Type Systems for Information Flow Control: The Question of Granularity*

Vineet Rajani Iulia Bastys Willard Rafnsson Deepak Garg

{vrajani, iulia_mb, willardr, dg}@mpi-sws.org

Max Planck Institute for Software Systems

Abstract

Information flow control is central to computer security. The objective of information flow control is to prevent unauthorized flows of secret information to the public outputs of a computation. This task is often accomplished using type systems that rely on modal operators to label and track information and, hence, this style of enforcing information flow control is deeply ingrained in logic. One key choice in designing a type system for information flow control, or dependence analysis in general, is the granularity at which dependencies are tracked. This article considers two extreme design points in this vast design space and examines their relative expressiveness.

1 Introduction

Information flow control (IFC) is a basic building block of computer security. IFC prevents the flow of high-confidentiality (or, simply, high) information to low-confidentiality (low) outputs that may be visible to attackers. For instance, one would not want private data stored on a file server to flow unencrypted to network packets since such packets can be read by all machines connected to the network, even those that are untrusted. Here, the private data is the high information and all unencrypted network packets are low outputs.

Ideally, IFC demands semantic independence of low outputs from high inputs. This is often called *noninterference* [8]: low outputs of a program should not be affected by changes to the program's high inputs. In practice, this ideal property is too restrictive but it is useful in designing enforcement techniques, which often start by aiming for noninterference, and then relax the property by allowing declassification in various ways [20].

Although IFC can be enforced through several techniques—OS kernel mediation of process I/O [6, 12, 24], static analysis and type systems [3, 15, 16, 4, 11, 1], language runtime modification [2, 9, 17], the use of dedicated libraries [13, 19, 22], or compilation [5, 7]—our focus in this article is the enforcement of IFC in higher-order languages using type systems. Building on the seminal work of Volpano, Smith and Irvine [23], which was not in a higher-order setting, many type systems have been proposed to enforce IFC in many different languages, including higher-order ones [1, 16, 4].

The common denominator of all these type systems is type annotations or *labels* to mark program inputs, outputs and intermediate values as high or low, and a mechanism to track dependencies between program values, including inputs and outputs, within the type system. However, there is significant variance in how the type systems track dependencies. Broadly speaking, dependencies may be tracked at *coarse-granularity* or at *fine-granularity.*

*This is a full version of an article of the same title that appeared in the ACM SIGLOG News, Vol. 4, No. 11. This version contains an appendix with many details and proofs and makes some changes to the presentation of the formalism.

In coarse-grained dependence analysis, the type system forces any output temporally after the analysis (elimination) of a high-labeled value to be labeled high, since there could *potentially* be a dependence from the analyzed value to the output. Obviously, this introduces a coarse approximation, since not all outputs after the analysis of a high value may actually depend on the analyzed value. In information flow terminology, this unnecessary forcing of labels to high is called a *label creep*. To prevent label creep, the language may provide a scoping mechanism that syntactically delimits the effect of the analysis of a value. Despite the problem of label creep, the main advantage of coarse-grained dependence analysis is that it significantly reduces the need to label intermediate values since, by design, their labels are known implicitly from the labels of values analyzed in the past.

In contrast to coarse-grained dependence analysis, fine-grained analysis requires annotating (or inferring) the label of every intermediate value, and then carefully tracks dependencies among values. This makes the type system more precise but increases the annotation burden for either the programmer or a type-label inference engine.

The goal of this article is to provide an introduction to coarse- and fine-grained dependence analysis for IFC and to comment on their relative expressiveness. Specifically, we describe one type system each for coarse- and fine-grained dependence analysis. For coarse-grained dependence analysis, we choose a type system that tracks dependencies using a construct similar to an indexed family of monads. This type system is a simplification of an existing hybrid (mixed static and dynamic) system for dependence analysis called HLIO [4]. We call this type system CG (for coarse-grained). For fine-grained dependence analysis, we choose a slight variant of Flow Caml [16], an extension of ML's type system with information flow types. We call this type system FG (for fine-grained). In both cases, our setting is a simply-typed call-by-value lambda-calculus with references. To keep the presentation simple, we do not delve into concurrency or other evaluation strategies like call-by-name, which have nontrivial implications for dependence analysis and IFC.

Having presented the two type systems, we examine their relative expressiveness through translations. Specifically, we show that programs typable in CG can be translated in a type-preserving manner to FG. Although this may be unsurprising given the description of coarse- and fine-grained analysis above, the translation shows how the dependence analysis in CG can be simulated using specific monads in FG. We then attempt a translation from FG to CG, relying on a scope restriction construct in CG to prevent label creep. While we fail to do this (we explain why), we show that a fragment of FG can be translated, type-preserving, to CG.[1]

It is not our goal to provide a comprehensive survey of all existing work on type systems for IFC. Indeed, this area is vast. Instead, we focus on one dimension of the design space—the granularity of the dependence analysis.

2 Type Systems for Information-Flow Control

We first present two state-of-the-art information-flow security type systems, FG and CG, for higher-order, stateful functional programming languages. The two type systems differ substantially in the approaches they follow to track dependencies. This is a consequence of how FG and CG differ computationally: FG allows (side-) effects in all expressions, à la ML. Since effects can occur so freely, information flows must be tracked pervasively. Hence, FG is fine-grained. In contrast, CG isolates effects to a monad, à la Haskell. As a result, flows have to be tracked only at the granularity of the monad, but not within pure expressions. This makes CG coarse-grained.

Both FG and CG use *labels* drawn from a *lattice* $(\mathcal{L}, \sqsubseteq)$ of confidentiality *levels* l. Labels higher in the lattice represent higher confidentiality. The goal of dependence analysis for information flow is to ensure that terms labeled l can depend only on terms labeled l or lower. In examples, we often use the two-point lattice, $\mathsf{LH} = (\{L, H\}, \sqsubseteq)$, which contains two levels L (low) and H (high) with $L \sqsubseteq H$ and $H \not\sqsubseteq L$. We use $\perp$ and $\top$ to denote the least and the greatest elements of any lattice. In LH, $\perp = L$ and $\top = H$.

[1]Due to lack of space, we omit some details of the translations in the main body of the paper. These are included in the appendix at the end.

2.1 Fine-grained type system

Syntax, types, constraints:

Expressions	e	$::=$	$x \mid \lambda x.e \mid e\ e \mid (e,e) \mid \mathsf{fst}(e) \mid \mathsf{snd}(e) \mid \mathsf{inl}(e) \mid \mathsf{inr}(e) \mid \mathsf{case}(e, x.e, x.e) \mid \mathsf{new}\ e \mid$ $!e \mid e := e \mid () \mid \Lambda e \mid e\ [] \mid \nu\ e \mid e\ \bullet$
Labels	ℓ, pc	$::=$	$l \mid \alpha \mid \ell \sqcup \ell \mid \ell \sqcap \ell$
Types	τ	$::=$	A^ℓ
Base types	A	$::=$	$\mathsf{b} \mid \tau \xrightarrow{\ell_e} \tau \mid \tau \times \tau \mid \tau + \tau \mid \mathsf{ref}\ \tau \mid \mathsf{unit} \mid \forall \alpha.(\ell_e, \tau) \mid c \overset{\ell_e}{\Rightarrow} \tau$
Constraints	c	$::=$	$\ell \sqsubseteq \ell \mid (c, c)$

Type system: $\boxed{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau}$

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash_{pc} x : \tau}\ \text{FG-var} \qquad \frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} \lambda x.e : (\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp}\ \text{FG-lam}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\ell_e} \tau_2)^\ell \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 \searrow \ell \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1\ e_2 : \tau_2}\ \text{FG-app}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\mathsf{ref}\ \tau)^\ell \qquad \Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \tau' \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} !e : \tau'}\ \text{FG-deref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^\ell \qquad \Sigma; \Psi \vdash \tau_1 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{fst}(e) : \tau_1}\ \text{FG-fst} \qquad \frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_1}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inl}(e) : (\tau_1 + \tau_2)^\perp}\ \text{FG-inl}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 + \tau_2)^\ell \qquad \Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_1 : \tau \qquad \Sigma; \Psi; \Gamma, y : \tau_2 \vdash_{pc \sqcup \ell} e_2 : \tau \qquad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{case}(e, x.e_1, y.e_2) : \tau}\ \text{FG-case}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc'} e : \tau' \qquad \Sigma; \Psi \vdash pc \sqsubseteq pc' \qquad \Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau}\ \text{FG-sub}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau \qquad \Sigma; \Psi \vdash \tau \searrow pc}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{new}\ e : (\mathsf{ref}\ \tau)^\perp}\ \text{FG-ref} \qquad \frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : \tau_1 \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^\perp}\ \text{FG-prod}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\mathsf{ref}\ \tau)^\ell \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau \qquad \Sigma; \Psi \vdash \tau \searrow (pc \sqcup \ell)}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 := e_2 : \mathsf{unit}}\ \text{FG-assign}$$

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash_\ell e : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \Lambda e : (\forall \alpha.(\ell, \tau))^\perp}\ \text{FG-FI} \qquad \frac{\Sigma; \Psi, c; \Gamma \vdash_\ell e : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \nu\ e : (c \overset{\ell}{\Rightarrow} \tau)^\perp}\ \text{FG-CI}$$

$$\frac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e : (\forall \alpha.(\ell, \tau))^{\ell'} \qquad \ell'' \in FV(\Sigma) \qquad \Sigma; \Psi \vdash pc \sqcup \ell' \sqsubseteq \ell[\ell''/\alpha] \\ \Sigma; \Psi \vdash \tau[\ell''/\alpha] \searrow \ell'\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} e\ [] : \tau[\ell''/\alpha]}\ \text{FG-FE}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (c \overset{\ell}{\Rightarrow} \tau)^{\ell'} \qquad \Sigma; \Psi \vdash c \qquad \Sigma; \Psi \vdash pc \sqcup \ell' \sqsubseteq \ell \qquad \Sigma; \Psi \vdash \tau \searrow \ell'}{\Sigma; \Psi; \Gamma \vdash_{pc} e\ \bullet : \tau}\ \text{FG-CE}$$

Figure 1: Syntax and type system of FG.

$$\frac{\Sigma; \Psi \vdash \ell \sqsubseteq \ell' \qquad \Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}'}{\Sigma; \Psi \vdash \mathsf{A}^{\ell} <: \mathsf{A}'^{\ell'}} \text{ FGsub-label} \qquad \frac{}{\Sigma; \Psi \vdash \mathsf{b} <: \mathsf{b}} \text{ FGsub-base}$$

$$\frac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \tau <: \mathsf{ref}\ \tau} \text{ FGsub-ref} \qquad \frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'} \text{ FGsub-prod}$$

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'} \text{ FGsub-sum}$$

$$\frac{\Sigma; \Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2' \qquad \Sigma; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'} \text{ FGsub-arrow} \qquad \frac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}} \text{ FGsub-unit}$$

$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2 \qquad \Sigma, \alpha; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash \forall \alpha.(\ell_e, \tau_1) <: \forall \alpha.(\ell_e', \tau_2)} \text{ FGsub-forall}$$

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi, c_2 \vdash \tau_1 <: \tau_2 \qquad \Sigma; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash c_1 \overset{\ell_e}{\Rightarrow} \tau_1 <: c_2 \overset{\ell_e'}{\Rightarrow} \tau_2} \text{ FGsub-constraint}$$

Figure 2: FG subtyping

The fine-grained type system we consider, FG, is shown in Figure 1. FG is a slight modification of Flow Caml [16], an extension of ML's type system for information flow control. Computationally, FG is the call-by-value simply-typed lambda calculus, extended with products, sums, references, label polymorphism, and ordering constraints on labels.

Since side-effects may appear in any sub-expression in this language, FG must, when analyzing sub-expressions, account for all information that data concerning the sub-expression can contain. To this end, FG labels *all* of the (otherwise standard) types for this language with a *structural label* ℓ, reflecting an upper bound on the information conveyed by observing the structure of the expression. For instance, say bool is one of the base types that the symbol b in Figure 1 ranges over. Then observing a value of type bool^H may reveal H information.

When analyzing non-ground expressions, FG tracks the propagation of information through the evaluation of expressions. For instance, FG concludes that the conjunction of a bool^H and a bool^L value is a bool^H value, as observing the result may convey information about each component in the conjunction.

This tracking alone, however, is insufficient; since (sub)expressions can be evaluated conditionally, observing the presence or absence of effects can convey information about the *control-flow* conditions that facilitated or prevented the effects. Structural labels do not account for this information. For instance, let $x_{\mathsf{C}} : (\mathsf{unit}^L + \mathsf{unit}^L)^H$, $x : (\mathsf{ref}\ \mathsf{nat}^L)^L$, and consider $e = \mathsf{case}(x_{\mathsf{C}}, \_.(), \_.x := 42)$.[2] The result of evaluating e is invariably (), so no information is conveyed by observing the result. However, on evaluation, e reveals whether $x_{\mathsf{C}} = \mathsf{inl}(())$ or $x = \mathsf{inr}(())$ through the absence or presence of the write to x. FG tracks this information by recording control flow information in a *control label pc* (aka program counter), making it a lower bound on the write effects that the (sub)expression being typed can perform. For instance, when attempting to type the previous example, FG raises the *pc* by the information in the control-flow condition x, which is H, and checks whether the branches only have write effects at or above this new *pc*. However, the right branch writes 42 to x, which stores L-labeled natural numbers. So, with these labels on the types of x and x_{C}, e does not type-check.

[2]We use the symbol _ to denote a variable, label or type whose actual value is irrelevant. Here, _ denotes anonymous variables. Later, we use _ to denote labels and types that are irrelevant to the discussion.

Effects in a function's body are suspended until the function is applied. Further, since our language is higher-order, a function can take another function as a parameter and apply it. This necessitates additional type annotations on function types. For instance, let $x_{\mathsf{C}} : (\mathsf{unit}^L + \mathsf{unit}^L)^H$ and $x : (\mathsf{ref}\ \mathsf{nat}^L)^L$. Consider $e = \lambda x_{\mathsf{F}}.\mathsf{case}(x_{\mathsf{C}}, \_.\,(), \_.\,(x_{\mathsf{F}}\ ()))$. Assuming that x_{F} maps unit^L to unit^L, e maps such mappings to unit^H, possibly applying x_{F} in the process. Now consider $e' = \lambda\_.\,(x := 42)$, a function with a suspended effect, which maps unit^L to unit^L. While $e\ e'$ always returns a result of type unit^H, $e\ e'$ conditionally applies e', and thus, the L effect in e' leaks the control condition (x_{C}) in e, which is H. FG resolves this by having function types carry a separate control label; in $\tau \xrightarrow{\ell_e} \tau'$, ℓ_e is a lower bound on the level of the write effects that can occur when a function of this type is applied. In the example, $e' : (\mathsf{unit}^L \xrightarrow{L} \mathsf{unit}^L)^L$; thus FG rejects $e\ e'$ since e applies a function with L effects in a H context. Finally, note that functions of type $(\tau \xrightarrow{L} \tau')^H$ can be constructed but not applied in FG. This is because such a function can leak its identity, which is labeled H, to L when it is applied. However, if the function is merely passed around, it cannot leak information.

For the same reason, the types $\forall\alpha.(\ell_e, \tau)$ and $c \overset{\ell_e}{\Rightarrow} \tau$ also carry the control label ℓ_e. In FG, values of these types (Λe and $\nu\ e$, respectively) are also suspended computations.

FG performs security checks by checking the satisfiability of flow constraints, using the judgment $\Sigma, \Psi \vdash c$. A constraint c is a conjunction of terms of the form $\ell \sqsubseteq \ell'$, where ℓ ranges over levels, label-variables, and lattice operations on these. Let Ψ range over sets of constraints, and Σ range over sets of label parameters α. The judgment $\Sigma, \Psi \vdash c$ checks whether, for all instantiations of Σ, assuming Ψ, c holds. Label ℓ *covers* type $\mathsf{A}^{\ell'}$ (from below), written $\Sigma, \Psi \vdash \mathsf{A}^{\ell'} \searrow \ell$, iff $\Sigma, \Psi \vdash \ell \sqsubseteq \ell'$.

Subtyping FG uses subtyping to allow upwards-flows of information. Subtyping amounts to weakening a guarantee for an expression. In our case, this guarantee is the type of an expression, which specifies how the information is classified. The subtyping judgment, defined in Figure 2, has the form $\Sigma; \Psi \vdash \tau <: \tau'$. In effect, this judgment extends ($\sqsubseteq$) to labeled expression types. For any A^ℓ, $<:$ is covariant in ℓ. This weakening of the type amounts to up-classifying information, which is safe since it only labels less confidential information as more confidential. Subtyping is covariant everywhere else, with two exceptions: control labels, and function arguments. A control label guarantees a lower bound on effects. This guarantee is weakened if the control label is lowered. For instance, if an expression has type $(\mathsf{nat}^H \xrightarrow{H} \mathsf{unit}^H)^L$, the function may produce effects at or above H. This implies the weaker statement that the function may produce effects at or above L. Hence $(\mathsf{nat}^H \xrightarrow{H} \mathsf{unit}^H)^L <: (\mathsf{nat}^H \xrightarrow{L} \mathsf{unit}^H)^L$. A function argument appears as an assumption in the function type, and strengthening an assumption amounts to weakening the guarantee. For instance, if an expression has type $(\mathsf{nat}^H \xrightarrow{H} \mathsf{unit}^H)^L$, the function does not leak despite receiving H input. The function still will not leak if given L input. Hence, $(\mathsf{nat}^H \xrightarrow{H} \mathsf{unit}^H)^L <: (\mathsf{nat}^L \xrightarrow{H} \mathsf{unit}^H)^L$.

Typing judgment and typing rules FG's type system prevents illicit flows of information by ensuring that

- eliminating an expression labeled ℓ produces a result covered by ℓ.
- an expression executing under *pc* can only cause write effects at or above *pc*.

The typing judgment has the form $\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau$. It reads: for all Σ, assuming Ψ and Γ, e has type τ, and *pc* is a lower bound on the level of all write effects which can occur when e is evaluated. We focus on three constructs, since these involve the *pc*: case, abstraction, and references.

In the rule FG-case, since case deconstructs its sum, the results of the branches must be covered by the label on the sum. Also, since either one or the other branch is evaluated depending on the sum, in typing the branches, the *pc* label is raised by the label on the sum, thus ensuring that the branches do not have write effects below the label of the sum.

In the rule FG-lam, FG can disregard the *pc* when typing the body of the function, because the body will not be evaluated immediately. FG thus only needs to check that the function satisfies what the type $(\tau_1 \xrightarrow{\ell_e} \tau_2)^\perp$ says it satisfies: (1) that the body has type τ_2 given input of type τ_1, and (2) that all of its effects are at or above ℓ_e, which is ensured by checking the body of the function with *pc* set to ℓ_e. The outermost label on the conclusion's type $\tau_1 \xrightarrow{\ell_e} \tau_2$ is $\bot$ because the fact that the function is constructed at this point in the program reveals no information. In fact, the outermost label is $\bot$ in the introduction rules of all types, not just $\tau_1 \xrightarrow{\ell_e} \tau_2$. Rule FG-app checks that the result of applying a function is covered by the label on the function type, and that the effect of running the function does not leak contextual information, or structural information about the function.

In rules FG-ref and FG-assign, *pc* must cover the type of the value written to the reference. This ensures that write effects of the expression being typed are lower-bounded by *pc*. Additionally, in FG-assign, the label of the value written must cover the label on the reference to prevent leaking which reference was written. In the rule FG-deref, reading a reference conveys information about which reference was read; the result of the read must thus be covered by the label on the reference. (We implicitly assume that in the type $\mathsf{ref}\ \tau$, the type τ is closed, i.e., it has no free label parameters. Not enforcing this can break both subject reduction and the following noninterference property.)

Noninterference FG enforces noninterference: The result of evaluating an expression of a labeled base type cannot depend on an input whose label does not cover the label of the base type.

Theorem 2.1. [Noninterference for FG] Suppose (1) $\ell_i \not\sqsubseteq \ell$, (2) $x : \mathsf{A}^{\ell_i} \vdash_{pc} e : \mathsf{b}^{\ell}$, and (3) $v_1, v_2 : \mathsf{A}^{\ell_i}$. If both $e[v_1/x]$ and $e[v_2/x]$ terminate, then they produce the same value (of type b).

2.2 Coarse-grained type system

Next, we describe CG, a type system for coarse-grained dependence analysis. CG is not a new type system: It is the static fragment of HLIO [4], a hybrid type system that mixes static and dynamic analyses to track flows. One minor difference from HLIO is that CG has call-by-value semantics to match those of FG whereas HLIO's semantics are call-by-name. We make this change to make CG's reduction strategy match FG's.

CG is designed to minimize type-label annotations. To this end, it isolates all effects in a monad-like type construct. The syntax and typing rules of CG are shown in Figure 3. Unlike FG, standard typing constructs like products, arrows and sums are not refined with labels. These types behave exactly as in the simply typed lambda calculus (which CG extends conservatively) and the corresponding expressions do not have side-effects. For labeling, CG has a dedicated *type constructor* $\mathsf{Labeled}\ \ell\ \tau$, which means τ labeled with ℓ. This is the only way to label a type in CG. Expressions are augmented with the constructs $\mathsf{Lb}_\ell(e)$ and $\mathsf{unlabel}(e)$ to introduce and eliminate $\mathsf{Labeled}\ \ell\ \tau$.[3]

Effects are limited to computations that have the type $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$. This type is similar to a monad and has the usual monadic return and bind constructs. Importantly, the bind construct is used to track dependencies coarsely. Finally, CG adds a scoping construct $\mathsf{toLabeled}(e)$ that limits label creep. References in CG store only labeled values. A reference of type $\mathsf{ref}\ \ell\ \tau$ stores values of type $\mathsf{Labeled}\ \ell\ \tau$.

The type $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$ The type $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$ ascribes (suspended) computations that have effects. We define two kinds of effects in CG. *Input effects* cause a computation to learn new information and happen when a computation unlabels a labeled value. An *output effect* causes a computation to release information. This happens when a computation either creates a labeled value or writes to a reference. (Since references store only labeled values, merely reading a reference is not an input effect—to learn the actual content, the program must unlabel the value. Strictly speaking, it is also not essential to treat writing a reference as an output effect in CG. However, in many practical scenarios, attackers can observe writes to memory through side-channels outside the language, so we treat all writes as outputs.)

The type system enforces that the output effects of a computation of type $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$ are lower-bounded by ℓ_i and that its input effects are upper-bounded by ℓ_o. We call ℓ_i the "initial" program counter (pc) and ℓ_o the "final" pc for the computation. For instance, when writing to a reference, it is checked that the initial pc is below the label of the written value (last premise of rule CG-assign). When a value of type $\mathsf{Labeled}\ \ell\ \tau$ is unlabeled, the final pc of the computation is joined with ℓ (rule CG-unlabel).

[3]Due to an oversight, the original SIGLOG article omitted the construct $\mathsf{Lb}_\ell(e)$. Instead, it had a construct $\mathsf{label}_\ell(e)$, which is not really needed: It can be defined as $\mathsf{label}_\ell(e) = \mathsf{ret}(\mathsf{Lb}_\ell(e))$.

Syntax, types, constraints:

Expressions	e	$::=$	$x \mid \lambda x.e \mid e\ e \mid (e,e) \mid \mathsf{fst}(e) \mid \mathsf{snd}(e) \mid \mathsf{inl}(e) \mid \mathsf{inr}(e) \mid \mathsf{case}(e, x.e, y.e) \mid \mathsf{new}\ e \mid\ !e \mid e := e \mid () \mid \Lambda e \mid e\ [] \mid \nu\ e \mid e\ \bullet \mid \mathsf{Lb}_\ell(e) \mid \mathsf{unlabel}(e) \mid \mathsf{toLabeled}(e) \mid \mathsf{ret}(e) \mid \mathsf{bind}(e, x.e)$
Labels	ℓ	$::=$	$l \mid \alpha \mid \ell \sqcup \ell \mid \ell \sqcap \ell$
Types	τ	$::=$	$\mathsf{b} \mid \tau \to \tau \mid \tau \times \tau \mid \tau + \tau \mid \mathsf{ref}\ \ell\ \tau \mid \mathsf{unit} \mid \forall \alpha.\tau \mid c \Rightarrow \tau \mid \mathsf{Labeled}\ \ell\ \tau \mid \mathsf{CG}\ \ell_i\ \ell_o\ \tau$
Constraints	c	$::=$	$\ell \sqsubseteq \ell \mid (c, c)$

Type system: $\boxed{\Sigma; \Psi; \Gamma \vdash e : \tau}$

(All rules of the simply typed lambda-calculus pertaining to the types $\mathsf{b}, \tau \to \tau, \tau \times \tau, \tau + \tau, \mathsf{unit}$ are included.)

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{Lb}_\ell(e) : \mathsf{Labeled}\ \ell\ \tau}\ \text{CG-label} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{Labeled}\ \ell\ \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{unlabel}(e) : \mathsf{CG}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau}\ \text{CG-unlabel}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{CG}\ \ell_i\ \ell_o\ \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{toLabeled}(e) : \mathsf{CG}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau)}\ \text{CG-toLabeled} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{ret}(e) : \mathsf{CG}\ \ell_i\ \ell_i\ \tau}\ \text{CG-ret}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \mathsf{CG}\ \ell_i\ \ell\ \tau \qquad \Sigma; \Psi; \Gamma, x : \tau \vdash e_2 : \mathsf{CG}\ \ell\ \ell_o\ \tau'}{\Sigma; \Psi; \Gamma \vdash \mathsf{bind}(e_1, x.e_2) : \mathsf{CG}\ \ell_i\ \ell_o\ \tau'}\ \text{CG-bind}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau' \qquad \Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi; \Gamma \vdash e : \tau}\ \text{CG-sub} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{Labeled}\ \ell'\ \tau \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash \mathsf{new}\ e : \mathsf{CG}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau)}\ \text{CG-ref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{ref}\ \ell\ \tau}{\Sigma; \Psi; \Gamma \vdash\ !e : \mathsf{CG}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)}\ \text{CG-deref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \mathsf{ref}\ \ell'\ \tau \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \mathsf{Labeled}\ \ell'\ \tau \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash e_1 := e_2 : \mathsf{CG}\ \ell\ \ell\ \mathsf{unit}}\ \text{CG-assign} \qquad \frac{\Sigma, \alpha; \Psi; \Gamma \vdash e : \tau}{\Sigma; \Gamma \vdash \Lambda e : \forall \alpha.\tau}\ \text{CG-FI}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \forall \alpha.\tau \qquad FV(\ell) \in \Sigma}{\Sigma; \Psi; \Gamma \vdash e\ [] : \tau[\ell/\alpha]}\ \text{CG-FE} \qquad \frac{\Sigma; \Psi, c; \Gamma \vdash e : \tau}{\Sigma; \Gamma \vdash \nu\ e : c \Rightarrow \tau}\ \text{CG-CI}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : c \Rightarrow \tau \qquad \Sigma; \Psi \vdash c}{\Sigma; \Psi; \Gamma \vdash e\ \bullet : \tau}\ \text{CG-CE}$$

Figure 3: Syntax and type system of CG.

The construct $\mathsf{bind}(e_1, x.e_2)$ allows sequencing two computations of types $\mathsf{CG}\ \ell_i\ \ell\ \tau$ and $\tau \to \mathsf{CG}\ \ell\ \ell_o\ \tau'$ to obtain a computation of type $\mathsf{CG}\ \ell_i\ \ell_o\ \tau'$. Importantly, the final pc ℓ of the first computation must match the initial pc of the second computation. This ensures that the second computation's output effects (which are lower-bounded by ℓ) are at labels higher than the input effects of the first computation (which are upper-bounded by ℓ) and, hence, prevents any information leak. This is the only mechanism for tracking dependencies in CG.

It is an invariant of the type system that if $e : \mathsf{CG}\ \ell_i\ \ell_o\ \tau$, then $\ell_i \sqsubseteq \ell_o$. This invariant can be enforced using a well-formedness relation on types, whose straightforward details we omit here.

Construct $\mathsf{toLabeled}(e)$ As described above, sequencing a second computation after a computation of type $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$ using bind requires that the second computation's output effects be labeled higher than ℓ_o. This causes a label creep when the second computation does not actually examine the result of the first computation (e.g., the second computation may write the first computation's result to memory without examining it). To work around such a label creep, CG provides the expression construct $\mathsf{toLabeled}$ that coerces the type $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$ to $\mathsf{CG}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau)$. The computation returned by $\mathsf{toLabeled}$, when forced, forces the original computation and labels the result with ℓ_o.[4] A computation of the type $\mathsf{CG}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau)$ can be followed by a second computation whose output effects are at level ℓ_i or higher. The pc increases to ℓ_o only if the second computation actually unlabels the result of the first computation.

$$\frac{}{\Sigma; \Psi \vdash \tau <: \tau} \qquad \frac{\Sigma; \Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \to \tau_2 <: \tau_1' \to \tau_2'} \qquad \frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}$$

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'} \qquad \frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell\ \tau <: \mathsf{Labeled}\ \ell'\ \tau'}$$

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell_i' \sqsubseteq \ell_i \qquad \Sigma; \Psi \vdash \ell_o \sqsubseteq \ell_o'}{\Sigma; \Psi \vdash \mathsf{CG}\ \ell_i\ \ell_o\ \tau <: \mathsf{CG}\ \ell_i'\ \ell_o'\ \tau'} \qquad \frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash \forall\alpha.\tau_1 <: \forall\alpha.\tau_2}$$

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash c_1 \Rightarrow \tau_1 <: c_2 \Rightarrow \tau_2}$$

Figure 4: CG subtyping.

Subtyping CG includes the usual subtyping rules of the simply typed lambda calculus. Subtyping for $\mathsf{Labeled}\ \ell\ \tau$ is covariant in ℓ. Subtyping for $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$ is contravariant in ℓ_i and covariant in ℓ_o. This is natural since ℓ_i is a lower-bound (on the output effects) and ℓ_o is an upper-bound (on the input effects). The subtyping rules of CG are shown in Figure 4.

Noninterference CG satisfies noninterference: If a computation has only low input effects and returns a value of base type, then the returned value must be independent of any high input.

Theorem 2.2. [Noninterference for CG] Suppose (1) $\ell_i \not\sqsubseteq \ell$, (2) $x : \mathsf{Labeled}\ \ell_i\ \tau \vdash e : \mathsf{CG}\ \_\ \ell\ \mathsf{b}$, and (3) $v_1, v_2 : \mathsf{Labeled}\ \ell_i\ \tau$. If both $e[v_1/x]$ and $e[v_2/x]$ terminate when forced, then they produce the same value (of type b).

[4] The term "forcing" is used here in the sense of monads. Forcing a value of type $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$ runs the suspended computation, records its write effects and eventually returns whatever the computation returns.

3 Translations

Having described the fine- and coarse-grained dependence analysis type systems FG and CG, we now turn to understanding their relative expressiveness. We do so by presenting (attempted) type-preserving translations from CG to FG, and vice-versa. We start by showing a type-preserving translation from CG to FG in Section 3.1. We then attempt a translation in the reverse direction, show where it fails and why (Section 3.2). Based on our attempt, we identify a smaller fragment of FG which can be translated to CG, preserving types.

3.1 Translating CG to FG

In this section, we define a translation $[\![\cdot]\!]$ from CG to FG and show that it is type-preserving. The translation of types is shown below.

$$\begin{aligned}
[\![\mathsf{b}]\!] &= \mathsf{b}^{\perp} \\
[\![\tau_1 \to \tau_2]\!] &= ([\![\tau_1]\!] \xrightarrow{\top} [\![\tau_2]\!])^{\perp} \\
[\![\tau_1 \times \tau_2]\!] &= ([\![\tau_1]\!] \times [\![\tau_2]\!])^{\perp} \\
[\![\tau_1 + \tau_2]\!] &= ([\![\tau_1]\!] + [\![\tau_2]\!])^{\perp} \\
[\![\mathsf{Labeled}\ \ell\ \tau]\!] &= ([\![\tau]\!] + \mathsf{unit})^{\ell}
\end{aligned}
\qquad
\begin{aligned}
[\![\mathsf{unit}]\!] &= \mathsf{unit}^{\perp} \\
[\![\mathsf{ref}\ \ell\ \tau]\!] &= (\mathsf{ref}\ ([\![\tau]\!] + \mathsf{unit})^{\ell})^{\perp} \\
[\![\mathsf{CG}\ \ell_i\ \ell_o\ \tau]\!] &= (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau]\!] + \mathsf{unit})^{\ell_o})^{\perp} \\
[\![c \Rightarrow \tau]\!] &= (c \overset{\top}{\Rightarrow} [\![\tau]\!])^{\perp} \\
[\![\forall\alpha.\tau]\!] &= (\forall\alpha.(\top, [\![\tau]\!]))^{\perp}
\end{aligned}$$

This translation relies on three key ideas. First, in CG, labels are limited to the type construct $\mathsf{Labeled}\ \ell\ \tau$, so the translation of all other types can simply use the outer label $\perp$. There are several choices for translating $\mathsf{Labeled}\ \ell\ \tau$. A natural translation would be $\mathsf{A}^{\ell' \sqcup \ell}$, where $\mathsf{A}^{\ell'}$ is the translation of τ. However, this translation "flattens" nested labels of the form $\mathsf{Labeled}\ \ell\ (\mathsf{Labeled}\ \ell'\ \tau)$, making it impossible to simulate, in the translation, the selective unlabeling of only the outer ℓ, but not the inner ℓ', which is allowed in CG. To keep the labels ℓ and ℓ' separate in the translation, we translate $\mathsf{Labeled}\ \ell\ \tau$ to $([\![\tau]\!] + \mathsf{unit})^{\ell}$, which keeps the label on $[\![\tau]\!]$ separate from ℓ. The corresponding translation of expressions uses inl, thus never actually returning the unit value during execution.

Second, in CG, side-effects are confined to the type $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$, so when translating CG's remaining types, which represent pure terms, we can always use $pc = \top$ in FG (since there are no side-effects in the pure terms, $\top$ is trivially the strictest lower-bound on the output effects). As a result, the control labels on $\to$, $\Rightarrow$ and $\forall$ in the translations of $\tau_1 \to \tau_2$, $c \Rightarrow \tau$ and $\forall\alpha.\tau$ are all $\top$.

The type $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$ represents a suspended computation whose effects are visible only after it is forced. This is emulated in FG using a thunk, a function that takes an argument of unit type. Specifically, $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$ translates to $(\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau]\!] + \mathsf{unit})^{\ell_o})^{\perp}$, which is a decorated variant of the thunk type $\mathsf{unit} \to [\![\tau]\!]$. The thunk can be forced when needed by applying it to $()$. The ℓ_i on the arrow means (in FG) that the write-effects of the computation (the thunk) are lower-bounded by ℓ_i, which is exactly the meaning of ℓ_i in $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$. The label ℓ_o on $([\![\tau]\!] + \mathsf{unit})$ implies that the result of the computation cannot be analyzed without raising the pc to ℓ_o in FG, which is exactly the consequence of having ℓ_o in the type $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$ in CG. (We note that the translation simulates $\mathsf{CG}\ \ell_i\ \ell_o\ \tau$ using a combination of the type forms $\mathsf{unit} \to [\![\tau]\!]$ and $[\![\tau]\!] + \mathsf{unit}$, both of which are monads.)

Finally, in CG, a reference of type $\mathsf{ref}\ \ell\ \tau$ stores values of type $\mathsf{Labeled}\ \ell\ \tau$. Hence, the translation of $\mathsf{ref}\ \ell\ \tau$ is $(\mathsf{ref}\ ([\![\tau]\!] + \mathsf{unit})^{\ell})^{\perp}$.

The translation $[\![\cdot]\!]$ is lifted pointwise to contexts: $[\![\Gamma]\!] \triangleq \{x : [\![\tau]\!] \mid x : \tau \in \Gamma\}$. The translation of expressions is type derivation-directed and is written $\Sigma; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e'$. Selected rules of the translation are shown in Figure 5. They should be unsurprising given the type translation.

The following theorem shows that this translation preserves types, in the sense that $\rightsquigarrow$ always maps a valid CG typing derivation to a valid FG typing derivation.

Theorem 3.1 (Type soundness, CG $\rightsquigarrow$ FG)**.** *If $\Sigma; \Psi; \Gamma \vdash e : \tau$ has a valid CG typing derivation, then there exists an e' such that $\Sigma; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e'$ and $\Sigma; \Psi; [\![\Gamma]\!] \vdash_{\top} e' : [\![\tau]\!]$ has a valid FG typing derivation.*

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{Lb}_\ell(e) : \mathsf{Labeled}\ \ell\ \tau \rightsquigarrow \mathsf{inl}(e_F)} \text{ label}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{Labeled}\ \ell\ \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{unlabel}(e) : \mathsf{CG}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau \rightsquigarrow \lambda\_.e_F} \text{ unlabel}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{CG}\ \ell_i\ \ell_o\ \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{toLabeled}(e) : \mathsf{CG}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(e_F\ ())} \text{ toLabeled}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{ret}(e) : \mathsf{CG}\ \ell_i\ \ell_i\ \tau \rightsquigarrow \lambda\_.\mathsf{inl}(e_F)} \text{ ret}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \mathsf{CG}\ \ell_i\ \ell\ \tau \rightsquigarrow e_{F1} \qquad \Sigma; \Psi; \Gamma, x : \tau \vdash e_2 : \mathsf{CG}\ \ell\ \ell_o\ \tau' \rightsquigarrow e_{F2}}{\Sigma; \Psi; \Gamma \vdash \mathsf{bind}(e_1, x.e_2) : \mathsf{CG}\ \ell_i\ \ell_o\ \tau' \rightsquigarrow \lambda\_.\mathsf{case}(e_{F1}(), x.e_{F2}(), y.\mathsf{inr}())} \text{ bind}$$

Figure 5: Type derivation-directed expression translation from CG into FG, selected rules.

3.2 Translating FG to CG

Next, we consider translating FG to CG. We start with an incorrect strawman translation, which we refine, eventually getting to a point where no further progress seems possible. At that point, we identify a fragment of FG for which the refined translation works. The goal of going through this exercise is to impress upon the reader the difficulty of translating a fine-grained dependence analysis to a coarse-grained one, and to argue that there does not seem to be a straightforward translation from all of FG to CG, despite CG having the construct toLabeled to prevent label creep.

Strawman translation We construct a strawman translation, $[\![\cdot]\!]$, from FG to CG that we soon show to be incorrect. We translate the type A^ℓ to $\mathsf{Labeled}\ \ell\ [\![\mathsf{A}]\!]$ since this is the only type construct that adds a label in CG.

Next, consider the function type $\tau_1 \xrightarrow{\ell_e} \tau_2$ in FG. Since the body of a function of this type can have a write effect at level ℓ_e or higher, an intuitive translation of this type could have the form $[\![\tau_1]\!] \to \mathsf{CG}\ \ell_e\ \ell_o\ [\![\tau_2]\!]$. For the translation of the function's body to be well-typed in CG, the label ℓ_o must be an upper-bound on the labels of everything the function's body analyzes. Nothing in the FG type specifies this upper-bound, so we must find some other alternative. Fortunately, it is possible to *confine* the effects of value analysis using the construct toLabeled in CG. As a result, we may hope that we can choose $\ell_o = \ell_e$ and translate $\tau_1 \xrightarrow{\ell_e} \tau_2$ to $[\![\tau_1]\!] \to \mathsf{CG}\ \ell_e\ \ell_e\ [\![\tau_2]\!]$.

Independent of what ℓ_o we choose, this translation has a label creep problem. Consider a FG function f of type $\mathsf{unit} \xrightarrow{H} \mathsf{A}^L$ in the lattice LH. This function may write high values to references but it eventually returns a low value. In FG, the *result* of f's application can be written to a reference of type $\mathsf{ref}\ \mathsf{A}^L$. However, after translation, this write would be impossible because f's type would translate to $[\![\mathsf{unit}]\!] \to \mathsf{CG}\ H\ H\ (\mathsf{Labeled}\ L\ \mathsf{A})$. Applying this type would result in a computation, say c, of type $\mathsf{CG}\ H\ H\ (\mathsf{Labeled}\ L\ \mathsf{A})$. There is no way to extract a low labeled value from this computation. At best, we may use subtyping, bind and toLabeled as in $\mathsf{toLabeled}(\mathsf{bind}(c, x.\mathsf{unlabel}(x)))$ to coerce the type to $\mathsf{CG}\ L\ L\ (\mathsf{Labeled}\ H\ \mathsf{A})$, but the resulting value still has the label H.

Based on this, we may be tempted to translate $\tau_1 \xrightarrow{\ell_e} \tau_2$ to $[\![\tau_1]\!] \to \mathsf{CG}\ \bot\ \bot\ [\![\tau_2]\!]$ instead (this is sound because $\bot$ is trivially a lower bound on any write effect in the function's body). Although this translation would solve the label creep problem mentioned in the previous paragraph, it suffers from a different problem: Now, the translation cannot simulate an application of the previous paragraph's function f in a high context, i.e., in a case branch where the analyzed sum is labeled H. To see this, consider the FG expression $\mathsf{case}(h, x.f(), ...)$, where $h : (\tau + \tau')^H$. In FG, the type of this expression is A^H. In CG, we would correspondingly like to construct a result of type $\mathsf{Labeled}\ H\ [\![\mathsf{A}]\!]$. However, this is impossible. Since h's translation has type $\mathsf{Labeled}\ H\ (\llbracket\tau\rrbracket + \llbracket\tau'\rrbracket)$, to perform a case analysis on it, we must first $\mathsf{unlabel}$ it. This will result in a computation of type $\mathsf{CG}\ L\ H\ (\llbracket\tau\rrbracket + \llbracket\tau'\rrbracket)$. Next, we can bind this computation and case analyze the value of type $\llbracket\tau\rrbracket + \llbracket\tau'\rrbracket$. However, due to the restrictions in typing bind, any further binds we perform must be on values of type $\mathsf{CG}\ H\ H\ \_$. The body of f's translation has the type $\mathsf{CG}\ L\ L\ (\mathsf{Labeled}\ L\ \llbracket\mathsf{A}\rrbracket)$ ($L = \bot$ here) and there is no way to coerce this to the form $\mathsf{CG}\ H\ H\ \_$ because subtyping for $\mathsf{CG}\ \ell_i\ \ell_e\ \tau$ is contravariant in ℓ_i. So, we cannot bind the body of f, and, hence, cannot obtain a value of type $\mathsf{Labeled}\ \_\ \llbracket\mathsf{A}\rrbracket$.

Using label polymorphism The problems with the strawman translation above can be addressed using label polymorphism. For instance, we could translate $\tau_1 \xrightarrow{\ell_e} \tau_2$ to $\llbracket\tau_1\rrbracket \to \forall\alpha.\mathsf{CG}\ \alpha\ \alpha\ \llbracket\tau_2\rrbracket$. This would allow us to use the earlier function f in both contexts, instantiating α with L in the first context and with H in the second context. However, this translation is unsound. Specifically, instantiating α with some $\ell'_e \not\sqsubseteq \ell_e$ allows us to establish that every write in the function's body is at the level ℓ'_e or higher, which is clearly false, since the function's body may write at level ℓ_e (according to the FG type $\tau_1 \xrightarrow{\ell_e} \tau_2$).

Consequently, we consider a revised translation that maps $\tau_1 \xrightarrow{\ell_e} \tau_2$ to $\llbracket\tau_1\rrbracket \to \forall\alpha.(\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \llbracket\tau_2\rrbracket$. The entire type translation is shown below. (The translation of $c \overset{\ell_e}{\Rightarrow} \tau$ and $\forall\alpha.(\ell_e, \tau)$ follows the same intuition as the translation of $\tau_1 \xrightarrow{\ell_e} \tau_2$.)

$$
\begin{aligned}
\llbracket\mathsf{b}\rrbracket &= \mathsf{b} \\
\llbracket\tau_1 \xrightarrow{\ell_e} \tau_2\rrbracket &= \llbracket\tau_1\rrbracket \to \forall\alpha.(\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \llbracket\tau_2\rrbracket \\
\llbracket c \overset{\ell_e}{\Rightarrow} \tau\rrbracket &= \forall\alpha.(\alpha \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \llbracket\tau\rrbracket \\
\llbracket\forall\alpha.(\ell_e, \tau)\rrbracket &= \forall\alpha.\forall\alpha'.(\alpha' \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \llbracket\tau\rrbracket \\
\llbracket\mathsf{A}^\ell\rrbracket &= \mathsf{Labeled}\ \ell\ \llbracket\mathsf{A}\rrbracket
\end{aligned}
\qquad
\begin{aligned}
\llbracket\mathsf{unit}\rrbracket &= \mathsf{unit} \\
\llbracket\tau_1 \times \tau_2\rrbracket &= \llbracket\tau_1\rrbracket \times \llbracket\tau_2\rrbracket \\
\llbracket\tau_1 + \tau_2\rrbracket &= \llbracket\tau_1\rrbracket + \llbracket\tau_2\rrbracket \\
\llbracket\mathsf{ref}\ \mathsf{A}^\ell\rrbracket &= \mathsf{ref}\ \ell\ \llbracket\mathsf{A}\rrbracket
\end{aligned}
$$

The translation of contexts Γ is defined pointwise and a FG typing judgment $\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau$ translates to a CG judgment of the form $\Sigma; \Psi; \llbracket\Gamma\rrbracket \vdash e' : \forall\alpha.(\alpha \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \llbracket\tau\rrbracket$, mirroring the label polymorphism in the bodies of function types (e' is the translation of e).

Unfortunately, this translation has a different problem! Consider how we would (inductively) translate the rule FG-case from Figure 1. Inductively, from the premises we obtain e', e'_1 and e'_2 (the translations of e, e_1 and e_2, respectively) such that:

1. $\Sigma; \Psi; \llbracket\Gamma\rrbracket \vdash e' : \forall\alpha.(\alpha \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ (\mathsf{Labeled}\ \ell\ (\llbracket\tau_1\rrbracket + \llbracket\tau_2\rrbracket))$
2. $\Sigma; \Psi; \llbracket\Gamma\rrbracket, x : \llbracket\tau_1\rrbracket \vdash e'_1 : \forall\alpha_1.(\alpha_1 \sqsubseteq (pc \sqcup \ell)) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ \llbracket\tau\rrbracket$
3. $\Sigma; \Psi; \llbracket\Gamma\rrbracket, y : \llbracket\tau_2\rrbracket \vdash e'_2 : \forall\alpha_2.(\alpha_2 \sqsubseteq (pc \sqcup \ell)) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau\rrbracket$

The goal is to construct a term e'' (the translation of $\mathsf{case}(e, x.e_1, y.e_2)$) such that

$$\Sigma; \Psi; \llbracket\Gamma\rrbracket \vdash e'' : \forall\alpha'.(\alpha' \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \llbracket\tau\rrbracket$$

We try to search for the appropriate term e'' (much as we would look for a proof in a formal proof system). We pick some α' such that $\alpha' \sqsubseteq pc$. We must construct a term of the type $\mathsf{CG}\ \alpha'\ \alpha'\ \llbracket\tau\rrbracket$. Our only option is to case analyze the value of type $(\llbracket\tau_1\rrbracket + \llbracket\tau_2\rrbracket)$ in (1), so we must instantiate the quantified α in (1) and bind the resulting computation type. Since the eventual goal is to obtain something of type $\mathsf{CG}\ \alpha'\ \_\ \_$, we must pick $\alpha = \alpha'$. We instantiate $\alpha = \alpha'$, and bind the computation of type $\mathsf{CG}\ \alpha'\ \alpha'\ (\mathsf{Labeled}\ \ell\ (\llbracket\tau_1\rrbracket + \llbracket\tau_2\rrbracket))$ in (1), obtaining a local variable of type $\mathsf{Labeled}\ \ell\ (\llbracket\tau_1\rrbracket + \llbracket\tau_2\rrbracket)$. We $\mathsf{unlabel}$ this to obtain a computation of type $\mathsf{CG}\ \alpha'\ (\alpha' \sqcup \ell)\ (\llbracket\tau_1\rrbracket + \llbracket\tau_2\rrbracket)$, which we bind again to obtain a variable of type $\llbracket\tau_1\rrbracket + \llbracket\tau_2\rrbracket$. This variable can be case-analyzed. To construct the case branches we must instantiate and bind the computations in (2) and (3). We show only the operations on (2), those on (3) being similar. First, we must pick a suitable α_1. Since the next computation we construct must have a type of the form $\mathsf{CG}\ (\alpha' \sqcup \ell)\ \_\ \_$, we must pick $\alpha_1 = \alpha' \sqcup \ell$ (which is indeed below $(pc \sqcup \ell)$, as required by the constraint in (2)). Second, we instantiate (2) with this substitution to obtain a computation of type $\mathsf{CG}\ (\alpha' \sqcup \ell)\ (\alpha' \sqcup \ell)\ \llbracket\tau\rrbracket$. Repeating this process on (3), we obtain an end-to-end computation of type $\mathsf{CG}\ \alpha'\ (\alpha' \sqcup \ell)\ \llbracket\tau\rrbracket$.

This is *almost* what we wanted. To complete the proof, we have to coerce the type $\mathsf{CG}\ \alpha'\ (\alpha' \sqcup \ell)\ [\![\tau]\!]$ to the type $\mathsf{CG}\ \alpha'\ \alpha'\ [\![\tau]\!]$. For this, we consider the cases $\alpha' \sqsubseteq \ell$ and $\alpha' \not\sqsubseteq \ell$ separately. Strictly speaking, CG does not allow a case analysis on constraints. However, we show below that the proof cannot even be completed in the second case, so the case analysis has expository value.

When $\alpha' \sqsubseteq \ell$, then $\mathsf{CG}\ \alpha'\ (\alpha' \sqcup \ell)\ [\![\tau]\!] = \mathsf{CG}\ \alpha'\ \ell\ [\![\tau]\!]$ and it is not difficult to write a coercion function from $\mathsf{CG}\ \alpha'\ \ell\ [\![\tau]\!]$ to $\mathsf{CG}\ \alpha'\ \alpha'\ [\![\tau]\!]$. The fourth premise of the FG-case rule is $\tau \searrow \ell$, so $\tau = \mathsf{A}^{\ell'}$ for some $\ell' \sqsupseteq \ell$ and $[\![\tau]\!] = \mathsf{Labeled}\ \ell'\ [\![\mathsf{A}]\!]$. The required coercion function is $\lambda x : (\mathsf{CG}\ \alpha'\ \ell\ [\![\tau]\!]).\ \mathsf{toLabeled}(\mathsf{bind}(x, y.\mathsf{unlabel}(y)))$.

However, in the case $\alpha' \not\sqsubseteq \ell$, such a coercion function may not exist. Concretely, consider the lattice $L \sqsubseteq \{M_1, M_2\} \sqsubseteq H$ with M_1, M_2 incomparable, $\alpha' = M_1$, $\ell = M_2$ and $\tau = \mathsf{A}^{M_2}$. In this case, our goal is to coerce $\mathsf{CG}\ M_1\ H\ (\mathsf{Labeled}\ M_2\ [\![\mathsf{A}]\!])$ to $\mathsf{CG}\ M_1\ M_1\ (\mathsf{Labeled}\ M_2\ [\![\mathsf{A}]\!])$. This is impossible in CG: Our only hope of getting rid of the H in the given type is to use $\mathsf{toLabeled}$, but that would push the H into the label of the resulting value.

It follows, therefore, that even our revised translation does not work. However, on any fragment of FG where the second case $\alpha' \not\sqsubseteq \ell$ can never arise, this translation *would* work. In the following, we identify such a fragment, FG^-.

The fragment FG^- Because α' is arbitrary and the only constraint on it is $\alpha' \sqsubseteq pc$, disallowing $\alpha' \not\sqsubseteq \ell$ is the same as always forcing $pc \sqsubseteq \ell$. One simple way of ensuring $pc \sqsubseteq \ell$ is to restrict FG to a fragment in which $\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau$ implies $\tau \searrow pc$. Then, (1) would force $pc \sqsubseteq \ell$. Defining such a fragment is straightforward. We only need to restrict the types in the conclusions of the typing rules for all introduction forms like pairing, functions, inl, inr, etc. to be labeled pc (currently, these rules allow the label $\bot$). Elimination rules do not require any changes (although some premises in the elimination rules become redundant, e.g., the premise $\tau \searrow \ell$ in the rule FG-case). We can then show inductively that $\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau$ implies $\tau \searrow pc$.

For instance, the rules FG-var and FG-lam of Figure 1 are replaced with the following more restrictive rules.

$$\frac{\Sigma; \Psi \vdash \tau \sqsubseteq \tau' \qquad \tau' \searrow pc}{\Sigma; \Psi; \Gamma, x : \tau \vdash_{pc} x : \tau'}\ \text{FG}^-\text{-var} \qquad\qquad \frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} \lambda x.e : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{pc}}\ \text{FG}^-\text{-lam}$$

Lemma 3.2. $\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau$ *in FG^- implies* $\Sigma; \Psi \vdash \tau \searrow pc$.

We can prove that on the fragment FG^-, the translation $[\![\cdot]\!]$ defined above is total and type-preserving. We have to first define a type derivation-directed translation of expressions, whose straightforward details we elide here (the details can be found in the appendix at the end). This translation is written $\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau \rightsquigarrow e'$.

Theorem 3.3 (Type soundness, $\text{FG}^- \rightsquigarrow \text{CG}$)**.** *If $\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau$ has a valid FG^- typing derivation, then there exists an e' such that $\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau \rightsquigarrow e'$ and $\Sigma; \Psi; [\![\Gamma]\!] \vdash e' : \forall \alpha.(\alpha \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau]\!]$ has a valid CG typing derivation.*

4 Other type systems

Several other type systems for information flow control can be classified as either fine-grained [16, 23, 10] or coarse-grained [14, 18, 4]. Of particular note is the dependency core calculus (DCC) [1]. DCC uses a monad to track dependencies, in a manner similar to CG, but is otherwise pure. [1] show how several calculi for dependence analysis can be translated to DCC. One of these calculi is a first-order calculus with references [21]. This calculus has a rule very similar to the case analysis rule of FG, whose translation failed in Section 3.2. A priori, it seems that we ought to be able to examine the translation from [21] to DCC to understand how to translate FG's case analysis rule to CG. However, [1]'s translation is not parametric in the security lattice: It is defined only for the lattice LH, and treats the (analogues of the) FG judgments $\Sigma; \Psi; \Gamma \vdash_L e : \tau$ and $\Sigma; \Psi; \Gamma \vdash_H e : \tau$ completely differently. Indeed, we expect that such a non-parametric translation would also exist from FG to CG, at least for the lattice LH.

5 Conclusion

At their core, type systems for information flow control perform dependence analysis. Moving from a fine-grained to a coarse-grained dependence analysis trades off precision for fewer type-label annotations. In this article, we have initiated a study of the relative expressiveness of these two approaches by considering type-preserving translations from a coarse-grained type system to a fine-grained type system and vice-versa. Our analysis indicates that the former is straightforward (as expected) whereas the latter is not.

In ongoing work, we are examining two problems that we have not yet addressed satisfactorily. First, we would like to prove that the translations are operationally sound (not just type-preserving). Ideally, we would like to derive the noninterference theorem for one system from the noninterference theorem of the other system and properties of the translation. Prior work has established similar results for other translations. For example, [1] establish similar results for the translation of several dependency-tracking calculi into DCC. In our setting, the problem is harder due to the presence of state, whose combination with higher-order functions would complicate any model of types. Second, we would like to find a translation from all of FG to CG or show that such a translation does not exist. Since Section 3.2 already shows a translation from FG^- to CG, the problem of translating FG to CG simplifies to that of finding a translation from FG to FG^-.

Acknowledgments We would like to thank Alejandro Russo for discussions on coarse-grained dependence analysis and for feedback on a draft of this article. This work was supported in part by the Deutsche Forschungsgemeinschaft (DFG) grant "Information Flow Control for Browser Clients" under the priority program "Reliably Secure Software Systems" (RS^3) and the DFG collaborative research center grant SFB 1223 "Methods and Tools for Understanding and Controlling Privacy".

References

[1] Martín Abadi, Anindya Banerjee, Nevin Heintze, and Jon G. Riecke. A core calculus of dependency. In *Proceedings of the 26th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, (POPL)*, pages 147–160, 1999.

[2] Thomas H. Austin and Cormac Flanagan. Efficient purely-dynamic information flow analysis. In *Proceedings of the 2009 Workshop on Programming Languages and Analysis for Security (PLAS)*, pages 113–124, 2009.

[3] Gilles Barthe, Pedro R. D'Argenio, and Tamara Rezk. Secure information flow by self-composition. *Mathematical Structures in Computer Science*, 21(6):1207–1252, 2011.

[4] Pablo Buiras, Dimitrios Vytiniotis, and Alejandro Russo. HLIO: mixing static and dynamic typing for information-flow control in haskell. In *Proceedings of the 20th ACM SIGPLAN International Conference on Functional Programming (ICFP)*, pages 289–301, 2015.

[5] Andrey Chudnov and David A. Naumann. Inlined information flow monitoring for javascript. In *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 629–643, 2015.

[6] Eslam Elnikety, Aastha Mehta, Anjo Vahldiek-Oberwagner, Deepak Garg, and Peter Druschel. Thoth: Comprehensive policy compliance in data retrieval systems. In *Proceedings of the 25th USENIX Security Symposium (USENIX Security)*, pages 637–654, 2016.

[7] Cédric Fournet, Gurvan Le Guernic, and Tamara Rezk. A security-preserving compiler for distributed programs: From information-flow policies to cryptographic mechanisms. In *Proceedings of the 16th ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 432–441, 2009.

[8] Joseph A. Goguen and José Meseguer. Security policies and security models. In *Proceedings of the 1982 IEEE Symposium on Security and Privacy (Oakland)*, pages 11–20, 1982.

[9] Daniel Hedin and Andrei Sabelfeld. Information-flow security for a core of javascript. In *Proceedings of the 25th IEEE Computer Security Foundations Symposium (CSF)*, pages 3–18, 2012.

[10] Nevin Heintze and Jon G. Riecke. The slam calculus: Programming with secrecy and integrity. In *Proceedings of the 25th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)*, pages 365–377, 1998.

[11] Sebastian Hunt and David Sands. On flow-sensitive security types. In *Proceedings of the 33rd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)*, pages 79–90, 2006.

[12] Maxwell N. Krohn, Alexander Yip, Micah Z. Brodsky, Natan Cliffer, M. Frans Kaashoek, Eddie Kohler, and Robert Morris. Information flow control for standard OS abstractions. In *Proceedings of the 21st ACM Symposium on Operating Systems Principles (SOSP*, pages 321–334, 2007.

[13] Peng Li and Steve Zdancewic. Encoding information flow in haskell. In *Proceedings of the 19th IEEE Computer Security Foundations Workshop (CSFW)*, 2006.

[14] Ana Almeida Matos. *Typing secure information flow: Declassification and mobility*. PhD thesis, École Nationale Supérieure des Mines de Paris, 2006.

[15] Andrew C. Myers. Jflow: Practical mostly-static information flow control. In *Proceedings of the 26th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)*, pages 228–241, 1999.

[16] François Pottier and Vincent Simonet. Information flow inference for ML. *ACM Transactions on Programming Languages and Systems*, 25(1):117–158, 2003.

[17] Vineet Rajani, Abhishek Bichhawat, Deepak Garg, and Christian Hammer. Information flow control for event handling and the DOM in web browsers. In *Proceedings of the 28th IEEE Computer Security Foundations Symposium (CSF)*, pages 366–379, 2015.

[18] Alejandro Russo. Functional pearl: Two can keep a secret, if one of them uses haskell. In *Proceedings of the 20th ACM SIGPLAN International Conference on Functional Programming (ICFP)*, pages 280–288, 2015.

[19] Alejandro Russo, Koen Clasessen, and John Hughes. A library for light-weight information-flow security in haskell. In *Proceedings of the 1st ACM SIGPLAN Symposium on Haskell (Haskell)*, pages 13–24, 2008.

[20] Andrei Sabelfeld and David Sands. Declassification: Dimensions and principles. *Journal of Computer Security*, 17(5):517–548, 2009.

[21] Geoffrey Smith and Dennis M. Volpano. Secure information flow in a multi-threaded imperative language. In *Proceedings of the 25th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)*, pages 355–364, 1998.

[22] Deian Stefan, Alejandro Russo, John C. Mitchell, and David Mazières. Flexible dynamic information flow control in haskell. In *Proceedings of the 4th ACM SIGPLAN Symposium on Haskell (Haskell)*, pages 95–106, 2011.

[23] Dennis M. Volpano, Cynthia E. Irvine, and Geoffrey Smith. A sound type system for secure flow analysis. *Journal of Computer Security*, 4(2/3):167–188, 1996.

[24] Nickolai Zeldovich, Silas Boyd-Wickizer, Eddie Kohler, and David Mazières. Making information flow explicit in histar. In *Proceedings of the 7th Symposium on Operating Systems Design and Implementation (OSDI)*, pages 263–278, 2006.

A CG

This section describes the CG type system. The type system consists of the standard base types, function type, reference type, sum and product type. Additionally we also add a monad-like type constructor to the type system, $\mathsf{CG}\ \ell_1\ \ell_2\ \tau$, for a computation that starts with pc ℓ_1, ends with pc ℓ_2 and computes a value of type τ. We also add the type $\mathsf{Labeled}\ \ell\ \tau$ for a value of type τ at label ℓ. Along with this we add the forall and constraint types. To the expression language, we add explicit introduction and elimination constructs for the types described above. Additionally we add a scoping construct, $\mathsf{toLabeled}(e)$, that encapsulates the effect of a computation into a labeled type.

Expressions	e	$::=$	$() \mid x \mid e_1\ e_2 \mid \lambda x.e \mid (e_1, e_2) \mid \mathsf{fst}(e) \mid \mathsf{snd}(e) \mid \mathsf{inl}(e) \mid \mathsf{inr}(e) \mid \mathsf{case}(e, x.e_1, y.e_2) \mid$
			$\mathsf{Lb}_\ell(e) \mid \mathsf{unlabel}(e) \mid \mathsf{toLabeled}(e) \mid \mathsf{ret}(e) \mid \mathsf{bind}(e_1, x.e_2) \mid \Lambda e \mid e[] \mid \nu e \mid e \bullet$
Types	τ	$::=$	$\mathsf{unit} \mid \mathsf{b} \mid \tau_1 \to \tau_2 \mid \tau_1 \times \tau_2 \mid \tau_1 + \tau_2 \mid \mathsf{ref}\ \ell\ \tau \mid \mathsf{Labeled}\ \ell\ \tau \mid \mathsf{CG}\ \ell_i\ \ell_o\ \tau \mid \forall\alpha.\tau \mid c \Rightarrow \tau$
Label	ℓ	$::=$	$\alpha \mid \bot \mid \ \ldots\ \mid \top \mid \ell \sqsubseteq \ell \mid \ell \sqcap \ell$
Constraints	c	$::=$	$\ell \sqsubseteq \ell \mid (c, c)$

Figure 6: Language and type syntax

$\boxed{\Sigma; \Psi; \Gamma \vdash e : \tau}$

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash x : \tau} \text{ CG-var} \qquad \frac{\Sigma; \Psi; \Gamma, x : \tau \vdash e : \tau'}{\Sigma; \Psi; \Gamma \vdash \lambda x.e : \tau \to \tau'} \text{ CG-lam}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \tau \to \tau' \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \tau}{\Sigma; \Psi; \Gamma \vdash e_1\ e_2 : \tau'} \text{ CG-app} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e_1 : \tau_1 \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \tau_2}{\Sigma; \Psi; \Gamma \vdash (e_1, e_2) : \tau_1 \times \tau_2} \text{ CG-prod}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1 \times \tau_2}{\Sigma; \Psi; \Gamma \vdash \mathsf{fst}(e) : \tau_1} \text{ CG-fst} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1 \times \tau_2}{\Sigma; \Psi; \Gamma \vdash \mathsf{snd}(e) : \tau_2} \text{ CG-snd} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1}{\Sigma; \Psi; \Gamma \vdash \mathsf{inl}(e) : \tau_1 + \tau_2} \text{ CG-inl}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau_2}{\Sigma; \Psi; \Gamma \vdash \mathsf{inr}(e) : \tau_1 + \tau_2} \text{ CG-inr}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1 + \tau_2 \qquad \Sigma; \Psi; \Gamma, x : \tau_1 \vdash e_1 : \tau \qquad \Sigma; \Psi; \Gamma, y : \tau_2 \vdash e_2 : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{case}(e, x.e_1, y.e_2) : \tau} \text{ CG-case}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{Lb}_\ell(e) : \mathsf{Labeled}\ \ell\ \tau} \text{ CG-label} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{Labeled}\ \ell\ \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{unlabel}(e) : \mathsf{CG}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau} \text{ CG-unlabel}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{CG}\ \ell_i\ \ell_o\ \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{toLabeled}(e) : \mathsf{CG}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau)} \text{ CG-toLabeled} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \tau}{\Sigma; \Psi; \Gamma \vdash \mathsf{ret}(e) : \mathsf{CG}\ \ell_i\ \ell_i\ \tau} \text{ CG-ret}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \mathsf{CG}\ \ell_i\ \ell\ \tau \qquad \Sigma; \Psi; \Gamma, x : \tau \vdash e_2 : \mathsf{CG}\ \ell\ \ell_o\ \tau'}{\Sigma; \Psi; \Gamma \vdash \mathsf{bind}(e_1, x.e_2) : \mathsf{CG}\ \ell_i\ \ell_o\ \tau'} \text{ CG-bind} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \tau' \qquad \Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi; \Gamma \vdash e : \tau} \text{ CG-sub}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{Labeled}\ \ell'\ \tau \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash \mathsf{new}\ e : \mathsf{CG}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau)} \text{ CG-ref} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{ref}\ \ell\ \tau}{\Sigma; \Psi; \Gamma \vdash !e : \mathsf{CG}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau)} \text{ CG-deref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \mathsf{ref}\ \ell'\ \tau \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \mathsf{Labeled}\ \ell'\ \tau \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash e_1 := e_2 : \mathsf{CG}\ \ell\ \ell\ \mathsf{unit}} \text{ CG-assign} \qquad \frac{\Sigma, \alpha; \Psi; \Gamma \vdash e : \tau}{\Sigma; \Gamma \vdash \Lambda e : \forall \alpha.\tau} \text{ CG-FI}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \forall \alpha.\tau \qquad FV(\ell) \subseteq \Sigma}{\Sigma; \Psi; \Gamma \vdash e[] : \tau[\ell/\alpha]} \text{ CG-FE} \qquad \frac{\Sigma; \Psi, c; \Gamma \vdash e : \tau}{\Sigma; \Gamma \vdash \nu e : c \Rightarrow \tau} \text{ CG-CI} \qquad \frac{\Sigma; \Psi; \Gamma \vdash e : c \Rightarrow \tau \qquad \Sigma; \Psi \vdash c}{\Sigma; \Psi; \Gamma \vdash e \bullet : \tau} \text{ CG-CE}$$

Figure 7: Type system of CG.

$$\frac{}{\Sigma; \Psi \vdash \tau <: \tau}\ \text{CGsub-base} \qquad \frac{\Sigma; \Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \to \tau_2 <: \tau_1' \to \tau_2'}\ \text{CGsub-arrow}$$

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}\ \text{CGsub-prod} \qquad \frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}\ \text{CGsub-sum}$$

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell\ \tau <: \mathsf{Labeled}\ \ell'\ \tau'}\ \text{CGsub-labeled}$$

$$\frac{\Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \ell_i' \sqsubseteq \ell_i \qquad \Sigma; \Psi \vdash \ell_o \sqsubseteq \ell_o'}{\Sigma; \Psi \vdash \mathsf{CG}\ \ell_i\ \ell_o\ \tau <: \mathsf{CG}\ \ell_i'\ \ell_o'\ \tau'}\ \text{CGsub-monad} \qquad \frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash \forall \alpha.\tau_1 <: \forall \alpha.\tau_2}\ \text{CGsub-forall}$$

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi \vdash \tau_1 <: \tau_2}{\Sigma; \Psi \vdash c_1 \Rightarrow \tau_1 <: c_2 \Rightarrow \tau_2}\ \text{CGsub-constraint}$$

Figure 8: CG subtyping.

$$\frac{}{\Sigma; \Psi \vdash \mathsf{b}\ WF}\ \text{CG-wff-base} \qquad \frac{}{\Sigma; \Psi \vdash \mathsf{unit}\ WF}\ \text{CG-wff-unit}$$

$$\frac{\Sigma; \Psi \vdash \tau_1\ WF \qquad \Sigma; \Psi \vdash \tau_2\ WF}{\Sigma; \Psi \vdash (\tau_1 \xrightarrow{\ell_e} \tau_2)\ WF}\ \text{CG-wff-arrow} \qquad \frac{\Sigma; \Psi \vdash \tau_1\ WF \qquad \Sigma; \Psi \vdash \tau_2\ WF}{\Sigma; \Psi \vdash (\tau_1 \times \tau_2)\ WF}\ \text{CG-wff-times}$$

$$\frac{\Sigma; \Psi \vdash \tau_1\ WF \qquad \Sigma; \Psi \vdash \tau_2\ WF}{\Sigma; \Psi \vdash (\tau_1 + \tau_2)\ WF}\ \text{CG-wff-sum} \qquad \frac{FV(\ell) = \emptyset \qquad FV(\tau) = \emptyset}{\Sigma; \Psi \vdash (\mathsf{ref}\ \ell\ \tau)\ WF}\ \text{CG-wff-ref}$$

$$\frac{\Sigma, \alpha; \Psi \vdash \tau\ WF}{\Sigma; \Psi \vdash (\forall \alpha.\ (\tau))\ WF}\ \text{CG-wff-forall} \qquad \frac{\Sigma; \Psi, c \vdash \tau\ WF}{\Sigma; \Psi \vdash (c \overset{\ell_e}{\Rightarrow} \tau)\ WF}\ \text{CG-wff-constraint}$$

$$\frac{\Sigma; \Psi \vdash \tau\ WF}{\Sigma; \Psi \vdash (\mathsf{Labeled}\ \ell\ \tau)\ WF}\ \text{CG-wff-labeled} \qquad \frac{\Sigma; \Psi \vdash \tau\ WF}{\Sigma; \Psi \vdash (\mathsf{CG}\ \ell_i\ \ell_o\ \tau)\ WF}\ \text{CG-wff-monad}$$

Figure 9: Well-formedness relation for closedness of reference types in CG

B FG

$$\frac{\Sigma; \Psi \vdash \ell \sqsubseteq \ell' \qquad \Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}'}{\Sigma; \Psi \vdash \mathsf{A}^{\ell} <: \mathsf{A}'^{\ell'}} \text{ FGsub-label} \qquad \frac{}{\Sigma; \Psi \vdash \mathsf{b} <: \mathsf{b}} \text{ FGsub-base}$$

$$\frac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \tau <: \mathsf{ref}\ \tau} \text{ FGsub-ref} \qquad \frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'} \text{ FGsub-prod}$$

$$\frac{\Sigma; \Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2'}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'} \text{ FGsub-sum}$$

$$\frac{\Sigma; \Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 <: \tau_2' \qquad \Sigma; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'} \text{ FGsub-arrow} \qquad \frac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}} \text{ FGsub-unit}$$

$$\frac{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2 \qquad \Sigma, \alpha; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash \forall \alpha.(\ell_e, \tau_1) <: \forall \alpha.(\ell_e', \tau_2)} \text{ FGsub-forall}$$

$$\frac{\Sigma; \Psi \vdash c_2 \implies c_1 \qquad \Sigma; \Psi, c_2 \vdash \tau_1 <: \tau_2 \qquad \Sigma; \Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma; \Psi \vdash c_1 \overset{\ell_e}{\Rightarrow} \tau_1 <: c_2 \overset{\ell_e'}{\Rightarrow} \tau_2} \text{ FGsub-constraint}$$

Figure 10: FG subtyping.

$\boxed{\Sigma, \Psi \vdash \tau \searrow \ell}$ τ leaks to level ℓ and higher only

$$\frac{\Sigma, \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma, \Psi \vdash \mathsf{A}^{\ell'} \searrow \ell}$$

Figure 11: Covers relation (FG types).

Expressions	e	$::=$	$() \mid x \mid e_1\ e_2 \mid \lambda x.e \mid (e_1, e_2) \mid \mathsf{fst}(e) \mid \mathsf{snd}(e) \mid \mathsf{inl}(e) \mid \mathsf{inr}(e) \mid \mathsf{case}(e, x.e_1, y.e_2) \mid \Lambda e \mid e\ [] \mid \nu\ e \mid e \bullet$
Base Types	A	$::=$	$\mathsf{unit} \mid \mathsf{b} \mid \tau + \tau \mid \tau \times \tau \mid \tau \xrightarrow{\ell_e} \tau \mid \mathsf{ref}\ \tau \mid \forall \alpha.(\ell, \tau) \mid c \overset{\ell}{\Rightarrow} \tau$
Types	τ	$::=$	A^{ℓ}
Constraints	c	$::=$	$\ell \sqsubseteq \ell \mid (c, c)$

Lemma B.1 (Reflexivity of subtyping)**.** *The following hold:*

1. *For all* Σ, Ψ, τ*:* $\Sigma; \Psi \vdash \tau <: \tau$
2. *For all* Σ, Ψ, A*:* $\Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}$

Proof. Proof by simultaneous induction on τ and A.

Proof of statement (1)

$$\boxed{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau}$$

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash_{pc} x : \tau}\ \text{FG-var} \qquad \frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} \lambda x.e : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\perp}}\ \text{FG-lam}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 \searrow \ell \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1\ e_2 : \tau_2}\ \text{FG-app}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : \tau_1 \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^{\perp}}\ \text{FG-prod} \qquad \frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^{\ell} \qquad \Sigma; \Psi \vdash \tau_1 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{fst}(e) : \tau_1}\ \text{FG-fst}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^{\ell} \qquad \Sigma; \Psi \vdash \tau_2 \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{snd}(e) : \tau_2}\ \text{FG-snd} \qquad \frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_1}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inl}(e) : (\tau_1 + \tau_2)^{\perp}}\ \text{FG-inl}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_2}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inr}(e) : (\tau_1 + \tau_2)^{\perp}}\ \text{FG-inr}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 + \tau_2)^{\ell} \qquad \Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_1 : \tau \qquad \Sigma; \Psi; \Gamma, y : \tau_2 \vdash_{pc \sqcup \ell} e_2 : \tau \qquad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{case}(e, x.e_1, y.e_2) : \tau}\ \text{FG-case}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc'} e : \tau' \qquad \Sigma; \Psi \vdash pc \sqsubseteq pc' \qquad \Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau}\ \text{FG-sub} \qquad \frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau \qquad \Sigma; \Psi \vdash \tau \searrow pc}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{new}\ e : (\mathsf{ref}\ \tau)^{\perp}}\ \text{FG-ref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\mathsf{ref}\ \tau)^{\ell} \qquad \Sigma; \Psi \vdash \tau <: \tau' \qquad \Sigma; \Psi \vdash \tau' \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} !e : \tau'}\ \text{FG-deref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\mathsf{ref}\ \tau)^{\ell} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau \qquad \Sigma; \Psi \vdash \tau \searrow (pc \sqcup \ell)}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 := e_2 : \mathsf{unit}}\ \text{FG-assign}$$

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash_{\ell_e} e : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \Lambda e : (\forall \alpha.(\ell_e, \tau))^{\perp}}\ \text{FG-FI} \qquad \frac{\Sigma; \Psi, c; \Gamma \vdash_{\ell_e} e : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \nu\ e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\perp}}\ \text{FG-CI}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\forall \alpha.(\ell_e, \tau))^{\ell} \qquad FV(\ell'') \subseteq \Sigma \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell''/\alpha] \qquad \Sigma; \Psi \vdash \tau[\ell''/\alpha] \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e\ [] : \tau[\ell''/\alpha]}\ \text{FG-FE}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell} \qquad \Sigma; \Psi \vdash c \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e \qquad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e \bullet : \tau}\ \text{FG-CE}$$

Figure 12: Type system of FG.

$$\frac{\Sigma; \Psi \vdash \mathsf{A}\ WF}{\Sigma; \Psi \vdash \mathsf{A}^{\ell}\ WF}\ \text{FG-wff-label} \qquad \frac{}{\Sigma; \Psi \vdash \mathsf{b}\ WF}\ \text{FG-wff-base} \qquad \frac{}{\Sigma; \Psi \vdash \mathsf{unit}\ WF}\ \text{FG-wff-unit}$$

$$\frac{\Sigma; \Psi \vdash \tau_1\ WF \qquad \Sigma; \Psi \vdash \tau_2\ WF}{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2\ WF}\ \text{FG-wff-arrow} \qquad \frac{\Sigma; \Psi \vdash \tau_1\ WF \qquad \Sigma; \Psi \vdash \tau_2\ WF}{\Sigma; \Psi \vdash \tau_1 \times \tau_2\ WF}\ \text{FG-wff-prod}$$

$$\frac{\Sigma; \Psi \vdash \tau_1\ WF \qquad \Sigma; \Psi \vdash \tau_2\ WF}{\Sigma; \Psi \vdash \tau_1 + \tau_2\ WF}\ \text{FG-wff-sum} \qquad \frac{FV(\tau) = \emptyset}{\Sigma; \Psi \vdash (\mathsf{ref}\ \tau)\ WF}\ \text{FG-wff-ref}$$

$$\frac{\Sigma, \alpha; \Psi \vdash \tau\ WF}{\Sigma; \Psi \vdash (\forall\ (\ell_e, \tau))\ WF}\ \text{FG-wff-forall} \qquad \frac{\Sigma; \Psi, c \vdash \tau\ WF}{\Sigma; \Psi \vdash (c \overset{\ell_e}{\Rightarrow} \tau))\ WF}\ \text{FG-wff-constraint}$$

Figure 13: Well-formedness relation for closedness of reference types in FG

Let $\tau = \mathsf{A}^{\ell}$. Then, we have:

$$\frac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{A} <: \mathsf{A}}\ \text{IH(2)} \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell}{\Sigma; \Psi \vdash \mathsf{A}^{\ell} <: \mathsf{A}^{\ell}}\ \text{FGsub-label}$$

Proof of statement (2)

We proceed by cases on A.

1. $\mathsf{A} = \mathsf{b}$:

$$\frac{}{\Sigma; \Psi \vdash \mathsf{b} <: \mathsf{b}}\ \text{FGsub-base}$$

2. $\mathsf{A} = \mathsf{ref}\ \tau$:

$$\frac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \tau <: \mathsf{ref}\ \tau}\ \text{FGsub-ref}$$

3. $\mathsf{A} = \tau_1 \times \tau_2$:

$$\frac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\ \text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\ \text{IH(1) on } \tau_2}{\Sigma; \Psi \vdash \tau_1 \times \tau_2 <: \tau_1 \times \tau_2}$$

4. $\mathsf{A} = \tau_1 + \tau_2$:

$$\frac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\ \text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\ \text{IH(1) on } \tau_2}{\Sigma; \Psi \vdash \tau_1 + \tau_2 <: \tau_1 + \tau_2}$$

5. $\mathsf{A} = \tau_1 \xrightarrow{\ell_e} \tau_2$:

$$\frac{\dfrac{}{\Sigma; \Psi \vdash \tau_1 <: \tau_1}\ \text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash \tau_2 <: \tau_2}\ \text{IH(2) on } \tau_2 \qquad \dfrac{}{\Sigma; \Psi \vdash \ell_e \sqsubseteq \ell_e}}{\Sigma; \Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1 \xrightarrow{\ell_e} \tau_2}$$

6. $\mathsf{A} = \mathsf{unit}$:

$$\frac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}}$$

7. $\mathsf{A} = \forall \alpha.\tau_i$:

$$\frac{\dfrac{}{\Sigma, \alpha; \Psi \vdash \tau_i <: \tau_i}\ \text{IH(1) on } \tau_i}{\Sigma; \Psi \vdash \forall \alpha.\tau_i <: \forall \alpha.\tau_i}$$

8. $\mathsf{A} = c \Rightarrow \tau_i$:

$$\frac{\dfrac{}{\Sigma; \Psi \vdash c \implies c} \qquad \dfrac{}{\Sigma; \Psi, c \vdash \tau_i <: \tau_i}\ \text{IH(1) on } \tau_i}{\Sigma; \Psi \vdash c \Rightarrow \tau <: c \Rightarrow \tau_i}$$

$\square$

C FG$^-$

$\boxed{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau}$

$$\frac{\begin{array}{c}\Sigma, \alpha; \Psi; \Gamma \vdash_{\ell_e} e : \tau \\ \Sigma; \Psi \vdash pc \sqsubseteq \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\forall \alpha.(\ell_e, \tau))^{\ell}}\ \text{FG}^-\text{-FI} \qquad \frac{\begin{array}{c}\Sigma; \Psi, c; \Gamma \vdash_{\ell_e} e : \tau \\ \Sigma; \Psi \vdash pc \sqsubseteq \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} \nu e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell}}\ \text{FG}^-\text{-CI}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\forall \alpha.(\ell_e, \tau))^{\ell} \qquad FV(\ell'') \subseteq \Sigma \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell''/\alpha] \qquad \Sigma; \Psi \vdash \tau[\ell''/\alpha] \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e[] : \tau[\ell''/\alpha]}\ \text{FG}^-\text{-FE}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} \nu e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell} \qquad \Sigma; \Psi \vdash c \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e \qquad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e \bullet : \tau}\ \text{FG}^-\text{-CE}$$

$$\frac{\Sigma; \Psi \vdash \tau \sqcup pc \sqsubseteq \tau'}{\Sigma; \Psi; \Gamma, x : \tau \vdash_{pc} x : \tau'}\ \text{FG}^-\text{-var} \qquad \frac{\begin{array}{c}\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e : \tau_2 \\ \Sigma; \Psi \vdash pc \sqsubseteq \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} \lambda x.e : (\tau_1 \overset{\ell_e}{\rightarrow} \tau_2)^{\ell}}\ \text{FG}^-\text{-lam}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\tau_1 \overset{\ell_e}{\rightarrow} \tau_2)^{\ell} \qquad \Gamma \vdash_{pc} e_2 : \tau_1 \qquad \Sigma; \Psi \vdash \tau_2 \searrow \ell \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell_e}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1\ e_2 : \tau_2}\ \text{FG}^-\text{-app}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : \tau_1 \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_2 \qquad \Sigma; \Psi \vdash pc \sqsubseteq \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^{\ell}}\ \text{FG}^-\text{-prod} \qquad \frac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 \times \tau_2)^{\ell} \\ \Sigma; \Psi \vdash \tau_1 \searrow \ell\end{array}}{\Sigma; \Psi; \Gamma_{pc} \vdash \mathsf{fst}(e) : \tau_1}\ \text{FG}^-\text{-fst}$$

$$\frac{\begin{array}{c}\Sigma; \Psi; \Gamma_{pc} \vdash e : (\tau_1 \times \tau_2)^{\ell} \\ \Sigma; \Psi \vdash \tau_2 \searrow \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{snd}(e) : \tau_2}\ \text{FG}^-\text{-snd} \qquad \frac{\begin{array}{c}\Sigma; \Psi; \Gamma_{pc} \vdash e : \tau_1 \\ \Sigma; \Psi \vdash pc \sqsubseteq \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inl}(e) : (\tau_1 + \tau_2)^{\ell}}\ \text{FG}^-\text{-inl}$$

$$\frac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_2 \\ \Sigma; \Psi \vdash pc \sqsubseteq \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{inr}(e) : (\tau_1 + \tau_2)^{\ell}}\ \text{FG}^-\text{-inr}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\tau_1 + \tau_2)^{\ell} \qquad \Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{pc \sqcup \ell} e_1 : \tau \qquad \Sigma; \Psi; \Gamma, y : \tau_2 \vdash_{pc \sqcup \ell} e_2 : \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{case}(e, x.e_1, y.e_2) : \tau}\ \text{FG}^-\text{-case}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc'} e : \tau' \qquad \Sigma; \Psi \vdash pc \sqsubseteq pc' \qquad \Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau}\ \text{FG}^-\text{-sub} \qquad \frac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau \\ \Sigma; \Psi \vdash pc \sqsubseteq \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} \mathsf{new}\ e : (\mathsf{ref}\ \tau)^{\ell}}\ \text{FG}^-\text{-ref}$$

$$\frac{\begin{array}{c}\Sigma; \Psi; \Gamma \vdash_{pc} e : (\mathsf{ref}\ \tau)^{\ell} \qquad \tau <: \tau' \\ \Sigma; \Psi \vdash \tau' \searrow \ell\end{array}}{\Sigma; \Psi; \Gamma \vdash_{pc} !e : \tau'}\ \text{FG}^-\text{-deref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\mathsf{ref}\ \tau)^{\ell} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau \qquad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 := e_2 : \mathsf{unit}^{\ell}}\ \text{FG}^-\text{-assign}$$

Figure 14: Type system of FG$^-$

$$\frac{\Sigma;\Psi \vdash \ell \sqsubseteq \ell' \qquad \Sigma;\Psi \vdash \mathsf{A} <: \mathsf{A}'}{\Sigma;\Psi \vdash \mathsf{A}^{\ell} <: \mathsf{A}'^{\ell'}}\ \text{FG}^{-}\text{sub-label} \qquad \frac{}{\Sigma;\Psi \vdash \mathsf{b} <: \mathsf{b}}\ \text{FG}^{-}\text{sub-base}$$

$$\frac{}{\Sigma;\Psi \vdash \mathsf{ref}\ \tau <: \mathsf{ref}\ \tau}\ \text{FG}^{-}\text{sub-ref} \qquad \frac{\Sigma;\Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma;\Psi \vdash \tau_2 <: \tau_2'}{\Sigma;\Psi \vdash \tau_1 \times \tau_2 <: \tau_1' \times \tau_2'}\ \text{FG}^{-}\text{sub-prod}$$

$$\frac{\Sigma;\Psi \vdash \tau_1 <: \tau_1' \qquad \Sigma;\Psi \vdash \tau_2 <: \tau_2'}{\Sigma;\Psi \vdash \tau_1 + \tau_2 <: \tau_1' + \tau_2'}\ \text{FG}^{-}\text{sub-sum}$$

$$\frac{\Sigma;\Psi \vdash \tau_1' <: \tau_1 \qquad \Sigma;\Psi \vdash \tau_2 <: \tau_2' \qquad \Sigma;\Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma;\Psi \vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'}\ \text{FG}^{-}\text{sub-arrow} \qquad \frac{}{\Sigma;\Psi \vdash \mathsf{unit} <: \mathsf{unit}}\ \text{FG}^{-}\text{sub-unit}$$

$$\frac{\Sigma,\alpha;\Psi \vdash \tau_1 <: \tau_2 \qquad \Sigma,\alpha;\Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma;\Psi \vdash \forall\alpha.(\ell_e,\tau_1) <: \forall\alpha.(\ell_e',\tau_2)}\ \text{FG}^{-}\text{sub-forall}$$

$$\frac{\Sigma;\Psi \vdash c_2 \implies c_1 \qquad \Sigma;\Psi,c_2 \vdash \tau_1 <: \tau_2 \qquad \Sigma;\Psi \vdash \ell_e' \sqsubseteq \ell_e}{\Sigma;\Psi \vdash c_1 \overset{\ell_e}{\Rightarrow} \tau_1 <: c_2 \overset{\ell_e'}{\Rightarrow} \tau_2}\ \text{FG}^{-}\text{sub-constraint}$$

Figure 15: FG^{-} subtyping.

$$\frac{\Sigma;\Psi \vdash \mathsf{A}\ WF}{\Sigma;\Psi \vdash \mathsf{A}^{\ell}\ WF}\ \text{FG}^{-}\text{-wff-label} \qquad \frac{}{\Sigma;\Psi \vdash \mathsf{b}\ WF}\ \text{FG}^{-}\text{-wff-base} \qquad \frac{}{\Sigma;\Psi \vdash \mathsf{unit}\ WF}\ \text{FG}^{-}\text{-wff-unit}$$

$$\frac{\Sigma;\Psi \vdash \tau_1\ WF \qquad \Sigma;\Psi \vdash \tau_2\ WF}{\Sigma;\Psi \vdash (\tau_1 \xrightarrow{\ell_e} \tau_2)\ WF}\ \text{FG}^{-}\text{-wff-arrow} \qquad \frac{\Sigma;\Psi \vdash \tau_1\ WF \qquad \Sigma;\Psi \vdash \tau_2\ WF}{\Sigma;\Psi \vdash (\tau_1 \times \tau_2)\ WF}\ \text{FG}^{-}\text{-wff-prod}$$

$$\frac{\Sigma;\Psi \vdash \tau_1\ WF \qquad \Sigma;\Psi \vdash \tau_2\ WF}{\Sigma;\Psi \vdash (\tau_1 + \tau_2)\ WF}\ \text{FG}^{-}\text{-wff-sum} \qquad \frac{FV(\tau) = \emptyset}{\Sigma;\Psi \vdash (\mathsf{ref}\ \tau)\ WF}\ \text{FG}^{-}\text{-wff-ref}$$

$$\frac{\Sigma,\alpha;\Psi \vdash \tau\ WF}{\Sigma;\Psi \vdash (\forall\ (\ell_e,\tau))\ WF}\ \text{FG}^{-}\text{-wff-forall} \qquad \frac{\Sigma;\Psi,c \vdash \tau\ WF}{\Sigma;\Psi \vdash (c \overset{\ell_e}{\Rightarrow} \tau)\ WF}\ \text{FG}^{-}\text{-wff-constraint}$$

Figure 16: Well-formedness relation for closedness of reference types in FG^{-}

Definition C.1 (Join label with type)**.**

$$\tau \sqcup \ell \triangleq \left\{ \begin{array}{ll} \mathsf{A}^{\ell \sqcup \ell_i} & \tau = \mathsf{A}^{\ell_i} \end{array} \right.$$

Lemma C.2. $\forall \Sigma, \Psi, \Gamma, e, \tau, pc.$
$\Sigma; \Psi; \Gamma \vdash_{pc} e : \tau_r \implies \Sigma; \Psi \vdash \tau_r \searrow pc$

Proof. Proof by induction on the typing relation

1. FG$^-$-FI:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{Given}}{\Sigma; \Psi \vdash (\forall \alpha.(\ell_e, \tau))^{\ell} \searrow pc}$$

2. FG$^-$-FE:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\forall \alpha.(\ell_e, \tau))^{\ell} \searrow pc}\ \text{IH}}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{By inversion} \qquad \dfrac{}{\Sigma; \Psi \vdash \tau[\ell''/\alpha] \searrow \ell}\ \text{Given}}{\Sigma; \Psi \vdash \tau[\ell''/\alpha] \searrow pc}$$

3. FG$^-$-CI:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{Given}}{\Sigma; \Psi \vdash (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell} \searrow pc}$$

4. FG$^-$-CE:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell} \searrow pc}\ \text{IH}}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{By inversion} \qquad \dfrac{}{\Sigma; \Psi \vdash \tau \searrow \ell}\ \text{Given}}{\Sigma; \Psi \vdash \tau \searrow pc}$$

5. FG$^-$-var:

$$\dfrac{\Sigma; \Psi \vdash \tau \sqcup pc \sqsubseteq \tau'}{\Sigma; \Psi \vdash \tau' \searrow pc}\ \text{Lemma C.3}$$

6. FG$^-$-lam:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{Given}}{\Sigma; \Psi \vdash (\tau_1 \overset{\ell_e}{\to} \tau_2)^{\ell} \searrow pc}$$

7. FG$^-$-app:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\tau_1 \overset{\ell_e}{\to} \tau_2)^{\ell} \searrow pc}\ \text{IH}}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{By inversion} \qquad \dfrac{}{\Sigma; \Psi \vdash \tau_2 \searrow \ell}\ \text{Given}}{\Sigma; \Psi \vdash \tau_2 \searrow pc}$$

8. FG$^-$-prod:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{Given}}{\Sigma; \Psi \vdash (\tau_1 \times \tau_2)^\ell \searrow pc}$$

9. FG$^-$-fst:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\tau_1 \times \tau_2)^\ell \searrow pc}\ \text{IH}}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{By inversion} \qquad \dfrac{}{\Sigma; \Psi \vdash \tau_1 \searrow \ell}\ \text{Given}}{\Sigma; \Psi \vdash \tau_1 \searrow pc}$$

10. FG$^-$-snd:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\tau_1 \times \tau_2)^\ell \searrow pc}\ \text{IH}}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{By inversion} \qquad \dfrac{}{\Sigma; \Psi \vdash \tau_2 \searrow \ell}\ \text{Given}}{\Sigma; \Psi \vdash \tau_2 \searrow pc}$$

11. FG$^-$-inl:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{Given}}{\Sigma; \Psi \vdash (\tau_1 + \tau_2)^\ell \searrow pc}$$

12. FG$^-$-inr:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{Given}}{\Sigma; \Psi \vdash (\tau_1 + \tau_2)^\ell \searrow pc}$$

13. FG$^-$-case:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\tau_1 + \tau_2)^\ell \searrow pc}\ \text{IH1}}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{By inversion} \qquad \dfrac{}{\Sigma; \Psi \vdash \tau \searrow (pc \sqcup \ell)}\ \text{IH2}}{\Sigma; \Psi \vdash \tau \searrow pc}$$

14. FG$^-$-sub:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \tau' \searrow pc'}\ \text{IH} \qquad \dfrac{}{\Sigma; \Psi \vdash pc \sqsubseteq pc'}\ \text{Given}}{\Sigma; \Psi \vdash \tau' \searrow pc} \qquad \dfrac{}{\Sigma; \Psi \vdash \tau' \sqsubseteq \tau}\ \text{Given}}{\Sigma; \Psi \vdash \tau \searrow pc}\ \text{Lemma C.4}$$

15. FG$^-$-ref:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{Given}}{\Sigma; \Psi \vdash (\mathsf{ref}\ \tau)^\ell \searrow pc}$$

16. FG^{-}-deref:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\mathsf{ref}\ \tau)^{\ell} \searrow pc}\ \text{IH}}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{By inversion} \qquad \dfrac{}{\Sigma; \Psi \vdash \tau' \searrow \ell}\ \text{Given}}{\Sigma; \Psi \vdash \tau' \searrow pc}$$

17. FG^{-}-assign:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash (\mathsf{ref}\ \tau)^{\ell} \searrow pc}\ \text{IH}}{\Sigma; \Psi \vdash pc \sqsubseteq \ell}\ \text{By inversion}}{\Sigma; \Psi \vdash \mathsf{unit}^{\ell} \searrow pc}$$

□

Lemma C.3. $\forall \Sigma; \Psi, \tau, pc, \tau'.$
$\Sigma; \Psi \vdash \tau \sqcup pc \sqsubseteq \tau' \implies \Sigma; \Psi \vdash \tau' \searrow pc$

Proof. Say $\tau = \mathsf{A}^{\ell_g}$ and $\tau' = \mathsf{A}'^{\ell'_g}$
From Definition C.1, $\tau \sqcup pc = \mathsf{A}^{\ell_g \sqcup pc}$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{A}^{\ell_g \sqcup pc} \sqsubseteq \mathsf{A}'^{\ell'_g}}\ \text{Given}}{\Sigma; \Psi \vdash \ell_g \sqcup pc \sqsubseteq \ell'_g}\ \text{By inversion}}{\Sigma; \Psi \vdash pc \sqsubseteq \ell'_g}}{\Sigma; \Psi \vdash \mathsf{A}'^{\ell'_g} \searrow pc}\ \text{Definition of } \searrow$$

□

Lemma C.4. $\forall \Sigma; \Psi, \tau, pc, \tau'.$
$\Sigma; \Psi \vdash \tau' \searrow pc \wedge \Sigma; \Psi \vdash \tau' <: \tau \implies \Sigma; \Psi \vdash \tau \searrow pc$

Proof. Say $\tau = \mathsf{A}^{\ell_g}$ and $\tau' = \mathsf{A}'^{\ell'_g}$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\mathsf{A}'^{\ell'_g} \searrow pc}\ \text{Given}}{\Sigma; \Psi \vdash pc \sqsubseteq \ell'_g}\ \text{By inversion} \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{A}'^{\ell'_g} <: \mathsf{A}^{\ell_g}}\ \text{Given}}{\Sigma; \Psi \vdash \ell'_g \sqsubseteq \ell_g}\ \text{By inversion}}{\Sigma; \Psi \vdash pc \sqsubseteq \ell_g}}{\Sigma; \Psi \vdash \mathsf{A}^{\ell_g} \searrow pc}\ \text{Definition of } \searrow$$

□

D FG$^-$ $\rightsquigarrow$ CG

Definition D.1 (Translation of FG$^-$ types)**.**

$$
[\![\mathsf{A}_F]\!] \triangleq \begin{cases}
\mathsf{unit} & \mathsf{A}_F = \mathsf{unit} \\
\mathsf{b} & \mathsf{A}_F = \mathsf{b} \\
[\![\tau_{F1}]\!] \to \forall\alpha.(\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau_{F2}]\!] & \mathsf{A}_F = \tau_{F1} \xrightarrow{\ell_e} \tau_{F2} \\
[\![\tau_{F1}]\!] + [\![\tau_{F2}]\!] & \mathsf{A}_F = \tau_{F1} + \tau_{F2} \\
[\![\tau_{F1}]\!] \times [\![\tau_{F2}]\!] & \mathsf{A}_F = \tau_{F1} \times \tau_{F2} \\
\mathsf{ref}\ \ell_i\ [\![\mathsf{A}]\!] & \mathsf{A}_F = \mathsf{ref}\ \mathsf{A}^{\ell_i} \\
\forall\alpha.\forall\alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!] & \mathsf{A}_F = \forall\alpha.(\ell_e, \tau) \\
\forall\alpha.(\alpha \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau]\!] & \mathsf{A}_F = c \overset{\ell_e}{\Rightarrow} \tau
\end{cases}
$$

$$
[\![\tau_F]\!] \triangleq \left\{\ \mathsf{Labeled}\ \ell\ [\![\mathsf{A}_F]\!] \qquad \tau_F = \mathsf{A}_F^{\ell} \right.
$$

Definition D.2 (Translation of type environment)**.** Typing environments are translated as follows:
$[\![[]]\!] := []$
$[\![x : \tau, \Gamma']\!] := x : [\![\tau]\!], [\![\Gamma']\!]$

The translation of expressions is defined by the judgment $\boxed{\Sigma; \Psi; \Gamma \vdash_{pc} e_F : \tau_F \rightsquigarrow e_C}$. Its rules are shown below.

$$
\frac{\Sigma, \alpha; \Psi; \Gamma \vdash_{\ell_e} e : \tau \rightsquigarrow e_C \qquad \Sigma; \Psi \vdash pc \sqsubseteq \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\forall\alpha.(\ell_e, \tau))^{\ell} \rightsquigarrow \Lambda(\nu(\mathsf{ret}(\mathsf{Lb}_{\ell}(\Lambda e_C))))}\ \text{FI}
$$

$$
\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e : (\forall\alpha.(\ell_e, \tau))^{\ell} \rightsquigarrow e_C \qquad FV(\ell'') \in \Sigma \qquad \Sigma; \Psi \vdash pc \sqcup \ell \sqsubseteq \ell_e[\ell''/\alpha] \qquad \Sigma; \Psi \vdash \tau[\ell''/\alpha] \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e[] : \tau[\ell''/\alpha] \rightsquigarrow \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.b[][]\bullet)))))}\ \text{FE}
$$

$$
\frac{\Sigma; \Psi, c; \Gamma \vdash_{\ell_e} e : \tau \rightsquigarrow e_C \qquad \Sigma; \Psi \vdash pc \sqsubseteq \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} \nu e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell} \rightsquigarrow \Lambda(\nu(\mathsf{ret}(\mathsf{Lb}_{\ell}(e_C))))}\ \text{CI}
$$

$$
\frac{\Sigma; \Psi; \Gamma \vdash_{pc} \nu e : (c \overset{\ell_e}{\Rightarrow} \tau)^{\ell} \rightsquigarrow e_C \qquad \Sigma; \Psi \vdash c \qquad \Sigma; \Psi \vdash (pc \sqcup \ell) \sqsubseteq \ell_e \qquad \Sigma; \Psi \vdash \tau \searrow \ell}{\Sigma; \Psi; \Gamma \vdash_{pc} e\ \bullet : \tau \rightsquigarrow \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.b[]\bullet)))))}\ \text{CE}
$$

$$
\frac{\Sigma; \Psi \vdash \tau \sqcup pc \sqsubseteq \tau'}{\Sigma; \Psi; \Gamma, x : \tau \vdash_{pc} x : \tau' \rightsquigarrow \Lambda(\nu(\mathsf{ret}(x)))}\ \text{var}
$$

$$
\frac{\Sigma; \Psi; \Gamma, x : \tau_1 \vdash_{\ell_e} e : \tau_2 \rightsquigarrow e_C : \qquad \Sigma; \Psi \vdash pc \sqsubseteq \ell}{pc; \Gamma \vdash \lambda x.e : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell} \rightsquigarrow \Lambda(\nu(\mathsf{ret}(\mathsf{Lb}_{\ell}(\lambda x.e_C))))}\ \text{lam}
$$

$$
\frac{\Sigma; \Psi; \Gamma \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\ell_e} \tau_2)^{\ell} \rightsquigarrow e_{C1} \qquad \Sigma; \Psi; \Gamma \vdash_{pc} e_2 : \tau_1 \rightsquigarrow e_{C2} \qquad \Sigma; \Psi \vdash \tau_2 \searrow \ell \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell_e}{\Sigma; \Psi; \Gamma \vdash_{pc} e_1\ e_2 : \tau_2 \rightsquigarrow e_t}\ \text{app}
$$

where
$e_t = \Lambda(\nu(\mathsf{toLabeled}(\mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{bind}(e_{C2}[]\bullet, b.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b)[]\bullet)))))))$

$$\frac{\Sigma;\Psi;\Gamma\vdash_{pc} e_1:\tau_1 \rightsquigarrow e_{C1} \qquad \Sigma;\Psi;\Gamma\vdash_{pc} e_2:\tau_2 \rightsquigarrow e_{C2} \qquad \Sigma;\Psi\vdash pc\sqsubseteq \ell}{\Sigma;\Psi;\Gamma\vdash_{pc} (e_1,e_2):(\tau_1\times\tau_2)^\ell \rightsquigarrow \Lambda(\nu(\mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{bind}(e_{C2}[]\bullet, b.\mathsf{ret}(\mathsf{Lb}_\ell(a,b))))))}\ \text{prod}$$

$$\frac{\Sigma;\Psi;\Gamma\vdash_{pc} e:(\tau_1\times\tau_2)^\ell \rightsquigarrow e_C \qquad \Sigma;\Psi\vdash \tau_1 \searrow \ell}{\Sigma;\Psi;\Gamma\vdash_{pc} \mathsf{fst}(e):\tau_1 \rightsquigarrow \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{fst}\ b))))))}\ \text{fst}$$

$$\frac{\Sigma;\Psi;\Gamma\vdash_{pc} e:(\tau_1\times\tau_2)^\ell \rightsquigarrow e_C \qquad \Sigma;\Psi\vdash \tau_2 \searrow \ell}{\Sigma;\Psi;\Gamma\vdash \mathsf{snd}(e):\tau_1 \rightsquigarrow \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{snd}\ b))))))}\ \text{snd}$$

$$\frac{\Sigma;\Psi;\Gamma\vdash_{pc} e:\tau_1 \rightsquigarrow e_C \qquad \Sigma;\Psi\vdash pc\sqsubseteq \ell}{\Sigma;\Psi;\Gamma\vdash_{pc} \mathsf{inl}(e):(\tau_1+\tau_2)^\ell \rightsquigarrow \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{ret}(\mathsf{Lb}_\ell(\mathsf{inl}(a))))))}\ \text{inl}$$

$$\frac{\Sigma;\Psi;\Gamma\vdash_{pc} e:\tau_2 \rightsquigarrow e_C \qquad \Sigma;\Psi\vdash pc\sqsubseteq \ell}{\Sigma;\Psi;\Gamma\vdash_{pc} \mathsf{inr}(e):(\tau_1+\tau_2)^\ell \rightsquigarrow \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{ret}(\mathsf{Lb}_\ell(\mathsf{inr}(a))))))}\ \text{inr}$$

$$\frac{\Sigma;\Psi;\Gamma\vdash_{pc} e_1:(\tau_1+\tau_2)^\ell \rightsquigarrow e_{C1} \qquad \Sigma;\Psi;\Gamma,x:\tau_1\vdash_{pc\sqcup\ell} e_2:\tau \rightsquigarrow e_{C2} \qquad \Sigma;\Psi;\Gamma,y:\tau_2\vdash_{pc\sqcup\ell} e_3:\tau \rightsquigarrow e_{C3}}{\Sigma;\Psi;\Gamma\vdash_{pc} \mathsf{case}(e_1,x.e_2,y.e_3):\tau \rightsquigarrow e_t}\ \text{case}$$

where
$e_t = \Lambda(\nu(\mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{case}\ b, x.e_{C2}[]\bullet, y.e_{C3}[]\bullet))))))$

$$\frac{\Sigma;\Psi;\Gamma\vdash_{pc'} e:\tau' \rightsquigarrow e_C \qquad \Sigma;\Psi\vdash pc\sqsubseteq pc' \qquad \Sigma;\Psi\vdash \tau' <: \tau}{\Sigma;\Psi;\Gamma\vdash_{pc} e:\tau \rightsquigarrow \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{ret}(a))))}\ \text{sub}$$

$$\frac{\Sigma;\Psi;\Gamma\vdash_{pc} e:\mathsf{A}^{\ell_i} \rightsquigarrow e_C \qquad \Sigma;\Psi\vdash pc\sqsubseteq \ell_o}{\Sigma;\Psi;\Gamma\vdash_{pc} \mathsf{new}\ \ e:(\mathsf{ref}\ \mathsf{A}^{\ell_i})^{\ell_o} \rightsquigarrow \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{new}\ (a)))))}\ \text{ref}$$

$$\frac{\Sigma;\Psi;\Gamma\vdash_{pc} e:(\mathsf{ref}\ \mathsf{A}^{\ell_i})^{\ell_o} \rightsquigarrow e_C \qquad \Sigma;\Psi\vdash \mathsf{A}^{\ell_i} <: \mathsf{A}'^{\ell_i'} \qquad \Sigma;\Psi\vdash \mathsf{A}'^{\ell_i'} \searrow \ell_o}{\Sigma;\Psi;\Gamma\vdash !e:\mathsf{A}^{\ell_i} \rightsquigarrow \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))))}\ \text{deref}$$

$$\frac{\Sigma;\Psi;\Gamma\vdash_{pc} e_1:(\mathsf{ref}\ \mathsf{A}^{\ell_i})^{\ell_o} \rightsquigarrow e_{C1} \qquad \Sigma;\Psi;\Gamma\vdash_{pc} e_2:\mathsf{A}^{\ell_i} \rightsquigarrow e_{C2} \qquad \Sigma;\Psi\vdash \mathsf{A}^{\ell_i} \searrow \ell_o}{\Sigma;\Psi;\Gamma\vdash_{pc} e_1 := e_2:\mathsf{unit}^{\ell_o} \rightsquigarrow e_t}\ \text{assign}$$

where
$e_t = \Lambda(\nu(\mathsf{toLabeled}(\mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{bind}(e_{C2}[]\bullet, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b))))))$

Theorem D.3 (Type soundness, $\mathrm{FG}^- \rightsquigarrow \mathrm{CG}$)**.** $\forall pc, \Sigma, \Psi, \Gamma, e, \tau.$
$\Sigma;\Psi;\Gamma\vdash_{pc} e:\tau$ *is a valid typing derivation in FG*$^-$ $\implies$
$\exists e_C.$
$\Sigma;\Psi;\Gamma\vdash_{pc} e:\tau \rightsquigarrow e_C\ \wedge$
$\Sigma;\Psi;[\![\Gamma]\!]\vdash e_C : \forall\alpha.(\alpha\sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau]\!]$ *is a valid typing derivation in CG*

Proof. Proof by induction on the $\rightsquigarrow$ relation

1. FI:

$T_1 = \forall\alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ (\forall\alpha.\forall\alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]))$

$T_{1.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ (\forall\alpha.\forall\alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]))$

$T_{1.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ (\forall\alpha.\forall\alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]))$

$T_2 = \forall\alpha_1.(\alpha_1 \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ \ [\![\tau]\!]$

$T_{2.1} = \forall\alpha.\forall\alpha_1.(\alpha_1 \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ \ [\![\tau]\!]$

$T_{2.2} = (\mathsf{Labeled}\ \ell\ (\forall\alpha.\forall\alpha_1.(\alpha_1 \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ \ [\![\tau]\!]))$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi;[\![\Gamma]\!] \vdash e_C : T_2}\text{IH} \qquad \alpha \notin T_2}{\Sigma,\alpha_2,\alpha;\Psi,(\alpha_2 \sqsubseteq pc);[\![\Gamma]\!] \vdash \Lambda e_C : T_{2.1}}\text{CG-FI, Weakening}}{\Sigma,\alpha_2;\Psi,(\alpha_2 \sqsubseteq pc);[\![\Gamma]\!] \vdash \mathsf{Lb}_\ell(\Lambda e_C) : T_{2.2}}\text{CG-label}}{\Sigma,\alpha_2;\Psi,(\alpha_2 \sqsubseteq pc);[\![\Gamma]\!] \vdash \mathsf{ret}(\mathsf{Lb}_\ell(\Lambda e_C)) : T_{1.2}}\text{CG-ret}}{\Sigma;\alpha_2;\Psi;[\![\Gamma]\!] \vdash \nu(\mathsf{ret}(\mathsf{Lb}_\ell(\Lambda e_C))) : T_{1.1}}\text{CG-CI}}{\Sigma;\Psi;[\![\Gamma]\!] \vdash \Lambda(\nu(\mathsf{ret}(\mathsf{Lb}_\ell(\Lambda e_C)))) : T_1}\text{CG-FI}$$

2. FE:

$T_1 = \forall\alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \ [\![\tau[\ell''/\alpha]]\!]$

$T_{1.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \ [\![\tau[\ell''/\alpha]]\!]$

$T_{1.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ \ [\![\tau[\ell''/\alpha]]\!]$

$T_2 = \forall\alpha_1.(\alpha_1 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ (\mathsf{Labeled}\ \ell\ (\forall\alpha.\forall\alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]))$

$T_{2.1} = (\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ (\mathsf{Labeled}\ \ell\ (\forall\alpha.\forall\alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]))$

$T_{2.2} = \mathsf{CG}\ \alpha_3\ \alpha_3\ (\mathsf{Labeled}\ \ell\ (\forall\alpha.\forall\alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]))$

$T_{2.3} = (\mathsf{Labeled}\ \ell\ (\forall\alpha.\forall\alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]))$

$T_3 = \mathsf{CG}\ \alpha_2\ \alpha_2 \sqcup \ell\ ((\forall\alpha.\forall\alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]))$

$T_{3.1} = \forall\alpha.\forall\alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]$

$T_{3.2} = \forall\alpha'.\alpha' \sqsubseteq \ell_e[\ell''/\alpha] \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]\,[\ell''/\alpha]$

$T_{3.3} = (\alpha_2 \sqcup \ell) \sqsubseteq \ell_e[\ell''/\alpha] \Rightarrow \mathsf{CG}\ (\alpha_2 \sqcup \ell)\ (\alpha_2 \sqcup \ell)\ \ [\![\tau]\!]\,[\ell''/\alpha]$

$T_{3.4} = \mathsf{CG}\ (\alpha_2 \sqcup \ell)\ (\alpha_2 \sqcup \ell)\ \ [\![\tau]\!]\,[\ell''/\alpha]$

$T_{3.5} = \mathsf{CG}\ (\alpha_2)\ (\alpha_2 \sqcup \ell)\ \ [\![\tau]\!]\,[\ell''/\alpha]$

$T_{3.6} = \mathsf{CG}\ (\alpha_2)\ (\alpha_2 \sqcup \ell)\ \mathsf{Labeled}\ \ell \sqcup \ell_x\ \mathsf{A}[\ell''/\alpha]$

$T_{3.7} = \mathsf{CG}\ (\alpha_2)\ (\alpha_2)\ \mathsf{Labeled}\ \alpha_2 \sqcup \ell \sqcup \ell_x\ \mathsf{A}[\ell''/\alpha]$

$T_{3.8} = \mathsf{CG}\ (\alpha_2)\ (\alpha_2)\ \ [\![\tau]\!]\,[\ell''/\alpha]$

P6:

$$\dfrac{}{pc \sqsubseteq \ell}\text{Lemma C.2}$$

P5:

$$\dfrac{\dfrac{\dfrac{}{\Sigma,\alpha_2;\Psi,(\alpha_2 \sqsubseteq pc);[\![\Gamma]\!],a : T_{2.3}, b : T_{3.1} \vdash b : T_{3.1}}\text{CG-var}}{\Sigma,\alpha_2;\Psi,(\alpha_2 \sqsubseteq pc);[\![\Gamma]\!],a : T_{2.3}, b : T_{3.1} \vdash b[] : T_{3.2}}\text{CG-FE}}{\Sigma,\alpha_2;\Psi,(\alpha_2 \sqsubseteq pc);[\![\Gamma]\!],a : T_{2.3}, b : T_{3.1} \vdash b[][] : T_{3.3}}\text{CG-FE}$$

P4:

$$\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash a : T_{2.3}}\ \text{CG-var}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash \mathsf{unlabel}\ a : T_3}\ \text{CG-unlabel}$$

P3:

$$\dfrac{P4 \qquad \dfrac{P5}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3}, b : T_{3.1} \vdash b[\,][\,]\bullet : T_{3.4}}\ \text{CG-FE}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.b[\,][\,]\bullet) : T_{3.5}}\ \text{CG-bind}$$

P2:

$$\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C : T_2}\ \text{IH}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C[\,] : T_{2.1}}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C[\,]\bullet : T_{2.2}}$$

P1:

$$\dfrac{\dfrac{P2 \qquad \dfrac{\dfrac{\dfrac{P3}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.b[\,][\,]\bullet) : T_{3.6}}\ \text{Lemma D.5}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.b[\,][\,]\bullet)) : T_{3.7}}\ \text{CG-toLabeled} \qquad P6}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.b[\,][\,]\bullet)) : T_{3.8}}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{bind}(e_C[\,]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.b[\,][\,]\bullet))) : T_{3.8}}\ \text{CG-bind}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{bind}(e_C[\,]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.b[\,][\,]\bullet))) : T_{1.2}}\ \text{Lemma D.8}$$

Main derivation:

$$\dfrac{\dfrac{P1}{\Sigma, \alpha_2; \Psi; [\![\Gamma]\!] \vdash \nu(\mathsf{bind}(e_C[\,]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.b[\,][\,]\bullet)))) : T_{1.1}}\ \text{CG-CI}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash \Lambda(\nu(\mathsf{bind}(e_C[\,]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.b[\,][\,]\bullet))))) : T_1}\ \text{CG-FI}$$

3. CI:

$T_1 = \forall \alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ \forall \alpha_3.(\alpha_3 \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau]\!])$

$T_{1.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ \forall \alpha_3.(\alpha_3 \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau]\!])$

$T_{1.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ \forall \alpha_3.(\alpha_3 \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau]\!])$

$T_{1.3} = \mathsf{Labeled}\ \ell\ \forall \alpha_3.(\alpha_3 \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau]\!]$

$T_2 = \forall \alpha_1.(\alpha_1 \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ [\![\tau]\!]$

$T_{2.1} = \forall \alpha_1.(\alpha_1 \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ [\![\tau]\!]$

Main derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C : T_2}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C : T_{2.1}}\ \text{Weakening}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{Lb}_\ell(e_C) : T_{1.3}}\ \text{CG-label}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{ret}(\mathsf{Lb}_\ell(e_C)) : T_{1.2}}\ \text{CG-ret}}{\Sigma, \alpha_2; \Psi; [\![\Gamma]\!] \vdash \nu(\mathsf{ret}(\mathsf{Lb}_\ell(e_C))) : T_{1.1}}\ \text{CG-CI}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash \Lambda(\nu(\mathsf{ret}(\mathsf{Lb}_\ell(e_C)))) : T_1}\ \text{CG-FI}$$

4. CE:

$T_1 = \forall\alpha_3.(\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ \llbracket\tau\rrbracket$

$T_{1.1} = (\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ \llbracket\tau\rrbracket$

$T_{1.2} = \mathsf{CG}\ \alpha_3\ \alpha_3\ \llbracket\tau\rrbracket$

$T_2 = \forall\alpha_1.(\alpha_1 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ (\mathsf{Labeled}\ \ell\ \forall\alpha_2.(\alpha_2 \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau\rrbracket)$

$T_{2.1} = (\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ (\mathsf{Labeled}\ \ell\ \forall\alpha_2.(\alpha_2 \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau\rrbracket)$

$T_{2.2} = \mathsf{CG}\ \alpha_3\ \alpha_3\ (\mathsf{Labeled}\ \ell\ \forall\alpha_2.(\alpha_2 \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau\rrbracket)$

$T_{2.3} = (\mathsf{Labeled}\ \ell\ \forall\alpha_2.(\alpha_2 \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau\rrbracket)$

$T_{2.4} = \mathsf{CG}\ \alpha_3\ \alpha_3 \sqcup \ell\ (\forall\alpha_2.(\alpha_2 \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau\rrbracket)$

$T_{2.5} = (\forall\alpha_2.(\alpha_2 \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau\rrbracket)$

$T_{2.6} = (((\alpha_3 \sqcup \ell) \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ (\alpha_3 \sqcup \ell)\ (\alpha_3 \sqcup \ell)\ \llbracket\tau\rrbracket)$

$T_{2.7} = (\mathsf{CG}\ (\alpha_3 \sqcup \ell)\ (\alpha_3 \sqcup \ell)\ \llbracket\tau\rrbracket)$

$T_{2.8} = (\mathsf{CG}\ (\alpha_3)\ (\alpha_3 \sqcup \ell)\ \llbracket\tau\rrbracket)$

$T_{2.9} = \mathsf{CG}\ (\alpha_3)\ (\alpha_3 \sqcup \ell)\ \mathsf{Labeled}\ \ell \sqcup \ell_x\ A$

$T_3 = \mathsf{CG}\ (\alpha_3)\ (\alpha_3)\ \mathsf{Labeled}\ \alpha_3 \sqcup \ell \sqcup \ell_x\ A$

$T_{3.1} = \mathsf{CG}\ (\alpha_3)\ (\alpha_3)\ \mathsf{Labeled}\ \ell \sqcup \ell_x\ A$

P4:

$$\dfrac{\dfrac{}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc) \vdash c}\ \text{Given, Weakening} \qquad \dfrac{\dfrac{}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc) \vdash (pc \sqcup \ell \sqsubseteq \ell_e)}\ \text{Given, Weakening}}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc) \vdash (\alpha_3 \sqcup \ell \sqsubseteq \ell_e)} \qquad \dfrac{\dfrac{}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc);\llbracket\Gamma\rrbracket, a : T_{2.3}, b : T_{2.5} \vdash b : T_{2.5}}\ \text{CG-var}}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc);\llbracket\Gamma\rrbracket, a : T_{2.3}, b : T_{2.5} \vdash b[] : T_{2.6}}\ \text{CG-FE}}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc);\llbracket\Gamma\rrbracket, a : T_{2.3}, b : T_{2.5} \vdash b[]\bullet : T_{2.7}}\ \text{CG-CE}$$

P3:

$$\dfrac{\dfrac{\dfrac{}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc);\llbracket\Gamma\rrbracket, a : T_{2.3} \vdash a : T_{2.3}}\ \text{CG-var}}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc);\llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{unlabel}\ a : T_{2.4}}\ \text{CG-unlabel} \qquad P4}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc);\llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.b[]\bullet)) : T_{2.8}}\ \text{CG-bind}$$

P2:

$$\dfrac{\dfrac{}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc);\llbracket\Gamma\rrbracket \vdash e_C : T_2}\ \text{IH}}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc);\llbracket\Gamma\rrbracket \vdash e_C[] : T_{2.1}}\ \text{CG-FE}$$

P1:

$$\dfrac{\dfrac{P2}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc);\llbracket\Gamma\rrbracket \vdash e_C[]\bullet : T_{2.2}}\ \text{CG-CE} \qquad \dfrac{\dfrac{\dfrac{P3}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc);\llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.b[]\bullet) : T_{2.9}}\ \text{Lemma D.5}}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc);\llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.b[]\bullet)) : T_3}\ \text{CG-tolabeled} \qquad \dfrac{}{pc \sqsubseteq \ell}\ \text{Lemma C.2}}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc);\llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.b[]\bullet)) : T_{3.1}}}{\Sigma,\alpha_3;\Psi,(\alpha_3 \sqsubseteq pc);\llbracket\Gamma\rrbracket \vdash \mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.b[]\bullet))) : T_{1.2}}\ \text{CG-bind, Lemma D.5}$$

Main derivation:

$$\dfrac{\dfrac{P1}{\Sigma, \alpha_3; \Psi; [\![\Gamma]\!] \vdash \nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.b[]\bullet)))) : T_{1.1}}\ \text{CG-CI}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.b[]\bullet))))) : T_1}\ \text{CG-FI}$$

5. var:

$T_3 = \forall \alpha.(\alpha \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau']\!]$

$T_2 = (\alpha \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau']\!]$

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha; \Psi; [\![\Gamma]\!], x : [\![\tau]\!] \vdash x : [\![\tau]\!]}\ \text{CG-var} \qquad \dfrac{\dfrac{\dfrac{}{\tau \sqcup pc \sqsubseteq \tau'}\ \text{Given}}{\tau \sqsubseteq \tau'}}{[\![\tau]\!] <: [\![\tau']\!]}\ \text{Lemma D.4}}{\Sigma, \alpha; \Psi; [\![\Gamma]\!], x : [\![\tau]\!] \vdash \mathsf{ret}(x) : \mathsf{CG}\ \alpha\ \alpha\ [\![\tau']\!]}\ \text{CG-ret, CG-sub}}{\Sigma, \alpha; \Psi; [\![\Gamma]\!], x : [\![\tau]\!] \vdash \nu(\mathsf{ret}(x)) : T_2}\ \text{CG-CI}}{\Sigma; \Psi; [\![\Gamma]\!], x : [\![\tau]\!] \vdash \Lambda(\nu(\mathsf{ret}(x))) : T_3}\ \text{CG-FI}$$

6. lam:

$T_1 = \forall \alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] \to \forall \alpha_1.(\alpha_1 \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ [\![\tau_2]\!]))$

$T_2 = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] \to \forall \alpha_1.(\alpha_1 \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ [\![\tau_2]\!]))$

$T_3 = \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] \to \forall \alpha_1.(\alpha_1 \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ [\![\tau_2]\!]))$

$T_{3.1} = \mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] \to \forall \alpha_1.(\alpha_1 \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ [\![\tau_2]\!])$

$T_4 = ([\![\tau_1]\!] \to \forall \alpha_1.(\alpha_1 \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ [\![\tau_2]\!])$

$T_5 = (\forall \alpha_1.(\alpha_1 \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ [\![\tau_2]\!])$

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], x : [\![\tau_1]\!] \vdash e_C : T_5}\ \text{IH}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \lambda x.e_C : T_4}\ \text{CG-lam}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{Lb}_\ell(\lambda x.e_C) : T_{3.1}}\ \text{CG-label}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{ret}(\mathsf{Lb}_\ell(\lambda x.e_C)) : T_3}\ \text{CG-ret}}{\Sigma, \alpha_2; \Psi; [\![\Gamma]\!] \vdash \nu(\mathsf{ret}(\mathsf{Lb}_\ell(\lambda x.e_C))) : T_2}\ \text{CG-CI}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \Lambda(\nu(\mathsf{ret}(\mathsf{Lb}_\ell(\lambda x.e_C)))) : T_1}\ \text{CG-FI}$$

7. app:

$T_1 = \forall \alpha_3.(\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau_2]\!]$

$T_2 = (\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau_2]\!]$

$T_3 = \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau_2]\!]$

$T_4 = \mathsf{CG}\ \alpha_3\ \alpha_3 \sqcup \ell\ [\![\mathsf{Labeled}\ \ell \sqcup \ell_x\ \mathsf{A}]\!]$

$T_5 = \mathsf{CG}\ \alpha_3\ \alpha_3\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] \to \forall \alpha.(\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_2]\!]))$

$T_6 = (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] \to \forall \alpha.(\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_2]\!]))$

$T_{6.1} = \mathsf{CG}\ \alpha_3\ \alpha_3 \sqcup \ell\ ([\![\tau_1]\!] \to \forall \alpha.(\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_2]\!])$

$T_{6.2} = ([\![\tau_1]\!] \to \forall \alpha.(\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_2]\!])$

$T_{6.3} = (\forall \alpha.(\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_2]\!])$

$T_{6.4} = (((\alpha_3 \sqcup \ell) \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ (\alpha_3 \sqcup \ell)\ (\alpha_3 \sqcup \ell)\ [\![\tau_2]\!])$
$T_{6.5} = (\mathsf{CG}\ (\alpha_3 \sqcup \ell)\ (\alpha_3 \sqcup \ell)\ [\![\tau_2]\!])$
$T_{6.6} = \mathsf{CG}\ (\alpha_3)\ (\alpha_3 \sqcup \ell)\ (\mathsf{Labeled}\ (\ell \sqcup \ell_x)\ \mathsf{A}_2)$
$T_{6.7} = \mathsf{CG}\ (\alpha_3)\ (\alpha_3)\ (\mathsf{Labeled}\ (\alpha_3 \sqcup \ell \sqcup \ell_x)\ \mathsf{A}_2)$
$T_{6.8} = \mathsf{CG}\ (\alpha_3)\ (\alpha_3)\ [\![\tau_2]\!]$
$T_7 = \forall \alpha_1.(\alpha_1 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] \rightarrow \forall \alpha.(\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_2]\!]))$
$T_8 = (\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] \rightarrow \forall \alpha.(\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_2]\!]))$
$T_9 = \forall \alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ [\![\tau_1]\!]$
$T_{10} = (\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau_1]\!]$
$T_{11} = \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau_1]\!]$

P4:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : T_6, b : [\![\tau_1]\!] \vdash \mathsf{unlabel}\ a : T_{6.1}}\ \text{CG-unlabel}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : T_6, b : [\![\tau_1]\!], c : T_{6.2} \vdash (c\ b) : T_{6.3}}\ \text{CG-app}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : T_6, b : [\![\tau_1]\!], c : T_{6.2} \vdash (c\ b)[] : T_{6.4}}\ \text{CG-FE} \quad \dfrac{\dfrac{}{\alpha_3 \sqsubseteq pc \sqsubseteq \ell}\ \text{Given and Lemma C.2} \quad \dfrac{}{\ell \sqsubseteq \ell_e}\ \text{Given}}{\alpha_3 \sqcup \ell \sqsubseteq \ell_e}}{\dfrac{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : T_6, b : [\![\tau_1]\!], c : T_{6.2} \vdash (c\ b)[]\bullet : T_{6.5}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : T_6, b : [\![\tau_1]\!] \vdash \mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b)[]\bullet) : T_{6.6}}\ \text{CG-bind, Lemma D.5}}\ \text{CG-CE}$$

P3:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : T_6 \vdash e_{C2} : T_9}\ \text{IH2}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : T_6 \vdash e_{C2}[] : T_{10}}\ \text{CG-FE}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : T_6 \vdash e_{C2}[]\bullet : T_{11}}\ \text{CG-CE} \quad \dfrac{\dfrac{P4}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : T_6, b : [\![\tau_1]\!] \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b)[]\bullet)) : T_{6.7}}\ \text{CG-tolabeled}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : T_6, b : [\![\tau_1]\!] \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b)[]\bullet)) : T_{6.8}}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : T_6 \vdash \mathsf{bind}(e_{C2}[]\bullet, b.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b)[]\bullet))) : T_{6.8}}\ \text{CG-bind}$$

P2:

$$\dfrac{\dfrac{}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_{C1} : T_7}\ \text{IH1}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_{C1}[] : T_8}\ \text{CG-FE}$$

P1:

$$\dfrac{\dfrac{P2}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_{C1}[]\bullet : T_5}\ \text{CG-CE} \qquad P3}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{bind}(e_{C2}[]\bullet, b.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b)[]\bullet)))) : T_{6.8}}\ \text{CG-bind}$$

Main derivation:

$$\dfrac{\dfrac{P1}{\Sigma, \alpha_3; \Psi; [\![\Gamma]\!] \vdash \nu(\mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{bind}(e_{C2}[]\bullet, b.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b)[]\bullet))))) : T_2}\ \text{CG-CI}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash \Lambda(\nu(\mathsf{toLabeled}(\mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{bind}(e_{C2}[]\bullet, b.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, c.(c\ b)[]\bullet))))))) : T_1}\ \text{CG-FI}$$

8. prod:

$T_1 = \forall \alpha_3.(\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ (\mathsf{Labeled}\ \ell\ [\![\tau_1]\!] \times [\![\tau_2]\!])$

$T_2 = (\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ (\mathsf{Labeled}\ \ell\ [\![\tau_1]\!] \times [\![\tau_2]\!])$

$T_3 = \mathsf{CG}\ \alpha_3\ \alpha_3\ (\mathsf{Labeled}\ \ell\ [\![\tau_1]\!] \times [\![\tau_2]\!])$

$T_{3.1} = \mathsf{Labeled}\ \ell\ [\![\tau_1]\!] \times [\![\tau_2]\!]$

$T_4 = \forall \alpha_1.(\alpha_1 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ [\![\tau_1]\!]$

$T_{4.1} = (\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau_1]\!]$

$T_{4.2} = \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau_1]\!]$

$T_5 = \forall \alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ [\![\tau_2]\!]$

$T_{5.1} = (\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau_2]\!]$

$T_{5.2} = \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau_2]\!]$

P3:

$$\dfrac{\dfrac{}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau_1]\!] \vdash e_{C2} : T_5}\ \text{IH2}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau_1]\!] \vdash e_{C2}[] : T_{5.1}}\ \text{CG-FE}$$

P2:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{P3}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau_1]\!] \vdash e_{C2}[]\bullet : T_{5.2}}\ \text{CG-CE}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau_1]\!], b : [\![\tau_2]\!] \vdash (a, b) : ([\![\tau_1]\!] \times [\![\tau_2]\!])}\ \text{CG-prod}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau_1]\!], b : [\![\tau_2]\!] \vdash \mathsf{Lb}_\ell(a, b) : T_{3.1}}\ \text{CG-label}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau_1]\!], b : [\![\tau_2]\!] \vdash \mathsf{ret}(\mathsf{Lb}_\ell(a, b)) : T_3}\ \text{CG-ret}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau_1]\!] \vdash \mathsf{bind}(e_{C2}[]\bullet, b.\mathsf{ret}(\mathsf{Lb}_\ell(a, b))) : T_3}\ \text{CG-bind}$$

P1:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_{C1} : T_4}\ \text{IH1}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_{C1}[] : T_{4.1}}\ \text{CG-FE}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_{C1}[]\bullet : T_{4.2}}\ \text{CG-CE} \qquad P2}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{bind}(e_{C2}[]\bullet, b.\mathsf{ret}(\mathsf{Lb}_\ell(a, b)))) : T_3}\ \text{CG-bind}$$

Main derivation:

$$\dfrac{\dfrac{P1}{\Sigma, \alpha_3; \Psi; [\![\Gamma]\!] \vdash \nu(\mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{bind}(e_{C2}[]\bullet, b.\mathsf{ret}(\mathsf{Lb}_\ell(a, b))))) : T_2}\ \text{CG-CI}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash \Lambda(\nu(\mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{bind}(e_{C2}[]\bullet, b.\mathsf{ret}(\mathsf{Lb}_\ell(a, b)))))) : T_1}\ \text{CG-FI}$$

9. fst:

$T_1 = \forall \alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ [\![\tau_1]\!]$

$T_{1.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ [\![\tau_1]\!]$

$T_{1.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ [\![\tau_1]\!]$

$T_2 = \forall \alpha_1.(\alpha_1 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ (\mathsf{Labeled}\ \ell\ [\![\tau_1]\!] \times [\![\tau_2]\!])$

$T_{2.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ \llbracket\tau_1\rrbracket \times \llbracket\tau_2\rrbracket)$

$T_{2.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ \llbracket\tau_1\rrbracket \times \llbracket\tau_2\rrbracket)$

$T_{2.3} = \mathsf{Labeled}\ \ell\ \llbracket\tau_1\rrbracket \times \llbracket\tau_2\rrbracket$

$T_3 = \mathsf{CG}\ \alpha_2\ (\alpha_2 \sqcup \ell)\ \llbracket\tau_1\rrbracket \times \llbracket\tau_2\rrbracket$

$T_{3.1} = \llbracket\tau_1\rrbracket \times \llbracket\tau_2\rrbracket$

$T_4 = \mathsf{CG}\ (\alpha_2 \sqcup \ell)\ (\alpha_2 \sqcup \ell)\ \llbracket\tau_1\rrbracket$

$T_5 = \mathsf{CG}\ (\alpha_2)\ (\alpha_2 \sqcup \ell)\ \llbracket\tau_1\rrbracket$

$T_6 = \mathsf{CG}\ (\alpha_2)\ (\alpha_2 \sqcup \ell)\ (\mathsf{Labeled}\ \ell \sqcup \ell_x\ \mathsf{A})$

$T_7 = \mathsf{CG}\ (\alpha_2)\ (\alpha_2)\ (\mathsf{Labeled}\ \alpha_2 \sqcup \ell \sqcup \ell_x\ \mathsf{A})$

P3:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{unlabel}\ a : T_3}\ \text{CG-unlabel}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3}, b : T_{3.1} \vdash \mathsf{fst}\ b : \llbracket\tau_1\rrbracket}\ \text{CG-fst}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3}, b : T_{3.1} \vdash \mathsf{ret}(\mathsf{fst}\ b) : T_4}\ \text{CG-ret}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{fst}\ b)) : T_5}\ \text{CG-bind}$$

P2:

$$\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash e_C : T_2}\ \text{IH}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash e_C[] : T_{2.1}}\ \text{CG-FE}$$

P1.1:

$$\dfrac{\dfrac{\dfrac{P3}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{fst}\ b)) : T_6}\ \text{Lemma D.5}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{fst}\ b))) : T_7}\ \text{CG-tolabeled} \quad \dfrac{}{pc \sqsubseteq \ell}\ \text{Lemma C.2}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{fst}\ b))) : T_{1.2}}\ \text{Lemma D.5}$$

P1:

$$\dfrac{\dfrac{P2}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash e_C[]\bullet : T_{2.2}}\ \text{CG-CE} \qquad P1.1}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash \mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{fst}\ b)))) : T_{1.2}}\ \text{CG-bind}$$

Main derivation:

$$\dfrac{\dfrac{P1}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash \nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{fst}\ b))))) : T_{1.1}}\ \text{CG-CI}}{\Sigma; \Psi; \llbracket\Gamma\rrbracket \vdash \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{fst}\ b)))))) : T_1}\ \text{CG-FI}$$

10. snd:

$T_1 = \forall\alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau_2\rrbracket$

$T_{1.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau_2\rrbracket$

$T_{1.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau_2\rrbracket$

$T_2 = \forall\alpha_1.(\alpha_1 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ (\mathsf{Labeled}\ \ell\ \llbracket\tau_1\rrbracket \times \llbracket\tau_2\rrbracket)$

$T_{2.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ [\![\tau_1]\!] \times [\![\tau_2]\!])$

$T_{2.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ [\![\tau_1]\!] \times [\![\tau_2]\!])$

$T_{2.3} = \mathsf{Labeled}\ \ell\ [\![\tau_1]\!] \times [\![\tau_2]\!]$

$T_3 = \mathsf{CG}\ \alpha_2\ (\alpha_2 \sqcup \ell)\ [\![\tau_1]\!] \times [\![\tau_2]\!]$

$T_{3.1} = [\![\tau_1]\!] \times [\![\tau_2]\!]$

$T_4 = \mathsf{CG}\ (\alpha_2 \sqcup \ell)\ (\alpha_2 \sqcup \ell)\ [\![\tau_2]\!]$

$T_5 = \mathsf{CG}\ (\alpha_2)\ (\alpha_2 \sqcup \ell)\ [\![\tau_2]\!]$

$T_6 = \mathsf{CG}\ (\alpha_2)\ (\alpha_2 \sqcup \ell)\ (\mathsf{Labeled}\ \ell \sqcup \ell_x\ \mathsf{A})$

$T_7 = \mathsf{CG}\ (\alpha_2)\ (\alpha_2)\ (\mathsf{Labeled}\ \alpha_2 \sqcup \ell \sqcup \ell_x\ \mathsf{A})$

P3:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash \mathsf{unlabel}\ a : T_3}\ \text{CG-unlabel}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3}, b : T_{3.1} \vdash \mathsf{snd}\ b : [\![\tau_2]\!]}\ \text{CG-snd}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3}, b : T_{3.1} \vdash \mathsf{ret}(\mathsf{snd}\ b) : T_4}\ \text{CG-ret}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{snd}\ b)) : T_5}\ \text{CG-bind}$$

P2:

$$\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C : T_2}\ \text{IH}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C[] : T_{2.1}}\ \text{CG-FE}$$

P1.1:

$$\dfrac{\begin{array}{c}\dfrac{\dfrac{P3}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{snd}\ b)) : T_6}\ \text{Lemma D.5}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{snd}\ b))) : T_7}\ \text{CG-tolabeled} \\ \dfrac{}{pc \sqsubseteq \ell}\ \text{Lemma C.2}\end{array}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{snd}\ b))) : T_{1.2}}\ \text{Lemma D.5}$$

P1:

$$\dfrac{\dfrac{P2}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C[]\bullet : T_{2.2}}\ \text{CG-CE} \qquad P1.1}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{snd}\ b)))) : T_{1.2}}\ \text{CG-bind}$$

Main derivation:

$$\dfrac{\dfrac{P1}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{snd}\ b))))) : T_{1.1}}\ \text{CG-CI}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{snd}\ b)))))) : T_1}\ \text{CG-FI}$$

11. inl:

$T_1 = \forall \alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] + [\![\tau_2]\!]))$

$T_{1.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] + [\![\tau_2]\!]))$

$T_{1.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] + [\![\tau_2]\!]))$

$T_{1.3} = \mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] + [\![\tau_2]\!])$

$T_2 = \forall \alpha_1.(\alpha_1 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ \ [\![\tau_1]\!]$

$T_{2.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \ [\![\tau_1]\!]$

$T_{2.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ \ [\![\tau_1]\!]$

P3:

$$\frac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau_1]\!] \vdash \mathsf{inl}(a) : [\![\tau_1]\!] + [\![\tau_2]\!]} \text{ CG-inl}$$

P2:

$$\frac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C : T_2} \text{ IH}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C[\,] : T_{2.1}} \text{ CG-FE}$$

P1:

$$\frac{\dfrac{P2}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C[\,]\bullet : T_{2.2}} \text{ CG-CE} \quad \dfrac{\dfrac{P3}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau_1]\!] \vdash \mathsf{Lb}_\ell(\mathsf{inl}(a)) : T_{1.3}} \text{ CG-label}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau_1]\!] \vdash \mathsf{ret}(\mathsf{Lb}_\ell(\mathsf{inl}(a))) : T_{1.2}} \text{ CG-ret}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{bind}(e_C[\,]\bullet, a.\mathsf{ret}(\mathsf{Lb}_\ell(\mathsf{inl}(a)))) : T_{1.2}} \text{ CG-bind}$$

Main derivation:

$$\frac{\dfrac{P1}{\Sigma, \alpha_2; \Psi; [\![\Gamma]\!] \vdash \nu(\mathsf{bind}(e_C[\,]\bullet, a.\mathsf{ret}(\mathsf{Lb}_\ell(\mathsf{inl}(a))))) : T_{1.1}} \text{ CG-CI}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash \Lambda(\nu(\mathsf{bind}(e_C[\,]\bullet, a.\mathsf{ret}(\mathsf{Lb}_\ell(\mathsf{inl}(a)))))) : T_1} \text{ CG-FI}$$

12. inr:

$T_1 = \forall \alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] + [\![\tau_2]\!]))$

$T_{1.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] + [\![\tau_2]\!]))$

$T_{1.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] + [\![\tau_2]\!]))$

$T_{1.3} = \mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] + [\![\tau_2]\!])$

$T_2 = \forall \alpha_1.(\alpha_1 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ \ [\![\tau_2]\!]$

$T_{2.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \ [\![\tau_2]\!]$

$T_{2.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ \ [\![\tau_2]\!]$

P3:

$$\frac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau_2]\!] \vdash \mathsf{inr}(a) : [\![\tau_1]\!] + [\![\tau_2]\!]} \text{ CG-inr}$$

P2:

$$\frac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C : T_2} \text{ IH}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C[\,] : T_{2.1}} \text{ CG-FE}$$

P1:

$$\frac{\dfrac{P2}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C[\,]\bullet : T_{2.2}} \text{ CG-CE} \quad \dfrac{\dfrac{P3}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau_2]\!] \vdash \mathsf{Lb}_\ell(\mathsf{inr}(a)) : T_{1.3}} \text{ CG-label}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau_2]\!] \vdash \mathsf{ret}(\mathsf{Lb}_\ell(\mathsf{inr}(a))) : T_{1.2}} \text{ CG-ret}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{bind}(e_C[\,]\bullet, a.\mathsf{ret}(\mathsf{Lb}_\ell(\mathsf{inr}(a)))) : T_{1.2}} \text{ CG-bind}$$

Main derivation:

$$\dfrac{\dfrac{P1}{\Sigma, \alpha_2; \Psi; [\![\Gamma]\!] \vdash \nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{ret}(\mathsf{Lb}_\ell(\mathsf{inr}(a))))) : T_{1.1}}\ \text{CG-CI}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{ret}(\mathsf{Lb}_\ell(\mathsf{inr}(a)))))) : T_1}\ \text{CG-FI}$$

13. case:

$T_1 = \forall\alpha_4.(\alpha_4 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_4\ \alpha_4\ [\![\tau]\!]$

$T_{1.1} = (\alpha_4 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_4\ \alpha_4\ [\![\tau]\!]$

$T_2 : \forall\alpha_1.(\alpha_1 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] + [\![\tau_2]\!]))$

$T_{2.1} : (\alpha_4 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_4\ \alpha_4\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] + [\![\tau_2]\!]))$

$T_{2.2} : \mathsf{CG}\ \alpha_4\ \alpha_4\ (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] + [\![\tau_2]\!]))$

$T_{2.3} : (\mathsf{Labeled}\ \ell\ ([\![\tau_1]\!] + [\![\tau_2]\!]))$

$T_{2.4} : \mathsf{CG}\ \alpha_4\ (\alpha_4 \sqcup \ell)\ ([\![\tau_1]\!] + [\![\tau_2]\!])$

$T_{2.5} : ([\![\tau_1]\!] + [\![\tau_2]\!])$

$T_3 = \forall\alpha_2.(\alpha_2 \sqsubseteq (pc \sqcup \ell)) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ [\![\tau]\!]$

$T_{3.1} = ((\alpha_4 \sqcup \ell) \sqsubseteq (pc \sqcup \ell)) \Rightarrow \mathsf{CG}\ (\alpha_4 \sqcup \ell)\ (\alpha_4 \sqcup \ell)\ [\![\tau]\!]$

$T_{3.2} = \mathsf{CG}\ (\alpha_4 \sqcup \ell)\ (\alpha_4 \sqcup \ell)\ [\![\tau]\!]$

$T_4 = \forall\alpha_3.(\alpha_3 \sqsubseteq (pc \sqcup \ell)) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ [\![\tau]\!]$

$T_{4.1} = ((\alpha_4 \sqcup \ell) \sqsubseteq (pc \sqcup \ell)) \Rightarrow \mathsf{CG}\ (\alpha_4 \sqcup \ell)\ (\alpha_4 \sqcup \ell)\ [\![\tau]\!]$

$T_{4.2} = \mathsf{CG}\ (\alpha_4 \sqcup \ell)\ (\alpha_4 \sqcup \ell)\ [\![\tau]\!]$

$T_{4.3} = \mathsf{CG}\ (\alpha_4)\ (\alpha_4 \sqcup \ell)\ (\mathsf{Labeled}\ \ell \sqcup \ell_x\ \mathsf{A})$

$T_{4.4} = \mathsf{CG}\ (\alpha_4)\ (\alpha_4)\ (\mathsf{Labeled}\ \alpha_4 \sqcup \ell \sqcup \ell_x\ \mathsf{A})$

$T_{4.5} = \mathsf{CG}\ (\alpha_4)\ (\alpha_4)\ [\![\tau]\!]$

$E_1 = \mathsf{case}\ b, x.e_{C2}[]\bullet, y.e_{C3}[]\bullet$

P6:

$$\dfrac{\dfrac{}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3}, b : T_{2.5}, y : [\![\tau_2]\!] \vdash e_{C3} : T_4}\ \text{IH3}}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3}, b : T_{2.5}, y : [\![\tau_2]\!] \vdash e_{C3}[] : T_{4.1}}\ \text{CG-FE}$$

P5:

$$\dfrac{\dfrac{}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3}, b : T_{2.5}, x : [\![\tau_1]\!] \vdash e_{C2} : T_3}\ \text{IH2}}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3}, b : T_{2.5}, x : [\![\tau_1]\!] \vdash e_{C2}[] : T_{3.1}}\ \text{CG-FE}$$

P4:

$$\dfrac{\begin{array}{c}\dfrac{}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3}, b : T_{2.5} \vdash b : T_{2.5}}\ \text{CG-var} \\ \dfrac{P5}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3}, b : T_{2.5}, x : [\![\tau_1]\!] \vdash e_{C2}[]\bullet : T_{3.2}}\ \text{CG-CE} \\ \dfrac{P6}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3}, b : T_{2.5}, y : [\![\tau_2]\!] \vdash e_{C3}[]\bullet : T_{4.2}}\ \text{CG-CE}\end{array}}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3}, b : T_{2.5} \vdash \mathsf{case}\ b, x.e_{C2}[]\bullet, y.e_{C3}[]\bullet : T_{4.2}}\ \text{CG-case}$$

P3:

$$\dfrac{\dfrac{}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{unlabel}\ a : T_{2.4}}\text{ CG-unlabel} \quad P4}{\dfrac{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3}, b : T_{2.5} \vdash \mathsf{case}\ b, x.e_{C2}[]\bullet, y.e_{C3}[]\bullet : T_{4.3}}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(\mathsf{case}\ b, x.e_{C2}[]\bullet, y.e_{C3}[]\bullet)) : T_{4.3}}\text{ CG-bind}}\text{ CG-sub, Lemma D.5}$$

P2:

$$\dfrac{\dfrac{}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash e_{C1} : T_2}\text{ IH1}}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash e_{C1}[] : T_{2.1}}\text{ CG-FE}$$

P2.0

$$\dfrac{P3}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(E_1))) : T_{4.4}}\text{ CG-tolabeled}$$

P2.1:

$$\dfrac{P2.0 \qquad \dfrac{}{pc \sqsubseteq \ell}\text{ Lemma C.2}}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(E_1))) : T_{4.5}}\text{ Lemma D.5}$$

P1:

$$\dfrac{\dfrac{P2}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash e_{C1}[]\bullet : T_{2.2}}\text{ CG-CE} \qquad P2.1}{\Sigma, \alpha_4; \Psi, (\alpha_4 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash \mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(E_1)))) : T_{4.5}}\text{ CG-bind}$$

Main derivation:

$$\dfrac{\dfrac{}{\Sigma, \alpha_4; \Psi; \llbracket\Gamma\rrbracket \vdash \nu(\mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(E_1))))) : T_{1.1}}\text{ CG-CI}}{\Sigma; \Psi; \llbracket\Gamma\rrbracket \vdash \Lambda(\nu(\mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.\mathsf{ret}(E_1)))))) : T_1}\text{ CG-FI}$$

14. sub:

$T_1 = \forall\alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau\rrbracket$

$T_{1.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau\rrbracket$

$T_2 = \forall\alpha_1.(\alpha_1 \sqsubseteq pc') \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ \llbracket\tau'\rrbracket$

$T_{2.1} = (\alpha_2 \sqsubseteq pc') \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau'\rrbracket$

$T_{2.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau'\rrbracket$

$T_3 = \mathsf{CG}\ \alpha_2\ \alpha_2\ \llbracket\tau\rrbracket$

P2:

$$\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash e_C : T_2}\text{ IH}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash e_C[] : T_{2.1}}\text{ CG-FE}$$

P1:

$$
\dfrac{
\dfrac{P2 \qquad \dfrac{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc) \vdash \alpha_2 \sqsubseteq pc \qquad \Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc) \vdash pc \sqsubseteq pc'}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc) \vdash \alpha_2 \sqsubseteq pc'}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C[]\bullet : T_{2.2}}\;\text{CG-CE}
\qquad
\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau']\!] \vdash a : [\![\tau']\!]}\;\text{CG-var} \qquad \dfrac{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc) \vdash \tau' \sqsubseteq \tau}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc) \vdash [\![\tau']\!] <: [\![\tau]\!]}\;\text{Lemma D.4}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau']\!] \vdash a : [\![\tau]\!]}\;\text{CG-sub}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : [\![\tau']\!] \vdash \mathsf{ret}(a) : T_3}\;\text{CG-ret}
}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{bind}(e_C[]\bullet, a.\mathsf{ret}(a)) : T_3}\;\text{CG-bind}
$$

Main derivation:

$$
\dfrac{\dfrac{P1}{\Sigma, \alpha_2; \Psi; [\![\Gamma]\!] \vdash \nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{ret}(a))) : T_{1.1}}\;\text{CG-CI}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{ret}(a)))) : T_1}\;\text{CG-FI}
$$

15. ref:

$T_1 = \forall \alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \mathsf{Labeled}\ \ell_o\ \mathsf{ref}\ \ell_i\ [\![\mathsf{A}]\!]$

$T_{1.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \mathsf{Labeled}\ \ell_o\ \mathsf{ref}\ \ell_i\ [\![\mathsf{A}]\!]$

$T_{1.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ \mathsf{Labeled}\ \ell_o\ \mathsf{ref}\ \ell_i\ [\![\mathsf{A}]\!]$

$T_2 = \forall \alpha_1.(\alpha_1 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ \mathsf{Labeled}\ \ell_i\ [\![\mathsf{A}]\!]$

$T_{2.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \mathsf{Labeled}\ \ell_i\ [\![\mathsf{A}]\!]$

$T_{2.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ \mathsf{Labeled}\ \ell_i\ [\![\mathsf{A}]\!]$

$T_{2.3} = \mathsf{Labeled}\ \ell_i\ [\![\mathsf{A}]\!]$

$T_3 = \mathsf{CG}\ \alpha_2\ \alpha_2\ (\mathsf{ref}\ \ell_i\ [\![\mathsf{A}]\!])$

$T_{3.1} = \mathsf{CG}\ \alpha_2\ \ell_o\ (\mathsf{ref}\ \ell_i\ [\![\mathsf{A}]\!])$

$T_{3.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ \mathsf{Labeled}\ \ell_o\ (\mathsf{ref}\ \ell_i\ [\![\mathsf{A}]\!])$

P3:

$$
\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash a : T_{2.3}}\;\text{CG-var}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc) \vdash \mathsf{A}^{\ell_i} \searrow pc}\;\text{Lemma C.2} \qquad \alpha_2 \sqsubseteq pc}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc) \vdash \alpha_2 \sqsubseteq \ell_i}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash \mathsf{new}\ (a) : T_3}\;\text{CG-ref}
$$

P2:

$$
\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C : T_2}\;\text{IH}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C[] : T_{2.1}}\;\text{CG-FE}
$$

P1:

$$
\dfrac{\dfrac{P2}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_C[]\bullet : T_{2.2}}\;\text{CG-CE} \qquad \dfrac{\dfrac{P3}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash \mathsf{new}\ (a) : T_{3.1}}\;\text{CG-sub}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!], a : T_{2.3} \vdash \mathsf{toLabeled}(\mathsf{new}\ (a)) : T_{3.2}}\;\text{CG-tolabeled}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{new}\ (a))) : T_{3.2}}\;\text{CG-bind}
$$

Main derivation:

$$\dfrac{\dfrac{P1}{\Sigma, \alpha_2; \Psi; \llbracket\Gamma\rrbracket \vdash \nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{new}\ (a)))) : T_{1.1}}\ \text{CG-CI}}{\Sigma; \Psi; \llbracket\Gamma\rrbracket \vdash \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{new}\ (a))))) : T_1}\ \text{CG-FI}$$

16. deref:

$T_1 = \forall\alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \mathsf{Labeled}\ \ell_i'\ \llbracket\mathsf{A}'\rrbracket$

$T_{1.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \mathsf{Labeled}\ \ell_i'\ \llbracket\mathsf{A}'\rrbracket$

$T_{1.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ \mathsf{Labeled}\ \ell_i'\ \llbracket\mathsf{A}'\rrbracket$

$T_2 = \forall\alpha_1.(\alpha_1 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ \mathsf{Labeled}\ \ell_o\ \mathsf{ref}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{2.1} = (\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_2\ \alpha_2\ \mathsf{Labeled}\ \ell_o\ \mathsf{ref}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{2.2} = \mathsf{CG}\ \alpha_2\ \alpha_2\ \mathsf{Labeled}\ \ell_o\ \mathsf{ref}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{2.3} = \mathsf{Labeled}\ \ell_o\ \mathsf{ref}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{2.4} = \mathsf{CG}\ \alpha_2\ \alpha_2 \sqcup \ell_o\ \mathsf{ref}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{2.5} = \mathsf{ref}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_3 = \mathsf{CG}\ (\alpha_2 \sqcup \ell_o)\ (\alpha_2 \sqcup \ell_o)\ \mathsf{Labeled}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_4 = \mathsf{CG}\ (\alpha_2)\ (\alpha_2 \sqcup \ell_o)\ \mathsf{Labeled}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{4.1} = \mathsf{CG}\ (\alpha_2)\ (\alpha_2 \sqcup \ell_o)\ \mathsf{Labeled}\ \ell_i'\ \llbracket\mathsf{A}'\rrbracket$

$T_5 = \mathsf{CG}\ (\alpha_2)\ (\alpha_2)\ \mathsf{Labeled}\ \ell_o \sqcup \ell_i'\ \llbracket\mathsf{A}'\rrbracket$

P5:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{A}^{\ell_i} \searrow \ell_o}\ \text{Given}}{\Sigma; \Psi \vdash \ell_o \sqsubseteq \ell_i}\ \text{Definition of } \searrow \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{A}^{\ell_i} <: \mathsf{A}'^{\ell_i'}}\ \text{Given}}{\Sigma; \Psi \vdash \ell_i \sqsubseteq \ell_i'}\ \text{By inversion}}{\Sigma; \Psi \vdash \ell_o \sqsubseteq \ell_i'}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc) \vdash \ell_o \sqsubseteq \ell_i'}\ \text{Weakening}$$

P4:

$$\dfrac{\dfrac{P3 \qquad \dfrac{\dfrac{}{\mathsf{A}^{\ell_i} <: \mathsf{A}'^{\ell_i'}}\ \text{Given}}{\ell_i \sqsubseteq \ell_i'}\ \text{By inversion} \qquad \dfrac{\dfrac{}{\mathsf{A}^{\ell_i} <: \mathsf{A}'^{\ell_i'}}\ \text{Given}}{\mathsf{A} <: \mathsf{A}'}\ \text{By inversion}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.!b) : T_{4.1}}\ \text{Lemma D.4}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)) : T_5}\ \text{CG-tolabeled}$$

P3:

$$\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{unlabel}\ a : T_{2.4}}\ \text{CG-unlabel} \qquad \dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3}, b : T_{2.5} \vdash !b : T_3}\ \text{CG-deref}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, b.!b) : T_4}\ \text{CG-bind}$$

P2:

$$\dfrac{\dfrac{}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash e_C : T_2}\ \text{IH}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash e_C[] : T_{2.1}}\ \text{CG-FE}$$

P1:

$$\dfrac{\dfrac{\dfrac{P2}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash e_C[]\bullet : T_{2.2}}\text{CG-CE} \qquad P4 \qquad P5}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{2.3} \vdash \mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)) : T_{1.2}}}{\Sigma, \alpha_2; \Psi, (\alpha_2 \sqsubseteq pc); \llbracket\Gamma\rrbracket \vdash \mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.!b))) : T_{1.2}}\text{CG-bind}$$

Main derivation:

$$\dfrac{\dfrac{P1}{\Sigma, \alpha_2; \Psi; \llbracket\Gamma\rrbracket \vdash \nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.!b)))) : T_{1.1}}\text{CG-CI}}{\Sigma; \Psi; \llbracket\Gamma\rrbracket \vdash \Lambda(\nu(\mathsf{bind}(e_C[]\bullet, a.\mathsf{toLabeled}(\mathsf{bind}(\mathsf{unlabel}\ a, b.!b))))) : T_1}\text{CG-FI}$$

17. assign:

$T_1 = \forall\alpha_3.(\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ \mathsf{Labeled}\ \ell_o\ \mathsf{unit}$

$T_{1.1} = (\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ \mathsf{Labeled}\ \ell_o\ \mathsf{unit}$

$T_{1.2} = \mathsf{CG}\ \alpha_3\ \alpha_3\ \mathsf{Labeled}\ \ell_o\ \mathsf{unit}$

$T_2 = \forall\alpha_2.(\alpha_2 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ \mathsf{Labeled}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{2.1} = (\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ \mathsf{Labeled}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{2.2} = \mathsf{CG}\ \alpha_3\ \alpha_3\ \mathsf{Labeled}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{2.3} = \mathsf{Labeled}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_3 = \forall\alpha_1.(\alpha_1 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_1\ \alpha_1\ \mathsf{Labeled}\ \ell_o\ \mathsf{ref}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{3.1} = (\alpha_3 \sqsubseteq pc) \Rightarrow \mathsf{CG}\ \alpha_3\ \alpha_3\ \mathsf{Labeled}\ \ell_o\ \mathsf{ref}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{3.2} = \mathsf{CG}\ \alpha_3\ \alpha_3\ \mathsf{Labeled}\ \ell_o\ \mathsf{ref}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{3.3} = \mathsf{Labeled}\ \ell_o\ \mathsf{ref}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{3.4} = \mathsf{CG}\ \alpha_3\ \alpha_3 \sqcup \ell_o\ \mathsf{ref}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_{3.5} = \mathsf{ref}\ \ell_i\ \llbracket\mathsf{A}\rrbracket$

$T_4 = \mathsf{CG}\ (\alpha_3 \sqcup \ell_o)\ (\alpha_3 \sqcup \ell_o)\ \mathsf{unit}$

$T_5 = \mathsf{CG}\ (\alpha_3)\ (\alpha_3 \sqcup \ell_o)\ \mathsf{unit}$

$E_1 = \mathsf{bind}(\mathsf{unlabel}\ a, c.c := b)$

P6:

$$\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{3.3}, b : T_{2.3} \vdash a : T_{3.3}}\text{CG-var}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{3.3}, b : T_{2.3} \vdash \mathsf{unlabel}\ a : T_{3.4}}\text{CG-unlabel} \qquad \dfrac{\dfrac{\dfrac{}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc) \vdash \alpha_3 \sqsubseteq pc \sqsubseteq \ell_o}\text{Lemma C.2} \qquad \dfrac{\dfrac{}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc) \vdash \mathsf{A}^{\ell_i} \searrow \ell_o}\text{Given}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc) \vdash \ell_o \sqsubseteq \ell_i}\text{Definition of } \searrow}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc) \vdash \alpha_3 \sqcup \ell_o \sqsubseteq \ell_i}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{3.3}, b : T_{2.3}, c : T_{3.5} \vdash c := b : T_4}\text{CG-assign}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{3.3}, b : T_{2.3} \vdash \mathsf{bind}(\mathsf{unlabel}\ a, c.c := b) : T_5}\text{CG-bind}$$

P5:

$$\dfrac{\dfrac{}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{3.3} \vdash e_{C2} : T_2}\text{IH2}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); \llbracket\Gamma\rrbracket, a : T_{3.3} \vdash e_{C2}[] : T_{2.1}}\text{CG-FE}$$

P4:

$$\dfrac{\dfrac{P5}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : T_{3.3} \vdash e_{C2}[]\bullet : T_{2.2}}\ \text{CG-CE} \qquad P6}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!], a : T_{3.3} \vdash \mathsf{bind}(e_{C2}[]\bullet, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b))) : T_5}\ \text{CG-bind}$$

P3:

$$\dfrac{\dfrac{}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_{C1} : T_3}\ \text{IH1}}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_{C1}[] : T_{3.1}}\ \text{CG-FE}$$

P2:

$$\dfrac{\dfrac{P3}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!] \vdash e_{C1}[]\bullet : T_{3.2}}\ \text{CG-CE} \qquad P4}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{bind}(e_{C2}[]\bullet, b.\mathsf{bind}(\mathsf{unlabel}\ a, c.c := b))) : T_5}\ \text{CG-bind}$$

P1:

$$\dfrac{P2}{\Sigma, \alpha_3; \Psi, (\alpha_3 \sqsubseteq pc); [\![\Gamma]\!] \vdash \mathsf{toLabeled}(\mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{bind}(e_{C2}[]\bullet, b.E_1))) : T_{1.2}}\ \text{CG-tolabeled}$$

Main derivation:

$$\dfrac{\dfrac{P1}{\Sigma, \alpha_3; \Psi; [\![\Gamma]\!] \vdash \nu(\mathsf{toLabeled}(\mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{bind}(e_{C2}[]\bullet, b.E_1)))) : T_{1.1}}\ \text{CG-CI}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash \Lambda(\nu(\mathsf{toLabeled}(\mathsf{bind}(e_{C1}[]\bullet, a.\mathsf{bind}(e_{C2}[]\bullet, b.E_1))))) : T_1}\ \text{CG-FI}$$

□

Lemma D.4 (Subtyping of translated types)**.** *Forall* Σ *and* Ψ *the following holds:*

1. $\forall \tau_a, \tau_b.$
   $\Sigma; \Psi \vdash \tau_a \sqsubseteq \tau_b \implies \Sigma; \Psi \vdash [\![\tau_a]\!] <: [\![\tau_b]\!]$
2. $\forall \mathsf{A}_a, \mathsf{A}_b.$
   $\Sigma; \Psi \vdash \mathsf{A}_a \sqsubseteq \mathsf{A}_b \implies \Sigma; \Psi \vdash [\![\mathsf{A}_a]\!] <: [\![\mathsf{A}_b]\!]$

Proof. Proof by simultaneous induciton on the FG$^-$ subtyping relation
Proof of statement (1)
Let $\tau_a = \mathsf{A}_a^{\ell_a}$ and $\tau_b = \mathsf{A}_b^{\ell_b}$

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{A}_a^{\ell_a} \sqsubseteq \mathsf{A}_b^{\ell_b}}\ \text{Given}}{\Sigma; \Psi \vdash \ell_a \sqsubseteq \ell_b}\ \text{By inversion} \qquad \dfrac{}{\Sigma; \Psi \vdash [\![\mathsf{A}_a]\!] <: [\![\mathsf{A}_b]\!]}\ \text{IH(2)}}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell_a\ \ [\![\mathsf{A}_a]\!] <: \mathsf{Labeled}\ \ell_b\ \ [\![\mathsf{A}_b]\!]}\ \text{SLsub-base}$$

Proof of statement (2) We proceed by cases on the last rule in the given derivation of $\mathsf{A}_a <: \mathsf{A}_b$.

1. FG$^-$sub-base:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{b} <: \mathsf{b}}\ \text{CGsub-base}}{\Sigma; \Psi \vdash [\![\mathsf{b}]\!] <: [\![\mathsf{b}]\!]}\ \text{Definition of } [\![\cdot]\!]$$

2. FG$^-$sub-ref:

   Let $\tau_a = \tau_b = \mathsf{ref}\ \mathsf{A}_i^{\ell_i}$

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \ell_i\ [\![\mathsf{A}_i]\!] <: \mathsf{ref}\ \ell_i\ [\![\mathsf{A}_i]\!]}\text{ CGsub-base}}{\Sigma; \Psi \vdash \left[\!\!\left[\mathsf{ref}\ \mathsf{A}_i^{\ell_i}\right]\!\!\right] <: \left[\!\!\left[\mathsf{ref}\ \mathsf{A}_i^{\ell_i}\right]\!\!\right]}\text{ Definition of } [\![\cdot]\!]$$

3. FG$^-$sub-prod:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi\vdash [\![\tau_1]\!] <: [\![\tau_1']\!]}\text{ IH(1) on }\tau_2 \qquad \dfrac{}{\Sigma;\Psi\vdash [\![\tau_2]\!] <: [\![\tau_2']\!]}\text{ IH(1) on }\tau_1}{\Sigma;\Psi\vdash [\![\tau_1]\!]\times[\![\tau_2]\!] <: [\![\tau_1']\!]\times[\![\tau_2']\!]}\text{ CGsub-prod}}{\Sigma;\Psi\vdash [\![\tau_1\times\tau_2]\!] <: [\![\tau_1'\times\tau_2']\!]}\text{ Definition of }[\![\cdot]\!]$$

4. FG$^-$sub-sum:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi\vdash [\![\tau_1]\!] <: [\![\tau_1']\!]}\text{ IH(1) on }\tau_2 \qquad \dfrac{}{\Sigma;\Psi\vdash [\![\tau_2]\!] <: [\![\tau_2']\!]}\text{ IH(1) on }\tau_1}{\Sigma;\Psi\vdash [\![\tau_1]\!]+[\![\tau_2]\!] <: [\![\tau_1']\!]+[\![\tau_2']\!]}\text{ CGsub-sum}}{\Sigma;\Psi\vdash [\![\tau_1+\tau_2]\!] <: [\![\tau_1'+\tau_2']\!]}\text{ Definition of }[\![\cdot]\!]$$

5. FG$^-$sub-arrow:

   P2:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi\vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'}\text{ Given}}{\Sigma;\Psi\vdash \tau_2 <: \tau_2'}\text{ By inversion}}{\Sigma,\alpha;\Psi\vdash [\![\tau_2]\!] <: [\![\tau_2']\!]}\text{ IH(1) and Weakening}}{\Sigma,\alpha;\Psi\vdash \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau_2]\!] <: \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau_2']\!]}\text{ CGsub-monad}$$

   P1:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi\vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'}\text{ Given}}{\Sigma;\Psi\vdash \ell_e' \sqsubseteq \ell_e}\text{ By inversion}}{\Sigma,\alpha;\Psi\vdash (\alpha\sqsubseteq\ell_e') \implies (\alpha\sqsubseteq\ell_e')} \qquad P2}{\Sigma,\alpha;\Psi\vdash (\alpha\sqsubseteq\ell_e)\Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau_2]\!] <: (\alpha\sqsubseteq\ell_e')\Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau_2']\!]}\text{ CGsub-constraint}}{\Sigma;\Psi\vdash \forall\alpha.(\alpha\sqsubseteq\ell_e)\Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau_2]\!] <: \forall\alpha.(\alpha\sqsubseteq\ell_e')\Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau_2']\!]}\text{ CGsub-forall}$$

   Main derivation:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi\vdash \tau_1 \xrightarrow{\ell_e} \tau_2 <: \tau_1' \xrightarrow{\ell_e'} \tau_2'}\text{ Given}}{\Sigma;\Psi\vdash \tau_1' <: \tau_1}\text{ By inversion}}{\Sigma;\Psi\vdash [\![\tau_1']\!] <: [\![\tau_1]\!]}\text{ IH(1)} \qquad P1}{\Sigma;\Psi\vdash [\![\tau_1]\!]\to\forall\alpha.(\alpha\sqsubseteq\ell_e)\Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau_2]\!] <: [\![\tau_1']\!]\to\forall\alpha.(\alpha\sqsubseteq\ell_e')\Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau_2']\!]}\text{ CGsub-arrow}}{\Sigma;\Psi\vdash \left[\!\!\left[\tau_1 \xrightarrow{\ell_e} \tau_2\right]\!\!\right] <: \left[\!\!\left[\tau_1' \xrightarrow{\ell_e'} \tau_2'\right]\!\!\right]}\text{ Definition of }[\![\cdot]\!]$$

6. FG$^-$sub-unit:

$$\cfrac{\overline{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}}\ \text{CGsub-base}}{\Sigma; \Psi \vdash [\![\mathsf{unit}]\!] <: [\![\mathsf{unit}]\!]}\ \text{Definition of } [\![\cdot]\!]$$

7. FG$^-$sub-forall:

P0:

$$\cfrac{\overline{\Sigma; \Psi \vdash \forall \alpha.(\ell_e, \tau_1) <: \forall (\ell'_e, \tau_2)}\ \text{Given}}{\Sigma, \alpha; \Psi \vdash \ell'_e \sqsubseteq \ell_e}\ \text{By inversion}$$

P0.1:

$$\cfrac{\overline{\Sigma; \Psi \vdash \forall \alpha.(\ell_e, \tau_1) <: \forall (\ell'_e, \tau_2)}\ \text{Given}}{\Sigma, \alpha; \Psi \vdash \tau_1 <: \tau_2}\ \text{By inversion}$$

P2:

$$\cfrac{\cfrac{P0.1}{\Sigma, \alpha, \alpha'; \Psi \vdash [\![\tau_1]\!] <: [\![\tau_2]\!]}\ \text{IH(1) and Weakening}}{\Sigma, \alpha, \alpha'; \Psi \vdash \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau_1]\!] <: \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau_2]\!]}\ \text{CGsub-monad}$$

P1:

$$\cfrac{\cfrac{\cfrac{P0}{\Sigma, \alpha, \alpha'; \Psi \vdash \alpha' \sqsubseteq \ell'_e \implies \alpha' \sqsubseteq \ell_e} \qquad P2}{\Sigma, \alpha, \alpha'; \Psi \vdash \alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau_1]\!] <: \alpha' \sqsubseteq \ell'_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau_2]\!]}\ \text{CGsub-constraint}}{\Sigma, \alpha; \Psi \vdash \forall \alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau_1]\!] <: \forall \alpha'.\alpha' \sqsubseteq \ell'_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau_2]\!]}\ \text{CGsub-forall}$$

Main derivation:

$$\cfrac{\cfrac{P1}{\Sigma; \Psi \vdash \forall \alpha.\forall \alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau_1]\!] <: \forall \alpha.\forall \alpha'.\alpha' \sqsubseteq \ell'_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau_2]\!]}\ \text{CGsub-forall}}{\Sigma; \Psi \vdash [\![\forall (\ell_e, \tau_1)]\!] <: [\![\forall (\ell'_e, \tau_2)]\!]}\ \text{Definition of } [\![\cdot]\!]$$

8. FG$^-$sub-constraint:

P0:

$$\cfrac{\overline{\Sigma; \Psi \vdash c_1 \overset{\ell_e}{\Rightarrow} \tau_1 <: c_2 \overset{\ell'_e}{\Rightarrow} \tau_2}\ \text{Given}}{\Sigma; \Psi \vdash \ell'_e \sqsubseteq \ell_e}\ \text{By inversion}$$

P0.1:

$$\cfrac{\overline{\Sigma; \Psi \vdash c_1 \overset{\ell_e}{\Rightarrow} \tau_1 <: c_2 \overset{\ell'_e}{\Rightarrow} \tau_2}\ \text{Given}}{\Sigma; \Psi \vdash c_2 \implies c_1}\ \text{By inversion}$$

P0.2:

$$\cfrac{\overline{\Sigma; \Psi \vdash c_1 \overset{\ell_e}{\Rightarrow} \tau_1 <: c_2 \overset{\ell'_e}{\Rightarrow} \tau_2}\ \text{Given}}{\Sigma; \Psi \vdash \tau_1 <: \tau_2}\ \text{By inversion}$$

P2:

$$\dfrac{\dfrac{P0.2}{\Sigma, \alpha; \Psi \vdash [\![\tau_1]\!] <: [\![\tau_2]\!]}\ \text{IH(1) and Weakening}}{\Sigma, \alpha; \Psi \vdash \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_1]\!] <: \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_2]\!]}\ \text{CGsub-monad}$$

P1:

$$\dfrac{\dfrac{P0 \qquad P0.1}{\Sigma; \Psi \vdash \alpha \sqsubseteq \ell'_e, c_2 \implies \alpha \sqsubseteq \ell_e, c_1} \qquad P2}{\Sigma, \alpha; \Psi \vdash (\alpha \sqsubseteq \ell_e, c_1) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_1]\!] <: (\alpha \sqsubseteq \ell'_e, c_2) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_2]\!]}\ \text{CGsub-constraint}$$

Main derivation:

$$\dfrac{\dfrac{P1}{\Sigma; \Psi \vdash \forall \alpha.(\alpha \sqsubseteq \ell_e, c_1) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_1]\!] <: \forall \alpha.(\alpha \sqsubseteq \ell'_e, c_2) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_2]\!]}\ \text{CGsub-forall}}{\Sigma; \Psi \vdash \left[\!\!\left[c_1 \overset{\ell_e}{\Rightarrow} \tau_1 \right]\!\!\right] <: \left[\!\!\left[c_2 \overset{\ell'_e}{\Rightarrow} \tau_2 \right]\!\!\right]}\ \text{Definition of } [\![\cdot]\!]$$

□

Lemma D.5 (Expanded label)**.** $\forall \tau, \ell, \mathsf{A}_F, \mathsf{A}_L, \ell', \Sigma, \Psi.$
$\Sigma; \Psi \vdash (\tau = \mathsf{A}_F^{\ell'}) \searrow \ell \implies$
$\exists \ell_x.\ [\![\tau]\!] = \mathsf{Labeled}\ \ell \sqcup \ell_x\ \mathsf{A}_L$ *where* $\mathsf{A}_L = [\![\mathsf{A}_F]\!]$

Proof. Since $\Sigma; \Psi \vdash (\tau = \mathsf{A}_F^{\ell'}) \searrow \ell$ from the definition of $\searrow$, we get $\ell \sqsubseteq \ell'$. Therefore, $\exists \ell_x.\ \ell \sqcup \ell_x = \ell'$
From Definition D.1, $[\![\tau]\!] = \mathsf{Labeled}\ \ell'\ [\![\mathsf{A}_F]\!] = \mathsf{Labeled}\ \ell \sqcup \ell_x\ [\![\mathsf{A}_F]\!]$ for some ℓ_x □

Lemma D.6 (Preservation of well-formedness)**.** *Forall* Σ *and* Ψ *the following hold:*

1. $\forall \tau.\ \Sigma; \Psi \vdash \tau\ WF \implies \Sigma; \Psi \vdash [\![\tau]\!]\ WF$
2. $\forall \mathsf{A}.\ \Sigma; \Psi \vdash \mathsf{A}\ WF \implies \Sigma; \Psi \vdash [\![\mathsf{A}]\!]\ WF$

Proof. Proof by simulataneous induction on the WF relation of FG$^-$
Proof of statement (1)
Let $\tau = \mathsf{A}^\ell$

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\mathsf{A}]\!]\ WF}\ \text{IH(2) on } \mathsf{A}}{\Sigma; \Psi \vdash \mathsf{Labeled}\ \ell\ [\![\mathsf{A}]\!]\ WF}\ \text{CG-wff-labeled}$$

Proof of statement (2)
We proceed by case analyzing the last rule of given WF judgment.

1. FG$^-$-wff-base:

$$\dfrac{}{\Sigma; \Psi \vdash \mathsf{b}\ WF}\ \text{CG-wff-base}$$

2. FG$^-$-wff-unit:

$$\dfrac{}{\Sigma; \Psi \vdash \mathsf{unit}\ WF}\ \text{CG-wff-unit}$$

3. FG$^-$-wff-arrow:

P1:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha; \Psi, (\alpha \sqsubseteq \ell_e) \vdash [\![\tau_{F2}]\!]\ WF}\ \text{IH(1) on } \tau_{F2}\text{, Weakening}}{\Sigma, \alpha; \Psi, (\alpha \sqsubseteq \ell_e) \vdash \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau_{F2}]\!]\ \ WF}\ \text{CG-wff-monad}}{\Sigma, \alpha; \Psi \vdash (\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau_{F2}]\!]\ \ WF}\ \text{CG-wff-constraint}}{\Sigma; \Psi \vdash \forall \alpha.(\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau_{F2}]\!]\ \ WF}\ \text{CG-wff-forall}$$

Main derivation:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_{F1}]\!]\ \ WF}\ \text{IH(1) on } \tau_{F1} \qquad P1}{\Sigma; \Psi \vdash ([\![\tau_{F1}]\!] \to \forall \alpha.(\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau_{F2}]\!])\ WF}\ \text{CG-wff-arrow}$$

4. FG$^-$-wff-prod:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1]\!]\ \ WF}\ \text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash [\![\tau_2]\!]\ \ WF}\ \text{IH(1) on } \tau_2}{\Sigma; \Psi \vdash [\![\tau_1]\!] \times [\![\tau_2]\!]\ \ WF}\ \text{CG-wff-prod}$$

5. FG$^-$-wff-sum:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1]\!]\ \ WF}\ \text{IH(1) on } \tau_1 \qquad \dfrac{}{\Sigma; \Psi \vdash [\![\tau_2]\!]\ \ WF}\ \text{IH(1) on } \tau_2}{\Sigma; \Psi \vdash [\![\tau_1]\!] + [\![\tau_2]\!]\ \ WF}\ \text{CG-wff-prod}$$

6. FG$^-$-wff-ref:

Let $\tau = \mathsf{A}^\ell$

$$\dfrac{\dfrac{\dfrac{}{FV(\mathsf{A}) = \emptyset}\ \text{Given}}{FV([\![\mathsf{A}]\!]) = \emptyset}\ \text{Lemma D.7} \qquad \dfrac{}{FV(\ell) = \emptyset}\ \text{Given}}{\Sigma; \Psi \vdash \mathsf{ref}\ \ell\ [\![\mathsf{A}]\!]\ WF}\ \text{CG-wff-ref}$$

7. FG$^-$-wff-forall:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha, \alpha'; \Psi, \alpha' \sqsubseteq \ell_e \vdash [\![\tau]\!]\ WF}\ \text{IH(1) on } \tau}{\Sigma, \alpha, \alpha'; \Psi, \alpha' \sqsubseteq \ell_e \vdash \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]\ \ WF}\ \text{CG-wff-monad}}{\Sigma, \alpha, \alpha'; \Psi \vdash \alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]\ \ WF}\ \text{CG-wff-constraint}}{\Sigma, \alpha; \Psi \vdash \forall \alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]\ \ WF}\ \text{CG-wff-forall}}{\Sigma; \Psi \vdash \forall \alpha.\forall \alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \ [\![\tau]\!]\ \ WF}\ \text{CG-wff-forall}$$

8. FG$^-$-wff-constraint:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma, \alpha; \Psi, (\alpha \sqsubseteq \ell_e, c) \vdash [\![\tau]\!]\ WF}\ \text{IH(1) on } \tau\text{, Weakening}}{\Sigma, \alpha; \Psi, (\alpha \sqsubseteq \ell_e, c) \vdash \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau]\!]\ \ WF}\ \text{CG-wff-monad}}{\Sigma, \alpha; \Psi \vdash (\alpha \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau]\!]\ \ WF}\ \text{CG-wff-constraint}}{\Sigma; \Psi \vdash \forall \alpha.(\alpha \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \ [\![\tau]\!]\ \ WF}\ \text{CG-wff-forall}$$

□

Lemma D.7. *The following hold:*

1. $\forall \tau.\ FV(\llbracket \tau \rrbracket) \subseteq FV(\tau)$
2. $\forall \mathsf{A}.\ FV(\llbracket \mathsf{A} \rrbracket) \subseteq FV(\mathsf{A})$

Proof. Proof by simultaneous induction on τ and A

Proof for (1)

Let $\tau = \mathsf{A}^{\ell_i}$

$$\begin{array}{lll} & FV(\llbracket \mathsf{A}^{\ell_i} \rrbracket) & \\ = & FV(\mathsf{Labeled}\ \ell_i\ \llbracket \mathsf{A} \rrbracket) & \text{Definition of } \llbracket\cdot\rrbracket \\ = & FV(\ell_i) \cup FV(\llbracket \mathsf{A} \rrbracket) & \\ \subseteq & FV(\ell_i) \cup FV(\mathsf{A}) & \text{IH(2) on } \mathsf{A} \\ = & FV(\mathsf{A}^{\ell_i}) & \end{array}$$

Proof for (2)

1. $\mathsf{A} = \mathsf{b}$:

$$\begin{array}{lll} & FV(\llbracket \mathsf{b} \rrbracket) & \\ = & FV(\mathsf{b}) & \text{Definition of } \llbracket\cdot\rrbracket \end{array}$$

2. $\mathsf{A} = \mathsf{unit}$:

$$\begin{array}{lll} & FV(\llbracket \mathsf{unit} \rrbracket) & \\ = & FV(\mathsf{unit}) & \text{Definition of } \llbracket\cdot\rrbracket \end{array}$$

3. $\mathsf{A} = \tau_1 \xrightarrow{\ell_e} \tau_2$:

$$\begin{array}{lll} & FV(\left\llbracket \tau_1 \xrightarrow{\ell_e} \tau_2 \right\rrbracket) & \\ = & FV(\llbracket \tau_1 \rrbracket \to \forall \alpha.(\alpha \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \llbracket \tau_2 \rrbracket) & \text{Definition of } \llbracket\cdot\rrbracket \\ = & FV(\llbracket \tau_1 \rrbracket) \cup FV(\ell_e) \cup FV(\llbracket \tau_2 \rrbracket) & \\ \subseteq & FV(\tau_1) \cup FV(\ell_e) \cup FV(\tau_2) & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & FV(\tau_1 \xrightarrow{\ell_e} \tau_2) & \end{array}$$

4. $\mathsf{A} = \tau_1 \times \tau_2$:

$$\begin{array}{lll} & FV(\llbracket \tau_1 \times \tau_2 \rrbracket) & \\ = & FV(\llbracket \tau_1 \rrbracket \times \llbracket \tau_2 \rrbracket) & \text{Definition of } \llbracket\cdot\rrbracket \\ = & FV(\llbracket \tau_1 \rrbracket) \cup FV(\llbracket \tau_2 \rrbracket) & \\ \subseteq & FV(\tau_1) \cup FV(\tau_2) & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & FV(\tau_1 \times \tau_2) & \end{array}$$

5. $\mathsf{A} = \tau_1 + \tau_2$:

$$\begin{array}{lll} & FV(\llbracket \tau_1 + \tau_2 \rrbracket) & \\ = & FV(\llbracket \tau_1 \rrbracket + \llbracket \tau_2 \rrbracket) & \text{Definition of } \llbracket\cdot\rrbracket \\ = & FV(\llbracket \tau_1 \rrbracket) \cup FV(\llbracket \tau_2 \rrbracket) & \\ \subseteq & FV(\tau_1) \cup FV(\tau_2) & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\ = & FV(\tau_1 + \tau_2) & \end{array}$$

6. $\mathsf{A} = \mathsf{ref}\ \tau_i$:

   Let $\tau_i = \mathsf{A}_i^{\ell_i}$

$$\begin{array}{lll}
 & FV(\llbracket \mathsf{ref}\ \tau_i \rrbracket) & \\
= & FV(\mathsf{ref}\ \ell_i\ \llbracket \mathsf{A}_i \rrbracket) & \text{Definition of } \llbracket\cdot\rrbracket \\
= & FV(\ell_i) \cup FV(\llbracket \mathsf{A}_i \rrbracket) & \\
\subseteq & FV(\ell_i) \cup FV(\mathsf{A}_i) & \text{IH(2) on } \mathsf{A}_i \\
= & FV(\mathsf{ref}\ \mathsf{A}_i^{\ell_i}) & \\
= & FV(\mathsf{ref}\ \tau_i) &
\end{array}$$

7. $\mathsf{A} = \forall\ (\ell_e, \tau_i)$:

$$\begin{array}{lll}
 & FV(\llbracket \forall\ (\ell_e, \tau_i) \rrbracket) & \\
= & FV(\forall\alpha.\forall\alpha'.\alpha' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \alpha'\ \alpha'\ \llbracket \tau_i \rrbracket) & \text{Definition of } \llbracket\cdot\rrbracket \\
= & FV(\ell_e) \cup FV(\llbracket \tau_i \rrbracket) & \\
\subseteq & FV(\ell_e) \cup FV(\tau_i) & \text{IH(1) on } \tau_i \\
= & FV(\forall\ (\ell_e, \tau_i)) &
\end{array}$$

8. $\mathsf{A} = c \overset{\ell_e}{\Rightarrow} \tau_i$:

$$\begin{array}{lll}
 & FV(\left\llbracket c \overset{\ell_e}{\Rightarrow} \tau_i \right\rrbracket) & \\
= & FV(\forall\alpha.(\alpha \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ \llbracket \tau_i \rrbracket) & \text{Definition of } \llbracket\cdot\rrbracket \\
= & FV(\ell_e) \cup FV(c) \cup FV(\llbracket \tau_i \rrbracket) & \\
\subseteq & FV(\ell_e) \cup FV(c) \cup FV(\tau_i) & \text{IH(1) on } \tau_i \\
= & FV(c \overset{\ell_e}{\Rightarrow} \tau_i) &
\end{array}$$

□

Lemma D.8 (Substitution Lemma). *Forall ℓ' the following hold:*

1. $\forall\tau.\ \llbracket \tau \rrbracket [\ell'/\alpha] = \llbracket \tau[\ell'/\alpha] \rrbracket$
2. $\forall\mathsf{A}.\ \llbracket \mathsf{A} \rrbracket [\ell'/\alpha] = \llbracket \mathsf{A}[\ell'/\alpha] \rrbracket$

Proof. Proof by simultaneous induction on τ and A

Proof of statement (1)

Let $\tau = \mathsf{A}^{\ell_i}$

$$\begin{array}{lll}
 & \llbracket \mathsf{A}^{\ell_i} \rrbracket\ [\ell'/\alpha] & \\
= & (\mathsf{Labeled}\ \ell_i\ \llbracket \mathsf{A} \rrbracket)\ [\ell'/\alpha] & \text{Definition of } \llbracket\cdot\rrbracket \\
= & (\mathsf{Labeled}\ \ell_i[\ell'/\alpha]\ \llbracket \mathsf{A} \rrbracket [\ell'/\alpha]) & \\
= & (\mathsf{Labeled}\ \ell_i[\ell'/\alpha]\ \llbracket \mathsf{A}[\ell'/\alpha] \rrbracket) & \text{IH(2) on } \mathsf{A} \\
= & \left\llbracket (\mathsf{A}[\ell'/\alpha])^{\ell_i[\ell'/\alpha]} \right\rrbracket & \\
= & \llbracket \mathsf{A}^{\ell_i}[\ell'/\alpha] \rrbracket &
\end{array}$$

Proof of statement (2)

We consider cases of A

1. $\mathsf{A} = \mathsf{b}$:

$$\begin{array}{lll}
 & \llbracket \mathsf{b} \rrbracket [\ell'/\alpha] & \\
= & \mathsf{b}[\ell'/\alpha] & (\text{Definition of } \llbracket\cdot\rrbracket) \\
= & \mathsf{b} & \alpha \notin FV(\mathsf{b}) \\
= & \llbracket \mathsf{b} \rrbracket & (\text{Definition of } \llbracket\cdot\rrbracket) \\
= & \llbracket \mathsf{b}[\ell'/\alpha] \rrbracket &
\end{array}$$

2. $\mathsf{A} = \mathsf{unit}$:

$$\begin{array}{lll}
 & \llbracket \mathsf{unit} \rrbracket [\ell'/\alpha] & \\
= & \mathsf{unit}[\ell'/\alpha] & (\text{Definition of } \llbracket\cdot\rrbracket) \\
= & \mathsf{unit} & \alpha \notin FV(\mathsf{unit}) \\
= & \llbracket \mathsf{unit} \rrbracket & (\text{Definition of } \llbracket\cdot\rrbracket) \\
= & \llbracket \mathsf{unit}[\ell'/\alpha] \rrbracket &
\end{array}$$

3. $\mathsf{A} = \mathsf{ref}\ \tau_i$:

$$\begin{array}{lll}
 & [\![\mathsf{ref}\ \tau_i]\!]\,[\ell'/\alpha] & \\
= & [\![\mathsf{ref}\ \mathsf{A}^{\ell_i}]\!]\,[\ell'/\alpha] & \text{Let } \tau = \mathsf{A}^{\ell_i} \\
= & (\mathsf{ref}\ \ell_i\ [\![\mathsf{A}]\!])[\ell'/\alpha] & \\
= & (\mathsf{ref}\ \ell_i[\ell'/\alpha]\ [\![\mathsf{A}]\!]\,[\ell'/\alpha]) & \\
= & (\mathsf{ref}\ \ell_i[\ell'/\alpha]\ [\![\mathsf{A}[\ell'/\alpha]]\!]) & \text{IH(2) on } \mathsf{A} \\
= & \left[\!\!\left[\mathsf{ref}\ \mathsf{A}[\ell'/\alpha]^{\ell_i[\ell'/\alpha]}\right]\!\!\right] & \\
= & [\![(\mathsf{ref}\ \mathsf{A}^{\ell_i})[\ell'/\alpha]]\!] & \\
= & [\![\mathsf{ref}\ \tau_i[\ell'/\alpha]]\!] &
\end{array}$$

4. $\mathsf{A} = \tau_1 \times \tau_2$:

$$\begin{array}{lll}
 & [\![\tau_1 \times \tau_2]\!]\,[\ell'/\alpha] & \\
= & ([\![\tau_1]\!] \times [\![\tau_2]\!])[\ell'/\alpha] & \text{(Definition of } [\![\cdot]\!]) \\
= & [\![\tau_1]\!][\ell'/\alpha] \times [\![\tau_2]\!][\ell'/\alpha] & \\
= & [\![\tau_1[\ell'/\alpha]]\!] \times [\![\tau_2[\ell'/\alpha]]\!] & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\
= & [\![(\tau_1[\ell'/\alpha] \times \tau_2[\ell'/\alpha])]\!] & \text{(Definition of } [\![\cdot]\!]) \\
= & [\![(\tau_1 \times \tau_2)[\ell'/\alpha]]\!] &
\end{array}$$

5. $\mathsf{A} = \tau_1 + \tau_2$:

$$\begin{array}{lll}
 & [\![\tau_1 + \tau_2]\!]\,[\ell'/\alpha] & \\
= & ([\![\tau_1]\!] + [\![\tau_2]\!])[\ell'/\alpha] & \text{(Definition of } [\![\cdot]\!]) \\
= & [\![\tau_1]\!][\ell'/\alpha] + [\![\tau_2]\!][\ell'/\alpha] & \\
= & [\![\tau_1[\ell'/\alpha]]\!] + [\![\tau_2[\ell'/\alpha]]\!] & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\
= & [\![(\tau_1[\ell'/\alpha] + \tau_2[\ell'/\alpha])]\!] & \text{(Definition of } [\![\cdot]\!]) \\
= & [\![(\tau_1 + \tau_2)[\ell'/\alpha]]\!] &
\end{array}$$

6. $\mathsf{A} = \tau_1 \xrightarrow{\ell_e} \tau_2$:

$$\begin{array}{lll}
 & \left[\!\!\left[\tau_1 \xrightarrow{\ell_e} \tau_2\right]\!\!\right]_{\ell}[\ell'/\alpha] & \\
= & ([\![\tau_1]\!] \to \forall\beta.(\beta \sqsubseteq \ell_e) \Rightarrow \mathsf{CG}\ \beta\ \beta\ \ [\![\tau_2]\!])\ [\ell'/\alpha] & \text{(Definition of } [\![\cdot]\!]) \\
= & ([\![\tau_1]\!]\,[\ell'/\alpha] \to \forall\beta.(\beta \sqsubseteq \ell_e[\ell'/\alpha]) \Rightarrow \mathsf{CG}\ \beta\ \beta\ \ [\![\tau_2]\!]\,[\ell'/\alpha]) & \\
= & ([\![\tau_1[\ell'/\alpha]]\!] \to \forall\beta.(\beta \sqsubseteq \ell_e[\ell'/\alpha]) \Rightarrow \mathsf{CG}\ \beta\ \beta\ \ [\![\tau_2[\ell'/\alpha]]\!]) & \text{IH(1) on } \tau_1 \text{ and } \tau_2 \\
= & \left[\!\!\left[(\tau_1[\ell'/\alpha] \xrightarrow{\ell_e[\ell'/\alpha]} \tau_2[\ell'/\alpha])\right]\!\!\right]_{\ell[\ell'/\alpha]} & \text{(Definition of } [\![\cdot]\!]) \\
= & \left[\!\!\left[(\tau_1 \xrightarrow{\ell_e} \tau_2)[\ell'/\alpha]\right]\!\!\right]_{\ell[\ell'/\alpha]} &
\end{array}$$

7. $\mathsf{A} = \forall\beta.(\ell_e, \tau_i)$:

$$\begin{array}{lll}
 & [\![\forall\beta.(\ell_e, \tau_i)]\!]\,[\ell'/\alpha] & \\
= & (\forall\beta.\forall\beta'.\beta' \sqsubseteq \ell_e \Rightarrow \mathsf{CG}\ \beta'\ \beta'\ \ [\![\tau_i]\!])[\ell'/\alpha] & \text{(Definition of } [\![\cdot]\!]) \\
= & (\forall\beta.\forall\beta'.\beta' \sqsubseteq \ell_e[\ell'/\alpha] \Rightarrow \mathsf{CG}\ \beta'\ \beta'\ \ [\![\tau_i]\!]\,[\ell'/\alpha]) & \\
= & (\forall\beta.\forall\beta'.\beta' \sqsubseteq \ell_e[\ell'/\alpha] \Rightarrow \mathsf{CG}\ \beta'\ \beta'\ \ [\![\tau_i[\ell'/\alpha]]\!]) & \text{IH(1) on } \tau_i \\
= & [\![\forall\beta.(\ell_e[\ell'/\alpha], \tau_i[\ell'/\alpha])]\!] & \text{(Definition of } [\![\cdot]\!]) \\
= & [\![\forall\beta.(\ell_e, \tau_i)[\ell'/\alpha]]\!] &
\end{array}$$

8. $\mathsf{A} = c \overset{\ell_e}{\Rightarrow} \tau_i$:

$$
\begin{array}{lll}
 & \left[\!\!\left[c \overset{\ell_e}{\Rightarrow} \tau_i\right]\!\!\right][\ell'/\alpha] & \\
= & (\forall\alpha.(\alpha \sqsubseteq \ell_e, c) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_i]\!])[\ell'/\alpha] & \text{(Definition of } [\![\cdot]\!]) \\
= & (\forall\alpha.(\alpha \sqsubseteq \ell_e[\ell'/\alpha], c[\ell'/\alpha]) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_i]\!][\ell'/\alpha]) & \\
= & (\forall\alpha.(\alpha \sqsubseteq \ell_e[\ell'/\alpha], c[\ell'/\alpha]) \Rightarrow \mathsf{CG}\ \alpha\ \alpha\ [\![\tau_i[\ell'/\alpha]]\!]) & \text{IH(1) on } \tau_i \\
= & \left[\!\!\left[c[\ell'/\alpha] \overset{\ell_e[\ell'/\alpha]}{\Rightarrow} \tau_i[\ell'/\alpha]\right]\!\!\right] & \text{(Definition of } [\![\cdot]\!]) \\
= & \left[\!\!\left[(c \overset{\ell_e}{\Rightarrow} \tau_i)[\ell'/\alpha]\right]\!\!\right] &
\end{array}
$$

□

E CG $\rightsquigarrow$ FG

CG types are translated into FG types by the following definition of $[\![\cdot]\!]$

$$
\begin{array}{rclcrcl}
[\![\mathsf{b}]\!] & = & \mathsf{b}^{\perp} & & & & \\
[\![\tau_1 \to \tau_2]\!] & = & ([\![\tau_1]\!] \overset{\top}{\to} [\![\tau_2]\!])^{\perp} & & [\![\mathsf{ref}\ \ell\ \tau]\!] & = & (\mathsf{ref}\ ([\![\tau]\!] + \mathsf{unit})^{\ell})^{\perp} \\
[\![\tau_1 \times \tau_2]\!] & = & ([\![\tau_1]\!] \times [\![\tau_2]\!])^{\perp} & & [\![\mathsf{CG}\ \ell_i\ \ell_o\ \tau]\!] & = & (\mathsf{unit} \overset{\ell_i}{\to} ([\![\tau]\!] + \mathsf{unit})^{\ell_o})^{\perp} \\
[\![\tau_1 + \tau_2]\!] & = & ([\![\tau_1]\!] + [\![\tau_2]\!])^{\perp} & & [\![c \Rightarrow \tau]\!] & = & (c \overset{\top}{\Rightarrow} [\![\tau]\!])^{\perp} \\
[\![\mathsf{Labeled}\ \ell\ \tau]\!] & = & ([\![\tau]\!] + \mathsf{unit})^{\ell} & & [\![\forall\alpha.\tau]\!] & = & (\forall\alpha.(\top, [\![\tau]\!]))^{\perp}
\end{array}
$$

The translation judgment for expressions is of the form $\boxed{\Sigma; \Psi; \Gamma \vdash_{pc} e_C : \tau_C \rightsquigarrow e_F}$. Its rules are shown below.

$$\frac{}{\Sigma; \Psi; \Gamma, x : \tau \vdash x : \tau \rightsquigarrow x}\ \text{var}$$

$$\frac{\Sigma; \Psi; \Gamma, x : \tau \vdash e : \tau' \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \lambda x.e : \tau \to \tau' \rightsquigarrow \lambda x.e_F}\ \text{lam}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \tau \to \tau' \rightsquigarrow e_{F1} \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \tau \rightsquigarrow e_{F2}}{\Sigma; \Psi; \Gamma \vdash e_1\ e_2 : \tau' \rightsquigarrow e_{F1}\ e_{F2}}\ \text{app}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \tau_1 \rightsquigarrow e_{F1} \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \tau_2 \rightsquigarrow e_{F2}}{\Sigma; \Psi; \Gamma \vdash (e_1, e_2) : (\tau_1 \times \tau_2)^{\perp} \rightsquigarrow (e_{F1}, e_{F2})}\ \text{prod}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1 \times \tau_2 \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{fst}(e) : \tau_1 \rightsquigarrow \mathsf{fst}(e_F)}\ \text{fst}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1 \times \tau_2 \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{snd}(e) : \tau_1 \rightsquigarrow \mathsf{snd}(e_F)}\ \text{snd}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1 \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{inl}(e) : \tau_1 + \tau_2 \rightsquigarrow \mathsf{inl}(e_F)}\ \text{inl}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1 \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{inr}(e) : \tau_1 + \tau_2 \rightsquigarrow \mathsf{inr}(e_F)}\ \text{inr}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau_1 + \tau_2 \rightsquigarrow e_F \qquad \Sigma; \Psi; \Gamma, x : \tau_1 \vdash e_1 : \tau \rightsquigarrow e_{F1} \qquad \Sigma; \Psi; \Gamma, y : \tau_2 \vdash e_2 : \tau \rightsquigarrow e_{F2}}{\Sigma; \Psi; \Gamma \vdash \mathsf{case}(e, x.e_1, y.e_2) : \tau \rightsquigarrow \mathsf{case}(e_F, x.e_{F1}, y.e_{F2})}\ \text{case}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{Lb}_{\ell}(e) : (\mathsf{Labeled}\ \ell\ \tau) \rightsquigarrow \mathsf{inl}(e_F)}\ \text{label}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{Labeled}\ \ell\ \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{unlabel}(e) : \mathsf{CG}\ \ell_i\ (\ell_i \sqcup \ell)\ \tau \rightsquigarrow \lambda\_.e_F}\ \text{unlabel}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{CG}\ \ell_i\ \ell_o\ \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{toLabeled}(e) : \mathsf{CG}\ \ell_i\ \ell_i\ (\mathsf{Labeled}\ \ell_o\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(e_F\ ())}\ \text{toLabeled}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \mathsf{ret}(e) : \mathsf{CG}\ \ell_i\ \ell_i\ \tau \rightsquigarrow \lambda\_.\mathsf{inl}(e_F)}\ \text{ret}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \mathsf{CG}\ \ell_i\ \ell\ \tau \rightsquigarrow e_{F1} \qquad \Sigma; \Psi; \Gamma, x : \tau \vdash e_2 : \mathsf{CG}\ \ell\ \ell_o\ \tau' \rightsquigarrow e_{F2}}{\Sigma; \Psi; \Gamma \vdash \mathsf{bind}(e_1, x.e_2) : \mathsf{CG}\ \ell_i\ \ell_o\ \tau' \rightsquigarrow \lambda\_.\mathsf{case}(e_{F1}(), x.e_{F2}(), y.\mathsf{inr}())}\ \text{bind}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{Labeled}\ \ell'\ \tau \rightsquigarrow e_F \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash \mathsf{new}\ e : \mathsf{CG}\ \ell\ \ell\ (\mathsf{ref}\ \ell'\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(\mathsf{new}\ (e_F))}\ \text{ref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \mathsf{ref}\ \ell\ \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash !e : \mathsf{CG}\ \ell'\ \ell'\ (\mathsf{Labeled}\ \ell\ \tau) \rightsquigarrow \lambda\_.\mathsf{inl}(e_F)}\ \text{deref}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e_1 : \mathsf{ref}\ \ell'\ \tau \rightsquigarrow e_{F1} \qquad \Sigma; \Psi; \Gamma \vdash e_2 : \mathsf{Labeled}\ \ell'\ \tau \rightsquigarrow e_{F2} \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi; \Gamma \vdash e_1 := e_2 : \mathsf{CG}\ \ell\ \ell\ \mathsf{unit} \rightsquigarrow \lambda\_.\mathsf{inl}(e_{F1} := e_{F2})}\ \text{assign}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \tau' \rightsquigarrow e_F \qquad \Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e_F}\ \text{sub}$$

$$\frac{\Sigma, \alpha; \Psi; \Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \Lambda e : \forall \alpha.\tau \rightsquigarrow \Lambda e_F}\ \text{FI}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : \forall \alpha.\tau \rightsquigarrow e_F \qquad FV(\ell) \in \Sigma}{\Sigma; \Psi; \Gamma \vdash e\ [] : \tau[\ell/\alpha] \rightsquigarrow e_F[]}\ \text{FE}$$

$$\frac{\Sigma; \Psi, c; \Gamma \vdash e : \tau \rightsquigarrow e_F}{\Sigma; \Psi; \Gamma \vdash \nu\ e : c \Rightarrow \tau \rightsquigarrow \nu\ e_F}\ \text{CI}$$

$$\frac{\Sigma; \Psi; \Gamma \vdash e : c \Rightarrow \tau \rightsquigarrow e_F \qquad \Sigma; \Psi \vdash c}{\Sigma; \Psi; \Gamma \vdash e\ \bullet : \tau \rightsquigarrow e_F \bullet}\ \text{CE}$$

Assumption E.1. $\forall e, \tau, \Sigma, \Psi, \Gamma, \ell_i, \ell_o.$
$\Sigma; \Psi; \Gamma \vdash e : \mathsf{CG}\ \ell_i\ \ell_o\ \tau \implies \ell_i \sqsubseteq \ell_o$

Theorem E.2 (Type soundness, CG $\rightsquigarrow$ FG)**.** $\forall \Sigma, \Psi, \Gamma, e_C, \tau.$
$\Sigma; \Psi; \Gamma \vdash e_C : \tau$ *is a valid typing derivation in CG* $\implies$
$\exists e_F.$
$\Sigma; \Psi; \Gamma \vdash e_C : \tau \rightsquigarrow e_F\ \wedge$
$\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top e_F : [\![\tau]\!]$ *is a valid typing derivation in FG*

Proof. Proof by induction on the translation judgment. We show selected cases below.

1. label:

$$\dfrac{\dfrac{\overline{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top e_F : [\![\tau]\!]}\ \text{IH}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top \mathsf{inl}(e_F) : ([\![\tau]\!] + \mathsf{unit})^\perp}\ \text{FG-inl}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top \mathsf{inl}(e_F) : ([\![\tau]\!] + \mathsf{unit})^\ell}\ \text{FG-sub}$$

2. unlabel:

   P1:

$$\dfrac{\Sigma;\Psi \vdash \ell \sqsubseteq \ell_i \sqcup \ell \qquad \dfrac{}{\Sigma;\Psi \vdash (\llbracket\tau\rrbracket + \mathsf{unit}) <: (\llbracket\tau\rrbracket + \mathsf{unit})}\text{ Lemma B.1}}{\Sigma;\Psi \vdash (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell} <: (\llbracket\tau\rrbracket + \mathsf{unit})^{\ell_i \sqcup \ell}}\text{ FGsub-label}$$

   Main derivation:

$$\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi;\llbracket\Gamma\rrbracket, \_ : \mathsf{unit} \vdash_\top e_F : (\llbracket\tau\rrbracket+\mathsf{unit})^\ell}\text{ IH, Weakening} \qquad \Sigma;\Psi\vdash \ell_i \sqsubseteq \top \qquad P1}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_ : \mathsf{unit} \vdash_{\ell_i} e_F : (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell_i\sqcup\ell}}\text{ FG-sub}}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_:\mathsf{unit}\vdash_\top \lambda\_.e_F : (\mathsf{unit} \xrightarrow{\ell_i} (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell_i\sqcup\ell})^\perp}\text{ FG-lam}$$

3. toLabeled:

   P2:

$$\dfrac{\dfrac{}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_ : \mathsf{unit} \vdash_\top e_F : (\mathsf{unit} \xrightarrow{\ell_i} (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell_o})^\perp}\text{ IH, Weakening} \qquad \Sigma;\Psi\vdash \ell_i \sqsubseteq \top}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_ : \mathsf{unit} \vdash_{\ell_i} e_F : (\mathsf{unit} \xrightarrow{\ell_i} (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell_o})^\perp}\text{ FG-sub}$$

   P1:

$$\dfrac{P2 \qquad \dfrac{}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_ : \mathsf{unit} \vdash_{\ell_i} () : \mathsf{unit}} \qquad \Sigma;\Psi\vdash \ell_i \sqcup \perp \sqsubseteq \ell_i \qquad \Sigma;\Psi \vdash (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell_o} \searrow \perp}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_ : \mathsf{unit} \vdash_{\ell_i} e_F() : (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell_o}}\text{ FG-app}$$

   Main derivation:

$$\dfrac{\dfrac{P1 \qquad \Sigma;\Psi\vdash \perp \sqsubseteq \ell_i}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_ : \mathsf{unit} \vdash_{\ell_i} \mathsf{inl}(e_F()) : ((\llbracket\tau\rrbracket+\mathsf{unit})^{\ell_o}+\mathsf{unit})^{\ell_i}}\text{ FG-inl, FG-sub}}{\Sigma;\Psi;\llbracket\Gamma\rrbracket \vdash_\top \lambda\_.\mathsf{inl}(e_F()) : (\mathsf{unit} \xrightarrow{\ell_i} ((\llbracket\tau\rrbracket+\mathsf{unit})^{\ell_o}+\mathsf{unit})^{\ell_i})^\perp}\text{ FG-lam}$$

4. ret:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_ : \mathsf{unit} \vdash_\top e_F : \llbracket\tau\rrbracket}\text{ IH, Weakening} \qquad \Sigma;\Psi\vdash \ell_i \sqsubseteq \top}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_ : \mathsf{unit} \vdash_{\ell_i} e_F : \llbracket\tau\rrbracket}\text{ FG-sub} \qquad \Sigma;\Psi\vdash \perp \sqsubseteq \ell_i}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_ : \mathsf{unit} \vdash_{\ell_i} \mathsf{inl}(e_F) : (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell_i}}\text{ FG-sub, FG-inl}}{\Sigma;\Psi;\llbracket\Gamma\rrbracket \vdash_\top \lambda\_.\mathsf{inl}(e_F) : (\mathsf{unit} \xrightarrow{\ell_i} (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell_i})^\perp}\text{ FG-lam}$$

5. bind:

   P1.1:

$$\dfrac{\dfrac{}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_ : \mathsf{unit} \vdash_\top e_{F1} : (\mathsf{unit} \xrightarrow{\ell_i} (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell})^\perp}\text{ IH1, Weakening} \qquad \Sigma;\Psi\vdash \ell_i \sqsubseteq \top}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_ : \mathsf{unit} \vdash_{\ell_i} e_{F1} : (\mathsf{unit} \xrightarrow{\ell_i} (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell})^\perp}\text{ FG-sub}$$

   P1:

$$\dfrac{P1.1 \qquad \dfrac{}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_ : \mathsf{unit} \vdash_{\ell_i} () : \mathsf{unit}}\text{ FG-var} \qquad \Sigma;\Psi\vdash (\ell_i \sqcup \perp) \sqsubseteq \ell_i \qquad \dfrac{\Sigma;\Psi\vdash \perp \sqsubseteq \ell}{\Sigma;\Psi \vdash (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell} \searrow \perp}}{\Sigma;\Psi;\llbracket\Gamma\rrbracket,\_ : \mathsf{unit} \vdash_{\ell_i} e_{F1}() : (\llbracket\tau\rrbracket+\mathsf{unit})^{\ell}}\text{ FG-app}$$

P2.1:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit}, x : [\![\tau]\!] \vdash_\top e_{F2} : (\mathsf{unit} \xrightarrow{\ell} ([\![\tau']\!] + \mathsf{unit})^{\ell_o})^\perp}\ \text{IH2, Weakening} \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \top}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit}, x : [\![\tau]\!] \vdash_\ell e_{F2} : (\mathsf{unit} \xrightarrow{\ell} ([\![\tau']\!] + \mathsf{unit})^{\ell_o})^\perp}\ \text{FG-sub}$$

P2:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit}, x : [\![\tau]\!] \vdash_\ell () : \mathsf{unit}}\ \text{FG-var} \qquad \overset{P2.1}{\Sigma; \Psi \vdash (\ell \sqcup \bot) \sqsubseteq \ell} \qquad \dfrac{\Sigma; \Psi \vdash \bot \sqsubseteq \ell_o}{\Sigma; \Psi \vdash ([\![\tau']\!] + \mathsf{unit})^{\ell_o} \searrow \bot}}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit}, x : [\![\tau]\!] \vdash_{\ell_i \sqcup \ell} e_{F2}() : ([\![\tau']\!] + \mathsf{unit})^{\ell_o}}\ \text{FG-app}$$

P3:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit}, y : \mathsf{unit} \vdash_\ell () : \mathsf{unit}}\ \text{FG-var} \qquad \Sigma; \Psi \vdash \bot \sqsubseteq \ell_o}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit}, y : \mathsf{unit} \vdash_\ell \mathsf{inr}() : ([\![\tau']\!] + \mathsf{unit})^{\ell_o}}\ \text{FG-sub, FG-inr}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad P2 \qquad P3 \qquad \dfrac{\dfrac{\dfrac{}{\Sigma; \Psi; \Gamma \vdash e_2 : \mathsf{CG}\ \ell\ \ell_o\ \tau}\ \text{Given}}{\Sigma; \Psi \vdash \ell \sqsubseteq \ell_o}\ \text{Assumption E.1}}{\Sigma; \Psi \vdash ([\![\tau']\!] + \mathsf{unit})^{\ell_o} \searrow \ell}}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell_i} \mathsf{case}(e_{F1}(), x.e_{F2}(), y.\mathsf{inr}()) : ([\![\tau']\!] + \mathsf{unit})^{\ell_o}}\ \text{FG-case}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top \lambda\_.\mathsf{case}(e_{F1}(), x.e_{F2}(), y.\mathsf{inr}()) : (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau']\!] + \mathsf{unit})^{\ell_o})^\perp}\ \text{FG-lam, weak}$$

6. ref:

P1:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_\top e_F : ([\![\tau]\!] + \mathsf{unit})^{\ell'}}\ \text{IH, Weakening} \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \top}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_\ell e_F : ([\![\tau]\!] + \mathsf{unit})^{\ell'}}\ \text{FG-sub} \quad \dfrac{\Sigma; \Psi \vdash \ell \sqsubseteq \ell'}{\Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell'} \searrow \ell}}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_\ell \mathsf{new}\ e_F : (\mathsf{ref}([\![\tau]\!] + \mathsf{unit})^{\ell'})^\perp}\ \text{FG-ref}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad \Sigma; \Psi \vdash \bot \sqsubseteq \ell}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_\ell \mathsf{inl}(\mathsf{new}\ e_F) : ((\mathsf{ref}([\![\tau]\!] + \mathsf{unit})^{\ell'})^\perp + \mathsf{unit})^\ell}\ \text{FG-inl, FG-sub}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top \lambda\_.\mathsf{inl}(\mathsf{new}\ e_F) : (\mathsf{unit} \xrightarrow{\ell} ((\mathsf{ref}([\![\tau]\!] + \mathsf{unit})^{\ell'})^\perp + \mathsf{unit})^\ell)^\perp}\ \text{FG-lam}$$

7. deref:

P2:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_\top e_F : (\mathsf{ref}\ ([\![\tau]\!] + \mathsf{unit})^\ell)^\perp}\ \text{IH, Weakening} \qquad \Sigma; \Psi \vdash \ell' \sqsubseteq \top}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell'} e_F : (\mathsf{ref}\ ([\![\tau]\!] + \mathsf{unit})^\ell)^\perp}\ \text{FG-sub}$$

P1:

$$\dfrac{P2 \qquad \dfrac{}{\Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell} <: ([\![\tau]\!] + \mathsf{unit})^{\ell}}\text{Lemma B.1} \qquad \dfrac{}{\Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell} \searrow \bot}}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell'} !e_F : ([\![\tau]\!] + \mathsf{unit})^{\ell}}\text{FG-deref}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad \Sigma; \Psi \vdash \bot \sqsubseteq \ell' \qquad \dfrac{\Sigma; \Psi \vdash \ell \sqsubseteq \ell}{\Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell} <: ([\![\tau]\!] + \mathsf{unit})^{\ell}}}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell'} \mathsf{inl}(!e_F) : (([\![\tau]\!] + \mathsf{unit})^{\ell} + \mathsf{unit})^{\ell'}}\text{FG-inl, FG-sub}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_{\top} \lambda\_.\mathsf{inl}(!e_F) : (\mathsf{unit} \xrightarrow{\ell'} (([\![\tau]\!] + \mathsf{unit})^{\ell} + \mathsf{unit})^{\ell'})^{\bot}}\text{FG-lam}$$

8. assign:

P3:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\top} e_{F2} : ([\![\tau]\!] + \mathsf{unit})^{\ell'}}\text{IH2, Weakening} \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \top}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} e_{F2} : ([\![\tau]\!] + \mathsf{unit})^{\ell'}}\text{FG-sub}$$

P2:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\top} e_{F1} : (\mathsf{ref}([\![\tau]\!] + \mathsf{unit})^{\ell'})^{\bot}}\text{IH1, Weakening} \qquad \Sigma; \Psi \vdash \ell \sqsubseteq \top}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} e_{F1} : (\mathsf{ref}([\![\tau]\!] + \mathsf{unit})^{\ell'})^{\bot}}\text{FG-sub}$$

P1:

$$\dfrac{P2 \qquad P3 \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \ell \sqsubseteq \ell'}\text{Given}}{\Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell'} \searrow (\ell \sqcup \bot)}}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} e_{F1} := e_{F2} : \mathsf{unit}}\text{FG-assign}$$

Main derivation:

$$\dfrac{\dfrac{P1 \qquad \Sigma; \Psi \vdash \bot \sqsubseteq \ell}{\Sigma; \Psi; [\![\Gamma]\!], \_ : \mathsf{unit} \vdash_{\ell} \mathsf{inl}(e_{F1} := e_{F2}) : (\mathsf{unit} + \mathsf{unit})^{\ell}}\text{FG-inl, FG-sub}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_{\top} \lambda\_.\mathsf{inl}(e_{F1} := e_{F2}) : (\mathsf{unit} \xrightarrow{\ell} (\mathsf{unit} + \mathsf{unit})^{\ell})^{\bot}}\text{FG-lam}$$

9. sub:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_{\top} e_F : [\![\tau']\!]}\text{IH} \qquad \Sigma; \Psi \vdash \top \sqsubseteq \top \qquad \dfrac{\Sigma; \Psi \vdash \tau' <: \tau}{\Sigma; \Psi \vdash [\![\tau']\!] <: [\![\tau]\!]}\text{Lemma E.3}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_{\top} e_F : [\![\tau]\!]}\text{FG-sub}$$

10. FI:

$$\dfrac{\dfrac{}{\Sigma, \alpha; \Psi; [\![\Gamma]\!] \vdash_{\top} e_F : [\![\tau]\!]}\text{IH}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_{\top} \Lambda e_F : (\forall \alpha.(\top, [\![\tau]\!]))^{\bot}}\text{FG-FI}$$

11. FE:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_{\top} e_F : (\forall \alpha.(\top, [\![\tau]\!]))^{\bot}}\text{IH} \qquad FV(\ell) \in \Sigma \qquad \Sigma; \Psi \vdash \top \sqcup \bot \sqsubseteq \top \qquad \Sigma; \Psi \vdash [\![\tau[\ell/\alpha]]\!] \searrow \bot}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_{\top} e_F\ [\,] : [\![\tau]\!]\,[\ell/\alpha]}\text{FG-FE}$$

12. CI:

$$\dfrac{\dfrac{}{\Sigma; \Psi, c; [\![\Gamma]\!] \vdash_\top e_F : [\![\tau]\!]}\ \text{IH}}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top \nu\ e_F : (c \overset{\top}{\Rightarrow} [\![\tau]\!])^\perp}\ \text{FG-CI}$$

13. CE:

$$\dfrac{\dfrac{}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top e_F : (c \overset{\top}{\Rightarrow} [\![\tau]\!])^\perp}\ \text{IH} \qquad \Sigma; \Psi \vdash c \qquad \Sigma; \Psi \vdash \top \sqcup \bot \sqsubseteq \top \qquad \Sigma; \Psi \vdash [\![\tau]\!] \searrow \bot}{\Sigma; \Psi; [\![\Gamma]\!] \vdash_\top e_F \bullet : [\![\tau]\!]}\ \text{FG-CE}$$

∎

Lemma E.3. *For any CG types τ and τ', Σ, and Ψ, if $\Sigma; \Psi \vdash \tau <: \tau'$, then $\Sigma; \Psi \vdash [\![\tau]\!] <: [\![\tau']\!]$.*

Proof. Proof by induction on CG's subtyping relation

1. CGsub-base:

$$\dfrac{}{\Sigma; \Psi \vdash [\![\tau]\!] <: [\![\tau]\!]}\ \text{Lemma B.1}$$

2. CGsub-arrow:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1']\!] <: [\![\tau_1]\!]}\ \text{IH1} \qquad \dfrac{}{\Sigma; \Psi \vdash [\![\tau_2]\!] <: [\![\tau_2']\!]}\ \text{IH2} \qquad \Sigma; \Psi \vdash \top \sqsubseteq \top}{\Sigma; \Psi \vdash ([\![\tau_1]\!] \xrightarrow{\top} [\![\tau_2]\!])^\perp <: ([\![\tau_1']\!] \xrightarrow{\top} [\![\tau_2']\!])^\perp}\ \text{FGsub-arrow}}{\Sigma; \Psi \vdash \left[\!\!\left[(\tau_1 \xrightarrow{\ell_e} \tau_2)\right]\!\!\right] <: \left[\!\!\left[(\tau_1' \xrightarrow{\ell_e'} \tau_2')\right]\!\!\right]}\ \text{Definition of } [\![\cdot]\!]$$

3. CGsub-prod:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1]\!] <: [\![\tau_1']\!]}\ \text{IH1} \qquad \dfrac{}{\Sigma; \Psi \vdash [\![\tau_2]\!] <: [\![\tau_2']\!]}\ \text{IH2}}{\Sigma; \Psi \vdash ([\![\tau_1]\!] \times [\![\tau_2]\!])^\perp <: ([\![\tau_1']\!] \times [\![\tau_2']\!])^\perp}\ \text{FGsub-arrow}}{\Sigma; \Psi \vdash [\![(\tau_1 \times \tau_2)]\!] <: [\![(\tau_1' \times \tau_2')]\!]}\ \text{Definition of } [\![\cdot]\!]$$

4. CGsub-sum:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1]\!] <: [\![\tau_1']\!]}\ \text{IH1} \qquad \dfrac{}{\Sigma; \Psi \vdash [\![\tau_2]\!] <: [\![\tau_2']\!]}\ \text{IH2}}{\Sigma; \Psi \vdash ([\![\tau_1]\!] + [\![\tau_2]\!])^\perp <: ([\![\tau_1']\!] + [\![\tau_2']\!])^\perp}\ \text{FGsub-arrow}}{\Sigma; \Psi \vdash [\![(\tau_1 + \tau_2)]\!] <: [\![(\tau_1' + \tau_2')]\!]}\ \text{Definition of } [\![\cdot]\!]$$

5. CGsub-labeled:

$$\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1]\!] <: [\![\tau_1']\!]}\ \text{IH1} \qquad \dfrac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}}\ \text{FGsub-unit}}{\Sigma; \Psi \vdash ([\![\tau_1]\!] + \mathsf{unit}) <: ([\![\tau_1']\!] + \mathsf{unit})}\ \text{FGsub-sum} \qquad \dfrac{\dfrac{}{\mathsf{Labeled}\ \ell_1\ \tau_1 <: \mathsf{Labeled}\ \ell_1'\ \tau_1'}\ \text{Given}}{\ell_1 \sqsubseteq \ell_1'}\ \text{By inversion}}{\Sigma; \Psi \vdash ([\![\tau_1]\!] + \mathsf{unit})^{\ell_1} <: ([\![\tau_1']\!] + \mathsf{unit})^{\ell_1'}}\ \text{FGsub-arrow}}{\Sigma; \Psi \vdash [\![\mathsf{Labeled}\ \ell_1\ \tau_1]\!] <: [\![\mathsf{Labeled}\ \ell_1'\ \tau_1']\!]}\ \text{Definition of } [\![\cdot]\!]$$

6. CGsub-monad:

   P3:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1]\!] <: [\![\tau_1']\!]}\ \text{IH} \qquad \dfrac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}}\ \text{FGsub-unit}}{\Sigma; \Psi \vdash ([\![\tau_1]\!] + \mathsf{unit}) <: ([\![\tau_1']\!] + \mathsf{unit})}\ \text{FGsub-sum}$$

   P2:

$$\dfrac{P3 \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{CG}\ \ell_i\ \ell_o\ \tau_1 <: \mathsf{CG}\ \ell_i'\ \ell_o'\ \tau_1'}\ \text{Given}}{\Sigma; \Psi \vdash \ell_o \sqsubseteq \ell_o'}\ \text{By inversion}}{\Sigma; \Psi \vdash ([\![\tau_1]\!] + \mathsf{unit})^{\ell_o} <: ([\![\tau_1']\!] + \mathsf{unit})^{\ell_o'}}\ \text{FGsub-label}$$

   P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{unit} <: \mathsf{unit}} \qquad P2 \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{CG}\ \ell_i\ \ell_o\ \tau_1 <: \mathsf{CG}\ \ell_i'\ \ell_o'\ \tau_1'}\ \text{Given}}{\Sigma; \Psi \vdash \ell_i' \sqsubseteq \ell_i}}{\Sigma; \Psi \vdash (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau_1]\!] + \mathsf{unit})^{\ell_o}) <: (\mathsf{unit} \xrightarrow{\ell_i'} ([\![\tau_1']\!] + \mathsf{unit})^{\ell_o'})}\ \text{FGsub-arrow}$$

   Main derivation:

$$\dfrac{\dfrac{P1 \qquad \dfrac{}{\Sigma; \Psi \vdash \bot \sqsubseteq \bot}}{\Sigma; \Psi \vdash (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau_1]\!] + \mathsf{unit})^{\ell_o})^{\bot} <: (\mathsf{unit} \xrightarrow{\ell_i'} ([\![\tau_1']\!] + \mathsf{unit})^{\ell_o'})^{\bot}}\ \text{FGsub-label}}{\Sigma; \Psi \vdash [\![\mathsf{CG}\ \ell_i\ \ell_o\ \tau_1]\!] <: [\![\mathsf{CG}\ \ell_i'\ \ell_o'\ \tau_1']\!]}\ \text{Definition of } [\![\cdot]\!]$$

7. CGsub-forall:

   P1:

$$\dfrac{\dfrac{}{\Sigma, \alpha; \Psi \vdash [\![\tau]\!] <: [\![\tau']\!]}\ \text{IH, Weakening} \qquad \dfrac{}{\Sigma, \alpha; \Psi \vdash \top \sqsubseteq \top}}{\Sigma; \Psi \vdash (\forall \alpha.(\top, [\![\tau]\!])) <: (\forall \alpha.(\top, [\![\tau']\!]))}\ \text{FGsub-forall}$$

   Main derivation:

$$\dfrac{\dfrac{P1 \qquad \dfrac{}{\Sigma, \alpha; \Psi \vdash \bot \sqsubseteq \bot}}{\Sigma; \Psi \vdash (\forall \alpha.(\top, [\![\tau]\!]))^{\bot} <: (\forall \alpha.(\top, [\![\tau']\!]))^{\bot}}\ \text{FGsub-label}}{\Sigma; \Psi \vdash [\![\forall \alpha.\tau]\!] <: [\![\forall \alpha.\tau']\!]}$$

8. CGsub-constraint:

   P1:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau]\!] <: [\![\tau']\!]}\ \text{IH} \qquad \dfrac{}{\Sigma; \Psi \vdash \top \sqsubseteq \top} \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash c \Rightarrow \tau <: c' \Rightarrow \tau'}\ \text{Given}}{\Sigma; \Psi \vdash c' \implies c}\ \text{By inversion}}{\Sigma; \Psi \vdash (c \overset{\top}{\Rightarrow} [\![\tau]\!]) <: (c' \overset{\top}{\Rightarrow} [\![\tau']\!])}\ \text{FGsub-constraint}$$

   Main derivation:

$$\dfrac{\dfrac{P1 \qquad \dfrac{}{\Sigma, \alpha; \Psi \vdash \bot \sqsubseteq \bot}}{\Sigma; \Psi \vdash (c \overset{\top}{\Rightarrow} [\![\tau]\!])^{\bot} <: (c' \overset{\top}{\Rightarrow} [\![\tau']\!])^{\bot}}\ \text{FGsub-label}}{\Sigma; \Psi \vdash [\![c \Rightarrow \tau]\!] <: [\![c' \Rightarrow \tau']\!]}$$

$\square$

Lemma E.4 (Preservation of well-formedness for closed reference types)**.** $\forall \Sigma, \Psi, \tau.$
$\Sigma; \Psi \vdash \tau\ WF \implies \Sigma; \Psi \vdash [\![\tau]\!]\ WF$

Proof. Proof by induction on the $\tau\ WF$ relation.

1. CG-wff-base:

$$\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{b}\ WF}\ \text{FG-wff-base}}{\Sigma; \Psi \vdash \mathsf{b}^{\perp}\ WF}\ \text{FG-wff-label}$$

2. CG-wff-unit:

$$\dfrac{}{\Sigma; \Psi \vdash \mathsf{unit}\ WF}\ \text{FG-wff-unit}$$

3. CG-wff-arrow:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1]\!]\ WF}\ \text{IH1} \qquad \dfrac{}{\Sigma; \Psi \vdash [\![\tau_2]\!]\ WF}\ \text{IH2}}{\Sigma; \Psi \vdash ([\![\tau_1]\!] \xrightarrow{\top} [\![\tau_2]\!])\ WF}\ \text{FG-wff-arrow}}{\Sigma; \Psi \vdash ([\![\tau_1]\!] \xrightarrow{\top} [\![\tau_2]\!])^{\perp}\ WF}\ \text{FG-wff-label}$$

4. CG-wff-prod:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1]\!]\ WF}\ \text{IH1} \qquad \dfrac{}{\Sigma; \Psi \vdash [\![\tau_2]\!]\ WF}\ \text{IH2}}{\Sigma; \Psi \vdash [\![(]\!]\ \tau_1 \times [\![\tau_2]\!])\ WF}\ \text{FG-wff-prod}}{\Sigma; \Psi \vdash [\![(]\!]\ \tau_1 \times [\![\tau_2]\!])^{\perp}\ WF}\ \text{FG-wff-label}$$

5. CG-wff-sum:

$$\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash [\![\tau_1]\!]\ WF}\ \text{IH1} \qquad \dfrac{}{\Sigma; \Psi \vdash [\![\tau_2]\!]\ WF}\ \text{IH2}}{\Sigma; \Psi \vdash [\![\tau_1]\!] + [\![\tau_2]\!]\ WF}\ \text{FG-wff-prod}}{\Sigma; \Psi \vdash [\![(]\!]\ \tau_1 + [\![\tau_2]\!])^{\perp}\ WF}\ \text{FG-wff-label}$$

6. CG-wff-ref:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \ell\ \tau\ WF}\ \text{Given}}{FV(\tau) = \emptyset}\ \text{By inversion}}{FV([\![\tau]\!]) = \emptyset}\ \text{Lemma E.5} \qquad \dfrac{}{FV(\mathsf{unit}) = \emptyset} \qquad \dfrac{\dfrac{}{\Sigma; \Psi \vdash \mathsf{ref}\ \ell\ \tau\ WF}\ \text{Given}}{FV(\ell) = \emptyset}\ \text{By inversion}}{\Sigma; \Psi \vdash FV(([\![\tau]\!] + \mathsf{unit})^{\ell}) = \emptyset}}{\Sigma; \Psi \vdash \mathsf{ref}\ ([\![\tau]\!] + \mathsf{unit})^{\ell}\ WF}\ \text{FG-wff-ref}}{\Sigma; \Psi \vdash (\mathsf{ref}\ ([\![\tau]\!] + \mathsf{unit})^{\ell})^{\perp}\ WF}\ \text{FG-wff-label}$$

7. CG-wff-forall:

$$\dfrac{\dfrac{\overline{\Sigma, \alpha; \Psi \vdash [\![\tau]\!]\ WF}\ \text{IH}}{\Sigma; \Psi \vdash (\forall\alpha.(\top, [\![\tau]\!]))\ WF}\ \text{FG-wff-forall}}{\Sigma; \Psi \vdash (\forall\alpha.(\top, [\![\tau]\!]))^{\perp}\ WF}\ \text{CG-wff-label}$$

8. CG-wff-constraint:

$$\dfrac{\dfrac{\overline{\Sigma; \Psi, c \vdash [\![\tau]\!]\ WF}\ \text{IH}}{\Sigma; \Psi \vdash (c \stackrel{\top}{\Rightarrow} [\![\tau]\!])\ WF}\ \text{FG-wff-constraint}}{\Sigma; \Psi \vdash (c \stackrel{\top}{\Rightarrow} [\![\tau]\!])^{\perp}\ WF}\ \text{CG-wff-label}$$

9. CG-wff-labeled:

$$\dfrac{\dfrac{\overline{\Sigma; \Psi \vdash [\![\tau]\!]\ WF}\ \text{IH} \qquad \overline{\Sigma; \Psi \vdash \mathsf{unit}\ WF}\ \text{FG-wff-unit}}{\Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit})\ WF}\ \text{FG-wff-sum}}{\Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell}\ WF}\ \text{CG-wff-label}$$

10. CG-wff-monad:

P1:

$$\dfrac{\overline{\Sigma; \Psi \vdash [\![\tau]\!]\ \ WF}\ \text{IH} \qquad \overline{\Sigma; \Psi \vdash \mathsf{unit}\ WF}\ \text{FG-wff-unit}}{\Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit})\ WF}\ \text{FG-wff-sum}$$

Main derivation:

$$\dfrac{\dfrac{\overline{\Sigma; \Psi \vdash \mathsf{unit}\ WF}\ \text{FG-wff-unit} \qquad \dfrac{P1}{\Sigma; \Psi \vdash ([\![\tau]\!] + \mathsf{unit})^{\ell_o}\ \ WF}\ \text{FG-wff-label}}{\Sigma; \Psi \vdash (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau]\!] + \mathsf{unit})^{\ell_o})\ WF}\ \text{FG-wff-sum}}{\Sigma; \Psi \vdash (\mathsf{unit} \xrightarrow{\ell_i} ([\![\tau]\!] + \mathsf{unit})^{\ell_o})^{\perp}\ \ WF}\ \text{CG-wff-label}$$

$\square$

Lemma E.5. $\forall\tau.\ FV([\![\tau]\!]) \subseteq FV(\tau)$

Proof. Proof by inducitonon on the CG types, τ

1. $\tau = \mathsf{b}$:

$$\begin{array}{lll} & FV([\![\mathsf{b}]\!]) & \\ = & FV(\mathsf{b}^{\perp}) & \text{Definition of } [\![\cdot]\!] \\ = & \emptyset & \\ = & FV(\mathsf{b}) & \end{array}$$

2. $\tau = \mathsf{unit}$:

$$\begin{array}{lll} & FV([\![\mathsf{b}]\!]) & \\ = & FV(\mathsf{unit}^{\perp}) & \text{Definition of } [\![\cdot]\!] \\ = & \emptyset & \\ = & FV(\mathsf{unit}) & \end{array}$$

3. $\tau = \tau_1 \to \tau_2$:

$$\begin{array}{lll} & FV(\llbracket \tau_1 \to \tau_2 \rrbracket) & \\ = & FV(\llbracket \tau_1 \rrbracket \xrightarrow{\top} \llbracket \tau_2 \rrbracket)^{\perp} & \text{Definition of } \llbracket\cdot\rrbracket \\ = & FV(\llbracket \tau_1 \rrbracket) \cup FV(\llbracket \tau_2 \rrbracket) & \\ \subseteq & FV(\tau_1) \cup FV(\tau_2) & \text{IH on } \tau_1 \text{ and } \tau_2 \\ = & FV(\tau_1 \to \tau_2) & \end{array}$$

4. $\tau = \tau_1 \times \tau_2$:

$$\begin{array}{lll} & FV(\llbracket \tau_1 \times \tau_2 \rrbracket) & \\ = & FV(\llbracket \tau_1 \rrbracket \times \llbracket \tau_2 \rrbracket)^{\perp} & \text{Definition of } \llbracket\cdot\rrbracket \\ = & FV(\llbracket \tau_1 \rrbracket) \cup FV(\llbracket \tau_2 \rrbracket) & \\ \subseteq & FV(\tau_1) \cup FV(\tau_2) & \text{IH on } \tau_1 \text{ and } \tau_2 \\ = & FV(\tau_1 \times \tau_2) & \end{array}$$

5. $\tau = \tau_1 + \tau_2$:

$$\begin{array}{lll} & FV(\llbracket \tau_1 + \tau_2 \rrbracket) & \\ = & FV(\llbracket \tau_1 \rrbracket + \llbracket \tau_2 \rrbracket)^{\perp} & \text{Definition of } \llbracket\cdot\rrbracket \\ = & FV(\llbracket \tau_1 \rrbracket) \cup FV(\llbracket \tau_2 \rrbracket) & \\ \subseteq & FV(\tau_1) \cup FV(\tau_2) & \text{IH on } \tau_1 \text{ and } \tau_2 \\ = & FV(\tau_1 + \tau_2) & \end{array}$$

6. $\tau = \mathsf{ref}\ \ell_i\ \tau_i$:

$$\begin{array}{lll} & FV(\llbracket \mathsf{ref}\ \ell_i\ \tau_i \rrbracket) & \\ = & FV(\mathsf{ref}\ (\llbracket \tau_i \rrbracket + \mathsf{unit})^{\ell_i})^{\perp} & \text{Definition of } \llbracket\cdot\rrbracket \\ = & FV(\llbracket \tau_i \rrbracket) \cup FV(\ell_i) & \\ \subseteq & FV(\tau_i) \cup FV(\ell_i) & \text{IH} \\ = & FV(\mathsf{ref}\ \ell_i\ \tau_i) & \end{array}$$

7. $\tau = \forall \alpha.\tau_i$:

$$\begin{array}{lll} & FV(\llbracket \forall \alpha.\tau_i \rrbracket) & \\ = & FV(\forall \alpha.(\top, \llbracket \tau_i \rrbracket))^{\perp} & \text{Definition of } \llbracket\cdot\rrbracket \\ = & FV(\llbracket \tau_i \rrbracket) - \{\alpha\}) & \\ \subseteq & FV(\tau_i) - \{\alpha\}) & \text{IH} \\ = & FV(\forall \alpha.\tau_i) & \end{array}$$

8. $\tau = c \Rightarrow \tau_i$:

$$\begin{array}{lll} & FV(\llbracket c \Rightarrow \tau_i \rrbracket) & \\ = & FV(c \overset{\top}{\Rightarrow} \llbracket \tau_i \rrbracket)^{\perp} & \text{Definition of } \llbracket\cdot\rrbracket \\ = & FV(\llbracket c \rrbracket) \cup FV(\llbracket \tau_i \rrbracket) & \\ \subseteq & FV(\llbracket c \rrbracket) \cup FV(\tau_i) & \text{IH} \\ = & FV(c \Rightarrow \tau_i) & \end{array}$$

9. $\tau = \mathsf{Labeled}\ \ell_i\ \tau_i$:

$$\begin{array}{lll} & FV(\llbracket \mathsf{Labeled}\ \ell_i\ \tau_i \rrbracket) & \\ = & FV(\llbracket \tau_i \rrbracket + \mathsf{unit})^{\ell_i} & \text{Definition of } \llbracket\cdot\rrbracket \\ = & FV(\llbracket \tau_i \rrbracket) \cup FV(\ell_i) & \\ \subseteq & FV(\tau_i) \cup FV(\ell_i) & \text{IH} \\ = & FV(\mathsf{Labeled}\ \ell_i\ \tau_i) & \end{array}$$

10. $\tau = \mathsf{CG}\ \ell_i\ \ell_o\ \tau_i$:

$$
\begin{array}{rll}
& FV(\llbracket \mathsf{CG}\ \ell_i\ \ell_o\ \tau_i \rrbracket) & \\
= & FV(\mathsf{unit} \xrightarrow{\ell_i} (\llbracket \tau_i \rrbracket + \mathsf{unit})^{\ell_o})^{\perp} & \text{Definition of } \llbracket \cdot \rrbracket \\
= & FV(\llbracket \tau_i \rrbracket) \cup FV(\ell_i) \cup FV(\ell_o) & \\
\subseteq & FV(\tau_i) \cup FV(\ell_i) \cup FV(\ell_o) & \text{IH} \\
= & FV(\mathsf{CG}\ \ell_i\ \ell_o\ \tau_i) &
\end{array}
$$

$\square$