ \dfrac{\dfrac{\texttt{seq x} = \texttt{lift m}_2\ \texttt{in m}_1 \longrightarrow \texttt{m}_3}{\texttt{m}_1\{\texttt{m}_2/\texttt{x}\} = \texttt{m}_3}\ \downarrow\text{ev-seq2}}{\Delta;\Gamma \vdash \texttt{m}_3 : \texttt{t}_2}\ \text{pssub}\end{array}}\ \text{(ps-seq2)}$$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_1 : \texttt{t}_3\ \%\ \texttt{t}_1 \lhd \texttt{t}_2}{\Delta,\texttt{t}_1 \lhd \texttt{t}_2;\Gamma \vdash \texttt{m}_1 : \texttt{t}_3}\ \downarrow\text{ty-let} \quad \dfrac{\texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_1 \longrightarrow \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_2}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \downarrow\text{ev-let}}{\begin{array}{l}\bullet\ \dfrac{\Delta,\texttt{t}_1 \lhd \texttt{t}_2;\Gamma \vdash \texttt{m}_1 : \texttt{t}_3}{\Delta,\texttt{t}_1 \lhd \texttt{t}_2;\Gamma \vdash \texttt{m}_2 : \texttt{t}_3}\ \text{ps} \\ \bullet\ \dfrac{\Delta;\Gamma \vdash \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_1 : \texttt{t}_3\ \%\ \texttt{t}_1 \lhd \texttt{t}_2}{\Delta \vdash \texttt{t}_1 :: \texttt{P}}\ \downarrow\text{ty-let} \\ \bullet\ \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_1 : \texttt{t}_3\ \%\ \texttt{t}_1 \lhd \texttt{t}_2}{\Delta \vdash \texttt{t}_2 :: \texttt{PJ}}\ \downarrow\text{ty-let}}{\Delta;\Gamma \vdash \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_2 : \texttt{t}_3\ \%\ \texttt{t}_1 \lhd \texttt{t}_2}\ \text{ty-let}\end{array}}\ \text{(ps-let)}$$

$$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{pass x} = \texttt{m}_1\ \texttt{in m}_3 : \texttt{t}_4\ \%\ \texttt{t}_2 \lhd \texttt{t}_3}{\Delta;\Gamma \vdash \texttt{m}_1 : \texttt{t}_1\ \%\ \texttt{t}_2 \lhd \texttt{t}_3}\ \downarrow\text{ty-pass} \quad \dfrac{\texttt{pass x} = \texttt{m}_1\ \texttt{in m}_3 \longrightarrow \texttt{pass x} = \texttt{m}_2\ \texttt{in m}_3}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \text{ps}}{\begin{array}{l}\bullet\ \dfrac{\Delta;\Gamma \vdash \texttt{m}_2 : \texttt{t}_1\ \%\ \texttt{t}_2 \lhd \texttt{t}_3}{\Delta;\Gamma \vdash \texttt{pass x} = \texttt{m}_2\ \texttt{in m}_3 : \texttt{t}_4\ \%\ \texttt{t}_2 \lhd \texttt{t}_3}\ \downarrow\text{ev-pass1} \\ \bullet\ \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{pass x} = \texttt{m}_1\ \texttt{in m}_3 : \texttt{t}_4\ \%\ \texttt{t}_2 \lhd \texttt{t}_3}{\Delta,\texttt{t}_2 \lhd \texttt{t}_3;\Gamma,\texttt{x:t}_1 \vdash \texttt{m}_3 : \texttt{t}_4}\ \downarrow\text{ty-pass}}{\Delta;\Gamma \vdash \texttt{pass x} = \texttt{m}_2\ \texttt{in m}_3 : \texttt{t}_4\ \%\ \texttt{t}_2 \lhd \texttt{t}_3}\ \text{ty-pass}\end{array}}\ \text{(ps-pass1)}$$

$$\dfrac{\dfrac{\texttt{pass x} = \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_2\ \texttt{in m}_1 \longrightarrow \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_3}{\texttt{val m}_2}\ \downarrow\text{ev-pass2}}{\begin{array}{l}\vdots \\ \bullet\ \dfrac{\Delta;\Gamma \vdash \texttt{pass x} = \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_2\ \texttt{in m}_1 : \texttt{t}_4\ \%\ \texttt{t}_1 \lhd \texttt{t}_2}{\Delta,\texttt{t}_1 \lhd \texttt{t}_2;\Gamma,\texttt{x:t}_3 \vdash \texttt{m}_1 : \texttt{t}_4}\ \downarrow\text{ty-pass} \\ \bullet\ \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{pass x} = \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_2\ \texttt{in m}_1 : \texttt{t}_4\ \%\ \texttt{t}_1 \lhd \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_2 : \texttt{t}_3\ \%\ \texttt{t}_1 \lhd \texttt{t}_2}\ \downarrow\text{ty-let}}{\Delta,\texttt{t}_1 \lhd \texttt{t}_2;\Gamma \vdash \texttt{m}_2 : \texttt{t}_3}\ \downarrow\text{ty-pass} \\ \bullet\ \dfrac{\dfrac{\texttt{pass x} = \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_2\ \texttt{in m}_1 \longrightarrow \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_3}{\texttt{m}_1\{\texttt{m}_2/\texttt{x}\} = \texttt{m}_3}\ \downarrow\text{ev-pass2}}{\Delta,\texttt{t}_1 \lhd \texttt{t}_2;\Gamma \vdash \texttt{m}_3 : \texttt{t}_4}\ \text{pssub} \\ \bullet\ \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{pass x} = \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_2\ \texttt{in m}_1 : \texttt{t}_4\ \%\ \texttt{t}_1 \lhd \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_2 : \texttt{t}_3\ \%\ \texttt{t}_1 \lhd \texttt{t}_2}\ \downarrow\text{ty-let}}{\Delta \vdash \texttt{t}_1 :: \texttt{P}}\ \downarrow\text{ty-pass} \\ \bullet\ \dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{pass x} = \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_2\ \texttt{in m}_1 : \texttt{t}_4\ \%\ \texttt{t}_1 \lhd \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_2 : \texttt{t}_3\ \%\ \texttt{t}_1 \lhd \texttt{t}_2}\ \downarrow\text{ty-let}}{\Delta \vdash \texttt{t}_2 :: \texttt{PJ}}\ \downarrow\text{ty-let} \\ \dfrac{}{\Delta;\Gamma \vdash \texttt{let t}_1 \lhd \texttt{t}_2\ \texttt{in m}_3 : \texttt{t}_4\ \%\ \texttt{t}_1 \lhd \texttt{t}_2}\ \text{ty-let}\end{array}}\ \text{(ps-pass2)}$$

- $$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_1\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_3}{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{cert}}\downarrow\text{ty-if} \quad \dfrac{\texttt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 \longrightarrow \texttt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\ \text{ps}}{\Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{cert}}\downarrow\text{ev-if1}$$
- $$\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_1\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_3}{\Delta;\Gamma \vdash \mathtt{m}_3 : \mathtt{'t}_2}\downarrow\text{ty-if}$$
- $$\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_1\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_3}{\Delta;\Gamma \vdash \mathtt{m}_4 : \mathtt{'t}_3}\downarrow\text{ty-if}$$
- $$\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_1\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_3}{\Delta, \mathtt{t}_2 \lhd \mathtt{t}_3;\Gamma \vdash \mathtt{m}_5 : \mathtt{t}_1}\downarrow\text{ty-if}$$
- $$\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_1\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_3}{\Delta;\Gamma \vdash \mathtt{m}_6 : \mathtt{t}_1}\downarrow\text{ty-if}$$
- $$\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_1\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_3}{\Delta \vdash \mathtt{t}_2 :: \mathtt{P}}\downarrow\text{ty-if}$$
- $$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_1 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_1\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_3}{\Delta \vdash \mathtt{t}_3 :: \mathtt{PJ}}\downarrow\text{ty-if}}{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_3 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_1\ \%\ \mathtt{t}_2 \lhd \mathtt{t}_3}\ \text{ty-if}$$ (ps-if1)

$$\dfrac{\texttt{if}\ (\mathtt{m}_3 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 \longrightarrow \texttt{if}\ (\mathtt{m}_3 \Rightarrow \mathtt{m}_2 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6}{\begin{array}{c}\mathtt{val}\ \mathtt{m}_3\\ \vdots\end{array}}\downarrow\text{ev-if2}$$

- $$\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_3 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_3}{\Delta;\Gamma \vdash \mathtt{m}_3 : \mathtt{cert}}\downarrow\text{ty-if}$$
- $$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_3 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_3}{\Delta;\Gamma \vdash \mathtt{m}_1 : \mathtt{'t}_1}\downarrow\text{ty-if} \quad \dfrac{\texttt{if}\ (\mathtt{m}_3 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 \longrightarrow \texttt{if}\ (\mathtt{m}_3 \Rightarrow \mathtt{m}_2 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6}{\mathtt{m}_1 \longrightarrow \mathtt{m}_2}\ \text{ps}}{\Delta;\Gamma \vdash \mathtt{m}_2 : \mathtt{'t}_1}\downarrow\text{ev-if2}$$
- $$\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_3 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_3}{\Delta;\Gamma \vdash \mathtt{m}_4 : \mathtt{'t}_3}\downarrow\text{ty-if}$$
- $$\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_3 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_3}{\Delta, \mathtt{t}_1 \lhd \mathtt{t}_3;\Gamma \vdash \mathtt{m}_5 : \mathtt{t}_2}\downarrow\text{ty-if}$$
- $$\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_3 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_3}{\Delta;\Gamma \vdash \mathtt{m}_6 : \mathtt{t}_2}\downarrow\text{ty-if}$$
- $$\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_3 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_3}{\Delta \vdash \mathtt{t}_1 :: \mathtt{P}}\downarrow\text{ty-if}$$
- $$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_3 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_3}{\Delta \vdash \mathtt{t}_3 :: \mathtt{PJ}}\downarrow\text{ty-if}}{\Delta;\Gamma \vdash \texttt{if}\ (\mathtt{m}_3 \Rightarrow \mathtt{m}_2 \lhd \mathtt{m}_4)\ \mathtt{m}_5\ \mathtt{m}_6 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_3}\ \text{ty-if}$$ (ps-if2)

- $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_1}{\Delta;\Gamma\vdash \mathtt{m}_1 : {'}\mathtt{t}_1}\ \downarrow\text{ty-if}$
- $\dfrac{\mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4 \longrightarrow \mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4}{\mathtt{val}\ \mathtt{m}_1}\ \downarrow\text{ev-if3}$
- $\dfrac{\mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4 \longrightarrow \mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4}{\mathtt{val}\ \mathtt{m}_2}\ \downarrow\text{ev-if3}$

$\vdots$

- $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_1}{\Delta;\Gamma\vdash \mathtt{m}_2 : \mathtt{cert}}\ \downarrow\text{ty-if}$
- $\dfrac{\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_1}{\Delta;\Gamma\vdash \mathtt{m}_1 : {'}\mathtt{t}_1}\ \downarrow\text{ty-if} \quad \dfrac{\mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4 \longrightarrow \mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4}{\mathtt{m}_1 \longrightarrow \mathtt{m}_1}\ \downarrow\text{ev-if3}}{\Delta;\Gamma\vdash \mathtt{m}_1 : {'}\mathtt{t}_1}\ \text{ps}$
- $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_1}{\Delta;\Gamma\vdash \mathtt{m}_1 : {'}\mathtt{t}_1}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_1}{\Delta, \mathtt{t}_1 \lhd \mathtt{t}_1; \Gamma\vdash \mathtt{m}_3 : \mathtt{t}_2}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_1}{\Delta;\Gamma\vdash \mathtt{m}_4 : \mathtt{t}_2}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_1}{\Delta\vdash \mathtt{t}_1 :: \mathtt{P}}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_1}{\Delta\vdash \mathtt{t}_1 :: \mathtt{PJ}}\ \downarrow\text{ty-if}$

$$\overline{\Delta;\Gamma\vdash \mathtt{if}\ (\mathtt{m}_2 \Rightarrow \mathtt{m}_1 \lhd \mathtt{m}_1)\ \mathtt{m}_3\ \mathtt{m}_4 : \mathtt{t}_2\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_1}\ \text{ty-if} \qquad \text{(ps-if3)}$$

- - $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ ({'}\mathtt{t}_1 \Rightarrow {'}\mathtt{t}_2 \lhd {'}\mathtt{t}_3 \lhd {'}\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_5\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_2}{\Delta;\Gamma\vdash \mathtt{m}_2 : \mathtt{t}_5}\ \downarrow\text{ty-if}$
  - $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ ({'}\mathtt{t}_1 \Rightarrow {'}\mathtt{t}_2 \lhd {'}\mathtt{t}_3 \lhd {'}\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_5\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_2}{\Delta;\Gamma\vdash {'}\mathtt{t}_3 \lhd {'}\mathtt{t}_4 : {'}\mathtt{t}_2}\ \downarrow\text{ty-if}$
  - $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ ({'}\mathtt{t}_1 \Rightarrow {'}\mathtt{t}_2 \lhd {'}\mathtt{t}_3 \lhd {'}\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_5\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_2}{\Delta;\Gamma\vdash {'}\mathtt{t}_2 : {'}\mathtt{t}_1}\ \downarrow\text{ty-if}$
  - $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ ({'}\mathtt{t}_1 \Rightarrow {'}\mathtt{t}_2 \lhd {'}\mathtt{t}_3 \lhd {'}\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_5\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_2}{\Delta;\Gamma\vdash {'}\mathtt{t}_1 : \mathtt{cert}}\ \downarrow\text{ty-if}$
  - $\mathtt{if}\ ({'}\mathtt{t}_1 \Rightarrow {'}\mathtt{t}_2 \lhd {'}\mathtt{t}_3 \lhd {'}\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 \longrightarrow \mathtt{let}\ \mathtt{t}_1 \lhd \mathtt{t}_2\ \mathtt{in}\ \mathtt{m}_1$
  - $\dfrac{\mathtt{if}\ ({'}\mathtt{t}_1 \Rightarrow {'}\mathtt{t}_2 \lhd {'}\mathtt{t}_3 \lhd {'}\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 \longrightarrow \mathtt{let}\ \mathtt{t}_1 \lhd \mathtt{t}_2\ \mathtt{in}\ \mathtt{m}_1}{\vdash {'}\mathtt{t}_1 \lhd {'}\mathtt{t}_2 \Rightarrow {'}\mathtt{t}_3 \lhd {'}\mathtt{t}_4}\ \downarrow\text{ev-if4}$

  $\vdots$

- $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ ({'}\mathtt{t}_1 \Rightarrow {'}\mathtt{t}_2 \lhd {'}\mathtt{t}_3 \lhd {'}\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_5\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_2}{\Delta, \mathtt{t}_1 \lhd \mathtt{t}_2; \Gamma\vdash \mathtt{m}_1 : \mathtt{t}_5}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ ({'}\mathtt{t}_1 \Rightarrow {'}\mathtt{t}_2 \lhd {'}\mathtt{t}_3 \lhd {'}\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_5\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_2}{\Delta\vdash \mathtt{t}_1 :: \mathtt{P}}\ \downarrow\text{ty-if}$
- $\dfrac{\Delta;\Gamma\vdash \mathtt{if}\ ({'}\mathtt{t}_1 \Rightarrow {'}\mathtt{t}_2 \lhd {'}\mathtt{t}_3 \lhd {'}\mathtt{t}_4)\ \mathtt{m}_1\ \mathtt{m}_2 : \mathtt{t}_5\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_2}{\Delta\vdash \mathtt{t}_2 :: \mathtt{PJ}}\ \downarrow\text{ty-if}$

$$\overline{\Delta;\Gamma\vdash \mathtt{let}\ \mathtt{t}_1 \lhd \mathtt{t}_2\ \mathtt{in}\ \mathtt{m}_1 : \mathtt{t}_5\ \%\ \mathtt{t}_1 \lhd \mathtt{t}_2}\ \text{ty-let} \qquad \text{(ps-if4)}$$

- $$\frac{\Delta;\Gamma \vdash \texttt{if } (\texttt{'t}_4 \Rightarrow \texttt{'t}_5 \lhd \texttt{'t}_6 \lhd \texttt{'t}_7)\ \texttt{m}_2\ \texttt{m}_1 : \texttt{t}_1\ \texttt{\%}\ \texttt{t}_2 \lhd \texttt{t}_3}{\Delta \vdash \texttt{t}_3 :: \texttt{PJ}}\ \downarrow\text{ty-if}$$
- $$\frac{\Delta;\Gamma \vdash \texttt{if } (\texttt{'t}_4 \Rightarrow \texttt{'t}_5 \lhd \texttt{'t}_6 \lhd \texttt{'t}_7)\ \texttt{m}_2\ \texttt{m}_1 : \texttt{t}_1\ \texttt{\%}\ \texttt{t}_2 \lhd \texttt{t}_3}{\Delta \vdash \texttt{t}_2 :: \texttt{P}}\ \downarrow\text{ty-if}$$
- $$\frac{\Delta;\Gamma \vdash \texttt{if } (\texttt{'t}_4 \Rightarrow \texttt{'t}_5 \lhd \texttt{'t}_6 \lhd \texttt{'t}_7)\ \texttt{m}_2\ \texttt{m}_1 : \texttt{t}_1\ \texttt{\%}\ \texttt{t}_2 \lhd \texttt{t}_3}{\Delta, \texttt{t}_2 \lhd \texttt{t}_3;\Gamma \vdash \texttt{m}_2 : \texttt{t}_1}\ \downarrow\text{ty-if}$$
- $$\frac{\Delta;\Gamma \vdash \texttt{if } (\texttt{'t}_4 \Rightarrow \texttt{'t}_5 \lhd \texttt{'t}_6 \lhd \texttt{'t}_7)\ \texttt{m}_2\ \texttt{m}_1 : \texttt{t}_1\ \texttt{\%}\ \texttt{t}_2 \lhd \texttt{t}_3}{\Delta;\Gamma \vdash \texttt{'t}_6 \lhd \texttt{'t}_7 : \texttt{'t}_3}\ \downarrow\text{ty-if}$$
- $$\frac{\Delta;\Gamma \vdash \texttt{if } (\texttt{'t}_4 \Rightarrow \texttt{'t}_5 \lhd \texttt{'t}_6 \lhd \texttt{'t}_7)\ \texttt{m}_2\ \texttt{m}_1 : \texttt{t}_1\ \texttt{\%}\ \texttt{t}_2 \lhd \texttt{t}_3}{\Delta;\Gamma \vdash \texttt{'t}_5 : \texttt{'t}_2}\ \downarrow\text{ty-if}$$
- $$\frac{\Delta;\Gamma \vdash \texttt{if } (\texttt{'t}_4 \Rightarrow \texttt{'t}_5 \lhd \texttt{'t}_6 \lhd \texttt{'t}_7)\ \texttt{m}_2\ \texttt{m}_1 : \texttt{t}_1\ \texttt{\%}\ \texttt{t}_2 \lhd \texttt{t}_3}{\Delta;\Gamma \vdash \texttt{'t}_4 : \texttt{cert}}\ \downarrow\text{ty-if}$$
- $\texttt{if } (\texttt{'t}_4 \Rightarrow \texttt{'t}_5 \lhd \texttt{'t}_6 \lhd \texttt{'t}_7)\ \texttt{m}_2\ \texttt{m}_1 \longrightarrow \texttt{m}_1$
- $$\frac{\texttt{if } (\texttt{'t}_4 \Rightarrow \texttt{'t}_5 \lhd \texttt{'t}_6 \lhd \texttt{'t}_7)\ \texttt{m}_2\ \texttt{m}_1 \longrightarrow \texttt{m}_1}{\not\forall\ \texttt{'t}_4 \lhd \texttt{'t}_5 \Rightarrow\ \texttt{'t}_6 \lhd \texttt{'t}_7}\ \downarrow\text{ev-if5}$$

$$\vdots$$

$$\frac{\dfrac{\Delta;\Gamma \vdash \texttt{if } (\texttt{'t}_4 \Rightarrow \texttt{'t}_5 \lhd \texttt{'t}_6 \lhd \texttt{'t}_7)\ \texttt{m}_2\ \texttt{m}_1 : \texttt{t}_1\ \texttt{\%}\ \texttt{t}_2 \lhd \texttt{t}_3}{\Delta;\Gamma \vdash \texttt{m}_1 : \texttt{t}_1}\ \downarrow\text{ty-if} \quad \frac{}{\Delta \vdash \texttt{t}_1 \preceq \texttt{t}_1\ \texttt{\%}\ \texttt{t}_2 \lhd \texttt{t}_3}\ \text{st-auth2}}{\Delta;\Gamma \vdash \texttt{m}_1 : \texttt{t}_1\ \texttt{\%}\ \texttt{t}_2 \lhd \texttt{t}_3}\ \text{psst} \qquad \text{(ps-if5)}$$

D.7 Expression preservation

$$\boxed{\frac{\Delta;\Gamma \vdash \texttt{e}_1 : \texttt{t} \texttt{ ! } \epsilon_1 \quad \texttt{e}_1 \xrightarrow{\epsilon_2} \texttt{e}_2}{\Delta;\Gamma \vdash \texttt{e}_2 : \texttt{t} \texttt{ ! } \epsilon_1}} \qquad \boxed{\text{eps}}$$

$$\frac{\dfrac{\Delta;\Gamma \vdash \texttt{ret m}_1 : \texttt{t} \texttt{ ! } \top}{\Delta;\Gamma \vdash \texttt{m}_1 : \texttt{t}}\ \downarrow\text{ety-ret} \quad \dfrac{\texttt{ret m}_1 \xrightarrow{\top} \texttt{ret m}_2}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \text{ps}\ \downarrow\text{eev-ret}}{\dfrac{\Delta;\Gamma \vdash \texttt{m}_2 : \texttt{t}}{\Delta;\Gamma \vdash \texttt{ret m}_2 : \texttt{t} \texttt{ ! } \top}\ \text{ety-ret}} \qquad \text{(eps-ret)}$$

- $$\frac{\dfrac{\Delta;\Gamma \vdash \texttt{run x} = \texttt{m}_1 \texttt{ in e} : \texttt{t}_3 \texttt{ ! } \texttt{t}_2}{\Delta;\Gamma \vdash \texttt{m}_1 : \texttt{t}_1 \texttt{ ! } \texttt{t}_2}\ \downarrow\text{ety-run} \quad \dfrac{\texttt{run x} = \texttt{m}_1 \texttt{ in e} \xrightarrow{\top} \texttt{run x} = \texttt{m}_2 \texttt{ in e}}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\ \text{ps}\ \downarrow\text{eev-run1}}{\Delta;\Gamma \vdash \texttt{m}_2 : \texttt{t}_1 \texttt{ ! } \texttt{t}_2}$$
- $$\frac{\dfrac{\Delta;\Gamma \vdash \texttt{run x} = \texttt{m}_1 \texttt{ in e} : \texttt{t}_3 \texttt{ ! } \texttt{t}_2}{\Delta;\Gamma, \texttt{x}{:}\texttt{t}_1 \vdash \texttt{e} : \texttt{t}_3 \texttt{ ! } \texttt{t}_2}\ \downarrow\text{ety-run}}{\Delta;\Gamma \vdash \texttt{run x} = \texttt{m}_2 \texttt{ in e} : \texttt{t}_3 \texttt{ ! } \texttt{t}_2}\ \text{ety-run} \qquad \text{(eps-run1)}$$

$$\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{run x} = \texttt{ret m}_1 \texttt{ ! } \top \texttt{ in e} : \texttt{t}_2 \texttt{ ! } \top}{\Delta;\Gamma \vdash \texttt{ret m}_1 \texttt{ ! } \top : \texttt{t}_1 \texttt{ ! } \top}\downarrow\text{ety-run}}{\Delta;\Gamma \vdash \texttt{ret m}_1 : \texttt{t}_1 \texttt{ ! } \top}\downarrow\text{ty-eff}}{\Delta;\Gamma \vdash \texttt{m}_1 : \texttt{t}_1}\downarrow\text{ety-ret} \qquad \dfrac{\texttt{run x} = \texttt{ret m}_1 \texttt{ ! } \top \texttt{ in e} \xrightarrow{\top} \texttt{run x} = \texttt{ret m}_2 \texttt{ ! } \top \texttt{ in e}}{\texttt{m}_1 \longrightarrow \texttt{m}_2}\text{ ps}\downarrow\text{eev-run2}}{\dfrac{\Delta;\Gamma \vdash \texttt{m}_2 : \texttt{t}_1}{\Delta;\Gamma \vdash \texttt{ret m}_2 : \texttt{t}_1 \texttt{ ! } \top}\text{ ety-ret}}$$

- $$\dfrac{\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{run x} = \texttt{ret m}_1 \texttt{ ! } \top \texttt{ in e} : \texttt{t}_2 \texttt{ ! } \top}{\Delta;\Gamma \vdash \texttt{ret m}_1 \texttt{ ! } \top : \texttt{t}_1 \texttt{ ! } \top}\downarrow\text{ety-run}}{\Delta \vdash \top :: \texttt{L}}\downarrow\text{ty-eff}}{\Delta;\Gamma \vdash \texttt{ret m}_2 \texttt{ ! } \top : \texttt{t}_1 \texttt{ ! } \top}\text{ ty-eff}$$

- $$\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{run x} = \texttt{ret m}_1 \texttt{ ! } \top \texttt{ in e} : \texttt{t}_2 \texttt{ ! } \top}{\Delta;\Gamma, \texttt{x}:\texttt{t}_1 \vdash \texttt{e} : \texttt{t}_2 \texttt{ ! } \top}\downarrow\text{ety-run}}{\Delta;\Gamma \vdash \texttt{run x} = \texttt{ret m}_2 \texttt{ ! } \top \texttt{ in e} : \texttt{t}_2 \texttt{ ! } \top}\text{ ety-run}$$

(eps-run2)

$$\dfrac{\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{run x} = \texttt{ret m ! t}_3 \texttt{ in e}_1 : \texttt{t}_2 \texttt{ ! t}_3}{\Delta;\Gamma \vdash \texttt{ret m ! t}_3 : \texttt{t}_1 \texttt{ ! t}_3}\downarrow\text{ety-run}}{\Delta \vdash \texttt{t}_3 :: \texttt{L}}\downarrow\text{ty-eff} \qquad \dfrac{\texttt{run x} = \texttt{ret m ! t}_3 \texttt{ in e}_1 \xrightarrow{\texttt{t}_3} \texttt{e}_2}{\texttt{val m}}\downarrow\text{eev-run3}$$

$$\vdots$$

- $$\dfrac{\Delta;\Gamma \vdash \texttt{run x} = \texttt{ret m ! t}_3 \texttt{ in e}_1 : \texttt{t}_2 \texttt{ ! t}_3}{\Delta;\Gamma, \texttt{x}:\texttt{t}_1 \vdash \texttt{e}_1 : \texttt{t}_2 \texttt{ ! t}_3}\downarrow\text{ety-run}$$

- $$\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{run x} = \texttt{ret m ! t}_3 \texttt{ in e}_1 : \texttt{t}_2 \texttt{ ! t}_3}{\Delta;\Gamma \vdash \texttt{ret m ! t}_3 : \texttt{t}_1 \texttt{ ! t}_3}\downarrow\text{ety-run}}{\Delta;\Gamma \vdash \texttt{ret m} : \texttt{t}_1 \texttt{ ! t}_3}\downarrow\text{ty-eff}}{\Delta;\Gamma \vdash \texttt{ret m} : \texttt{t}_1 \texttt{ ! } \top}\text{ stinv}}{\Delta;\Gamma \vdash \texttt{m} : \texttt{t}_1}\downarrow\text{ety-ret}$$

- $$\dfrac{\dfrac{\texttt{run x} = \texttt{ret m ! t}_3 \texttt{ in e}_1 \xrightarrow{\texttt{t}_3} \texttt{e}_2}{\texttt{e}_1\{\texttt{m}/\texttt{x}\} = \texttt{e}_2}\downarrow\text{eev-run3}}{\Delta;\Gamma \vdash \texttt{e}_2 : \texttt{t}_2 \texttt{ ! t}_3}\text{ psemsub}$$

(eps-run3)

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\Delta;\Gamma \vdash \texttt{fix x:t!t. e}_1 : \texttt{t ! t}}{\Delta;\Gamma, \texttt{x:t!t} \vdash \texttt{e}_1 : \texttt{t ! t}}\downarrow\text{ety-fix}}{\Delta;\Gamma \vdash \texttt{fix x:t!t. e}_1 : \texttt{t ! t}}\downarrow\text{ety-fix}}{\Delta \vdash \texttt{t} \gg \dagger}\downarrow\text{ety-fix}}{\Delta;\Gamma \vdash \texttt{fix x:t!t. e}_1 : \texttt{t ! t}}\downarrow\text{ety-fix}}{\Delta;\Gamma \vdash \texttt{fix x:t!t. e}_1 : \texttt{t ! t}}\text{ ety-fix}$$

$$\dfrac{\dfrac{\texttt{fix x:t!t. e}_1 \xrightarrow{\top} \texttt{e}_2}{\texttt{e}_1\{\texttt{fix x:t!t. e}_1/\texttt{x}\} = \texttt{e}_2}\downarrow\text{eev-fix}}{\Delta;\Gamma \vdash \texttt{e}_2 : \texttt{t ! t}}\text{ pseesub}$$

(eps-fix)

E Noninterference

E.1 Logical equivalence for values

$$\texttt{<>} \sim_\zeta \texttt{<>} : \texttt{<>} \tag{R-Unit}$$

$$\frac{\mathtt{v}_1 \sim_\zeta \mathtt{v}_3 : \mathtt{t}_1 \quad \mathtt{v}_2 \sim_\zeta \mathtt{v}_4 : \mathtt{t}_2}{\texttt{<}\mathtt{v}_1, \mathtt{v}_2\texttt{>} \sim_\zeta \texttt{<}\mathtt{v}_2, \mathtt{v}_4\texttt{>} : \texttt{<}\mathtt{t}_1, \mathtt{t}_2\texttt{>}} \tag{R-Prod}$$

$$\frac{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}_1}{\texttt{inl}\ \mathtt{v}_1 \sim_\zeta \texttt{inl}\ \mathtt{v}_2 : \mathtt{t}_1 + \mathtt{t}_2} \tag{R-Inl}$$

$$\frac{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}_2}{\texttt{inr}\ \mathtt{v}_1 \sim_\zeta \texttt{inr}\ \mathtt{v}_2 : \mathtt{t}_1 + \mathtt{t}_2} \tag{R-Inr}$$

$$\frac{\forall(\mathtt{v}_3 \sim_\zeta \mathtt{v}_4 : \mathtt{t}_1).\ \mathtt{v}_1\ \mathtt{v}_3 \approx_\zeta \mathtt{v}_2\ \mathtt{v}_4 : \mathtt{t}_2}{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}_1 \to \mathtt{t}_2} \tag{R-Fun}$$

$$\frac{\ell \preceq \zeta \quad \mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}}{\mathtt{v}_1\{\ell\} \sim_\zeta \mathtt{v}_2\{\ell\} : \mathtt{t}\{\ell\}} \tag{R-Lab1}$$

$$\frac{\ell \not\preceq \zeta}{\mathtt{v}_1\{\ell\} \sim_\zeta \mathtt{v}_2\{\ell\} : \mathtt{t}\{\ell\}} \tag{R-Lab2}$$

$$\frac{\forall(\mathtt{t}_2 \preceq \mathtt{t}_1).\ \mathtt{v}_1\ [\mathtt{t}_2] \approx_\zeta \mathtt{v}_2\ [\mathtt{t}_2] : \mathtt{t}\{\mathtt{t}_2/\alpha\}}{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \forall\alpha \preceq \mathtt{t}_1.\ \mathtt{t}} \tag{R-All}$$

$$\frac{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}\{\mathtt{t}_1/\alpha\}}{\texttt{pack}\ (\mathtt{t}_1, \mathtt{v}_1)\ \texttt{as}\ \exists\alpha \preceq \mathtt{t}_2.\mathtt{t} \sim_\zeta \texttt{pack}\ (\mathtt{t}_1, \mathtt{v}_2)\ \texttt{as}\ \exists\alpha \preceq \mathtt{t}_2.\mathtt{t} : \exists\alpha \preceq \mathtt{t}_2.\mathtt{t}} \tag{R-Some}$$

$$\frac{\mathtt{e}_1 \approx_\zeta \mathtt{e}_2 : \mathtt{t}!\epsilon}{\mathtt{e}_1!\epsilon \sim_\zeta \mathtt{e}_2!\epsilon : \mathtt{t}!\epsilon} \tag{R-Eff}$$

$$\frac{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}}{\texttt{lift}\ \mathtt{v}_1 \sim_\zeta \texttt{lift}\ \mathtt{v}_2 : \mathtt{t}^\dagger} \tag{R-Lift}$$

$$\frac{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}}{\texttt{let}\ \mathtt{p}_1 \preceq \mathtt{p}_2\ \texttt{in}\ \mathtt{v}_1 \sim_\zeta \texttt{let}\ \mathtt{p}_1 \preceq \mathtt{p}_2\ \texttt{in}\ \mathtt{v}_2 : \mathtt{t}\ \%\ \mathtt{p}_1 \preceq \mathtt{p}_2} \tag{R-Auth}$$

$$\texttt{'p} \sim_\zeta \texttt{'p} : \texttt{'p} \tag{R-Sin}$$

$$\texttt{'p}_1 \lhd \texttt{'p}_2 \sim_\zeta \texttt{'p}_1 \lhd \texttt{'p}_2 : \texttt{'p}_1 \lhd \texttt{'p}_2 \tag{R-Cert}$$

$$\frac{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}}{\texttt{return}\ \mathtt{v}_1 \sim_\zeta \texttt{return}\ \mathtt{v}_2 : \mathtt{t}!\epsilon} \tag{R-Ret}$$

E.2 Logical equivalence for terms and expressions

$$\frac{\mathtt{m}_1 \longrightarrow^* \mathtt{v}_1 \quad \mathtt{m}_2 \longrightarrow^* \mathtt{v}_2 \quad \mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}}{\mathtt{m}_1 \approx_\zeta \mathtt{m}_2 : \mathtt{t}} \quad \text{(R-Term)}$$

$$\frac{\mathtt{e}_1 \stackrel{\zeta}{\Longrightarrow}^{\mathtt{n}} \mathtt{u}_1 \quad \mathtt{e}_2 \stackrel{\zeta}{\Longrightarrow}^{\mathtt{n}} \mathtt{u}_2 \quad \mathtt{u}_1 \sim_\zeta \mathtt{u}_2 : \mathtt{t}!\epsilon}{\mathtt{e}_1 \approx_\zeta \mathtt{e}_2 : \mathtt{t}!\epsilon} \quad \text{(R-Exp)}$$

$$\frac{\mathtt{m}_1 \longrightarrow^\omega \quad \mathtt{m}_2 \longrightarrow^\omega}{\mathtt{m}_1 \approx_\zeta \mathtt{m}_2 : \mathtt{t}} \quad \text{(R-Strong1)}$$

$$\frac{\mathtt{m}_1 \longrightarrow^\omega}{\mathtt{m}_1 \approx_\zeta \mathtt{m}_2 : \mathtt{t}} \quad \text{(R-Weak1)}$$

$$\frac{\mathtt{m}_2 \longrightarrow^\omega}{\mathtt{m}_1 \approx_\zeta \mathtt{m}_2 : \mathtt{t}} \quad \text{(R-Weak2)}$$

$$\frac{\mathtt{e}_1 \stackrel{\not\preceq\zeta}{\longrightarrow}^\omega \quad \mathtt{e}_2 \stackrel{\not\preceq\zeta}{\longrightarrow}^\omega}{\mathtt{e}_1 \approx_\zeta \mathtt{e}_2 : \mathtt{t}!\epsilon} \quad \text{(R-Strong2)}$$

$$\frac{\mathtt{e}_1 \stackrel{\not\preceq\zeta}{\longrightarrow}^\omega}{\mathtt{e}_1 \approx_\zeta \mathtt{e}_2 : \mathtt{t}!\epsilon} \quad \text{(R-Weak3)}$$

$$\frac{\mathtt{e}_2 \stackrel{\not\preceq\zeta}{\longrightarrow}^\omega}{\mathtt{e}_1 \approx_\zeta \mathtt{e}_2 : \mathtt{t}!\epsilon} \quad \text{(R-Weak4)}$$

E.3 Standard noninterference

Theorem 14 (Noninterference).

1. *If* $\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t}$ *and* $\delta \models \Delta$ *and* $\gamma_1 \sim_\zeta \gamma_2 : \delta(\Gamma)$*, then* $\delta\gamma_1(\mathtt{m}) \approx_\zeta \delta\gamma_2(\mathtt{m}) : \delta(\mathtt{t})$.
2. *If* $\Delta;\ \Gamma \vdash \mathtt{e} : \mathtt{t}!\epsilon$ *and* $\delta \models \Delta$ *and* $\gamma_1 \sim_\zeta \gamma_2 : \delta(\Gamma)$*, then* $\delta\gamma_1(\mathtt{e}) \approx_\zeta \delta\gamma_2(\mathtt{e}) : \delta(\mathtt{t})!\delta(\epsilon)$.

Proof. The idea is to strengthen the coinductive hypothesis by defining another equivalence $\dot{\approx}_\zeta$ that satisfies the same set of rules defined above for $\approx_\zeta$ but also relates diverging terms and is closed under related substitutions of closed values. Since $\approx_\zeta$ is the largest relation satisfying these equivalence rules by definition, and $\dot{\approx}_\zeta \supseteq \approx_\zeta$ by construction, it follows that $\dot{\approx}_\zeta = \approx_\zeta$. This proof is similar to bisimulation proofs in process calculi but our language here is deterministic.

Let $\mathtt{m} \dot{\approx}_\zeta \mathtt{m} : \mathtt{t}$ be the largest relation satisfying the following rules:

$$\frac{\mathtt{m}_1 \approx_\zeta \mathtt{m}_2 : \mathtt{t}}{\mathtt{m}_1 \dot{\approx}_\zeta \mathtt{m}_2 : \mathtt{t}} \quad \text{(RR-Term1)}$$

$$\frac{\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t} \quad \delta \models \Delta \quad \gamma_1 \dot{\approx}_\zeta \gamma_2 : \delta(\Gamma)}{\delta\gamma_1(\mathtt{m}) \dot{\approx}_\zeta \delta\gamma_2(\mathtt{m}) : \delta(\mathtt{t})} \quad \text{(RR-Term2)}$$

Similarly, let $\mathtt{e} \dot{\approx}_\zeta \mathtt{e} : \mathtt{t}$ be the largest relation satisfying the following rules:

$$\frac{\mathtt{e}_1 \approx_\zeta \mathtt{e}_2 : \mathtt{t}!\epsilon}{\mathtt{e}_1 \dot{\approx}_\zeta \mathtt{e}_2 : \mathtt{t}} \quad \text{(RR-Exp1)}$$

$$\frac{\Delta;\ \Gamma \vdash \mathtt{e} : \mathtt{t}!\epsilon \quad \delta \models \Delta \quad \gamma_1 \dot{\approx}_\zeta \gamma_2 : \delta(\Gamma)}{\delta\gamma_1(\mathtt{e}) \dot{\approx}_\zeta \delta\gamma_2(\mathtt{e}) : \delta(\mathtt{t})!\delta(\epsilon)} \quad \text{(RR-Exp2)}$$

Also, extend term substitutions γ to allow substitutions with terms and expressions, rather than just values:

$$\gamma \quad ::= \quad \cdot \mid \gamma, \mathtt{x} \mapsto \mathtt{m} \mid \gamma, \mathtt{x} \mapsto \mathtt{e}$$

Then, let $\gamma \mathrel{\dot{\approx}}_\zeta \gamma : \Gamma$ be the largest relation satisfying the following rules:

$$\frac{\gamma_1 \sim_\zeta \gamma_2 : \Gamma}{\gamma_1 \mathrel{\dot{\approx}}_\zeta \gamma_2 : \Gamma} \qquad \text{(RR-Sub1)}$$

$$\frac{\gamma_1 \mathrel{\dot{\approx}}_\zeta \gamma_2 : \delta(\Gamma)}{\gamma_1, \mathtt{x} \mapsto \delta\gamma_1(\mathtt{fix}\ \lambda\mathtt{x{:}t.m}) \mathrel{\dot{\approx}}_\zeta \gamma_2, \mathtt{x} \mapsto \delta\gamma_2(\mathtt{fix}\ \lambda\mathtt{x{:}t.m}) : \delta(\Gamma, \mathtt{x{:}t})} \qquad \text{(RR-Sub2)}$$

$$\frac{\gamma_1 \mathrel{\dot{\approx}}_\zeta \gamma_2 : \delta(\Gamma)}{\gamma_1, \mathtt{x} \mapsto \delta\gamma_1(\mathtt{fix\ x{:}t!}\epsilon\mathtt{.e}) \mathrel{\dot{\approx}}_\zeta \gamma_2, \mathtt{x} \mapsto \delta\gamma_2(\mathtt{fix\ x{:}t!}\epsilon\mathtt{.e}) : \delta(\Gamma, \mathtt{x{:}t!}\epsilon)} \qquad \text{(RR-Sub3)}$$

We claim without proving that the equivalence rules above (R-Weak* and R-Strong*) for terms and expressions are the same as the following rules:

$$\frac{\mathtt{m}_1 \longrightarrow^+ \mathtt{m}_3 \quad \mathtt{m}_2 \longrightarrow^+ \mathtt{m}_4 \quad \mathtt{m}_3 \approx_\zeta \mathtt{m}_4 : \mathtt{t}}{\mathtt{m}_1 \approx_\zeta \mathtt{m}_2 : \mathtt{t}} \qquad \text{(RR-Strong1)}$$

$$\frac{\mathtt{e}_1 \overset{\zeta}{\Longrightarrow} \mathtt{e}_3 \quad \mathtt{e}_2 \overset{\zeta}{\Longrightarrow} \mathtt{e}_4 \quad \mathtt{e}_3 \approx_\zeta \mathtt{e}_4 : \mathtt{t}}{\mathtt{e}_1 \approx_\zeta \mathtt{e}_2 : \mathtt{t}} \qquad \text{(RR-Strong2)}$$

$$\frac{\mathtt{m}_1 \longrightarrow \mathtt{m}_3 \quad \mathtt{m}_2 \longrightarrow^* \mathtt{m}_4 \quad \mathtt{m}_3 \approx_\zeta \mathtt{m}_4 : \mathtt{t}}{\mathtt{m}_1 \approx_\zeta \mathtt{m}_2 : \mathtt{t}} \qquad \text{(RR-Weak1)}$$

$$\frac{\mathtt{m}_1 \longrightarrow^* \mathtt{m}_3 \quad \mathtt{m}_2 \longrightarrow \mathtt{m}_4 \quad \mathtt{m}_3 \approx_\zeta \mathtt{m}_4 : \mathtt{t}}{\mathtt{m}_1 \approx_\zeta \mathtt{m}_2 : \mathtt{t}} \qquad \text{(RR-Weak2)}$$

$$\frac{\mathtt{v}_1 \sim_\zeta \mathtt{v}_2 : \mathtt{t}}{\mathtt{v}_1 \approx_\zeta \mathtt{v}_2 : \mathtt{t}} \qquad \text{(RR-Values1)}$$

$$\frac{\mathtt{u}_1 \sim_\zeta \mathtt{u}_2 : \mathtt{t}}{\mathtt{u}_1 \approx_\zeta \mathtt{u}_2 : \mathtt{t}} \qquad \text{(RR-Values2)}$$

Now, after setting up all these auxiliary definitions, we are ready to prove that $\mathrel{\dot{\approx}}_\zeta$ also satisfies the RR-* rules above. If the two terms are related by RR-Term1 or two expressions are related by RR-Exp1, then the case is trivial.

Assume that we are in the case of RR-Term2 or RR-Exp2. By inversion of RR-Term2, we have $\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t}$ and $\delta \models \Delta$ and $\gamma_1 \mathrel{\dot{\approx}}_\zeta \gamma_2 : \delta(\Gamma)$. By inversion of RR-Exp2, we have $\Delta;\ \Gamma \vdash \mathtt{e} : \mathtt{t!}\epsilon$ and $\delta \models \Delta$ and $\gamma_1 \mathrel{\dot{\approx}}_\zeta \gamma_2 : \delta(\Gamma)$. We proceed to complete the proof by mutual induction on $\Gamma \vdash \mathtt{e} : \mathtt{t}$ and $\Gamma \vdash \mathtt{m} : \mathtt{t}$.

We omit the cases for unit, sums and products, which are straight-forwarded. The proof here is for strong noninterference (no P-Weak), but can readily be generalized to handle weak noninterference. The cases for T-Bind, T-Ret and T-Run without fixpoints are shown in the main text of this paper; the proof for those cases with RR-* rules can be adapted by case analysis on their evaluations. The cases for T-Let, T-Pass and T-If are handled only in the condition version of noninterference (see next subsection).

- T-Var: if $\gamma_1 \mathrel{\dot{\approx}}_\zeta \gamma_2 : \Gamma$ by RR-Sub1, then $\gamma_1(\mathtt{x}) \sim_\zeta \gamma_2(\mathtt{x}) : \mathtt{t}$ by the definition of $\gamma \sim_\zeta \gamma : \Gamma$. Assume that we are in the case of RR-Sub2 and $\gamma_1(\mathtt{x}) = \delta\gamma_1(\mathtt{fix}\ \lambda\mathtt{x} : \mathtt{t.m})$ and $\gamma_2(\mathtt{x}) = \delta\gamma_2(\mathtt{fix}\ \lambda\mathtt{x} : \mathtt{t.m})$. Because $\gamma(\mathtt{x}) = \delta\gamma_1(\mathtt{fix}\ \lambda\mathtt{x{:}t.m})$ and thus $(\gamma_1, \mathtt{x} \mapsto \delta\gamma_1(\mathtt{fix}\ \lambda\mathtt{x{:}t.\ m})) = \gamma_1$, we have

$$\begin{array}{rl} & \delta\gamma_1(\mathtt{fix}\ \lambda\mathtt{x{:}t.m}) \\ = & \mathtt{fix}\ \lambda\mathtt{x{:}t.}\ \delta\gamma_1\ (\mathtt{m}) \\ \longrightarrow & \delta\gamma_1(\mathtt{m})\{\mathtt{fix}\ \lambda\mathtt{x{:}t.}\ \delta\gamma_1(\mathtt{m})/\mathtt{x}\} \\ = & \delta\gamma_1(\mathtt{m})\{\delta\gamma_1(\mathtt{fix}\ \lambda\mathtt{x{:}t.\ m})/\mathtt{x}\} \\ = & \delta(\gamma_1, \mathtt{x} \mapsto \delta\gamma_1(\mathtt{fix}\ \lambda\mathtt{x{:}t.\ m}))(\mathtt{m}) \\ = & \delta\gamma_1(\mathtt{m}) \end{array}$$

Similarly, $\delta\gamma_2(\texttt{fix}\ \lambda\texttt{x:t.m}) = \delta\gamma_2(\texttt{m})$. Hence, by RR-Strong1 and RR-Term2, we conclude that $\delta\gamma_1(\texttt{x}) \mathrel{\dot{\approx}_\zeta} \delta\gamma_2(\texttt{x}) : \delta(\texttt{t})$. The case for expressions with RR-Sub3 and RR-Strong2 is similar.

- T-Fix: By inversion, we have $\Delta; \Gamma \vdash \texttt{m} : \texttt{t} \to \texttt{t}$. By progress theorem, either $\delta\gamma_1(\texttt{m})$ takes a step ($\delta\gamma_1(\texttt{m}) \longrightarrow \texttt{m}_1$), or $\delta\gamma_1(\texttt{m})$ is a value ($\delta\gamma_1(\texttt{m}) = \texttt{v}_1$), which has the canonical form $\delta\gamma_1(\texttt{m}) = \lambda\texttt{x}:\texttt{t}.\ \texttt{m}_1$. Again, by progress theorem, either $\delta\gamma_2(\texttt{m})$ takes a step ($\delta\gamma_2(\texttt{m}) \longrightarrow \texttt{m}_2$) or $\delta\gamma_2(\texttt{m})$ is a value ($\delta\gamma_2(\texttt{m}) = \texttt{v}$), which has the canonical form $\delta\gamma_1(\texttt{m}) = \lambda\texttt{x:t}.\ \texttt{m}_2$.

  By RR-Term2, we have $\delta\gamma_1(\texttt{m}) \mathrel{\dot{\approx}_\zeta} \delta\gamma_2(\texttt{m}) : \delta(\texttt{t} \to \texttt{t})$. If $\delta\gamma_1(\texttt{fix m})$ and $\delta\gamma_2(\texttt{fix m})$ take steps, we have $\delta\gamma_1(\texttt{fix m}) \mathrel{\dot{\approx}_\zeta} \delta\gamma_1(\texttt{fix m}) : \delta(\texttt{t})$ by RR-Strong1. Otherwise,

$$\delta\gamma_1(\texttt{fix}\ (\lambda\texttt{x:t.}\ \texttt{m})) \longrightarrow \delta\gamma_1(\texttt{m})\{\delta\gamma_1(\texttt{fix}\ (\lambda\texttt{x:t.}\ \texttt{m}))/\texttt{x}\} = \delta\gamma_1(\texttt{m})$$

  in which case the reasoning is similar to the case for T-Var. Hence, by RR-Strong1 and RR-Term2, we conclude that $\delta\gamma_1(\texttt{fix m}) \mathrel{\dot{\approx}_\zeta} \gamma_2(\texttt{fix m}) : \delta(\texttt{t})$. The case for expressions with RR-Strong2 is similar.

- T-Poly: By inversion, we have $\Delta, \alpha \preceq \texttt{t}_1; \Gamma \vdash \texttt{m} : \texttt{t}_2$. Assume $\texttt{t} \preceq \texttt{t}_1$ and then extend $\delta_0 = \delta, \alpha \mapsto \texttt{t}$ such that $\delta_0 \models \Delta, \alpha \preceq \texttt{t}_1$. Since $\gamma_1 \mathrel{\dot{\approx}_\zeta} \gamma_2 : \delta(\Gamma)$ and $\alpha \notin \texttt{ftv}(\Gamma)$, we have $\gamma_1 \mathrel{\dot{\approx}_\zeta} \gamma_2 : \delta_0(\Gamma)$. By RR-Term2, we have $\delta_0\gamma_1(\texttt{m}) \mathrel{\dot{\approx}_\zeta} \delta_0\gamma_2(\texttt{m}) : \delta_0(\texttt{t}_2)$. Note that $\delta_0(\texttt{t}_2) = (\delta, \alpha \mapsto \texttt{t})(\texttt{t}_2) = \delta(\texttt{t}_2\{\texttt{t}/\alpha\})$. By R-All, we have $\delta\gamma_1(\Lambda\alpha \preceq \texttt{t}_1.\ \texttt{m}) \mathrel{\dot{\approx}_\zeta} \delta\gamma_2(\Lambda\alpha \preceq \texttt{t}_1.\ \texttt{m}) : \delta(\forall\alpha \preceq \texttt{t}_1.\ \texttt{m})$.

- T-Inst: By inversion, we have $\Delta; \Gamma \vdash \texttt{m} : \forall\alpha \preceq \texttt{t}_1.\texttt{t}_2$ and $\Delta \vdash \texttt{t}_3 \preceq \texttt{t}_1$. By RR-Term2, $\delta\gamma_1(\texttt{m}) \mathrel{\dot{\approx}_\zeta} \delta\gamma_2(\texttt{m}) : \delta(\forall\alpha \preceq \texttt{t}_1.\texttt{t}_2)$. If both $\delta\gamma_1(\texttt{m})$ and $\delta\gamma_2(\texttt{m})$ take steps, they are still related by RR-Strong1. Assume both terms are values: $\delta\gamma_1(\texttt{m}) = \texttt{v}_1$ and $\delta\gamma_2(\texttt{m}) = \texttt{v}_2$. By inversion of R-All, for all $\delta(\texttt{t}_3) \preceq \delta(\texttt{t}_1)$, we have $\texttt{v}_1\ [\delta(\texttt{t}_3)] \mathrel{\dot{\approx}_\zeta} \texttt{v}_2\ [\delta(\texttt{t}_3)] : \delta(\texttt{t}_2\{\texttt{t}_3/\alpha\})$. Hence, by RR-Strong1, we conclude that $\delta\gamma_1(\texttt{m}\ [\texttt{t}_3]) \mathrel{\dot{\approx}_\zeta} \delta\gamma_2(\texttt{m}\ [\texttt{t}_3]) : \delta(\texttt{t}_2\{\texttt{t}_3/\alpha\})$.

- T-Pack: By inversion, we have $\Delta; \Gamma \vdash \texttt{m} : \texttt{t}_3$. The case when $\texttt{m}$ takes a step is similar to that for T-Fix. Assume $\texttt{m}$ is a value. By RR-Term2, we have $\delta\gamma_1(\texttt{m}) \mathrel{\dot{\approx}_\zeta} \delta\gamma_2(\texttt{m}) : \delta(\texttt{t}_3)$. By R-Some, we have $\delta\gamma_1(\texttt{pack (t,m) as}\ \exists\alpha \preceq \texttt{t}_1.\texttt{t}_2) \mathrel{\dot{\approx}_\zeta} \delta\gamma_2(\texttt{pack (t,m) as}\ \exists\alpha \preceq \texttt{t}_1.\texttt{t}_2) : \delta(\exists\alpha \preceq \texttt{t}_1.\texttt{t}_2)$.

- T-Open: By inversion, we have $\Delta; \Gamma \vdash \texttt{m}_1 : \exists\alpha \preceq \texttt{t}_1.\texttt{t}_2$ and $\Delta, \alpha \preceq \texttt{t}_1; \Gamma, \texttt{x:t}_2 \vdash \texttt{m}_2 : \texttt{t}$. By RR-Term2, $\delta\gamma_1(\texttt{m}_1) \mathrel{\dot{\approx}_\zeta} \delta\gamma_2(\texttt{m}_1) : \delta(\exists\alpha \preceq \texttt{t}_1.\texttt{t}_2)$. If both $\delta\gamma_1(\texttt{m})$ and $\delta\gamma_2(\texttt{m})$ take steps, they are still related by RR-Strong1. Assume both terms are values: $\delta\gamma_1(\texttt{m}_1) = \texttt{pack}\ (\texttt{t}, \texttt{v}_1)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_1.\texttt{t}_2$ and $\delta\gamma_2(\texttt{m}_1) = \texttt{pack}\ (\texttt{t}, \texttt{v}_2)\ \texttt{as}\ \exists\alpha \preceq \texttt{t}_1.\texttt{t}_2$, where $\delta(\texttt{t}) \preceq \delta(\texttt{t}_1)$. By inversion of R-Some, we have $\texttt{v}_1 \mathrel{\dot{\sim}_\zeta} \texttt{v}_2 : \delta(\texttt{t}_2\{\texttt{t}/\alpha\})$.

  Extend $\delta_0 = \delta, \alpha \mapsto \texttt{t}$ such that $\delta_0 \models \Delta, \alpha \preceq \texttt{t}_1$. Also, extend $\gamma_3 = \gamma_1, \texttt{x} \mapsto \texttt{v}_1$ and $\gamma_4 = \gamma_2, \texttt{x} \mapsto \texttt{v}_2$ such that $\gamma_3 \mathrel{\dot{\approx}_\zeta} \gamma_4 : \delta(\Gamma), \texttt{x} : \delta(\texttt{t}_2\{\texttt{t}/\alpha\})$. Since $\alpha \notin \texttt{ftv}(\Gamma)$, we have $\gamma_3 \mathrel{\dot{\approx}_\zeta} \gamma_4 : \delta_0(\Gamma, \texttt{x:t}_2)$. By RR-Term2, $\delta_0\gamma_3(\texttt{m}_2) \mathrel{\dot{\approx}_\zeta} \delta_0\gamma_4(\texttt{m}_2) : \delta_0(\texttt{t})$. Since $\alpha \notin \texttt{ftv}(\Gamma)$, we have $\delta_0(\texttt{t}) = \delta(\texttt{t})$. Hence, by RR-Strong1, we conclude that $\delta\gamma_1(\texttt{open}\ (\alpha, \texttt{x}) = \texttt{m}_1\ \texttt{in}\ \texttt{m}_2) \mathrel{\dot{\approx}_\zeta} \delta\gamma_1(\texttt{open}\ (\alpha, \texttt{x}) = \texttt{m}_1\ \texttt{in}\ \texttt{m}_2) : \delta(\texttt{t})$.

- T-Eff: by mutual induction hypothesis (RR-Exp2).

- T-Fix: similar to T-Lab.

- T-Lift: similar to T-Lab.

- T-Seq: similar to T-Bind.

- T-Sin: by R-Sin.

- T-Cert: by R-Cert.

□

E.4 Authorities for proper types

$$\texttt{<>} \Rightarrow . \qquad \text{(M-Unit)}$$

$$\frac{\texttt{t}_1 \Rightarrow \Delta_1 \quad \texttt{t}_2 \Rightarrow \Delta_2}{\texttt{<t}_1\texttt{,t}_2\texttt{>} \Rightarrow \Delta_1, \Delta_2} \qquad \text{(M-Prod)}$$

$$\frac{\texttt{t}_1 \Rightarrow \Delta_1 \quad \texttt{t}_2 \Rightarrow \Delta_2}{\texttt{t}_1 + \texttt{t}_2 \Rightarrow \Delta_1, \Delta_2} \qquad \text{(M-Sum)}$$

$$\frac{\texttt{t}_2 \Rightarrow \texttt{t} \mathbin{\%} \Delta}{\texttt{t}_1 \to \texttt{t}_2 \Rightarrow \texttt{(t}_1 \to \texttt{t)} \mathbin{\%} \Delta} \qquad \text{(M-Fun)}$$

$$\top \Rightarrow . \qquad \text{(M-Top)}$$

$$\bot \Rightarrow . \qquad \text{(M-Bot)}$$

$$\alpha \Rightarrow . \qquad \text{(M-Var)}$$

$$\frac{\texttt{t}_2 \Rightarrow \texttt{t} \mathbin{\%} \Delta}{\forall \alpha \preceq \texttt{t}_1.\texttt{t}_2 \Rightarrow \texttt{(}\forall \alpha \preceq \texttt{t}_1.\texttt{t)} \mathbin{\%} \Delta} \qquad \text{(M-All)}$$

$$\frac{\texttt{t}_2 \Rightarrow \texttt{t} \mathbin{\%} \Delta}{\exists \alpha \preceq \texttt{t}_1.\texttt{t}_2 \Rightarrow \texttt{(}\exists \alpha \preceq \texttt{t}_1.\texttt{t)} \mathbin{\%} \Delta} \qquad \text{(M-Some)}$$

$$\frac{\texttt{t} \Rightarrow \Delta}{\texttt{t}\{\ell\} \Rightarrow \Delta} \qquad \text{(M-Lab)}$$

$$\frac{\texttt{t} \Rightarrow \Delta}{\texttt{t!}\epsilon \Rightarrow \Delta} \qquad \text{(M-Eff)}$$

$$\frac{\texttt{t} \Rightarrow \Delta}{\texttt{t}^\dagger \Rightarrow \Delta} \qquad \text{(M-Pot)}$$

$$\frac{\texttt{t} \Rightarrow \texttt{t}_0 \mathbin{\%} \Delta}{\texttt{t} \mathbin{\%} \texttt{p}_1 \lhd \texttt{p}_2 \Rightarrow \Delta, \texttt{p}_1 \lhd \texttt{p}_2} \qquad \text{(M-Auth)}$$

$$\texttt{'p} \Rightarrow . \qquad \text{(M-Sin)}$$

$$\texttt{cert} \Rightarrow . \qquad \text{(M-Cert)}$$

E.5 Conditioned noninterference

Theorem 15 (Conditioned and certified noninterference).

1. *Suppose* $\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t}$*, where* $\Delta = \Delta_\alpha, \Delta_\triangleleft$ *and* $\mathtt{t} \Rightarrow \mathtt{t}_0 \ \%\ \Delta_0$*, and* $\delta \models \Delta_\alpha$ *and* $\gamma_1 \sim_\zeta \gamma_2 : \delta(\Gamma)$*. If* $\Delta_0 \not\vdash \mathtt{p} \preceq \zeta$ *for all* $\mathtt{p} \in \mathtt{dom}(\Delta_\alpha)$ *that satisfy* $\Delta \not\vdash \mathtt{p} \preceq \zeta$*, then* $\delta\gamma_1(\mathtt{m}) \approx_\zeta \delta\gamma_2(\mathtt{m}) : \delta(\mathtt{t})$*.*

2. *Suppose* $\Delta;\ \Gamma \vdash \mathtt{e} : \mathtt{t}!\epsilon$*, where* $\Delta = \Delta_\alpha, \Delta_\triangleleft$ *and* $\mathtt{t} \Rightarrow \mathtt{t}_0 \ \%\ \Delta_0$*, and* $\delta \models \Delta_\alpha$ *and* $\gamma_1 \sim_\zeta \gamma_2 : \delta(\Gamma)$*. If* $\Delta_0 \not\vdash \mathtt{p} \preceq \zeta$ *for all* $\mathtt{p} \in \mathtt{dom}(\Delta_\alpha)$ *that satisfy* $\Delta \not\vdash \mathtt{p} \preceq \zeta$*, then* $\delta\gamma_1(\mathtt{e}) \approx_\zeta \delta\gamma_2(\mathtt{e}) : \delta(\mathtt{t})!\delta(\epsilon)$*.*

3. *Suppose* $\Delta;\ \Gamma \vdash \mathtt{m} : \mathtt{t}$*, where* $\Delta = \Delta_\alpha, \Delta_\triangleleft$ *and* $\mathtt{t} \Rightarrow \mathtt{t}_0 \ \%\ \Delta_0$*, and* $\delta \models \Delta_\alpha$ *and* $\gamma_1 \sim_\zeta \gamma_2 : \delta(\Gamma)$*. If* $\delta\gamma_1(\mathtt{m}) \not\approx_\zeta \delta\gamma_2(\mathtt{m}) : \delta(\mathtt{t})$*, then* $\mathtt{t} = \mathtt{t}_0 \ \%\ \Delta_0$ *and* $\Delta_0 \vdash \mathtt{p} \preceq \zeta$ *for some* $\mathtt{p}$ *that satisfies* $\Delta \not\vdash \mathtt{p} \preceq \zeta$

4. *Suppose* $\Delta;\ \Gamma \vdash \mathtt{e} : \mathtt{t}!\epsilon$*, where* $\Delta = \Delta_\alpha, \Delta_\triangleleft$ *and* $\mathtt{t} \Rightarrow \mathtt{t}_0 \ \%\ \Delta_0$*, and* $\delta \models \Delta_\alpha$ *and* $\gamma_1 \sim_\zeta \gamma_2 : \delta(\Gamma)$*. If* $\delta\gamma_1(\mathtt{e}) \not\approx_\zeta \delta\gamma_2(\mathtt{e}) : \delta(\mathtt{t})!\delta(\epsilon)$*, then* $\mathtt{t} = \mathtt{t}_0 \ \%\ \Delta_0$ *and* $\Delta_0 \vdash \mathtt{p} \preceq \zeta$ *for some* $\mathtt{p}$ *that satisfies* $\Delta \not\vdash \mathtt{p} \preceq \zeta$

Proof. The last two statements are the converse of the first two statements. As shown in the proof for the case T-Fun in Section 3.2, this conditioned version is only a slight generalization of the standard noninterference theorem and the proof goes through almost as before, except for T-Let.

Case T-Let: given the typing $\Delta;\ \Gamma \vdash \mathtt{let}\ \mathtt{p}_1 \triangleleft \mathtt{p}_2\ \mathtt{in}\ \mathtt{m} : \mathtt{t} \ \%\ \mathtt{p}_1 \triangleleft \mathtt{p}_2$, where $\Delta, \mathtt{p}_1 \preceq \mathtt{p}_2$; $\Gamma \vdash \mathtt{m} : \mathtt{t}$. By inversion of M-Auth, $\mathtt{t} \Rightarrow \Delta_0$ and $\mathtt{t} \ \%\ \mathtt{p}_1 \triangleleft \mathtt{p}_2 \Rightarrow \Delta_0, \mathtt{p}_1 \triangleleft \mathtt{p}_2$. Assume $\mathtt{p} \in \mathtt{dom}(\Delta_\alpha)$ and $\Delta \not\vdash \mathtt{p} \preceq \zeta$ such that $\Delta_0 \not\vdash \mathtt{p} \preceq \zeta$. By the induction hypothesis, $\delta\gamma_1(\mathtt{m}) \approx_\zeta \delta\gamma_2(\mathtt{m}) : \delta(\mathtt{t})$. Assume further that $\Delta_0, \mathtt{p}_1 \preceq \mathtt{p}_2 \vdash \mathtt{p} \preceq \zeta$. Then, by R-Auth, we can conclude that $\delta\gamma_1(\mathtt{let}\ \mathtt{p}_1 \triangleleft \mathtt{p}_2\ \mathtt{in}\ \mathtt{m}) \approx_\zeta \delta\gamma_2(\mathtt{let}\ \mathtt{p}_1 \triangleleft \mathtt{p}_2\ \mathtt{in}\ \mathtt{m}) : \delta(\mathtt{t} \ \%\ \mathtt{p}_1 \triangleleft \mathtt{p}_2)$. □

Index