A First Principles Approach to Provenance in Functional Languages via Justification Logic

Eduardo Bonelli[1][0000−0003−1856−2856]

Stevens Institute of Technology, Hoboken NJ 07030, USA, eabonelli@gmail.com

Abstract. Provenance refers to techniques that allow one to explain the origin of a result of a computation and how it was obtained. The notion stems from databases and has since been applied to other areas of computing. This paper explores a foundational approach to provenance in programming languages. We focus on formalizing provenance metadata, our object of study, integrating it into a core programming language, and doing so with a logical underpinning to ensure that the analysis is sound. We start from recent studies on a propositions-as-types correspondence for Artemov's *Justification Logic*, introducing a lambda calculus that incorporates a notion of *audit trail*. We turn the calculus into a programming language by providing a small-step reduction strategy, a big-step evaluation semantics, an abstract machine semantics, and finally prove that these approaches agree. This is done for call-by-value and call-by-name. With this, we hope to lay the necessary groundwork to better understand provenance and how it may be integrated into prototype functional languages guided by ideas from logic.

Keywords: Lambda Calculus · Modal Logic · Propositions-as-Types · Provenance · Call-by-Name · Call-by-Value · Abstract Machines.

1 Introduction

With the abundance of data produced from copious sources in a wide range of data formats, *provenance* is gaining increased significance. Provenance refers to techniques that allow one to explain the origin of a result of a computation, how it was obtained and, potentially, reproduce it. A largely cited first work that attempts to delimit the problem and analyze its characteristics is [14]. Although formulated in the setting of databases, provenance is studied in many domains, has led to hundreds of publications [22], and even a W3C Working Group [23]. Its varied motivations have prompted the need to model it using formal techniques to better understand it and the concerns it can help address [15].

We present a first principles approach to provenance in functional programming languages (FPL). The setting is that of Lambda Calculus and the embodiment of provenance we propose is that of an *audit trail*, an object denoting the full history of a computation. We model audit trails rigorously by resorting to logical principles. Our starting point is Artemov's *Logic of Proofs* (LP) [4,5], a fragment of the later introduced *Justification Logic (JL)* [6]. JL is a refinement of modal

logic in which modal propositions $\Box A$ are replaced by $[\![s]\!]A$ for s some notation encoding proofs. The *Lambda Calculus with Audited Units (λ^h)* [10,11,8] is a propositions-as-types calculus for the Logic of Proofs. It extends Lambda Calculus with *audited units*: $!_\rho M$. The modality "!" delimits an expression, namely M, whose computation is audited; we say that M is the scope of the audited unit. The object ρ is an audit trail and represents the "past" reduction steps that have led to the current expression M. Audited units are typed by the introduction rule for the $\Box$-connective. λ^h includes reduction rules that exactly mimic normalisation of Natural Deduction derivations of the Logic of Proofs. Such steps update ρ, contributing to its computation history and ensuring that typability is upheld as M itself changes. Although λ^h is a step forward towards our goal, a lambda calculus is arguably a far cry from a (functional) programming language.

From Lambda Calculus to Programming Languages. Consider the Lambda Calculus expression $\Delta\,((\lambda y.y\,I)\,I)$, where Δ is $(\lambda x.x\,x)$ and I is $\lambda y.y$. Reduction is modeled via the β-rule: $(\lambda x.M)\,N \to_\beta M\{x/N\}$. Here $(\lambda x.M)\,N$ is called a (β-)redex, N the argument to the function $\lambda x.M$, and $M\{x/N\}$ denotes the result of substituting all free occurrences of x in M with N, possibly renaming bound variables to avoid capture.

There are multiple ways in which expressions could be β-reduced. For example, in $\Delta\,(\underline{(\lambda y.y\,I)\,\overline{I)}}$ one could either reduce the underlined redex or the overlined one. Obtaining a FPL requires (at least) two steps. The first is to fix a *strategy* that selects the redex to reduce next. The best-known strategies are *call-by-value (CBV)* and *call-by-name (CBN)*: the former evaluates arguments of functions until they are values (abstractions) before consuming them, the latter consumes arbitrary terms as arguments. The second step is to select an *operational semantics* through which one provides "meaning" to programs, the standard ones being *small-step*, *big-step* and *abstract machine*. Small-step semantics sees an expression as a representation of the runtime state and looks at each operation that is performed on this state. Big-step semantics only looks at the result; the way one models interpreters using recursive functions that compute the final result of an expression based on those of its subexpressions. For non-terminating expressions small-step semantics can provide meaningful information, while big-step cannot. Abstract machines are closer to the implementation. Notably, the complicated notion of substitution is implemented using environments, functions are implemented as closures, and redex search is supported by a stack of expressions. All three offer complementary views on what it means to "run a program" and requires that they be proved to agree, as pioneered by Plotkin [25].

An example is shown in Fig. 1 (CBN). Small-step requires specifying evaluation contexts and redexes. Big-step involves defining an inductive relation associating a computation result to a term. The abstract machine requires introducing run-time configurations (a term, an environment and a stack) and defining a transition relation between configurations. Substitution is not present in the machine and all the transitions operate at the "root" of a configuration.

$$\mathcal{E} ::= \Box \mid \mathcal{E}\, M$$

$$\mathcal{E}\langle(\lambda x.M)\, N\rangle \to_\beta \mathcal{E}\langle M\{x/N\}\rangle$$

$$\frac{}{\lambda x.M \Downarrow \lambda x.M}\ \mathsf{Abs} \qquad \frac{M \Downarrow \lambda x.P \quad P\{x/N\} \Downarrow V}{M\, N \Downarrow V}\ \mathsf{Beta}$$

$$e ::= \epsilon \mid x = (N, e) :: e \quad \pi ::= \epsilon \mid (N, e) :: \pi$$

$$\begin{aligned}(\lambda x.M, e, (N, e') :: \pi) &\to_{pop} (M, x = (N, e') :: e, \pi)\\ (MN, e, \pi) &\to_{push} (M, e, (N, e) :: \pi)\\ (x, e, \pi) &\to_{read} (M, e', \pi), \text{if } e(x) = (M, e')\end{aligned}$$

Fig. 1. CBN: (clockwise from top) small-step, big-step and Krivine Machine

Contributions. We define CBV and CBN strategies for λ^h in all three presentations of operational semantics, and prove their correspondence. The contribution of this paper lies in the rigorous handling of trails and the (often subtle) properties required both to formulate and to relate the different operational semantics. Making audit trails the object of study should be taken seriously, is rather lacking in the literature and, I believe, will help begin to answer some of the pending questions regarding provenance in programming languages and in self-explaining computing [15,28,24]. Three ideas, contributions themselves, guide our approach.

- *Stratifying the language into a source language and a runtime language.* The source language is the one used be the programmer; it does not have explicit manifestations of audit trails. The runtime language is the one that is actually executed at runtime and includes audit trails that witness computation on terms in the *source language*. This stratification is guided by logic: the source syntax corresponds to the term assignment for the Natural Deduction presentation of LP. It suffices to encode all proofs but is not closed under proof normalisation[1]. The addition of audit trails fixes this [10,11].
- *Structural equality on audit trails.* The need will arise for a notion of equality on audit trails to be able to relate the different presentations of the operational semantics. For example, three computation steps in the small-step smenatics will be represented as $(\rho; \sigma); \tau$, where ";" is trail concatenation. However, when turning a big-step computation into a small-step one, the steps will be reordered as $\rho; (\sigma; \tau)$. Other similar structural axioms will lead to us to define *structural equivalence* on audit trails (Def. 1).
- *Modeling local scoping of audit trails in big-step semantics.* We admit computation under "!", but the audit trail under a "!" should not be visible from outside it. Modeling this will lead us to introduce evaluation judgements $M \shortmid \rho \shortmid \mathcal{F} \Downarrow V \shortmid \sigma$, which may be seen to represent the audit trail $\rho\mathcal{F}\langle M\rangle\mathcal{F}\langle\sigma\rangle\mathcal{F}\langle V\rangle$, where ρ is the history[2] of $\mathcal{F}\langle M\rangle$ and $\rho\mathcal{F}\langle M\rangle\mathcal{F}\langle\sigma\rangle$ is the history of $\mathcal{F}\langle V\rangle$ where $\mathcal{F}\langle M\rangle$ is understood as an empty step (*cf.* Rule E-! in Fig. 4).

[1] Subject Reduction fails, in type theoretic parlance.

[2] This is similar but not exactly the same as Levy's redexes with history [21].

Related work. The Logic of Proofs is presented in [4,5], and the more general Justification Logic in [6]. Natural deduction for LP is studied in [7]. Propositions-as-types for LP is studied in [10,11]. Audit trails as terms typable using propositions-as-types for LP is developed in [8]. Proof terms for higher-order rewriting, which correspond to our audit trails, are explored in [9] but are not based on modal logic. On the other hand [9] deals with permutation equivalence of trails, a richer notion that of structural equivalence.
In [26], the original proof of strong normalization for λ^h (which had a restriction on the nesting of "!"s) [10,11] is generalized to all typable terms using Girard's candidates of reducibility technique. Further work by the same authors [27] explored adding explicit substitutions to a de Bruijn indices presentation of λ^h with the aim of reducing terms more efficiently. The substitution subcalculus is based on $\lambda\sigma$. They propose an abstract machine for CBV reduction based on the SECD machine [20]. None of these works study big-step semantics. Call-by-name abstract machines are not studied either. Further literature on audit trails that we are aware of is [30,18].

Extended Report. An extended report with full proofs is available [12].

2 Source Syntax

The source syntax is the language for programmers; its expressions are called *terms*. We assume a denumerably infinite set of **term variables** $a, b, c, \ldots$ and **audited unit variables** $u, v, w, \ldots$. **Terms** and **types** are defined as follows:

$$\begin{array}{rl} s, t ::= & \iota_A \mid a \mid u \mid \lambda a^A.s \mid s\,t \mid !s \mid \mathit{let}\ u^A \triangleq s\ \mathit{in}\ t \\ A, B ::= & P \mid A \supset B \mid [\![s]\!]A \end{array}$$

$!s$ is an *audited (computation) unit*: the symbol "!" is a delimiter for the computation history and has s as scope. Computation below "!" is tracked and can be consulted using the ι_A constant. Reduction of the constant ι_A will produce an iterator (a "fold") for the trail currently in scope, namely the one inside the innermost enclosing !-constructor. The let-term $\mathit{let}\ u^A \triangleq s\ \mathit{in}\ t$ allows audited units to be composed. An example term is:

$$!(s; \mathit{if}\, \iota_{int}\, \mathsf{0}\,\mathsf{1}\,\mathsf{0}\,\mathsf{0}\,(\mathsf{+})\,(\mathsf{+1})\,(\mathsf{+})\,(\mathsf{+})\,\mathsf{>3}\ \mathit{then}\ t_1\ \mathit{else}\ t_2)$$

We have taken the liberty to include some additional constructs for the sake of readability: $s; t$ for s followed by t, "(+)" for addition, etc. This term evaluates s to some value, and then based on the whether the number of β-steps taken to obtain the value of s is greater than 3 or not, either continues with t_1 or t_2.

Typing Terms. A **term typing judgement** has the form $\Delta; \Gamma \vdash s : A$. Types are either propositional variables ($P, Q, \ldots$), function types or modal types. A term variable typing context Γ (resp. audited unit variable typing context Δ) is a partial function from term variables or truth variables (resp. audited unit variables or validity variables) to types [16]. We write $\Gamma, a : A$, with $a \notin \mathsf{dom}(\Gamma)$, for the typing context that results from extending Γ with the mapping of A to a. The term typing rules are defined in Fig. 2. A sample derivation is:

$$\frac{}{\Delta;\Gamma \vdash \iota_A : \mathtt{iter}_A}\ \mathsf{T\text{-}TI} \qquad \frac{a : A \in \Gamma}{\Delta;\Gamma \vdash a : A}\ \mathsf{T\text{-}VAR}$$

$$\frac{\Delta;\Gamma, a : A \vdash s : B}{\Delta;\Gamma \vdash \lambda a^A.s : A \supset B}\ \mathsf{T\text{-}ABS} \qquad \frac{\Delta;\Gamma \vdash s : A \supset B \quad \Delta;\Gamma \vdash t : A}{\Delta;\Gamma \vdash s\,t : B}\ \mathsf{T\text{-}APP}$$

$$\frac{u : A \in \Delta}{\Delta;\Gamma \vdash u : A}\ \mathsf{T\text{-}AVAR} \qquad \frac{\Delta;\cdot \vdash s : A}{\Delta;\Gamma \vdash\, !s : [\![s]\!]A}\ \mathsf{T\text{-}!} \qquad \frac{\Delta;\Gamma \vdash s : [\![r]\!]A \quad \Delta, u : A;\Gamma \vdash t : C}{\Delta;\Gamma \vdash \mathit{let}\ u^A \triangleq s\ \mathit{in}\ t : C\{r/u\}}\ \mathsf{T\text{-}LET}$$

Fig. 2. Typing Rules for the Source Syntax (Terms)

$$\dfrac{\dfrac{}{\cdot; a : [\![s]\!]A \vdash a : [\![s]\!]A} \qquad \dfrac{\dfrac{\dfrac{}{u : A;\cdot \vdash u : A}}{u : A;\cdot \vdash\, !u : [\![u]\!]A}}{u : A; a : [\![s]\!]A \vdash\, !!u : [\![!u]\!][\![u]\!]A}}{\cdot;\Gamma, a : [\![s]\!]A \vdash \mathit{let}\ u^A \triangleq a\ \mathit{in}\, !!u : [\![!s]\!][\![s]\!]A}$$

$$\cdot;\Gamma \vdash \lambda a^{[\![s]\!]A}.\mathit{let}\ u^A \triangleq a\ \mathit{in}\, !!u : [\![s]\!]A \supset [\![!s]\!][\![s]\!]A$$

Typing rules T-Var, T-Abs and T-App are standard. Rule T-TI assigns the type $\mathtt{iter}_A$ to the constant ι_A. As mentioned, reduction of ι_A produces the unfolding of the iterator for the Church encoding of (a *canonical* form, see below) of the current trail in scope (*cf.* Def. 2) whose type is denoted $\mathtt{iter}_A$ and abbreviates $A \supset A \supset A \supset A^2 \supset A^3 \supset A^2 \supset A^3 \supset A^3 \supset A$ where $A^n := A \supset \ldots \supset A \supset A$, n times, $n > 0$. The iterator takes one argument for each of the possible constructors with which trails may be built (Sec. 3). Rule T-! types audited units. As usual in S4-based modal type systems, s must not have occurrences of truth variables. Moreover, notice how the term s is internalized into the type expression $[\![s]\!]A$. Finally, T-Let is the eliminator for audited units. Type C may have free occurrences of the audited unit variable u and hence must be substituted in the conclusion: $C\{r/u\}$ substitutes all free occurrences of u in C with r. This operation is defined as expected: $P\{r/u\} := P$; $(A \supset B)\{r/u\} := A\{r/u\} \supset B\{r/u\}$ and $([\![s]\!]A)\{r/u\} := [\![s\{r/u\}]\!]A\{r/u\}$.

3 Runtime Syntax

The runtime syntax models the execution environment of the programs in the source syntax; its expressions are called **configurations**[3]. They are similar to terms except that audited units carry a **trail**:

$$M, N ::= \iota_A \mid a \mid u \mid \lambda a^A.M \mid M\,N \mid !_\rho M \mid \mathit{let}\ u^A \triangleq M\ \mathit{in}\ N$$
$$\rho, \sigma ::= s \mid \mathbf{ba}(s) \mid \mathbf{bb}(s) \mid \mathbf{ti}_A(\rho) \mid \rho;\sigma \mid \lambda a^A.\rho \mid \rho\,\sigma \mid \mathit{let}\ u^A \triangleq \rho\ \mathit{in}\ \sigma$$

[3] We use this terminology to avoid the overloaded "term" and "expression".

Trails represent computations from a source term in the source syntax to a target term in the source syntax. The source term s denotes a **unit step** from s to itself. A **unary step** is a trail which has a unique occurrence of $\mathbf{ba}(s)$, $\mathbf{bb}(s)$ or $\mathbf{ti}_A(\rho)$, denoting one of three kinds of computational steps that can take place in λ^h: a β-step, a $\beta_{\square}$-step or a trail inspection step, resp. These steps are described in detail in Sec. 4 and A. Expression $\rho;\sigma$ is the composition of ρ with σ. Expressions $\lambda a^A.\rho$, $\rho\,\sigma$ and $let\ u^A \triangleq \rho\ in\ \sigma$ denote computation taking place under lambda, application and let, resp. Computation under "!" is handled by the s case (as $!t$, for some t) since it is not visible from outside the unit. Substitution of trails in terms ($s\{\rho/u\}$) and substitution of audited unit variables with terms in trails ($\rho\{s/u\}$) is defined as expected (*cf.* Appendix)
Trails are equipped with a minimal structure which we borrow from proof-terms in first-order term rewriting [29, 8.3.1] and the higher-order case [9]. This structure includes, among other things, the statement that composition is associative and that unit steps are neutral for composition.

Definition 1. *Structural equivalence of trails is the contextual closure of the following axioms:*

$$\begin{array}{rr} \rho;s \simeq \rho & (\rho_1\,\sigma_1);(\rho_2\,\sigma_2) \simeq (\rho_1;\rho_2)\,(\sigma_1;\sigma_2) \\ s;\rho \simeq \rho & \lambda a^A.\rho;\lambda a^A.\sigma \simeq \lambda a^A.(\rho;\sigma) \\ (\rho;\sigma);\tau \simeq \rho;(\sigma;\tau) & let\ u^A \triangleq \rho_1\ in\ \sigma_1;let\ u^A \triangleq \rho_2\ in\ \sigma_2 \simeq \\ & let\ u^A \triangleq \rho_1;\rho_2\ in\ \sigma_1;\sigma_2 \end{array}$$

Unique representatives of $\simeq$-equivalence classes are known as trails in **canonical form**. The unique canonical form of ρ, written $\mathsf{can}(\rho)$, can be obtained by orienting the equations above and completing them with additional ones to close critical pairs. This leads to a confluent and terminating higher-order rewrite system (*cf.* Appendix). Structural equivalence extends to configurations as expected. In particular, $!_\rho M \simeq !_\sigma N$ implies $\rho \simeq \sigma$.

Typing Trails. A judgement of the form $\Delta;\Gamma \vdash \rho : s \geqslant_A t$ is a **trail typing judgement**. The meaning of such judgements is given by the rules in Fig. 3. Most of these rules are self-explanatory. For example, R-Refl states that s is a trail from s to itself. Rules R-β and R-$\beta_{\square}$ record the redex itself in the trail, together with an indication that it took place. Rule R-TI is about the trail inspection operation. As hinted at above, the target of this step is a term denoting an iterator over the Church encoding of the canonical form of the trail.

Definition 2 (Trail iterator). *The iterator for ρ, written $\mathtt{iter}_\rho$, is defined as follows, where $\boldsymbol{a}$ is the sequence of term variables $a_r, a_{ba}, a_{bb}, a_{ti}, a_{lam}, a_{app}, a_{let}$ and $\lambda\boldsymbol{a}$ is shorthand for $\lambda a_r.\ldots\lambda a_{let}$:*

$$\begin{array}{rlrl} \mathtt{iter}_s := & \lambda\boldsymbol{a}.a_r & \mathtt{iter}_{\rho;\sigma} := & \lambda\boldsymbol{a}.a_t\,(\mathtt{iter}_\rho\boldsymbol{a})\,(\mathtt{iter}_\sigma\,\boldsymbol{a}) \\ \mathtt{iter}_{\mathbf{ba}(s)} := & \lambda\boldsymbol{a}.a_{ba} & \mathtt{iter}_{\lambda a^A.\rho} := & \lambda\boldsymbol{a}.a_{lam}\,(\mathtt{iter}_\rho\,\boldsymbol{a}) \\ \mathtt{iter}_{\mathbf{bb}(s)} := & \lambda\boldsymbol{a}.a_{bb} & \mathtt{iter}_{\rho\,\sigma} := & \lambda\boldsymbol{a}.a_{app}\,(\mathtt{iter}_\rho\,\boldsymbol{a})\,(\mathtt{iter}_\sigma\,\boldsymbol{a}) \\ \mathtt{iter}_{\mathbf{ti}_A(\rho)} := & \lambda\boldsymbol{a}.a_{ti}\,(\mathtt{iter}_\rho\,\boldsymbol{a}) & \mathtt{iter}_{let\ u^A\triangleq\rho\ in\ \sigma} := & \lambda\boldsymbol{a}.a_{let}\,(\mathtt{iter}_\rho\,\boldsymbol{a})\,(\mathtt{iter}_\sigma\,\boldsymbol{a}) \end{array}$$

$$\frac{\Delta;\Gamma \vdash s : A}{\Delta;\cdot \vdash s : s \geqslant_A s}\ \textsf{R-Refl} \qquad \frac{\Delta;\Gamma \vdash \rho : r \geqslant_A s \quad \Delta;\Gamma \vdash \sigma : s \geqslant_A t}{\Delta;\Gamma \vdash \rho;\sigma : r \geqslant_A t}\ \textsf{R-Trans}$$

$$\frac{\Delta;\Gamma, a : A \vdash s : B \quad \Delta;\Gamma \vdash t : A}{\Delta;\Gamma \vdash \mathbf{ba}((\lambda a^A.s)\, t) : (\lambda a^A.s)\, t \geqslant_B s\{t/a\}}\ \textsf{R-}\beta$$

$$\frac{\Delta;\cdot \vdash s : A \quad \Delta, u : A;\Gamma \vdash t : C}{\Delta;\Gamma \vdash \mathbf{bb}(let\ u^A \triangleq\, !s\ in\ t) : let\ u^A \triangleq\, !s\ in\ t \geqslant_{C\{s/u\}} t\{s/u\}}\ \textsf{R-}\beta_{\square}$$

$$\frac{\Delta;\Gamma \vdash \rho : s \geqslant_A t}{\Delta;\Gamma \vdash \mathbf{ti}_B(\rho) : \iota_B \geqslant_{\mathtt{iter}_B} \mathtt{iter}_{\mathsf{can}(\rho)}}\ \textsf{R-TI}$$

$$\frac{\Delta;\Gamma, a : A \vdash \rho : s \geqslant_B t}{\Delta;\Gamma \vdash \lambda a^A.\rho : \lambda a^A.s \geqslant_{A\supset B} \lambda a^A.t}\ \textsf{R-ABS} \qquad \frac{\Delta;\Gamma \vdash \rho : s_1 \geqslant_{A\supset B} t_1 \quad \Delta;\Gamma \vdash \sigma : s_2 \geqslant_A t_2}{\Delta;\Gamma \vdash \rho\,\sigma : s_1\, s_2 \geqslant_B t_1\, t_2}\ \textsf{R-APP}$$

$$\frac{\Delta;\Gamma \vdash \rho : s_1 \geqslant_{[\![r]\!]A} t_1 \quad \Delta;\Gamma, u : A \vdash \sigma : s_2 \geqslant_C t_2}{\Delta;\Gamma \vdash \rho\,\sigma : let\ u^A \triangleq s_1\ in\ s_2 \geqslant_{C\{r/u\}} let\ u^A \triangleq t_1\ in\ t_2}\ \textsf{R-LET}$$

Fig. 3. Trail Typing Rules

Since, when presenting the operational semantics, we shall be reasoning over terms modulo structural equivalence, we want to avoid the behavior of trail inspection to differ in the case of structurally equivalent trails. Hence why the target in R-TI is $\mathtt{iter}_{\mathsf{can}(\rho)}$ rather than $\mathtt{iter}_{\rho}$.
Note the lack of a rule in Fig. 3 for denoting computation that takes place under a binder "!". Reduction under a binder is not visible outside its scope (it is encompassed by R-Refl).
Given Δ and Γ, if ρ is typable, then there is a unique $s \geqslant_A t$ such that the judgement $\Delta;\Gamma \vdash \rho : s \geqslant_A t$ is derivable. For typable ρ we can easily define $\rho^{src} := s$ and $\rho^{tgt} := t$. We say a typable trail ρ is **composable** with another typable trail σ iff $\rho^{tgt} = \sigma^{src}$. Moreover, if we restrict $\simeq$ to typed trails, then $\rho \simeq \sigma$ implies $\rho^{src} = \sigma^{src}$ and $\rho^{tgt} = \sigma^{tgt}$.

Typing Configurations. A **configuration typing judgement** has the form $\Delta;\Gamma \vdash M : A$. Typing rules defining the meaning of this judgement are those for terms (*cf.* Fig. 2) except that T-! is replaced with C-!:

$$\frac{\Delta;\cdot \vdash M : A \quad \Delta;\cdot \vdash \rho : s \geqslant_A \widehat{M}}{\Delta;\Gamma \vdash !_{\rho} M : [\![s]\!]A}\ \textsf{C-!}$$

Expression $\widehat{M}$ in C-! is a term called the **decompilation** of the configuration M. The decompilation function $\widehat{\_} : \mathbb{C} \longrightarrow \mathbb{T}$ produces the term that is currently being computed in the runtime configuration M:

$$\widehat{\mathfrak{a}} := \mathfrak{a} \qquad \widehat{(!_\rho M)} := !\rho^{src}$$
$$\widehat{(\lambda a^A.M)} := \lambda a^A.\widehat{M} \quad \widehat{(let\ u^A \triangleq M\ in\ N)} := let\ u^A \triangleq \widehat{M}\ in\ \widehat{N}$$
$$\widehat{(M\,N)} := \widehat{M}\,\widehat{N}$$

Note that since, as mentioned in the introduction, trails are locally scoped within their audited units, decompilation of $!_\rho M$ produces $!\rho^{src}$: any computation performed inside the audited unit is not visible from outside it.
A typed expression of the form $!_\rho N$ is said to be **well-formed** if $\rho^{tgt} = \widehat{N}$. A typed configuration M is **well-formed** if every sub-expression of M of the form $!_\rho N$ is well-formed. Note that well-typed configurations are well-formed.

4 Call-by-Name

We introduce evaluation semantics (Sec. 4.1), reduction semantics (Sec. 4.1) and an abstract machine (Sec. 4.2) for CBN λ^h and prove their correspondence.

4.1 Evaluation and Reduction

Evaluation Judgements. A **CBN evaluation judgement** is an expression $M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma$, where $M \shortmid \rho \shortmid \mathcal{F}$ is the **start tuple** and $V \shortmid \sigma$ is the **end tuple**. Letters $\mathcal{F}$ and V refer to **CBN shallow contexts** and **values**, resp.:

$$\mathcal{F} ::= \Box \mid \mathcal{F}\,M \mid let\ u^A \triangleq \mathcal{F}\ in\ M \qquad V ::= \lambda a^A.M \mid !_\rho V$$

Start tuple $M \shortmid \rho \shortmid \mathcal{F}$ states that trail ρ denotes a computation of $\mathcal{F}\langle M\rangle$ It is **well-formed** if $!_\rho\mathcal{F}\langle M\rangle$ is a well-formed configuration. Evaluation judgement $M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma$ states that evaluation of $!_\rho\mathcal{F}\langle M\rangle$ produces the configuration $!_{\rho;\widehat{\mathcal{F}}\langle\sigma\rangle}\mathcal{F}\langle V\rangle$. Here $\widehat{\mathcal{F}}$ is the result of decompiling $\mathcal{F}$ (defined just as for configurations and where $\Box$ is treated as a variable) and $\widehat{\mathcal{F}}\langle\sigma\rangle$ denotes that computation σ takes place under $\mathcal{F}$; in other words, trail σ is the "additional work" that is performed under $\mathcal{F}$, and on M, to produce V. Audited unit values require that the unit be fully evaluated. Any source term s can be mapped to the start tuple $\breve{s} \shortmid \breve{s} \shortmid \Box$, where $\breve{s}$ replaces all occurrences of $!t$ in s with $!_t t$.

Evaluation Rules. The evaluation rules are given in Fig. 4. Rule E-V does no work to produce V from V and hence reports the identity trail $\widehat{V}$ as computation history. Rule E-! allows evaluation to take place inside an audited unit. As mentioned in the introduction, notice that a new scope is opened for trail σ. The work performed inside the audited unit is recorded in the trail delimiter (τ in $!_{\sigma;\tau}V$). Moreover, this work is *not* visible outside its scope, hence the identity step $!\sigma^{src}$ is produced as overall computation trail. Rule E-β evaluates an application $M\,N$. Notice that the trails of each step in the evaluation process are collected. In particular, $\rho;\widehat{\mathcal{F}}\langle(\sigma\,\widehat{N});\mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{N})\rangle$ expresses that, in producing $P\{N/a\}$, a computation ρ producing $M\,N$ was followed by a computation $\sigma\,\widehat{N}$, where σ produces $\lambda a^A.P$ under $\mathcal{F}$ from M, and then a β

$$\frac{}{V \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F} \Downarrow^{\mathsf{cbn}} V \mathbin{\imath} \widehat{V}}\ \mathsf{E\text{-}V} \qquad \frac{M \mathbin{\imath} \sigma \mathbin{\imath} \Box \Downarrow^{\mathsf{cbn}} V \mathbin{\imath} \tau}{!_\sigma M \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F} \Downarrow^{\mathsf{cbn}} !_{\sigma;\tau} V \mathbin{\imath} !\sigma^{src}}\ \mathsf{E\text{-}!}$$

$$\frac{\begin{array}{c} M \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F}\langle \Box\, N\rangle \Downarrow^{\mathsf{cbn}} \lambda a^A.P \mathbin{\imath} \sigma \\ P\{N/a\} \mathbin{\imath} \rho; \widehat{\mathcal{F}}\langle (\sigma\, \widehat{N}); \mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{N})\rangle \mathbin{\imath} \mathcal{F} \Downarrow^{\mathsf{cbn}} W \mathbin{\imath} \upsilon \end{array}}{M\, N \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F} \Downarrow^{\mathsf{cbn}} W \mathbin{\imath} (\sigma\, \widehat{N}); \mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{N}); \upsilon}\ \mathsf{E}\text{-}\beta$$

$$\frac{\begin{array}{c} M \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F}\langle let\ u^A \triangleq \Box\ in\ N\rangle \Downarrow^{\mathsf{cbn}} !_\tau V \mathbin{\imath} \sigma \\ N\{!_\tau V/u\} \mathbin{\imath} \rho; \widehat{\mathcal{F}}\langle let\ u^A \triangleq \sigma\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{!_\tau V}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}\rangle \mathbin{\imath} \mathcal{F} \Downarrow^{\mathsf{cbn}} W \mathbin{\imath} \upsilon \end{array}}{let\ u^A \triangleq M\ in\ N \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F} \Downarrow^{\mathsf{cbn}} W \mathbin{\imath} let\ u^A \triangleq \sigma\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{!_\tau V}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon}\ \mathsf{E}\text{-}\beta_\Box$$

$$\frac{}{\iota_A \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F} \Downarrow^{\mathsf{cbn}} \mathtt{iter}_{\mathsf{can}(\rho)} \mathbin{\imath} \mathbf{ti}_A(\rho)}\ \mathsf{E\text{-}TI}$$

Fig. 4. CBN Evaluation Semantics

step follows. The trail may also have been written $\rho; \widehat{\mathcal{F}}\langle \sigma\, \widehat{N}\rangle; \widehat{\mathcal{F}}\langle \mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{N})\rangle$ among others; all of which are structurally equivalent. Regarding $\mathsf{E}\text{-}\beta_\Box$, the trail $\rho; \widehat{\mathcal{F}}\langle let\ u^A \triangleq \sigma\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{!_\tau V}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}\rangle$ appends the witness to the $\beta_\Box$ step with $\widehat{N}\{\tau/u\}$. The latter persists the trail τ that produced V. Also, the expression $N\{!_\tau V/u\}$ substitutes audited units inside configurations. This notion of substitution behaves as follows for variables: $v\{!_\rho N/u\} := N$, if $u = v$, and $v\{!_\rho N/u\} := v$, if $u \neq v$. Moreover, the case where N is an audited unit is worth highlighting: $(!_\sigma P)\{!_\rho Q/u\} := !_{\sigma\{\rho^{src}/u\}; \widehat{P}\{\rho/u\}} P\{!_\rho Q/u\}$. Note how the trail ρ is persisted (*cf.* $\widehat{P}\{\rho/u\}$). Finally, rule $\mathsf{E\text{-}TI}$ models trail inspection, producing the iterator $\mathtt{iter}_{\mathsf{can}(\rho)}$ as value and the unary step $\mathbf{ti}_A(\rho)$ as computation history.

Remark 1. s in Lambda Calculus, $s \Downarrow^{\mathsf{cbn}} V$ iff $s \mathbin{\imath} s \mathbin{\imath} \Box \Downarrow^{\mathsf{cbn}} V \mathbin{\imath} \sigma$, for some σ.

Reduction Semantics. Reduction, $\rightsquigarrow_{\mathsf{cbn}}$, always takes place inside some current audited unit, modeled by the following set of reduction contexts $\mathcal{E}$, where $\mathcal{F}$ is a CBN shallow context. It is specified by the $\mathsf{R\text{-}Ctxt}$ rule, where the relation $\mapsto$ is defined in Fig. 5:

$$\mathcal{E} ::= \Box \mid !_\rho \mathcal{F}\langle \mathcal{E}\rangle \qquad \frac{M \mapsto N}{\mathcal{E}\langle M\rangle \rightsquigarrow_{\mathsf{cbn}} \mathcal{E}\langle N\rangle}\ \mathsf{R\text{-}Ctxt}$$

Results. We first present the reduction-simulates-evaluation direction (Prop. 1), where $\rightsquigarrow^*_{\mathsf{cbn}}$ is the reflexive-transitive closure of $\rightsquigarrow_{\mathsf{cbn}}$; it is proved by induction on the derivation of $M \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F} \Downarrow^{\mathsf{cbn}} V \mathbin{\imath} \sigma$. Also it relies on being able to reason modulo structural equivalence.

$$\frac{R = (\lambda a^A.M)\, N}{!_\rho \mathcal{F}\langle R\rangle \mapsto !_{\rho;\widehat{\mathcal{F}}\langle \mathbf{ba}(\widehat{R})\rangle}\mathcal{F}\langle M\{N/a\}\rangle}\ \mathsf{R}\text{-}\beta \qquad \frac{R = let\ u^A \triangleq !_\sigma V\ in\ N}{!_\rho \mathcal{F}\langle R\rangle \mapsto !_{\rho;\widehat{\mathcal{F}}\langle \mathbf{bb}(\widehat{R});\widehat{N}\{\sigma/u\}\rangle}\mathcal{F}\langle N\{!_\sigma V/u\}\rangle}\ \mathsf{R}\text{-}\beta_{\square}$$

$$\frac{R = \iota_A}{!_\rho \mathcal{F}\langle R\rangle \mapsto !_{\rho;\widehat{\mathcal{F}}\langle \mathbf{ti}_A(\rho)\rangle}\mathcal{F}\langle \mathtt{iter}_{\mathsf{can}(\rho)}\rangle}\ \mathsf{R}\text{-}\mathsf{TI}$$

Fig. 5. CBN Reduction Semantics

Proposition 1 (Reduction simulates evaluation). *Let $M \shortmid \rho \shortmid \mathcal{F}$ be well-formed. Then $M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma$ implies $!_\rho \mathcal{F}\langle M\rangle \rightsquigarrow^*_{\mathsf{cbn}} !_{\rho;\widehat{\mathcal{F}}\langle\sigma\rangle}\mathcal{F}\langle V\rangle$.*

The proof of the evaluation-simulates-reduction result is more subtle. First we introduce some auxiliary results. In stating and proving them, we will make use of the following **CBN redex table**:

R	R'	ξ
$(\lambda a^A.M)\, N$	$M\{N/a\}$	$\mathbf{ba}(\widehat{R})$
$let\ u^A \triangleq !_\tau V\ in\ N$	$N\{!_\tau V/u\}$	$\mathbf{bb}(\widehat{R});\widehat{N}\{\tau/u\}$
ι_A	$\mathtt{iter}_{\mathsf{can}(\rho)}$	$\mathbf{ti}_A(\rho)$

The main result on which Prop. 2 rests is the Expansion Lemma (Lem. 1) which essentially winds time backword. In other words, if $\mathcal{E}\langle !_{\rho;\widehat{\mathcal{F}}\langle\xi\rangle}\mathcal{F}\langle R'\rangle\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \tau$, then $\mathcal{E}\langle !_\rho \mathcal{F}\langle R\rangle\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \tau$. Note how the witness to the last step (but the not the step itself!) performed under $\mathcal{F}$ in the former judgement, and which is the starting point of the evaluation, is included in the evaluation in the latter judgement. Thus, in a way, we are running the computation history $\rho;\widehat{\mathcal{F}}\langle r\rangle$ backwards. This lemma is first stated in a restricted form (in which computation takes place inside a shallow context (*cf.* Shallow Expansion Lemma in Appendix), and then is extended to its general form with the help of the Projection Lemma and the Substitution Lemma (also in the Appendix).

Lemma 1 (Expansion).
For all (R, R', ξ) in the CBN redex table,

(a) $\mathcal{F}\langle R'\rangle \shortmid \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}}\langle\xi\rangle\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \sigma$, implies $\mathcal{F}\langle R\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \widehat{\mathcal{F}}\langle\xi\rangle;\sigma$.
(b) $\mathcal{E}\langle !_{\rho;\widehat{\mathcal{F}}\langle r\rangle}\mathcal{F}\langle R'\rangle\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \tau$, implies $\mathcal{E}\langle !_\rho \mathcal{F}\langle R\rangle\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \tau$.

The proof of Prop. 2 is by induction on the length of the derivation sequence using Lem. 1.

Proposition 2 (Evaluation simulates reduction). *$M \rightsquigarrow^*_{\mathsf{cbn}} V$ implies, for all $\rho, \mathcal{G}$ there exists σ such that $M \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma$.*

4.2 Abstract Machine

The Audited KAM (AKAM) for CBN reduction in λ^h is based on Krivine's KAM [19]. Its states are tuples $s \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta$ where s is a source **term**, e is an **environment**, π is a **stack**, ξ is an **audit trail** and δ is a **trail dump**:

$$\begin{aligned} e &::= \epsilon \mid a{=}(t, e) :: e \mid u{=}(!_\sigma V, e) :: e \\ \pi &::= \epsilon \mid (t, e) :: \pi \mid (t, u, e) :: \pi \\ \xi &::= (e, s) \mid \mathbf{ba}(R) :: \xi \mid \mathbf{bb}(R) :: \xi \mid \mathbf{ti}_A(\pi) :: \xi \mid (\xi, \pi) :: \xi \\ \delta &::= \epsilon \mid (\xi, \pi) :: \delta \\ V &::= \lambda a^A.M \mid !_\xi V \end{aligned}$$

In the notion of value above, M is actually a configuration but where the trail decorations are in the syntax of trails defined above using stack notation. The details of the tuple R in $\mathbf{ba}(R)$ and $\mathbf{bb}(R)$ above is given below together with the transitions of the AM. Given a closed source term s, the starting state of the AM is $s \shortmid \epsilon \shortmid \epsilon \shortmid (\epsilon, s) \shortmid \epsilon$. The transitions of the AKAM are given in Fig. 6. Transitions pushb, appb and lookupt are the transitions for the standard CBN lambda calculus. pushb pushes the argument of an application into the stack (which may be thought of as the context under which the term in focus is currently placed). Rule appb processes the application of an abstraction to an argument by moving the argument from the stack into the environment. It also records a witness to the β-step in the current trail: $\mathbf{ba}(R) :: \xi$. The components of the tuple R will be used for reading back the trail when synthesing a configuration from an AM state in our simulation proposition (Prop. 3). Rule lookupt performs lookup for truth variables. Rule pushlet plays a similar role to push but for let-terms. Rule bang starts computation inside an audited unit. Note that the starting trail is the unit step (e, s). The current stack π and trail ξ are placed in the dump since computation in s will not be recorded in ξ. The related transitions bangbang and appbb deal with the case where computation inside an audited unit has concluded. Notice first that the stack is required to be empty since the value cannot be applied or be the argument of a let-term. The difference between bangbang and appbb is that the former deals with the case in which we have nested audited units such as when evaluating $!!s$. The latter covers the case where the just computed audited unit is an argument in a let-term. Rule lookupv performs variable lookup for validity variables[4]. Finally, ti performs trail lookup. The expression $\underline{\xi}$ is the readback of ξ and is defined below.

The main result (Prop. 3) is that the AM is sound with respect to CBN reduction. Stating it requires reading back configurations from machine states:

$$\underline{s \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta} := \underline{\delta}\langle !_{\underline{\xi}} \underline{\pi} \langle \underline{e} \langle \breve{s} \rangle \rangle \rangle$$

We next present each of the components on which this readback function relies on. The readback function for environments and stacks are as follows, where $\breve{s}$ is the **compilation** of s, meaning replacing all occurrences of $!t$ in s with $!_t \breve{t}$ and

[4] See Sec. 5 for further comments on this rule.

$$
\begin{array}{llll}
s\,t \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta & \mapsto_{\mathsf{push}} & s \shortmid e \shortmid (t,e) :: \pi \shortmid \xi \shortmid \delta & \\
\lambda a^A.s \shortmid e \shortmid (t,e') :: \pi \shortmid \xi \shortmid \delta & \mapsto_{\mathsf{appb}} & s \shortmid a{=}(t,e') :: e \shortmid \pi \shortmid \mathbf{ba}(R) :: \xi \shortmid \delta & R = (\lambda a^A.s, e, t, e', \pi) \\
a \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta & \mapsto_{\mathsf{lookupt}} & t \shortmid e' \shortmid \pi \shortmid \xi \shortmid \delta & e(a) = (t,e') \\
\mathit{let}\ u^A \triangleq s\ \mathit{in}\ t \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta & \mapsto_{\mathsf{pushlet}} & s \shortmid e \shortmid (t,u,e) :: \pi \shortmid \xi \shortmid \delta & \\
!s \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta & \mapsto_{\mathsf{bang}} & s \shortmid e \shortmid \epsilon \shortmid (e,s) \shortmid (\xi,\pi) :: \delta & \\
V \shortmid e \shortmid \epsilon \shortmid \sigma \shortmid (\xi,\epsilon) :: \delta & \mapsto_{\mathsf{bangbang}} & !_\sigma V \shortmid e \shortmid \epsilon \shortmid \xi \shortmid \delta & \\
V \shortmid e \shortmid \epsilon \shortmid \sigma \shortmid (\xi,(t,u,e') :: \pi) :: \delta & \mapsto_{\mathsf{appbb}} & t \shortmid u{=}(!_\sigma V, e') :: e \shortmid \pi \shortmid \mathbf{bb}(R) :: \xi \shortmid \delta & R = (V, e, t, u, e', \sigma, \pi) \\
u \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta & \mapsto_{\mathsf{lookupv}} & V \shortmid e' \shortmid \pi \shortmid \xi \shortmid \delta & e(u) = (!_\sigma V, e') \\
\iota_A \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta & \mapsto_{\mathsf{ti}} & \mathtt{iter}_{\mathsf{can}(\underline{\xi})} \shortmid e \shortmid \pi \shortmid \mathbf{ti}_A(\pi) :: \xi \shortmid \delta &
\end{array}
$$

Fig. 6. Transitions of the AKAM

simply traversing expressions of the form $!_\sigma V$. Compilation is required since the readback of AKAM states is to configurations.

$$
\begin{array}{rcl|rcl}
\underline{\epsilon} & := & \Box & \underline{\epsilon} & := & \Box \\
\underline{a{=}(t,e') :: e} & := & \underline{e}\langle \Box\{a/\underline{e'}\langle \breve{t}\rangle\}\rangle & \underline{(t,e) :: \pi} & := & \underline{\pi}\langle \Box\, \underline{e}\langle \breve{t}\rangle\rangle \\
\underline{u{=}(!_\sigma V, e') :: e} & := & \underline{e}\langle \Box\{u/\underline{e'}\langle !_\sigma \breve{V}\rangle\}\rangle & \underline{(t,u,e) :: \pi} & := & \underline{\pi}\langle \mathit{let}\ u^A \triangleq \Box\ \mathit{in}\ \underline{e}\langle \breve{t}\rangle\rangle
\end{array}
$$

The readback function for trails and dumps is given below. The former makes use of $\widehat{\pi}$ which is defined to be just $\underline{\widehat{\pi}}$, where recall from above that $\widehat{\bullet}$ is the decompilation function:

$$
\begin{array}{rcl|rcl}
\underline{(e,s)} & := & \underline{e}\langle s\rangle & & & \\
\underline{\mathbf{ba}(R) :: \xi} & := & \underline{\xi}; \widehat{\pi}\langle \mathbf{ba}(\underline{e}\langle \widehat{\lambda a^A.s}\rangle\, \underline{\widehat{e'\langle t\rangle}})\rangle & & & \\
\underline{\mathbf{bb}(R) :: \xi} & := & \underline{\xi}; \widehat{\pi}\langle \mathbf{bb}(\mathit{let}\ u^A \triangleq \underline{e}\langle \widehat{!_\sigma V}\rangle\ \mathit{in}\ \underline{\widehat{e'\langle t\rangle}}); \underline{\widehat{e'\langle t\rangle}}\{\sigma/u\}\rangle & & & \\
\underline{\mathbf{ti}_A(\pi) :: \xi} & := & \underline{\xi}; \widehat{\pi}\langle \mathbf{ti}_A(\underline{\xi})\rangle & & & \\
\hline
\multicolumn{3}{c|}{} & \underline{\epsilon} & := & \Box \\
\multicolumn{3}{c|}{} & \underline{(\xi,\pi) :: \delta} & := & \underline{\delta}\langle !\underline{\xi}\,\underline{\pi}\rangle
\end{array}
$$

Proposition 3 (Correctness). *If* $s \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta \mapsto_r s' \shortmid e' \shortmid \pi' \shortmid \xi' \shortmid \delta'$, *then*

(a) For $r \in \{\mathsf{push}, \mathsf{lookupt}, \mathsf{pushlet}, \mathsf{bang}, \mathsf{bangbang}, \mathsf{lookupv}\}$: $\underline{s \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta} = \underline{s' \shortmid e' \shortmid \pi' \shortmid \xi' \shortmid \delta'}$.
(b) For $r \in \{\mathsf{appb}, \mathsf{appbb}, \mathsf{ti}\}$: $\underline{s \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta} \rightsquigarrow_{\mathsf{cbn}} \underline{s' \shortmid e' \shortmid \pi' \shortmid \xi' \shortmid \delta'}$.

5 Conclusions

We have proposed notions of evaluation, reduction and abstract machine, using CBV and CBN, for a calculus of audited units λ^h, in the hopes of bringing λ^h closer to the programming language domain. λ^h was originally proposed as a term assignment for Justification Logic [10,11]. We have simplified the presentation with respect to both its original presentation and also those that build on it in the literature [26,27]. The key technical tool that allows our correspondence results between evaluation and reduction to follow through is to equip trails with additional structure. One might ponder on relating CBV and CBN as in the λ-calculus via CPS translations, however in principle this does not make

sense since program execution depends on the history of computation (effects) and these strategies reduce different redexes. Unless the notion of observation of trails is independent of the order in which redexes are contracted, in which case reasoning over trails would have to include redex permutations (as in Lévy permutation equivalence [21]).
One future avenue worth pursuing is devising a lambda calculus with distance explicit substitutions such as the Linear Substitution Calculus (LSC) [3,2]. LSC allows the KAM's linear head reduction to be expressed as a strategy on its terms. This would allow a tighter correspondence to be established between reduction steps in the AM and some appropriate extension of the LSC. It might also allow more "lazier" trail persistence. For example, rule lookupv could be replaced by:

$$u \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta \mapsto_{\mathsf{lookupv'}} V \shortmid e' \shortmid \pi \shortmid (\sigma, \pi) :: \xi \shortmid \delta \; e(u) = (!_\sigma V, e')$$

and $\underline{\mathbf{bb}(R) :: \xi}$ be defined as $\underline{\xi}; \widehat{\pi}\langle \mathbf{bb}(let\ u^A \triangleq \underline{e}\widehat{\langle !_\sigma V\rangle}\ in\ \underline{e'\langle t\rangle}\widehat{)}\rangle$. This decoding of trails does not persist the trails eagerly (notice the absence of $\underline{e'\langle t\rangle}\widehat{\{\sigma/u\}}$).

Acknowledgements. To Jason Gardella for fruitful discussions.

References

1. Accattoli, B., Barenbaum, P., Mazza, D.: Distilling abstract machines. In: Jeuring, J., Chakravarty, M.M.T. (eds.) Proceedings of the 19th ACM SIGPLAN international conference on Functional programming, Gothenburg, Sweden, September 1-3, 2014. pp. 363–376. ACM (2014)
2. Accattoli, B., Bonelli, E., Kesner, D., Lombardi, C.: A nonstandard standardization theorem. In: Jagannathan, S., Sewell, P. (eds.) The 41st Annual ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL '14, San Diego, CA, USA, January 20-21, 2014. pp. 659–670. ACM (2014)
3. Accattoli, B., Kesner, D.: The structural *lambda*-calculus. In: Dawar, A., Veith, H. (eds.) Computer Science Logic, 24th International Workshop, CSL 2010, 19th Annual Conference of the EACSL, Brno, Czech Republic, August 23-27, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6247, pp. 381–395. Springer (2010)
4. Artemov, S.: Operational modal logic. Tech. Rep. MSI 95-29, Cornell University (1995)
5. Artemov, S.: Explicit provability and constructive semantics. Bulletin of Symbolic Logic **7**(1), 1–36 (2001)
6. Artemov, S.: Justification logic. In: Hölldobler, S., Lutz, C., Wansing, H. (eds.) JELIA. Lecture Notes in Computer Science, vol. 5293, pp. 1–4. Springer (2008)
7. Artëmov, S.N., Bonelli, E.: The intensional lambda calculus. In: Artëmov, S.N., Nerode, A. (eds.) Logical Foundations of Computer Science, International Symposium, LFCS 2007, New York, NY, USA, June 4-7, 2007, Proceedings. Lecture Notes in Computer Science, vol. 4514, pp. 12–25. Springer (2007)
8. Barenbaum, P., Bonelli, E.: Rewrites as terms through justification logic. In: PPDP '20: 22nd International Symposium on Principles and Practice of Declarative Programming, Bologna, Italy, 9-10 September, 2020. pp. 11:1–11:13. ACM (2020)

9. Barenbaum, P., Bonelli, E.: Reductions in higher-order rewriting and their equivalence. In: Klin, B., Pimentel, E. (eds.) 31st EACSL Annual Conference on Computer Science Logic, CSL 2023, February 13-16, 2023, Warsaw, Poland. LIPIcs, vol. 252, pp. 8:1–8:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik (2023)
10. Bavera, F., Bonelli, E.: Justification logic and history based computation. In: Cavalcanti, A., Déharbe, D., Gaudel, M., Woodcock, J. (eds.) Theoretical Aspects of Computing - ICTAC 2010, 7th International Colloquium, Natal, Rio Grande do Norte, Brazil, September 1-3, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6255, pp. 337–351. Springer (2010)
11. Bavera, F., Bonelli, E.: Justification logic and audited computation. J. Log. Comput. **28**(5), 909–934 (2018), published online 19 June 2015
12. Bonelli, E.: A first principles approach to provenance in functional languages via justification logic (March 2023), `https://ebonelli.github.io/publications/wollic2023_extended_report.pdf`
13. Bruggink, H.S.: Equivalence of reductions in higher-order rewriting. Ph.D. thesis, Utrecht University (2008)
14. Buneman, P., Khanna, S., Wang-Chiew, T.: Why and where: A characterization of data provenance. In: Van den Bussche, J., Vianu, V. (eds.) Database Theory — ICDT 2001. pp. 316–330. Springer Berlin Heidelberg, Berlin, Heidelberg (2001)
15. Cheney, J., Acar, U.A., Perera, R.: Toward a theory of self-explaining computation. In: Tannen, V., Wong, L., Libkin, L., Fan, W., Tan, W., Fourman, M.P. (eds.) In Search of Elegance in the Theory and Practice of Computation - Essays Dedicated to Peter Buneman. Lecture Notes in Computer Science, vol. 8000, pp. 193–216. Springer (2013)
16. Davies, R., Pfenning, F.: A modal analysis of staged computation. J. ACM **48**(3), 555–604 (2001)
17. Felleisen, M., Friedman, D.P.: Control operators, the secd-machine, and the λ-calculus. In: Wirsing, M. (ed.) Formal Description of Programming Concepts - III: Proceedings of the IFIP TC 2/WG 2.2 Working Conference on Formal Description of Programming Concepts - III, Ebberup, Denmark, 25-28 August 1986. pp. 193–222. North-Holland (1987)
18. Jia, L., Vaughan, J.A., Mazurak, K., Zhao, J., Zarko, L., Schorr, J., Zdancewic, S.: AURA: a programming language for authorization and audit. In: Hook, J., Thiemann, P. (eds.) Proceeding of the 13th ACM SIGPLAN international conference on Functional programming, ICFP 2008, Victoria, BC, Canada, September 20-28, 2008. pp. 27–38. ACM (2008)
19. Krivine, J.: A call-by-name lambda-calculus machine. Higher-Order and Symbolic Computation **20**(3), 199–207 (2007)
20. Landin, P.J.: The mechanical evaluation of expressions. The Computer Journal **6**(4), 308–320 (Jan 1964)
21. Lévy, J.J.: Réductions correctes et optimales dans le lambda-calcul. Ph.D. thesis, Paris 7 (1978), thése d'Etat
22. Moreau, L.: The foundations for provenance on the web. Found. Trends Web Sci. **2**(2-3), 99–241 (2010)
23. Moreau L., M.P.e.: Prov-dm: The prov data model. w3c recommendation. Tech. rep., W3C (April 2013), `http://www.w3.org/TR/2013/REC-prov-dm-20130430/`
24. Perera, R., Acar, U.A., Cheney, J., Levy, P.B.: Functional programs that explain their work. In: Thiemann, P., Findler, R.B. (eds.) ACM SIGPLAN International Conference on Functional Programming, ICFP'12, Copenhagen, Denmark, September 9-15, 2012. pp. 365–376. ACM (2012)

25. Plotkin, G.D.: Call-by-name, call-by-value and the lambda-calculus. Theor. Comput. Sci. **1**(2), 125–159 (1975)
26. Ricciotti, W., Cheney, J.: Strongly normalizing audited computation. In: Goranko, V., Dam, M. (eds.) 26th EACSL Annual Conference on Computer Science Logic, CSL 2017, August 20-24, 2017, Stockholm, Sweden. LIPIcs, vol. 82, pp. 36:1–36:21. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik (2017)
27. Ricciotti, W., Cheney, J.: Explicit auditing. In: Fischer, B., Uustalu, T. (eds.) Theoretical Aspects of Computing - ICTAC 2018 - 15th International Colloquium, Stellenbosch, South Africa, October 16-19, 2018, Proceedings. Lecture Notes in Computer Science, vol. 11187, pp. 376–395. Springer (2018)
28. Ricciotti, W., Stolarek, J., Perera, R., Cheney, J.: Imperative functional programs that explain their work. Proc. ACM Program. Lang. **1**(ICFP), 14:1–14:28 (2017)
29. Terese: Term Rewiriting Systems. Cambridge University Press (2003)
30. Vaughan, J.A., Jia, L., Mazurak, K., Zdancewic, S.: Evidence-based audit. In: Proceedings of the 21st IEEE Computer Security Foundations Symposium, CSF 2008, Pittsburgh, Pennsylvania, USA, 23-25 June 2008. pp. 177–191. IEEE Computer Society (2008)

A Call-by-Value

Evaluation. CBV evaluation judgements have the form $M \intercal \rho \intercal \mathcal{F} \Downarrow^{\mathsf{cbv}} V \intercal \sigma$ except that **CBV shallow contexts** allow evaluation of an argument of an abstraction as usual:

$$\mathcal{F} ::= \Box \mid \mathcal{F}\, M \mid (\lambda a^A.M)\, \mathcal{F} \mid \mathit{let}\ u^A \triangleq \mathcal{F}\ \mathit{in}\ M$$

The set of values do not change, however. The CBV evaluation rules are those of CBN (Fig. 4) except that E-β is replaced with:

$$\frac{\begin{array}{c} M \intercal \rho \intercal \mathcal{F}\langle \Box\, N\rangle \Downarrow^{\mathsf{cbv}} \lambda a^A.P \intercal \sigma \\ N \intercal \rho; \widehat{\mathcal{F}}\langle \sigma\, \widehat{N}\rangle \intercal \mathcal{F}\langle (\lambda a^A.P)\, \Box\rangle \Downarrow^{\mathsf{cbv}} V \intercal \tau \\ P\{V/a\} \intercal \rho; \widehat{\mathcal{F}}\langle (\sigma\,\tau); \mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{V})\rangle \intercal \mathcal{F} \Downarrow^{\mathsf{cbv}} W \intercal \upsilon \end{array}}{M\, N \intercal \rho \intercal \mathcal{F} \Downarrow^{\mathsf{cbv}} W \intercal (\sigma\,\tau); \mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{V}); \upsilon}\ \mathsf{E}\text{-}\beta\text{-}\mathsf{V}$$

Notice that the trail $\rho; \widehat{\mathcal{F}}\langle (\sigma\,\tau); \mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{V})\rangle$ expresses that, in producing $P\{V/a\}$, a computation ρ producing $M\, N$ was followed by a computation $\sigma\,\tau$, where σ produces $\lambda a^A.P$ under $\mathcal{F}$ from M and τ produces V under $\mathcal{F}$ from N, and then a β step follows. The τ trail is not present in CBN, of course.

Reduction. One-step CBV reduction $\rightsquigarrow_{\mathsf{cbv}}$ is defined just as in CBN (Fig. 5) except that R-β is replaced with the following, where $\mathcal{F}$ is a CBV shallow context:

$$\frac{R = (\lambda a^A.M)\, V}{!_\rho \mathcal{F}\langle R\rangle \mapsto !_{\rho; \widehat{\mathcal{F}}\langle \mathbf{ba}(\widehat{R})\rangle} \mathcal{F}\langle M\{a/V\}\rangle}\ \mathsf{R}\text{-}\beta\text{-}\mathsf{V}$$

Moreover, we use CBV shallow contexts in the evaluation contexts $\mathcal{E} ::= \Box \mid !_\rho \mathcal{F}\langle \mathcal{E}\rangle$ used in R-Ctxt.

Results. The correspondence between CBN small-step and big-step semantics can be adapted to the CBV case:

Proposition 4 (Reduction simulates evaluation). *Let $M \shortmid \rho \shortmid \mathcal{F}$ be well-formed. $M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} V \shortmid \sigma$ implies $!_\rho \mathcal{F}\langle M\rangle \rightsquigarrow^*_{\mathsf{cbv}} !_{\rho;\widehat{\mathcal{F}}\langle\sigma\rangle}\mathcal{F}\langle V\rangle$.*

Proposition 5 (Evaluation simulates reduction). *$M \rightsquigarrow^*_{\mathsf{cbv}} V$ implies, for all $\rho, \mathcal{G}$ there exists σ such that $M \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} V \shortmid \sigma$.*

Abstract Machine The ACEK is an CBV abstract machine that is based on the CEK machine [1], the latter in turn based on Felleisen et al's adaptation of the KAM to CBV and control operators [17]. The states are as in the AKAM except that the elements of the stack are labeled as functions or arguments, reflecting whether the machine is launching the evaluation of an argument or ending it.

$$\pi ::= \epsilon \mid \mathtt{a}(t,e) :: \pi \mid \mathtt{f}(t,e) :: \pi \mid (t,u,e) :: \pi$$

The transitions are:

$$\begin{array}{lll}
s\,t \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta & \mapsto_{\mathsf{pusharg}} & s \shortmid e \shortmid \mathtt{a}(t,e) :: \pi \shortmid \xi \shortmid \delta \\
\lambda a^A.s \shortmid e \shortmid \mathtt{a}(t,e') :: \pi \shortmid \xi \shortmid \delta & \mapsto_{\mathsf{evalarg}} & t \shortmid e' \shortmid \mathtt{f}(\lambda a^A.s,e) :: \pi \shortmid \xi \shortmid \delta \\
\lambda a^A.s \shortmid e \shortmid \mathtt{f}(\lambda b^B.t,e') :: \pi \shortmid \xi \shortmid \delta & \mapsto_{\mathsf{app}} & t \shortmid b{=}(\lambda a^A.s,e) :: e' \shortmid \pi \shortmid \mathbf{ba}(R) :: \xi \shortmid \delta, \\
 & & R = (\lambda b^B.t, e', \lambda a^A.s, e, \pi)
\end{array}$$

together with the following ones from the AKAM (Fig. 6): lookupt, pushlet, bang, bangbang, appbb, lookupv and ti. Readback is as in the AKAM, except that the readback of stacks is as follows:

$$\begin{array}{cc}
\underline{\epsilon} := \square & \underline{\mathtt{f}(t,e) :: \pi} := \underline{\pi}\langle \underline{e}\langle \check{t}\rangle \square\rangle \\
\underline{\mathtt{a}(t,e) :: \pi} := \underline{\pi}\langle \square\, \underline{e}\langle \check{t}\rangle\rangle & \underline{(t,u,e) :: \pi} := \underline{\pi}\langle \mathit{let}\ u^A \triangleq \square\ \mathit{in}\ \underline{e}\langle \check{t}\rangle\rangle
\end{array}$$

Correctness of the ACEK for CBV reduction holds too:

Proposition 6 (Correctness). *If $s \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta \mapsto_r s' \shortmid e' \shortmid \pi' \shortmid \xi' \shortmid \delta'$, then*

(a) For $r \in \{$pusharg, evalarg, lookupt, pushlet, bang, bangbang, lookupv$\}$: $\underline{s \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta} = \underline{s' \shortmid e' \shortmid \pi' \shortmid \xi' \shortmid \delta'}$.
(b) For $r \in \{$app, appbb, ti$\}$: $\underline{s \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta} \rightsquigarrow_{\mathsf{cbv}} \underline{s' \shortmid e' \shortmid \pi' \shortmid \xi' \shortmid \delta'}$.

B Source Syntax

Definition 3 (Substitution of Terms for Variables). *The term resulting from replacing all free occurrences of x in s with t, written $s\{t/x\}$, is defined as follows:*

$$\begin{array}{rcl}
\iota_A\{t/x\} := & \iota_A & \\
y\{t/x\} := & \begin{cases} t, & x = y \\ y, & x \neq y \end{cases} & \\
(\lambda b^A.s)\{t/x\} := & \lambda b^A.s\{t/x\} & \\
(s\,s')\{t/x\} := & s\{t/x\}\ s'\{t/x\} & \\
(!s)\{t/x\} := & !s\{t/x\} & \\
(\mathit{let}\ u^A \triangleq s\ \mathit{in}\ s')\{t/x\} := & \mathit{let}\ u^A \triangleq s\{t/x\}\ \mathit{in}\ s'\{t/x\} &
\end{array}$$

C Runtime Syntax

C.1 Typing for Configurations

$$\frac{}{\Delta;\Gamma \vdash \iota_A : \mathtt{iter}_A}\ \textsf{C-TI} \qquad \frac{a : A \in \Gamma}{\Delta;\Gamma \vdash a : A}\ \textsf{C-VAR}$$

$$\frac{\Delta;\Gamma, a : A \vdash M : B}{\Delta;\Gamma \vdash \lambda a^A.M : A \supset B}\ \textsf{C-ABS} \qquad \frac{\Delta;\Gamma \vdash M : A \supset B \quad \Delta;\Gamma \vdash N : A}{\Delta;\Gamma \vdash M\,N : B}\ \textsf{C-APP}$$

$$\frac{u : A \in \Delta}{\Delta;\Gamma \vdash u : A}\ \textsf{C-AVAR} \qquad \frac{\Delta;\cdot \vdash M : A \quad \Delta;\cdot \vdash \rho : s \geqslant \widehat{M}}{\Delta;\Gamma \vdash !_\rho M : [\![s]\!]A}\ \textsf{C-BANG}$$

$$\frac{\Delta;\Gamma \vdash M : [\![r]\!]A \quad \Delta, u : A;\Gamma \vdash N : C}{\Delta;\Gamma \vdash \mathit{let}\ u^A \triangleq M\ \mathit{in}\ N : C\{r/u\}}\ \textsf{C-LET}$$

C.2 Audit Trails

The source and target of a trail are given by the following functions $\_^{src}, \_^{tgt} : \mathbb{R} \longrightarrow \mathbb{T}$:

$$\begin{aligned}
s^{src} &:= s & s^{tgt} &:= s\\
\mathbf{ba}(s)^{src} &:= s & \mathbf{ba}((\lambda a^A.s_1)s_2)^{tgt} &:= s_1\{s_2/a\}\\
\mathbf{bb}(s)^{src} &:= s & \mathbf{bb}(\mathit{let}\ u^A \triangleq !s_1\ \mathit{in}\ s_2)tgt &:= s_2\{s_1/u\}\\
\mathbf{ti}_A(\rho)^{src} &:= \iota_A & \mathbf{ti}_A(\rho)^{tgt} &:= \mathtt{iter}_{\mathsf{can}(\rho)}\\
(\rho;\sigma)^{src} &:= \rho^{src} & (\rho;\sigma)^{tgt} &:= \sigma^{tgt}\\
(\lambda a^A.\rho)^{src} &:= \lambda a^A.\rho^{src} & (\lambda a^A.\rho)^{tgt} &:= \lambda a^A.\rho^{tgt}\\
(\rho\,\sigma)^{src} &:= \rho^{src}\,\sigma^{src} & (\rho\,\sigma)^{tgt} &:= \rho^{tgt}\,\sigma^{tgt}\\
(\mathit{let}\ u^A \triangleq \rho\ \mathit{in}\ \sigma)^{src} &:= \mathit{let}\ u^A \triangleq \rho^{src}\ \mathit{in}\ \sigma^{src} & (\mathit{let}\ u^A \triangleq \rho\ \mathit{in}\ \sigma)^{tgt} &:= \mathit{let}\ u^A \triangleq \rho^{tgt}\ \mathit{in}\ \sigma^{tgt}
\end{aligned}$$

Substitution of trails in terms	$s\{\rho/u\}$
Substitution of terms in trails	$\rho\{s/u\}$

The result of substituting all free occurrences of audited unit variable u in s is the trail denoted $s\{\rho/u\}$ and defined as follows:

$$\begin{aligned}
\iota_A\{\rho/u\} &:= \iota_A\\
a\{\rho/u\} &:= a\\
v\{\rho/u\} &:= \begin{cases}\rho, & u = v\\ v, & u \neq v\end{cases}\\
(\lambda a^A.s)\{\rho/u\} &:= \lambda a^A.s\{\rho/u\}\\
(s\,t)\{\rho/u\} &:= s\{\rho/u\}\,t\{\rho/u\}\\
(!s)\{\rho/u\} &:= !s\{\rho^{src}/u\}\\
(\mathit{let}\ v^A \triangleq s\ \mathit{in}\ t)\{\rho/u\} &:= \mathit{let}\ v^A \triangleq s\{\rho/u\}\ \mathit{in}\ t\{\rho/u\}
\end{aligned}$$

The result of substituting all free occurrences of audited unit variable u in ρ with term s is the trail denoted $\rho\{s/u\}$ and defined as follows:

$$\begin{aligned}
t\{s/u\} &:= t\{s/u\} \\
\mathbf{ba}(r)\{s/u\} &:= \mathbf{ba}(r\{s/u\}) \\
\mathbf{bb}(r)\{s/u\} &:= \mathbf{bb}(r\{s/u\}) \\
\mathbf{ti}_A(\rho)\{s/u\} &:= \mathbf{ti}_{A\{s/u\}}(\rho\{s/u\}) \\
(\rho;\sigma)\{s/u\} &:= \rho\{s/u\};\sigma\{s/u\} \\
(\lambda a^A.\rho)\{s/u\} &:= \lambda a^A.\rho\{s/u\} \\
(\rho\,\sigma)\{s/u\} &:= \rho\{s/u\}\,\sigma\{s/u\} \\
(\mathit{let}\ v^A \triangleq \rho\ \mathit{in}\ \sigma)\{s/u\} &:= \mathit{let}\ v^A \triangleq \rho\{s/u\}\ \mathit{in}\ \sigma\{s/u\}
\end{aligned}$$

Substitution of Configurations for Term Variables	$M\{N/a\}$
Substitution of Audited Units for Audited Unit Variables	$M\{!_\rho N/u\}$

Substitution of all free occurrences of a in M with N, is defined as follows:

$$\begin{aligned}
\iota_A\{N/a\} &:= \iota_A \\
a\{N/b\} &:= \begin{cases} N, & a = b \\ a, & a \neq b \end{cases} \\
u\{N/a\} &:= u \\
(\lambda a^A.R)\{N/a\} &:= \lambda a^A.R\{N/a\} \\
(R\,S)\{N/a\} &:= R\{N/a\}\,S\{N/a\} \\
(!_\rho R)\{N/a\} &:= !_\rho R \\
(\mathit{let}\ v^A \triangleq R\ \mathit{in}\ S)\{N/a\} &:= \mathit{let}\ v^A \triangleq R\{N/a\}\ \mathit{in}\ S\{N/a\}
\end{aligned}$$

Substitution of audited units in configurations must be done with some care[5]. It would not be correct to blindly replace audited unit variables by trails. For example, $u;u \simeq u$ however replacing u with ρ leads to $\rho;\rho \simeq \rho$ which is, in general, incorrect since one cannot compose a trail with itself (unless it has the same source and target). This leads to the following definition (see, in particular, the next-to-last clause) [11,26]:

$$\begin{aligned}
\iota_A\{!_\rho N/u\} &:= \iota_A \\
a\{!_\rho N/u\} &:= a \\
v\{!_\rho N/u\} &:= \begin{cases} N, & u = v \\ v, & u \neq v \end{cases} \\
(\lambda a^A.R)\{!_\rho N/u\} &:= \lambda a^A.R\{!_\rho N/u\} \\
(R\,S)\{!_\rho N/u\} &:= R\{!_\rho N/u\}\,S\{!_\rho N/u\} \\
(!_\sigma R)\{!_\rho N/u\} &:= !_{\sigma\{\rho^{src}/u\};\widehat{R}\{\rho/u\}} R\{!_\rho N/u\} \\
(\mathit{let}\ v^A \triangleq R\ \mathit{in}\ S)\{!_\rho N/u\} &:= \mathit{let}\ v^A \triangleq R\{!_\rho N/u\}\ \mathit{in}\ S\{!_\rho N/u\}
\end{aligned}$$

As an example consider a term such as $\mathit{let}\ u^A \triangleq !_\rho V\ \mathit{in}\ !_{!_u}!_u u$ and suppose that s is the source of ρ. Its reduct is $(!_{!_u}!_u u)\{!_\rho V/u\} = !_{!_s;!_s}!_{s;\rho} V \simeq !_{!_s}!_\rho V$. Note how the trail has been persisted in the innermost computation. Also note how the outermost "!" cannot see the computation under it.

[5] A fact already noted in [13] where proof terms for Higher-Order Rewrite Systems are proposed.

Structural equivalence of configurations. Structural equivalence of configurations is defined as follows.

$$\frac{}{\mathfrak{a} \simeq \mathfrak{a}} \qquad \frac{M \simeq N}{\lambda a^A.M \simeq \lambda a^A.N} \qquad \frac{M \simeq P \quad N \simeq Q}{M\,N \simeq P\,Q}$$

$$\frac{M \simeq N \quad \rho \simeq \sigma}{!_\rho M \simeq !_\sigma N} \qquad \frac{M \simeq P \quad N \simeq Q}{let\ u^A \triangleq M\ in\ N \simeq let\ u^A \triangleq P\ in\ Q}$$

Tuples are considered up-to structural equivalence $\simeq$, where $M \shortmid \rho \shortmid \mathcal{F} \simeq N \shortmid \sigma \shortmid \mathcal{G}$ iff $M \simeq N$, $\rho \simeq \sigma$ and $\mathcal{F} \simeq \mathcal{G}$.
The canonical trails rewrite system is defined by the contextual closure of the following rewrite rules:

$$\begin{aligned}
\rho; s &\to \rho \\
s; \rho &\to \rho \\
(\rho; \sigma); \tau &\to \rho; (\sigma; \tau) \\
(\rho_1\,\sigma_1); (\rho_2\,\sigma_2) &\to (\rho_1; \rho_2)\,(\sigma_1; \sigma_2) \\
\lambda a^A.\rho; \lambda a^A.\sigma &\to \lambda a^A.(\rho; \sigma) \\
let\ u^A \triangleq \rho_1\ in\ \sigma_1; let\ u^A \triangleq \rho_2\ in\ \sigma_2 &\to let\ u^A \triangleq \rho_1; \rho_2\ in\ \sigma_1; \sigma_2 \\
(\rho_1\,\sigma_1); ((\rho_2\,\sigma_2); \tau) &\to ((\rho_1; \rho_2)\,(\sigma_1; \sigma_2)); \tau \\
\lambda a^A.\rho; ((\lambda a^A.\sigma); \tau) &\to (\lambda a^A.(\rho; \sigma)); \tau \\
let\ u^A \triangleq \rho_1\ in\ \sigma_1; ((let\ u^A \triangleq \rho_2\ in\ \sigma_2); \tau) &\to (let\ u^A \triangleq \rho_1; \rho_2\ in\ \sigma_1; \sigma_2); \tau
\end{aligned}$$

Lemma 2. *[29, 8.3.6]* $\to$ *reduction is strongly normalizing and confluent.*

D Call-by-Name

D.1 Evaluation

The following preservation of well-formedness result is proved by induction on the derivation of $M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma$.

Lemma 3. $M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma$ *and* $M \shortmid \rho \shortmid \mathcal{F}$ *well-formed implies*

(a) ρ *is composable with* $\widehat{\mathcal{F}}\langle\sigma\rangle$ (i.e. $\widehat{\mathcal{F}}\langle\sigma\rangle^{src} = \rho^{tgt}$)*; and*
(b) $!_{\rho;\widehat{\mathcal{F}}\langle\sigma\rangle}\mathcal{F}\langle V\rangle$ *is a well-formed configuration.*

Decompilation for CBN shallow contexts is defined as follows:

$$\widehat{\Box} := \Box \tag{1}$$

$$\widehat{(\mathcal{F}\,M)} := \widehat{\mathcal{F}}\,\widehat{M} \tag{2}$$

$$\widehat{(let\ u^A \triangleq \mathcal{F}\ in\ M)} := let\ u^A \triangleq \widehat{\mathcal{F}}\ in\ \widehat{M} \tag{3}$$

Lemma 4. $\widehat{\mathcal{F}\langle M\rangle} = \widehat{\mathcal{F}}\langle\widehat{M}\rangle$.

Proof. By induction on $\mathcal{F}$.

Lemma 5. $(\widehat{M\{N/a\}}) = \widehat{M}\{\widehat{N}/a\}$.

Proof. By induction on M.

We write $\pi\Big(M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma\Big)$ if $M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma$ is derivable with derivation π.

Lemma 6. *If* $\pi\Big(M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma\Big)$ *and* $M \shortmid \rho \shortmid \mathcal{F} \simeq M' \shortmid \rho' \shortmid \mathcal{F}'$, *then there exists* $V' \shortmid \sigma'$ *and* π' *such that* $\pi'\Big(M' \shortmid \rho' \shortmid \mathcal{F}' \Downarrow^{\mathsf{cbn}} V' \shortmid \sigma'\Big)$ *and* $V \shortmid \sigma \simeq V' \shortmid \sigma'$.

Proof. By induction on π.

Lemma 7. $M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma$ *and* $M \shortmid \rho \shortmid \mathcal{F}$ *well-formed implies*

(a) ρ *is composable with* $\widehat{\mathcal{F}}\langle\sigma\rangle$ (i.e. $\widehat{\mathcal{F}}\langle\sigma\rangle^{src} = \rho^{tgt}$)*; and*
(b) $!_{\rho;\widehat{\mathcal{F}}\langle\sigma\rangle}\mathcal{F}\langle V\rangle$ *is a well-formed configuration.*

Proof. By induction on the derivation of $M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma$.

– $\mathsf{E\text{-}V}$

$$\frac{}{V \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid \widehat{V}}\ \mathsf{E\text{-}V}$$

(a) For the first item we reason as follows: $(\widehat{\mathcal{F}}\langle\widehat{V}\rangle)^{src} = (\widehat{\mathcal{F}\langle V\rangle})^{src} = \widehat{\mathcal{F}\langle V\rangle} = \rho^{tgt}$. The last equality is from the hypothesis that $M \shortmid \rho \shortmid \mathcal{F}$ well-formed.
(b) For the second item we must show that $!_{\rho;\widehat{\mathcal{F}\langle V\rangle}}\mathcal{F}\langle V\rangle$ is well-formed. Note that $!_{\rho;\widehat{\mathcal{F}\langle V\rangle}}\mathcal{F}\langle V\rangle$ is consistent: $(\rho;\widehat{\mathcal{F}\langle V\rangle})^{tgt} = (\widehat{\mathcal{F}\langle V\rangle})^{tgt} = \widehat{\mathcal{F}\langle V\rangle}$. Moreover, every subterm of V and $\mathcal{F}$ of the form $!_\rho N$ is consistent by the hypothesis that $V \shortmid \rho \shortmid \mathcal{F}$ is well-formed.

– $\mathsf{E\text{-}!}$

$$\frac{M \shortmid \tau \shortmid \Box \Downarrow^{\mathsf{cbn}} V \shortmid \mu}{!_\tau M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} !_{\tau;\mu}V \shortmid !\tau^{src}}\ \mathsf{E\text{-}!}$$

(a) For the first item we reason as follows: $\widehat{\mathcal{F}}\langle\sigma\rangle^{src} = (\widehat{\mathcal{F}}\langle!\tau^{src}\rangle)^{src} = \widehat{\mathcal{F}}\langle!\tau^{src}\rangle = \rho^{tgt}$. The last equality is from the hypothesis that $!_\tau M \shortmid \rho \shortmid \mathcal{F}$ is well-formed.
(b) For the second item we must verify that: $!_{\rho;\widehat{\mathcal{F}}\langle!\tau^{src}\rangle}\mathcal{F}\langle!_{\tau;\mu}V\rangle$ is well-formed. We check two things:
- First we check that $!_{\rho;\widehat{\mathcal{F}}\langle!\tau^{src}\rangle}\mathcal{F}\langle!_{\tau;\mu}V\rangle$ is consistent. That is, $(\rho;\widehat{\mathcal{F}}\langle!\tau^{src}\rangle)^{tgt} = (\widehat{\mathcal{F}}\langle!\tau^{src}\rangle)^{tgt} = \widehat{\mathcal{F}\langle!_{\tau;\mu}V\rangle}$. For the LHS we use the definition of decompilation and target:

$$(\widehat{\mathcal{F}}\langle!\tau^{src}\rangle)^{tgt} = \widehat{\mathcal{F}}\langle!\tau^{src}\rangle$$

For the RHS we have

$$\widehat{\mathcal{F}\langle(\widehat{!_{\tau;\mu}V})\rangle} =_{Lem.\ 4} \widehat{\mathcal{F}}\langle(\widehat{!_{\tau;\mu}V})\rangle = \widehat{\mathcal{F}}\langle!(\tau;\mu)^{src}\rangle = \widehat{\mathcal{F}}\langle!\tau^{src}\rangle$$

- Moreover, every bang subterm of V and $\mathcal{F}$ is consistent from the hypothesis that $M \shortmid \rho \shortmid \mathcal{F}$ is well-formed. Finally, $!_{\tau;\mu}V$ is consistent from the i.h. on the derivation of $M \shortmid \tau \shortmid \Box \Big\Downarrow^{\mathsf{cbn}} V \shortmid \mu$.

– E-β

$$\frac{\pi_1\Big(M \shortmid \rho \shortmid \mathcal{F}\langle \Box\, N\rangle \Big\Downarrow^{\mathsf{cbn}} \lambda a^A.P \shortmid \mu\Big) \quad \pi_2\Big(P\{N/a\} \shortmid \rho; \widehat{\mathcal{F}}\langle (\mu\, \widehat{N}); \mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{N})\rangle \shortmid \mathcal{F} \Big\Downarrow^{\mathsf{cbn}} W \shortmid \upsilon\Big)}{M\, N \shortmid \rho \shortmid \mathcal{F} \Big\Downarrow^{\mathsf{cbn}} W \shortmid (\mu\, \widehat{N}); \mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{N}); \upsilon}\, E-\beta$$

(a) For the first item we reason as follows:

$$\widehat{\mathcal{F}}\langle\sigma\rangle^{src} = \widehat{\mathcal{F}}\langle (\mu\, \widehat{N}); \mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{N}); \upsilon\rangle^{src} = \widehat{\mathcal{F}}\langle \mu\, \widehat{N}\rangle^{src} = \widehat{\mathcal{F}}\langle \mu^{src}\, \widehat{N}^{src}\rangle = \widehat{\mathcal{F}}\langle \widehat{M}\, \widehat{N}\rangle$$

Note that $\mu^{src} = \widehat{M}$ and $\widehat{N}^{src} = \widehat{N}$, follows from the i.h.. By hypothesis

$$\rho^{tgt} = \widehat{\mathcal{F}\langle M\, N\rangle}$$

(b) We must verify that $!_{\widehat{N};((\mu\, \widehat{N});\mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{N});\upsilon)}\mathcal{F}\langle W\rangle$ is well-formed.

- First we check that $!_{\rho;((\mu\, \widehat{N});\mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{N});\upsilon)}\mathcal{F}\langle W\rangle$ is consistent. This implies checking that $(\rho; \widehat{\mathcal{F}}\langle (\mu\, \widehat{N}); \mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{N}); \upsilon\rangle)^{tgt} = \upsilon^{tgt} = \widehat{\mathcal{F}\langle W\rangle}$. This follows from the i.h. applied to π_1 and then to π_2, from which we conclude.
- Moreover, every bang subterm of N and $\mathcal{F}$ is consistent from the hypothesis that $M \shortmid \rho \shortmid \mathcal{F}$ is well-formed.

– E-$\beta_{\Box}$

$$\frac{\pi_1\Big(M \shortmid \rho \shortmid \mathcal{F}\langle let\ u^A \triangleq \Box\ in\ N\rangle \Big\Downarrow^{\mathsf{cbn}} !_\tau W \shortmid \mu\Big) \quad \pi_2\Big(N\{!_\tau W/u\} \shortmid \rho; \widehat{\mathcal{F}}\langle let\ u^A \triangleq \mu\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau W)}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}\rangle \shortmid \mathcal{F} \Big\Downarrow^{\mathsf{cbn}} V \shortmid \upsilon\Big)}{let\ u^A \triangleq M\ in\ N \shortmid \rho \shortmid \mathcal{F} \Big\Downarrow^{\mathsf{cbn}} V \shortmid let\ u^A \triangleq \mu\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau W)}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon}\, E-\beta_{\Box}$$

(a) For the first case we reason as follows:

$$\begin{aligned} &\widehat{\mathcal{F}}\langle\sigma\rangle^{src} \\ &= \widehat{\mathcal{F}}\langle let\ u^A \triangleq \mu\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau W)}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon\rangle^{src} \\ &= \widehat{\mathcal{F}}\langle let\ u^A \triangleq \mu\ in\ \widehat{N}\rangle^{src} \\ &= \widehat{\mathcal{F}}\langle let\ u^A \triangleq \mu^{src}\ in\ \widehat{N}\rangle \end{aligned}$$

By the i.h. on $M \shortmid \rho \shortmid \mathcal{F}\langle let\ u^A \triangleq \Box\ in\ Q\rangle \Big\Downarrow^{\mathsf{cbn}} !_\tau W \shortmid \mu$,

$$\rho^{tgt} = \widehat{\mathcal{F}}\langle let\ u^A \triangleq \mu\ in\ \widehat{N}\rangle^{src} = \widehat{\mathcal{G}\langle M\rangle}$$

for $\mathcal{G} = \mathcal{F}\langle let\ u^A \triangleq \Box\ in\ N\rangle$. This concludes the case since $\rho^{tgt} = \mathcal{F}\langle let\ \widehat{u^A \triangleq M}\ in\ N\rangle = \widehat{\mathcal{G}\langle M\rangle}$.

(b) We must verify that $!_{\rho;let\ u^A \triangleq \mu\ in\ \widehat{N};\mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau W)}\ in\ \widehat{N});\widehat{N}\{\tau/u\};\upsilon}\mathcal{F}\langle V\rangle$ is well-formed.
- First we check that $!_{\rho;let\ u^A \triangleq \mu\ in\ \widehat{N};\mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau W)}\ in\ \widehat{N});\widehat{N}\{\tau/u\};\upsilon}\mathcal{F}\langle V\rangle$ is compatible. This implies checking $\rho; let\ u^A \triangleq \mu\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau W)}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon^{tgt} = \upsilon^{tgt} = \widehat{\mathcal{F}\langle V\rangle}$. This follows from the i.h. on π_1 and then from the i.h. on π_2.
- Moreover, every bang subterm of V and $\mathcal{F}$ is consistent from the hypothesis that $M \shortmid \rho \shortmid \mathcal{F}$ is well-formed.

– E-TI. Then $\sigma = \mathbf{ti}_A(\rho)$ and the derivation ends:

$$\frac{}{\iota_A \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} \mathtt{iter}_{\mathsf{can}(\rho)} \shortmid \mathbf{ti}_A(\rho)}\ \text{E-TI}$$

(a) For the first case we reason as follows: $\widehat{\mathcal{F}}\langle\sigma\rangle^{src} = \widehat{\mathcal{F}}\langle\mathbf{ti}_A(\rho)\rangle^{src} = \widehat{\mathcal{F}}\langle\iota_A\rangle = \rho^{tgt}$. The last equality is from the hypothesis that $M \shortmid \rho \shortmid \mathcal{F}$ well-formed.
(b) For the second item we have to prove that $\widehat{\mathcal{F}}\langle\sigma\rangle^{tgt} = (\widehat{\mathcal{F}}\langle\mathbf{ti}_A(\rho)\rangle)^{tgt} = \widehat{\mathcal{F}}\langle\mathtt{iter}_{\mathsf{can}(\rho)}\rangle$. We reason as follows:

$$\begin{aligned}&(\widehat{\mathcal{F}}\langle\mathbf{ti}_A(\rho)\rangle)^{tgt}\\ =\ &\widehat{\mathcal{F}}\langle\mathbf{ti}_A(\rho)^{tgt}\rangle\\ =\ &\widehat{\mathcal{F}}\langle\mathtt{iter}_{\mathsf{can}(\rho)}\rangle\end{aligned}$$

Proof of Prop. 1 (Reduction simulates evaluation).

Proof. By induction on π.

– E-V. Then $M = V$ and π is:

$$\frac{}{V \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid \widehat{V}}\ \text{E-V}$$

Since $V \shortmid \rho \shortmid \mathcal{F}$ is well-formed, $\rho^{tgt} = \widehat{\mathcal{F}\langle V\rangle}$ and therefore ρ and $\widehat{\mathcal{F}\langle V\rangle}$ are composable. We conclude from $\rho \simeq \rho; \widehat{\mathcal{F}\langle V\rangle}$.

– E-!. Then $M = !_\tau N$ and π ends in:

$$\frac{N \shortmid \tau \shortmid \Box \Downarrow^{\mathsf{cbn}} V \shortmid \mu}{!_\tau N \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} !_{\tau;\mu} V \shortmid !\tau^{src}}\ \text{E-!}$$

Since $M \shortmid \rho \shortmid \mathcal{F}$ is well-formed, so is $N \shortmid \tau \shortmid \Box$. Moreover, $\widehat{\mathcal{F}\langle !_\tau N\rangle} = \widehat{\mathcal{F}}\langle !\tau^{src}\rangle$. By the i.h., $!_\tau N \rightsquigarrow^*_{\mathsf{cbn}} !_{\tau;\mu} V$. We therefore have $!_\rho \mathcal{F}\langle !_\tau N\rangle \rightsquigarrow^*_{\mathsf{cbn}} !_\rho \mathcal{F}\langle !_{\tau;\mu} V\rangle \simeq !_{\rho;\widehat{\mathcal{F}}\langle !\tau^{src}\rangle}\mathcal{F}\langle !_{\tau;\mu} V\rangle$.

– E-β. Then $M = P\,Q$ and π ends in an application of:

$$\frac{\pi_1\Big(P \shortmid \rho \shortmid \mathcal{F}\langle\Box\, Q\rangle \Downarrow^{\mathsf{cbn}} \lambda a^A.N \shortmid \mu\Big)\qquad \pi_2\Big(N\{Q/a\} \shortmid \widehat{Q}; \widehat{\mathcal{F}}\langle(\mu\,\widehat{Q}); \mathbf{ba}((\lambda a^A.\widehat{N})\,\widehat{Q})\rangle \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid \upsilon\Big)}{P\,Q \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbn}} V \shortmid (\mu\,\widehat{Q}); \mathbf{ba}((\lambda a^A.\widehat{N})\,\widehat{Q}); \upsilon}\ \text{E-}\beta$$

Since $P\,Q \intercal \rho \intercal \mathcal{F}$ is well-formed, then so is $P \intercal \rho \intercal \mathcal{F}\langle \Box\, Q\rangle$. Thus we can apply the i.h. to π_1:

$$!_\rho \mathcal{F}\langle P\,Q\rangle \rightsquigarrow^*_{\mathsf{cbn}} !_{\rho;\hat{\mathcal{F}}\langle \mu\, \hat{Q}\rangle} \mathcal{F}\langle (\lambda a^A.N)\, Q\rangle \tag{4}$$

By Lem. 7(2) on π_1 we also know that

$$!_{\rho;\hat{\mathcal{F}}\langle \mu\, \hat{Q}\rangle} \mathcal{F}\langle (\lambda a^A.N)\, Q\rangle \text{ is well-formed} \tag{5}$$

An additional application of R-β produces

$$\begin{array}{c} !_{\rho;\hat{\mathcal{F}}\langle \mu\, \hat{Q}\rangle} \mathcal{F}\langle (\lambda a^A.N)\, Q\rangle \\ \rightsquigarrow_{\mathsf{cbn}} !_{\rho;\hat{\mathcal{F}}\langle \mu\, \hat{Q}\rangle;\hat{\mathcal{F}}\langle \mathbf{ba}(\hat{R})\rangle} \mathcal{F}\langle N\{Q/a\}\rangle \end{array} \tag{6}$$

where $R := (\lambda a^A.N)\, Q$. From (5)

$$!_{\rho;\hat{\mathcal{F}}\langle \mu\, \hat{Q}\rangle;\hat{\mathcal{F}}\langle \mathbf{ba}(\hat{R})\rangle} \mathcal{F}\langle N\{Q/a\}\rangle.$$

is well-formed. We may then apply the i.h. on π_2 and deduce

$$!_{\rho;\hat{\mathcal{F}}\langle \mu\, \hat{Q}\rangle;\hat{\mathcal{F}}\langle \mathbf{ba}(\hat{R})\rangle} \mathcal{F}\langle N\{Q/a\}\rangle \rightsquigarrow^*_{\mathsf{cbn}} !_{\rho;\hat{\mathcal{F}}\langle \mu\, \hat{Q}\rangle;\hat{\mathcal{F}}\langle \mathbf{ba}(\hat{R})\rangle;\upsilon} \mathcal{F}\langle V\rangle \tag{7}$$

We conclude by adjoining 4, 6 and 7.

– E-$\beta_{\Box}$: Then $M = \mathit{let}\ u^A \triangleq P\ \mathit{in}\ N$ and π ends in an application of:

$$\frac{\pi_1\Big(P \intercal \rho \intercal \mathcal{F}\langle \mathit{let}\ u^A \triangleq \Box\ \mathit{in}\ N\rangle \Downarrow^{\mathsf{cbn}} !_\tau W \intercal \mu\Big) \qquad \pi_2\Big(N\{!_\tau W/u\} \intercal \rho;\widehat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N};\mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{!_\tau W}\ \mathit{in}\ \widehat{N});\widehat{N}\{\tau/u\}\rangle \intercal \mathcal{F} \Downarrow^{\mathsf{cbn}} V \intercal \upsilon\Big)}{\mathit{let}\ u^A \triangleq P\ \mathit{in}\ N \intercal \rho \intercal \mathcal{F} \Downarrow^{\mathsf{cbn}} V \intercal \mathit{let}\ u^A \triangleq \tau\ \mathit{in}\ \widehat{N};\mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{!_\tau W}\ \mathit{in}\ \widehat{N});\widehat{N}\{\tau/u\};\upsilon}\ \mathsf{E}\text{-}\beta_{\Box}$$

By the i.h. on π_1:

$$!_\rho \mathcal{F}\langle \mathit{let}\ u^A \triangleq P\ \mathit{in}\ N\rangle \rightsquigarrow^*_{\mathsf{cbn}} !_{\rho;\hat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}\rangle} \mathcal{F}\langle \mathit{let}\ u^A \triangleq !_\tau W\ \mathit{in}\ N\rangle \tag{8}$$

By Lem. 7 we also know that $!_{\rho;\hat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}\rangle} \mathcal{F}\langle \mathit{let}\ u^A \triangleq !_\tau W\ \mathit{in}\ N\rangle$ is well-formed. But then $!_{\rho;\hat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N};\hat{\mathcal{F}}\langle \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{(!_\tau V)}\ \mathit{in}\ \widehat{N});N\{\tau/u\}\rangle} N\{!_\tau W/u\}$ is well-formed too. This allows us to apply the i.h. on π_2 and deduce

$$!_{\rho;\hat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}\rangle} \mathcal{F}\langle N\{!_\tau W/u\}\rangle \rightsquigarrow^*_{\mathsf{cbn}} !_{\rho;\hat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}\rangle;\hat{\mathcal{F}}\langle \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{!_\tau V}\ \mathit{in}\ N);N\{\tau/u\}\rangle} \mathcal{F}\langle V\rangle \tag{9}$$

From R-$\beta_{\Box}$ we know:

$$!_{\rho;\hat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}\rangle} \mathcal{F}\langle \mathit{let}\ u^A \triangleq V\ \mathit{in}\ N\rangle \rightsquigarrow_{\mathsf{cbn}} !_{\rho;\hat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}\rangle;\hat{\mathcal{F}}\langle \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{!_\tau V}\ \mathit{in}\ N);N\{\tau/u\}\rangle} \mathcal{F}\langle N\{\tau/u\}\rangle \tag{10}$$

We conclude from 8, 9 and 10.

– E-TI. Then π is the derivation

$$\frac{}{\iota_A \intercal \rho \intercal \mathcal{F} \Downarrow^{\mathsf{cbn}} \mathtt{iter}_{\mathsf{can}(\rho)} \intercal \mathbf{ti}(\rho)}\ \mathsf{E}\text{-}\mathsf{TI}$$

We conclude from R-TI: $!_\rho \mathcal{F}\langle \iota_A\rangle \rightsquigarrow_{\mathsf{cbn}} !_{\rho;\hat{\mathcal{F}}\langle \mathbf{ti}(\rho)\rangle} \mathcal{F}\langle \mathtt{iter}_{\mathsf{can}(\rho)}\rangle$.

Lemma 8 (Root Expansion). *For all (R, R', ξ) in the CBN redex table, $R' \shortmid \rho; \widehat{\mathcal{G}}\langle\xi\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \sigma$, implies $R \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \xi; \sigma$.*

Proof. We consider each of the possible three cases for R:

- $R = (\lambda a^A.M)\, N$, $R' = M\{N/a\}$, $\xi = \mathbf{ba}(\widehat{R})$. Then we must prove:

$$(\lambda a^A.M)\, N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \mathbf{ba}(\widehat{R}); \sigma$$

  We can do so by constructing the following derivation:

$$\lambda a^A.M \shortmid \rho \shortmid \mathcal{G}\langle\Box\, N\rangle \Downarrow^{\mathsf{cbn}} \lambda a^A.M \shortmid \widehat{\lambda a^A.M}$$
$$\frac{M\{N/a\} \shortmid \rho; \widehat{\mathcal{G}}\langle\widehat{R}; \mathbf{ba}(\widehat{R})\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \sigma}{(\lambda a^A.M)\, N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \widehat{R}; \mathbf{ba}(\widehat{R}); \sigma}\, E-\beta$$

  The second evaluation judgement in the hypothesis holds as a consequence of $\widehat{\mathcal{G}}\langle\widehat{R}; \mathbf{ba}(\widehat{R})\rangle \simeq \widehat{\mathcal{G}}\langle\mathbf{ba}(\widehat{R})\rangle$ and the hypothesis $R' \shortmid \rho; \widehat{\mathcal{G}}\langle\xi\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \sigma$. Moreover, $\widehat{R}; \mathbf{ba}(\widehat{R}); \sigma \simeq \mathbf{ba}(\widehat{R}); \sigma$.
- $R = \mathit{let}\ u^A \triangleq !_\tau V\ \mathit{in}\ N$, $R' = N\{!_\tau V/u\}$ and $r = \mathbf{bb}(\widehat{R}); N\{\tau/u\}$. Then we reason as follows:

$$!_\tau V \shortmid \rho \shortmid \mathcal{G}\langle \mathit{let}\ u^A \triangleq \Box\ \mathit{in}\ N\rangle \Downarrow^{\mathsf{cbn}} !_\tau V \shortmid \widehat{!_\tau V}$$
$$\frac{N\{!_\tau V/u\} \shortmid \rho; \widehat{\mathcal{G}}\langle\widehat{R}; \mathbf{bb}(\widehat{R}); \widehat{N}\{\tau/u\}\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \sigma}{\mathit{let}\ u^A \triangleq !_\tau V\ \mathit{in}\ N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \widehat{R}; \mathbf{bb}(\widehat{R}); \widehat{N}\{\tau/u\}; \sigma}\, E-\beta_{\Box}$$

  The judgement just above the line follows from the hypothesis $R' \shortmid \rho; \widehat{\mathcal{G}}\langle\xi\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \sigma$.
- $R = \iota_A$, $R' = \mathtt{iter}_{\mathsf{can}(\rho)}$ and $r = \mathbf{ti}_A(\rho)$. Note that $\sigma = \widehat{R'}$ since R' is a value. We reason as follows:

$$\frac{}{\iota_A \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} \mathtt{iter}_{\mathsf{can}(\rho)} \shortmid \mathbf{ti}_A(\rho)}\, \mathsf{E\text{-}TI}$$

  Note that since $\mathtt{iter}_{\mathsf{can}(\rho)}$ is a value, the hypothesis $R' \shortmid \rho; \widehat{\mathcal{G}}\langle\xi\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \sigma$ reads $\mathtt{iter}_{\mathsf{can}(\rho)} \shortmid \rho; \widehat{\mathcal{G}}\langle\mathbf{ti}_A(\rho)\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} \mathtt{iter}_{\mathsf{can}(\rho)} \shortmid \widehat{\mathtt{iter}_\rho}$. Thus, $\sigma = \widehat{\mathtt{iter}_{\mathsf{can}(\rho)}}$ and $r; \sigma = \mathbf{ti}_A(\rho); \widehat{\mathtt{iter}_{\mathsf{can}(\rho)}} = \mathbf{ti}_A(\rho)$.

Next we address the Expansion Lemma (Lem. 1). We split it into its two items. The first item we call Shallow Expansion and is proved below.

Lemma 9 (Shallow Expansion (Lem. 1(1))). *For all (R, R', ξ) in the CBN redex table, $\mathcal{F}\langle R'\rangle \shortmid \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}}\langle\xi\rangle\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \sigma$, implies $\mathcal{F}\langle R\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \widehat{\mathcal{F}}\langle\xi\rangle; \sigma$.*

Proof. By induction on $\mathcal{F}$.

– $\mathcal{F} = \Box$. We must prove that if $R' \vdash \rho; \widehat{\mathcal{G}}\langle\xi\rangle \vdash \mathcal{G} \Downarrow^{\mathsf{cbn}} W \vdash \sigma$, then $R \vdash \rho \vdash \mathcal{G} \Downarrow^{\mathsf{cbn}} W \vdash \xi; \sigma$. This is Lem. 8.
– $\mathcal{F} = \mathcal{F}'\, M$. We have to prove $\mathcal{F}'\langle R\rangle\, M \vdash \rho \vdash \mathcal{G} \Downarrow^{\mathsf{cbn}} W \vdash (\widehat{\mathcal{F}'}\langle\xi\rangle\, \widehat{M}); \sigma$. From the hypothesis $\mathcal{F}'\langle R'\rangle\, M \vdash \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}'}\langle\xi\rangle\, \widehat{M}\rangle \vdash \mathcal{G} \Downarrow^{\mathsf{cbn}} W \vdash \sigma$ we have:

$$\frac{\begin{array}{c}\mathcal{F}'\langle R'\rangle \vdash \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}'}\langle\xi\rangle\, \widehat{M}\rangle \vdash \mathcal{G}\langle\Box\, \widehat{M}\rangle \Downarrow^{\mathsf{cbn}} \lambda a^A.P \vdash \tau \\ P\{M/a\} \vdash \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}'}\langle\xi\rangle\, \widehat{M}\rangle; \widehat{\mathcal{G}}\langle\tau\, \widehat{M}; \mathbf{ba}(\widehat{S})\rangle \vdash \mathcal{G} \Downarrow^{\mathsf{cbn}} W \vdash \nu\end{array}}{\mathcal{F}'\langle R'\rangle\, M \vdash \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}'}\langle\xi\rangle\, \widehat{M}\rangle \vdash \mathcal{G} \Downarrow^{\mathsf{cbn}} W \vdash \tau\, \widehat{M}; \mathbf{ba}(\widehat{S}); \nu}\, E-\beta \tag{11}$$

where $S := (\lambda a^A.P)\, M$. If we set $\mathcal{G}' := \mathcal{G}\langle\Box\, M\rangle$, then we may rewrite the topmost judgement in (11) as:

$$\mathcal{F}'\langle R'\rangle \vdash \rho; \widehat{\mathcal{G}'}\langle\widehat{\mathcal{F}'}\langle\xi\rangle\rangle \vdash \mathcal{G}' \Downarrow^{\mathsf{cbn}} \lambda a^A.P \vdash \tau \tag{12}$$

From the i.h. on (12), we deduce:

$$\mathcal{F}'\langle R\rangle \vdash \rho \vdash \mathcal{G}' \Downarrow^{\mathsf{cbn}} \lambda a^A.P \vdash \widehat{\mathcal{F}'}\langle\xi\rangle; \tau$$

We now prove the judgement $\mathcal{F}'\langle R\rangle\, M \vdash \rho \vdash \mathcal{G} \Downarrow^{\mathsf{cbn}} W \vdash (\widehat{\mathcal{F}'}\langle\xi\rangle\, \widehat{M}); \sigma$.

$$\frac{\begin{array}{c}\mathcal{F}'\langle R\rangle \vdash \rho \vdash \mathcal{G}\langle\Box\, M\rangle \Downarrow^{\mathsf{cbn}} \lambda a^A.P \vdash \widehat{\mathcal{F}'}\langle\xi\rangle; \tau \\ P\{M/a\} \vdash \rho; \widehat{\mathcal{G}}\langle(\widehat{\mathcal{F}'}\langle\xi\rangle; \tau)\, \widehat{M}; \mathbf{ba}(\widehat{S})\rangle \vdash \mathcal{G} \Downarrow^{\mathsf{cbn}} W \vdash \nu\end{array}}{\mathcal{F}'\langle R\rangle\, M \vdash \rho \vdash \mathcal{G} \Downarrow^{\mathsf{cbn}} W \vdash (\widehat{\mathcal{F}'}\langle\xi\rangle; \tau)\, \widehat{M}; \mathbf{ba}(\widehat{S}); \nu}\, E-\beta$$

Since

$$\widehat{\mathcal{G}}\langle\widehat{\mathcal{F}'}\langle\xi\rangle\, \widehat{M}\rangle; \widehat{\mathcal{G}}\langle\tau\, \widehat{M}\rangle \simeq \widehat{\mathcal{G}}\langle(\widehat{\mathcal{F}'}\langle\xi\rangle; \tau)\, \widehat{M}\rangle$$

and

$$\widehat{\mathcal{G}}\langle\widehat{\mathcal{F}'}\langle\xi\rangle\, \widehat{M}\rangle; \widehat{\mathcal{G}}\langle\tau\, \widehat{M}; \mathbf{ba}(\widehat{S})\rangle \simeq \widehat{\mathcal{G}}\langle(\widehat{\mathcal{F}'}\langle\xi\rangle; \tau)\, \widehat{M}; \mathbf{ba}(\widehat{S})\rangle$$

we conclude.
– $\mathcal{F} = \mathit{let}\ u^A \triangleq \mathcal{F}'\ \mathit{in}\ M$. We have to prove $\mathit{let}\ u^A \triangleq \mathcal{F}'\langle R\rangle\ \mathit{in}\ M \vdash \rho \vdash \mathcal{G} \Downarrow^{\mathsf{cbn}} W \vdash (\mathit{let}\ u^A \triangleq \mathcal{F}'\langle\xi\rangle\ \mathit{in}\ \widehat{M}); \sigma$. From the hypothesis $\mathcal{F}\langle R'\rangle \vdash \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}}\langle\xi\rangle\rangle \vdash \mathcal{G} \Downarrow^{\mathsf{cbn}} W \vdash \sigma$ we have the following, where $\sigma = \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}; \nu$:

$$\frac{\begin{array}{c}\mathcal{F}'\langle R'\rangle \vdash \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}}\langle\xi\rangle\rangle \vdash \mathcal{G}\langle\mathit{let}\ u^A \triangleq \Box\ \mathit{in}\ N\rangle \Downarrow^{\mathsf{cbn}} !_\tau V \vdash \mu \\ N\{!_\tau V/u\} \vdash \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}}\langle\xi\rangle; \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}\rangle \vdash \mathcal{G} \Downarrow^{\mathsf{cbn}} W \vdash \nu\end{array}}{\mathit{let}\ u^A \triangleq \mathcal{F}'\langle R'\rangle\ \mathit{in}\ N \vdash \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}}\langle\xi\rangle\rangle \vdash \mathcal{G} \Downarrow^{\mathsf{cbn}} W \vdash \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}; \nu}\, E-\beta_{\Box} \tag{13}$$

where $S := \mathit{let}\ u^A \triangleq !_\tau V\ \mathit{in}\ N$
If we set $\mathcal{G}' := \mathit{let}\ u^A \triangleq \Box\ \mathit{in}\ N$, then we may rewrite the topmost judgement in (13) as:

$$\mathcal{F}'\langle R'\rangle \vdash \rho; \widehat{\mathcal{G}'}\langle\widehat{\mathcal{F}'}\langle\xi\rangle\rangle \vdash \mathcal{G}' \Downarrow^{\mathsf{cbn}} !_\tau V \vdash \mu \tag{14}$$

From the i.h. on (14), we deduce:

$$\mathcal{F}'\langle R\rangle \shortmid \rho \shortmid \mathcal{G}' \Downarrow^{\mathsf{cbn}} !_\tau V \shortmid \widehat{\mathcal{F}'}\langle\xi\rangle; \mu$$

We now prove the judgement $let\ u^A \triangleq \mathcal{F}'\langle R\rangle\ in\ N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid let\ u^A \triangleq \widehat{\mathcal{F}'}\langle\xi\rangle\ in\ \widehat{N}; \sigma$.

$$\frac{\begin{array}{c}\mathcal{F}'\langle R\rangle \shortmid \rho \shortmid \widehat{\mathcal{G}}\langle let\ u^A \triangleq \Box\ in\ N\rangle \Downarrow^{\mathsf{cbn}} !_\tau V \shortmid \widehat{\mathcal{F}'}\langle r\rangle; \mu \\ N\{!_\tau V/u\} \shortmid \rho; \widehat{\mathcal{G}}\langle let\ u^A \triangleq (\widehat{\mathcal{F}}\langle r\rangle; \mu)\ in\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \nu\end{array}}{let\ u^A \triangleq \mathcal{F}'\langle R\rangle\ in\ N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid let\ u^A \triangleq (\widehat{\mathcal{F}}\langle r\rangle; \mu)\ in\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}; \nu}\ E - \beta_{\Box}$$

Note that

$$\begin{array}{ll} & let\ u^A \triangleq (\widehat{\mathcal{F}}\langle r\rangle; \mu)\ in\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}; \nu \\ \simeq & let\ u^A \triangleq \widehat{\mathcal{F}'}\langle r\rangle\ in\ \widehat{N}; let\ u^A \triangleq \mu\ in\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}; \nu \\ = & let\ u^A \triangleq \widehat{\mathcal{F}'}\langle r\rangle\ in\ \widehat{N}; \sigma \end{array}$$

Lemma 10 (Projection). *If* $\pi\Big(\mathcal{F}\langle M\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} U \shortmid \sigma\Big)$, *then there exists* V *and* τ *s.t.* $\pi \mid_p \Big(M \shortmid \rho \shortmid \mathcal{G}\langle\mathcal{F}\rangle \Downarrow^{\mathsf{cbn}} V \shortmid \tau\Big)$, *where* p *is the position of the hole in* $\mathcal{F}$.

Proof. By induction on $\mathcal{F}$. If $\mathcal{F} = \Box$, the result is immediate; we develop the inductive cases below:

- $\mathcal{F} = \mathcal{F}'\ N$. Then π ends as follows:

$$\frac{\begin{array}{c}\mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G}\langle\Box\ N\rangle \Downarrow^{\mathsf{cbn}} \lambda a^A.P \shortmid \sigma \\ P\{N/a\} \shortmid \rho; \widehat{\mathcal{G}}\langle(\sigma\ \widehat{N}); \mathbf{ba}((\lambda a^A.\widehat{P})\ \widehat{N})\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \upsilon\end{array}}{\mathcal{F}'\langle M\rangle\ N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid (\sigma\ \widehat{N}); \mathbf{ba}((\lambda a^A.\widehat{P})\ \widehat{N}); \upsilon}\ E - \beta$$

  We conclude from the i.h. applied to the derivation of $\mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G}\langle\Box\ N\rangle \Downarrow^{\mathsf{cbn}} \lambda a^A.P \shortmid \sigma$.
- $\mathcal{F} = let\ u^A \triangleq \mathcal{F}'\ in\ M$. Then π ends in

$$\frac{\begin{array}{c}\mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G}\langle let\ u^A \triangleq \Box\ in\ N\rangle \Downarrow^{\mathsf{cbn}} !_\tau V \shortmid \sigma \\ N\{!_\tau V/u\} \shortmid \rho; \widehat{\mathcal{G}}\langle let\ u^A \triangleq \sigma\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau V)}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \upsilon\end{array}}{let\ u^A \triangleq \mathcal{F}'\langle M\rangle\ in\ N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid let\ u^A \triangleq \sigma\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau V)}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon}\ E - \beta_{\Box}$$

We conclude from the i.h. on the derivation ending in the topmost judgement.

Lemma 11 (Substitution). *If*

- $\pi\Big(\mathcal{F}\langle M\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} U \shortmid \sigma\Big)$, *and*
- $\pi \mid_p \Big(M \shortmid \rho \shortmid \mathcal{G}\langle\mathcal{F}\rangle \Downarrow^{\mathsf{cbn}} V \shortmid \tau\Big)$, *for* p *the position of the hole in* $\mathcal{F}$ *and for some* V *and* τ, *and*

– $\pi_N\Big(N \shortmid \rho \shortmid \mathcal{G}\langle\mathcal{F}\rangle \Downarrow^{\mathsf{cbn}} V \shortmid \tau\Big)$.

Then $\pi \mid_p^{\pi_N} \Big(\mathcal{F}\langle N\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} U \shortmid \sigma\Big)$.

Proof. By induction on $\mathcal{F}$. If $\mathcal{F} = \Box$, then $U = V$ and $\sigma = \tau$ and the result holds immediately; we develop the inductive cases below:

– $\mathcal{F} = \mathcal{F}'\,N$. Then $p = 1.p'$, for p' the position of the hole in $\mathcal{F}'$, and π ends as follows:

$$\frac{\begin{array}{c}\mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G}\langle\Box\, N\rangle \Downarrow^{\mathsf{cbn}} \lambda a^A.P \shortmid \sigma \\ P\{N/a\} \shortmid \rho; \widehat{\mathcal{G}}\langle(\sigma\,\widehat{N}); \mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{N})\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \upsilon\end{array}}{\mathcal{F}'\langle M\rangle\, N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid (\sigma\,\widehat{N}); \mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{N}); \upsilon}\ \mathsf{E}\text{-}\beta$$

We conclude from the i.h. applied to the derivation of $\mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G}\langle\Box\, N\rangle \Downarrow^{\mathsf{cbn}} \lambda a^A.P \shortmid \sigma$ and then an application of E-β.

– $\mathcal{F} = \mathit{let}\ u^A \triangleq \mathcal{F}'\ \mathit{in}\ M$.

$$\frac{\begin{array}{c}\mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G}\langle \mathit{let}\ u^A \triangleq \Box\ \mathit{in}\ N\rangle \Downarrow^{\mathsf{cbn}} !_\tau V \shortmid \sigma \\ N\{!_\tau V/u\} \shortmid \rho; \widehat{\mathcal{G}}\langle \mathit{let}\ u^A \triangleq \sigma\ \mathit{in}\ \widehat{N}; \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{(!_\tau V)}\ \mathit{in}\ \widehat{N}); \widehat{N}\{\tau/u\}\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \upsilon\end{array}}{\mathit{let}\ u^A \triangleq \mathcal{F}'\langle M\rangle\ \mathit{in}\ N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \mathit{let}\ u^A \triangleq \sigma\ \mathit{in}\ \widehat{N}; \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{(!_\tau V)}\ \mathit{in}\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon}\ \mathsf{E}\text{-}\beta_{\Box}$$

We conclude from the i.h. on the derivation ending in the topmost judgement and then an application of E-$\beta_{\Box}$.

We now address the second item of the Expansion Lemma (Lem. 1).

Lemma 12 (Expansion (Lem. 1(2))). *For all* (R, R', ξ) *in the redex table, if* $\mathcal{E}\langle !_{\rho;\widehat{\mathcal{F}}\langle\xi\rangle}\mathcal{F}\langle R'\rangle\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \tau$, *then* $\mathcal{E}\langle !_\rho\mathcal{F}\langle R\rangle\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \tau$.

Proof. By induction on $\mathcal{E}$.

– If $\mathcal{E} = \Box$, then by hypothesis:

$$\frac{\mathcal{F}\langle R'\rangle \shortmid \rho; \widehat{\mathcal{F}}\langle\xi\rangle \shortmid \Box \Downarrow^{\mathsf{cbn}} V \shortmid \mu}{!_{\rho;\widehat{\mathcal{F}}\langle\xi\rangle}\mathcal{F}\langle R'\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} !_{(\rho;\widehat{\mathcal{F}}\langle\xi\rangle);\mu} V \shortmid \tau}\ \mathsf{E}\text{-}!$$

and $W = !_{(\rho;\widehat{\mathcal{F}}\langle\xi\rangle);\mu} V$. By Shallow Expansion (Lem. 1(1)) applied to $\mathcal{F}\langle R'\rangle \shortmid \rho; \widehat{\mathcal{F}}\langle\xi\rangle \shortmid \Box \Downarrow^{\mathsf{cbn}} V \shortmid \mu$, we deduce $\mathcal{F}\langle R\rangle \shortmid \rho \shortmid \Box \Downarrow^{\mathsf{cbn}} W \shortmid \widehat{\mathcal{F}}\langle\xi\rangle; \mu$. We conclude using E-Bang:

$$\frac{\mathcal{F}\langle R\rangle \shortmid \rho \shortmid \Box \Downarrow^{\mathsf{cbn}} V \shortmid \widehat{\mathcal{F}}\langle\xi\rangle; \mu}{!_\rho\mathcal{F}\langle R\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} !_{\rho;(\widehat{\mathcal{F}}\langle\xi\rangle;\mu)} V \shortmid \tau}\ \mathsf{E}\text{-}!$$

Note that $(\rho; \widehat{\mathcal{F}}\langle\xi\rangle); \mu \simeq \rho; (\widehat{\mathcal{F}}\langle\xi\rangle; \mu)$.

– Suppose $\mathcal{E} = !_{\rho'}\mathcal{F}'\langle\mathcal{E}'\rangle$. Then

$$\frac{\mathcal{F}'\langle\mathcal{E}'\langle!_{\rho;\widehat{\mathcal{F}\langle\xi\rangle}}\mathcal{F}\langle R'\rangle\rangle\rangle \shortmid \rho' \shortmid \Box \Downarrow^{\mathsf{cbn}} V' \shortmid \mu}{!_{\rho'}\mathcal{F}'\langle\mathcal{E}'\langle!_{\rho;\widehat{\mathcal{F}\langle\xi\rangle}}\mathcal{F}\langle R'\rangle\rangle\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \tau}\ \mathsf{E\text{-}!}$$

By Projection (Lem. 10), there exists U, ν s.t.

$$\pi \mid_p \Big(\mathcal{E}'\langle!_{\rho;\widehat{\mathcal{F}\langle\xi\rangle}}\mathcal{F}\langle R'\rangle\rangle \shortmid \rho' \shortmid \mathcal{F}' \Downarrow^{\mathsf{cbn}} U \shortmid \nu\Big)$$

where p is the position of the hole in $\mathcal{F}'$. By the i.h. ($\sigma := \rho'$ and $\mathcal{G} := \mathcal{F}'$) there exists π'

$$\pi'\Big(\mathcal{E}'\langle!_{\rho}\mathcal{F}\langle R\rangle\rangle \shortmid \rho' \shortmid \mathcal{F}' \Downarrow^{\mathsf{cbn}} U \shortmid \nu\Big)$$

By Substitution (Lem. 11),

$$\pi \mid_p^{\pi'} \Big(\mathcal{F}'\langle\mathcal{E}'\langle!_{\rho}\mathcal{F}\langle R\rangle\rangle\rangle \shortmid \rho' \shortmid \Box \Downarrow^{\mathsf{cbn}} V' \shortmid \mu\Big)$$

We then conclude using E-Bang:

$$\frac{\mathcal{F}'\langle\mathcal{E}'\langle!_{\rho}\mathcal{F}\langle R\rangle\rangle\rangle \shortmid \rho' \shortmid \Box \Downarrow^{\mathsf{cbn}} V' \shortmid \mu}{!_{\rho'}\mathcal{F}'\langle\mathcal{E}'\langle!_{\rho}\mathcal{F}\langle R\rangle\rangle\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} W \shortmid \tau}\ \mathsf{E\text{-}!}$$

Proposition 7 (Evaluation simulates reduction (2)). *$M \rightsquigarrow^*_{\mathsf{cbn}} V$ implies for all $\rho, \mathcal{G}$ there exists σ such that $M \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma$.*

Proof. By induction on the length n of the derivation sequence. If $n = 0$, then $M = V$ and $V \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma$ holds by taking $\sigma = \widehat{V}$. Suppose $M \rightsquigarrow_{\mathsf{cbn}} P \rightsquigarrow^n_{\mathsf{cbn}} V$. By the i.h., for all $\rho, \mathcal{G}$ there exists σ such that:

$$P \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma \tag{15}$$

Since $M \rightsquigarrow_{\mathsf{cbn}} P$, then $M = \mathcal{E}\langle!_{\tau}\mathcal{F}\langle R\rangle\rangle$ and $P = \mathcal{E}\langle!_{\tau;\widehat{\mathcal{F}\langle\xi\rangle}}\mathcal{F}\langle R'\rangle\rangle$, for some (R, R', ξ) in the CBN redex table. Then (15) reads $\mathcal{E}\langle!_{\tau;\widehat{\mathcal{F}\langle\xi\rangle}}\mathcal{F}\langle R'\rangle\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma$ and from Expansion (Lem. 1(2)) we deduce $\mathcal{E}\langle!_{\tau}\mathcal{F}\langle R\rangle\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbn}} V \shortmid \sigma$.

D.2 The AKAM Abstract Machine

Sample Reduction A sample reduction in the AKAM follows. It executes the term $\mathit{let}\ u^A \triangleq !(I\,I)\ \mathit{in}\ !(u\,3)$ abbreviated s. We adopt the following additional abbreviations. $I = \lambda a^A.a$, $R := (I, \epsilon, I, \epsilon, \epsilon)$, $S := (I, \epsilon, !u\,3, u, \epsilon, \mathbf{ba}(R) :: (\epsilon, I\,I), \epsilon)$, $T := (I, \epsilon, 3, e, \epsilon)$, and $e := u{=}(!_{\mathbf{bb}(R)::(\epsilon,I\,I)}I, \epsilon) :: \epsilon$.

term	**env**	**stack**	**trail**	**dump**
s	ϵ	ϵ	(ϵ, s)	ϵ
$!(I\,I)$	ϵ	$(!(u\,3), u, \epsilon) :: \epsilon$	(ϵ, s)	ϵ
$I\,I$	ϵ	ϵ	$(\epsilon, I\,I)$	$((\epsilon, s), (!(u\,3), u, \epsilon) :: \epsilon) :: \epsilon$
I	ϵ	$(I, \epsilon) :: \epsilon$	$(\epsilon, I\,I)$	$((\epsilon, s), (!(u\,3), u, \epsilon) :: \epsilon) :: \epsilon$
a	$a{=}(I, \epsilon) :: \epsilon$	ϵ	$\mathbf{ba}(R) :: (\epsilon, I\,I)$	$((\epsilon, s), (!(u\,3), u, \epsilon) :: \epsilon) :: \epsilon$
I	ϵ	ϵ	$\mathbf{ba}(R) :: (\epsilon, I\,I)$	$((\epsilon, s), (!(u\,3), u, \epsilon) :: \epsilon) :: \epsilon$
$!(u\,3)$	$u{=}(!_{\mathbf{bb}(R)::(\epsilon, I\,I)} I, \epsilon) :: \epsilon$	ϵ	$\mathbf{bb}(S) :: (\epsilon, s)$	ϵ
$u\,3$	e	ϵ	$(u{=}(!_{\mathbf{bb}(R)::(\epsilon, I\,I)} I, \epsilon) :: \epsilon, u\,3)$	$(\mathbf{bb}(S) :: (\epsilon, s), \epsilon) :: \epsilon$
u	e	$(3, e) :: \epsilon$	$(u{=}(!_{\mathbf{bb}(R)::(\epsilon, I\,I)} I, \epsilon) :: \epsilon, u\,3)$	$(\mathbf{bb}(S) :: (\epsilon, s), \epsilon) :: \epsilon$
I	ϵ	$(3, e) :: \epsilon$	$(u{=}(!_{\mathbf{bb}(R)::(\epsilon, I\,I)} I, \epsilon) :: \epsilon, u\,3)$	$(\mathbf{bb}(S) :: (\epsilon, s), \epsilon) :: \epsilon$
a	$a{=}(3, e) :: \epsilon$	ϵ	$\mathbf{ba}(T) :: (u{=}(!_{\mathbf{bb}(R)::(\epsilon, I\,I)} I, \epsilon) :: \epsilon, u\,3)$	$(\mathbf{bb}(S) :: (\epsilon, s), \epsilon) :: \epsilon$
3	ϵ	ϵ	$\mathbf{ba}(T) :: (u{=}(!_{\mathbf{bb}(R)::(\epsilon, I\,I)} I, \epsilon) :: \epsilon, u\,3)$	$(\mathbf{bb}(S) :: (\epsilon, s), \epsilon) :: \epsilon$
$!_{\mathbf{ba}(T)::(e, u\,3)} 3$	ϵ	ϵ	$\mathbf{bb}(S) :: (\epsilon, s)$	ϵ

Correctness A simple notion we will require is that of compiling terms to configurations: $\breve{\_} : \mathbb{T} \longrightarrow \mathbb{C}$.

$$\breve{\mathfrak{a}} := \mathfrak{a} \tag{16}$$

$$\widetilde{(\lambda a^A.s)} := \lambda a^A.\breve{s} \tag{17}$$

$$\widetilde{(s\,t)} := \breve{s}\,\breve{t} \tag{18}$$

$$\widetilde{(!s)} := !_s \breve{s} \tag{19}$$

$$(\widetilde{let\ u^A \triangleq s\ in\ t}) := let\ u^A \triangleq \breve{s}\ in\ \breve{t} \tag{20}$$

Proposition 8 (Correctness of the AKAM (3)). *If* $s \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta \mapsto_r s' \shortmid e' \shortmid \pi' \shortmid \xi' \shortmid \delta'$, *then*

(a) $s \shortmid e \widehat{\shortmid \pi \shortmid} \xi \shortmid \delta = s' \shortmid e' \widehat{\shortmid \pi' \shortmid} \xi' \shortmid \delta'$, *for* $r \in \{\mathsf{push}, \mathsf{lookupt}, \mathsf{pushlet}, \mathsf{bang}, \mathsf{bangbang}, \mathsf{lookupv}\}$; *and*

(b) $s \shortmid e \widehat{\shortmid \pi \shortmid} \xi \shortmid \delta = s' \shortmid e' \widehat{\shortmid \pi' \shortmid} \xi' \shortmid \delta'$, *for* $r \in \{\mathsf{appb}, \mathsf{appbb}, \mathsf{ti}\}$; *and*

Proof. – Case push. Then the AKAM step is of the form

$$s\,t \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta \mapsto_{\mathsf{push}} s \shortmid e \shortmid (t, e) :: \pi \shortmid \xi \shortmid \delta$$

$$\begin{aligned} & \underline{s\,t \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta} \\ = & \ \underline{\delta}\langle !_{\underline{\xi}} \underline{\pi} \langle \underline{e} \langle \breve{s}\,\breve{t} \rangle \rangle \rangle \end{aligned}$$

$$\begin{aligned} & \underline{s \shortmid e \shortmid (t, e) :: \pi \shortmid \xi \shortmid \delta} \\ = & \ \underline{\delta}\langle !_{\underline{\xi}} (t, e) :: \pi \langle \underline{e} \langle \breve{s} \rangle \rangle \rangle \\ = & \ \underline{\delta}\langle !_{\underline{\xi}} \underline{\pi} \langle \underline{e} \langle \breve{s} \rangle\, \underline{e} \langle \breve{t} \rangle \rangle \rangle \end{aligned}$$

Then

$$\underline{\delta}\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}\langle \breve{s}\,\breve{t}\rangle\rangle\rangle = \underline{\delta}\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}\langle \breve{s}\rangle\,\underline{e}\langle \breve{t}\rangle\rangle\rangle$$

– Case appb. Then the AKAM step is of the form

$$\lambda a^A.s \shortmid e \shortmid (t,e') :: \pi \shortmid \xi \shortmid \delta \mapsto_{\mathsf{appb}} s \shortmid a = (t,e') :: e \shortmid \pi \shortmid \mathbf{ba}(R) :: \xi \shortmid \delta$$

where $R = (\lambda a^A.s, e, t, e', \pi)$.

$$\begin{aligned}
&\underline{\lambda a^A.s \shortmid e \shortmid (t,e') :: \pi \shortmid \xi \shortmid \delta}\\
&= \underline{\delta}\langle !_{\underline{\xi}}(t,e') :: \pi\langle \underline{e}\langle \widetilde{\lambda a^A.s}\rangle\rangle\rangle\\
&= \underline{\delta}\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}\langle \widetilde{\lambda a^A.s}\rangle\,\underline{e}'\langle \breve{t}\rangle\rangle\rangle\\
&= \underline{\delta}\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}\langle \lambda a^A.\breve{s}\rangle\,\underline{e}'\langle \breve{t}\rangle\rangle\rangle
\end{aligned}$$

$$\begin{aligned}
&\underline{s \shortmid a = (t,e') :: e \shortmid \pi \shortmid \mathbf{ba}(R) :: \xi \shortmid \delta}\\
&= \underline{\delta}\langle !_{\mathbf{ba}(R)::\underline{\xi}}\underline{\pi}\langle \underline{a = (t,e') :: e}\langle \breve{s}\rangle\rangle\rangle\\
&= \underline{\delta}\langle !_{\underline{\xi};\hat{\pi}\langle \mathbf{ba}(\hat{R})\rangle}\underline{\pi}\langle \underline{e}\langle \breve{s}\{a/\underline{e}'\langle \breve{t}\rangle\}\rangle\rangle\rangle
\end{aligned}$$

Then, since we may assume $a \notin \mathsf{ran}(e)$,

$$\begin{aligned}
&\underline{\delta}\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}\langle \widetilde{\lambda a^A.s}\rangle\,\underline{e}'\langle \breve{t}\rangle\rangle\rangle\\
&= \underline{\delta}\langle !_{\underline{\xi}}\underline{\pi}\langle (\lambda a^A.\underline{e}\langle \breve{s}\rangle)\,\underline{e}'\langle \breve{t}\rangle\rangle\rangle\\
&\rightsquigarrow \underline{\delta}\langle !_{\underline{\xi};\hat{\pi}\langle \mathbf{ba}(\hat{R})\rangle}\underline{\pi}\langle \underline{e}\langle \breve{s}\rangle\{a/\underline{e}'\langle \breve{t}\rangle\}\rangle\rangle\\
&= \underline{\delta}\langle !_{\underline{\xi};\hat{\pi}\langle \mathbf{ba}(\hat{R})\rangle}\underline{\pi}\langle \underline{e}\langle \breve{s}\{a/\underline{e}'\langle \breve{t}\rangle\}\rangle\rangle\rangle
\end{aligned}$$

– Case lookupt. Then the AKAM step is of the form

$$a \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta \mapsto_{\mathsf{lookupt}} t \shortmid e' \shortmid \pi \shortmid \xi \shortmid \delta, \text{ where } e(a) = (t,e')$$

$$\begin{aligned}
&\underline{a \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta}\\
&= \underline{\delta}\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}\langle a\rangle\rangle\rangle
\end{aligned}$$

$$\begin{aligned}
&\underline{t \shortmid e' \shortmid \pi \shortmid \xi \shortmid \delta}\\
&= \underline{\delta}\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}'\langle \breve{t}\rangle\rangle\rangle
\end{aligned}$$

Then, by definition of $\underline{e}$,

$$\begin{aligned}
&\underline{\delta}\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}\langle a\rangle\rangle\rangle\\
&= \underline{\delta}\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}'\langle \breve{t}\rangle\rangle\rangle
\end{aligned}$$

– Case pushlet. Then the AKAM step is of the form

$$let\ u^A \triangleq s\ in\ t \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta \mapsto_{\mathsf{pushlet}} s \shortmid e \shortmid (t,u,e) :: \pi \shortmid \xi \shortmid \delta$$

$$\begin{aligned}
&\underline{let\ u^A \triangleq s\ in\ t \shortmid e \shortmid \pi \shortmid \xi \shortmid \delta}\\
&= \underline{\delta}\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}\langle \widetilde{let\ u^A \triangleq s\ in\ t}\rangle\rangle\rangle\\
&= \underline{\delta}\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}\langle let\ u^A \triangleq \breve{s}\ in\ \breve{t}\rangle\rangle\rangle
\end{aligned}$$

$$\begin{aligned}
&\underline{s \shortmid e \shortmid (t,u,e) :: \pi \shortmid \xi \shortmid \delta}\\
&= \underline{\delta}\langle !_{\underline{\xi}}(t,u,e) :: \pi\langle \underline{e}\langle s\rangle\rangle\rangle\\
&= \underline{\delta}\langle !_{\underline{\xi}}\underline{\pi}\langle let\ u^A \triangleq \underline{e}\langle \breve{s}\rangle\ in\ \underline{e}\langle \breve{t}\rangle\rangle\rangle
\end{aligned}$$

Then

$$\begin{aligned}&\underline{\delta}\langle!_{\underline{\xi}}\underline{\pi}\langle\underline{e}\langle let\ u^A \triangleq \breve{s}\ in\ \breve{t}\rangle\rangle\rangle\\ =\ &\underline{\delta}\langle!_{\underline{\xi}}\underline{\pi}\langle let\ u^A \triangleq \underline{e}\langle\breve{s}\rangle\ in\ \underline{e}\langle\breve{t}\rangle\rangle\rangle\end{aligned}$$

– Case bang. Then the AKAM step is of the form

$$!s \intercal e \intercal \pi \intercal \xi \intercal \delta \mapsto_{\mathsf{bang}} s \intercal e \intercal \epsilon \intercal (e,s) :: \epsilon \intercal (\xi,\pi) :: \delta$$

$$\begin{aligned}&\frac{!s \intercal e \intercal \pi \intercal \xi \intercal \delta}{}\\ =\ &\underline{\delta}\langle!_{\underline{\xi}}\underline{\pi}\langle\underline{e}\langle!_s\breve{s}\rangle\rangle\rangle\end{aligned}$$

$$\begin{aligned}&\frac{s \intercal e \intercal \epsilon \intercal (e,s) :: \epsilon \intercal (\xi,\pi) :: \delta}{}\\ =\ &\underline{(\xi,\pi) :: \delta}\langle!_{\underline{(e,s)::\epsilon}}\underline{\epsilon}\langle\underline{e}\langle\breve{s}\rangle\rangle\rangle\\ =\ &\underline{(\xi,\pi) :: \delta}\langle!_{\underline{(e,s)::\epsilon}}\underline{e}\langle\breve{s}\rangle\rangle\\ =\ &\underline{\delta}\langle!_{\underline{\xi}}\underline{\pi}\langle!_{\underline{e}\langle s\rangle}\underline{e}\langle\breve{s}\rangle\rangle\rangle\end{aligned}$$

Then

$$\begin{aligned}&\underline{\delta}\langle!_{\underline{\xi}}\underline{\pi}\langle\underline{e}\langle!_s\breve{s}\rangle\rangle\rangle\\ =\ &\underline{\delta}\langle!_{\underline{\xi}}\underline{\pi}\langle!_{\underline{e}\langle s\rangle}\underline{e}\langle\breve{s}\rangle\rangle\rangle\end{aligned}$$

– Case bangbang. Then the AKAM step is of the form

$$V \intercal e \intercal \epsilon \intercal \sigma \intercal (\xi,\epsilon) :: \delta \mapsto_{\mathsf{bangbang}} !_\sigma V \intercal e \intercal \epsilon \intercal \xi \intercal \delta$$

$$\begin{aligned}&\frac{V \intercal e \intercal \epsilon \intercal \sigma \intercal (\xi,\epsilon) :: \delta}{}\\ =\ &\underline{(\xi,\epsilon) :: \delta}\langle!_{\underline{\sigma}}\underline{\epsilon}\langle\underline{e}\langle\breve{V}\rangle\rangle\rangle\\ =\ &\underline{\delta}\langle!_{\underline{\xi}}\underline{\epsilon}\langle!_{\underline{\sigma}}\underline{\epsilon}\langle\underline{e}\langle\breve{V}\rangle\rangle\rangle\rangle\\ =\ &\underline{\delta}\langle!_{\underline{\xi}}!_{\underline{\sigma}}\underline{e}\langle\breve{V}\rangle\rangle\end{aligned}$$

$$\begin{aligned}&\frac{!_\sigma V \intercal e \intercal \epsilon \intercal \xi \intercal \delta}{}\\ =\ &\underline{\delta}\langle!_{\underline{\xi}}\underline{\epsilon}\langle\underline{e}\langle\widetilde{!_{\underline{\sigma}}V}\rangle\rangle\rangle\\ =\ &\underline{\delta}\langle!_{\underline{\xi}}\underline{e}\langle\widetilde{!_{\underline{\sigma}}V}\rangle\rangle\\ =\ &\underline{\delta}\langle!_{\underline{\xi}}\underline{e}\langle!_{\underline{\sigma}}\breve{V}\rangle\rangle\end{aligned}$$

Then

$$\begin{aligned}&\underline{\delta}\langle!_{\underline{\xi}}!_{\underline{\sigma}}\underline{e}\langle\breve{V}\rangle\rangle\\ =\ &\underline{\delta}\langle!_{\underline{\xi}}\underline{e}\langle!_{\underline{\sigma}}\breve{V}\rangle\rangle\end{aligned}$$

The last step holds since the trails produced by the AM do not contain free validity variables.

– Case appbb. Then the AKAM step is of the form

$$V \intercal e \intercal \epsilon \intercal \sigma \intercal (\xi,(t,u,e') :: \pi) :: \delta \mapsto_{\mathsf{appbb}} t \intercal u = (!_\sigma V, e') :: e \intercal \pi \intercal \mathbf{bb}(R) :: \xi \intercal \delta$$

where $R = (V, e, t, u, e', \sigma, \pi)$.

$$
\begin{aligned}
&\underline{V \intercal e \intercal \epsilon \intercal \sigma \intercal (\xi, (t,u,e') :: \pi) :: \delta} \\
&= \underline{(\xi, (t,u,e') :: \pi) :: \delta\langle !_{\underline{\sigma}}\underline{\epsilon}\langle \underline{e}\langle \check{V}\rangle\rangle\rangle} \\
&= \underline{\delta\langle !_{\underline{\xi}}(t,u,e') :: \pi\langle !_{\underline{\sigma}}\underline{\epsilon}\langle \underline{e}\langle \check{V}\rangle\rangle\rangle\rangle} \\
&= \underline{\delta\langle !_{\underline{\xi}}(t,u,e') :: \pi\langle !_{\underline{\sigma}}\underline{e}\langle \check{V}\rangle\rangle\rangle} \\
&= \underline{\delta\langle !_{\underline{\xi}}\underline{\pi}\langle let\ u^A \triangleq\ !_{\underline{\sigma}}\underline{e}\langle \check{V}\rangle\ in\ \underline{e'}\langle \check{t}\rangle\rangle\rangle}
\end{aligned}
$$

$$
\begin{aligned}
&\underline{t \intercal u = (!_\sigma V, e) :: e' \intercal \pi \intercal \mathbf{bb}(R) :: \xi \intercal \delta} \\
&= \underline{\delta\langle !_{\underline{\mathbf{bb}(R)::\xi}}\underline{\pi}\langle \underline{u = (!_\sigma V, e) :: e'}\langle \check{t}\rangle\rangle\rangle} \\
&= \underline{\delta\langle !_{\underline{\xi};\hat{\pi}\langle \mathbf{bb}(\hat{R});t\{\sigma/u\}\rangle}\underline{\pi}\langle \underline{e'}\langle \check{t}\{u/\underline{e}\langle !_\sigma \check{V}\rangle\}\rangle\rangle\rangle}
\end{aligned}
$$

Then

$$
\begin{aligned}
&\underline{\delta\langle !_{\underline{\xi}}\underline{\pi}\langle let\ u^A \triangleq\ !_{\underline{\sigma}}\underline{e}\langle \check{V}\rangle\ in\ \underline{e'}\langle \check{t}\rangle\rangle\rangle} \\
\rightsquigarrow\ &\underline{\delta\langle !_{\underline{\xi};\hat{\pi}\langle \mathbf{bb}(\hat{R});t\{\sigma/u\}\rangle}\underline{\pi}\langle \underline{e'}\langle \check{t}\rangle\{u/!_{\underline{\sigma}}\underline{e}\langle \check{V}\rangle\}\rangle\rangle\rangle} \\
=\ &\underline{\delta\langle !_{\underline{\xi};\hat{\pi}\langle \mathbf{bb}(\hat{R});t\{\sigma/u\}\rangle}\underline{\pi}\langle \underline{e'}\langle \check{t}\{u/\underline{e}\langle !_\sigma \check{V}\rangle\}\rangle\rangle\rangle}
\end{aligned}
$$

– Case lookupv. Then the AKAM step is of the form

$$u \intercal e \intercal \pi \intercal \xi \intercal \delta \mapsto_{\mathsf{lookupv}} V \intercal e' \intercal \pi \intercal \xi \intercal \delta$$

where $e(u) = (!_\sigma V, e')$

$$
\begin{aligned}
&\underline{u \intercal e \intercal \pi \intercal \xi \intercal \delta} \\
&= \underline{\delta\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}\langle u\rangle\rangle\rangle}
\end{aligned}
$$

$$
\begin{aligned}
&\underline{V \intercal e' \intercal \pi \intercal \xi \intercal \delta} \\
&= \underline{\delta\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e'}\langle \check{V}\rangle\rangle\rangle}
\end{aligned}
$$

Then

$$
\begin{aligned}
&\underline{\delta\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}\langle u\rangle\rangle\rangle} \\
&= \underline{\delta\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e'}\langle \check{V}\rangle\rangle\rangle}
\end{aligned}
$$

– Case TI. Then the AKAM step is of the form

$$\iota_A \intercal e \intercal \pi \intercal \xi \intercal \delta \mapsto_{\mathsf{TI}} \mathtt{iter}_{\mathsf{can}(\underline{\xi})} \intercal e \intercal \pi \intercal \mathbf{ti}_A(\pi) :: \xi \intercal \delta$$

$$
\begin{aligned}
&\underline{\iota_A \intercal e \intercal \pi \intercal \xi \intercal \delta} \\
&= \underline{\delta\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}\langle \iota_A\rangle\rangle\rangle}
\end{aligned}
$$

$$
\begin{aligned}
&\underline{\mathtt{iter}_{\mathsf{can}(\underline{\xi})} \intercal e \intercal \pi \intercal \mathbf{ti}_A(\pi) :: \xi \intercal \delta} \\
&= \underline{\delta\langle !_{\underline{\mathbf{ti}_A(\pi)::\xi}}\underline{\pi}\langle \underline{e}\langle \mathtt{iter}_{\mathsf{can}(\underline{\xi})}\rangle\rangle\rangle} \\
&= \underline{\delta\langle !_{\underline{\xi};\hat{\pi}\langle \mathbf{ti}_A(\underline{\xi})\rangle}\underline{\pi}\langle \underline{e}\langle \mathtt{iter}_{\mathsf{can}(\underline{\xi})}\rangle\rangle\rangle}
\end{aligned}
$$

Then

$$
\begin{aligned}
&\underline{\delta\langle !_{\underline{\xi}}\underline{\pi}\langle \underline{e}\langle \iota_A\rangle\rangle\rangle} \\
&= \underline{\delta\langle !_{\underline{\xi}}\underline{\pi}\langle \iota_A\rangle\rangle} \\
\rightsquigarrow\ &\underline{\delta\langle !_{\underline{\xi};\hat{\pi}\langle \mathbf{ti}_A(\underline{\xi})\rangle}\underline{\pi}\langle \underline{e}\langle \mathtt{iter}_{\mathsf{can}(\underline{\xi})}\rangle\rangle\rangle}
\end{aligned}
$$

$$\frac{}{V \intercal \rho \intercal \mathcal{F} \Downarrow^{\mathsf{cbv}} V \intercal \widehat{V}}\ \mathsf{E\text{-}V} \qquad \frac{M \intercal \sigma \intercal \Box \Downarrow^{\mathsf{cbv}} V \intercal \tau}{!_\sigma M \intercal \rho \intercal \mathcal{F} \Downarrow^{\mathsf{cbv}} !_{\sigma;\tau} V \intercal !\sigma^{src}}\ \mathsf{E\text{-}!}$$

$$\frac{\begin{array}{c} M \intercal \rho \intercal \mathcal{F}\langle \Box\, N\rangle \Downarrow^{\mathsf{cbv}} \lambda a^A.P \intercal \sigma \\ N \intercal \rho; \widehat{\mathcal{F}}\langle \sigma\, \widehat{N}\rangle \intercal \mathcal{F}\langle (\lambda a^A.P)\, \Box\rangle \Downarrow^{\mathsf{cbv}} V \intercal \tau \\ P\{V/a\} \intercal \rho; \widehat{\mathcal{F}}\langle (\sigma\,\tau); \mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{V})\rangle \intercal \mathcal{F} \Downarrow^{\mathsf{cbv}} W \intercal \upsilon \end{array}}{M\, N \intercal \rho \intercal \mathcal{F} \Downarrow^{\mathsf{cbv}} W \intercal (\sigma\,\tau); \mathbf{ba}((\lambda a^A.\widehat{P})\, \widehat{V}); \upsilon}\ \mathsf{E}\text{-}\beta\text{-}\mathsf{V}$$

$$\frac{\begin{array}{c} M \intercal \rho \intercal \mathcal{F}\langle let\ u^A \triangleq \Box\ in\ N\rangle \Downarrow^{\mathsf{cbv}} !_\tau V \intercal \sigma \\ N\{!_\tau V/u\} \intercal \rho; \widehat{\mathcal{F}}\langle let\ u^A \triangleq \sigma\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{!_\tau V}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}\rangle \intercal \mathcal{F} \Downarrow^{\mathsf{cbv}} W \intercal \upsilon \end{array}}{let\ u^A \triangleq M\ in\ N \intercal \rho \intercal \mathcal{F} \Downarrow^{\mathsf{cbv}} W \intercal let\ u^A \triangleq \sigma\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{!_\tau V}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon}\ \mathsf{E}\text{-}\beta_{\Box}$$

$$\frac{}{\iota_A \intercal \rho \intercal \mathcal{F} \Downarrow^{\mathsf{cbv}} \mathtt{iter}_{\mathsf{can}(\rho)} \intercal \mathbf{ti}_A(\rho)}\ \mathsf{E\text{-}TI}$$

Fig. 7. CBV Evaluation

E Call-by-Value

E.1 Evaluation

The full set of evaluation rules for CBV are given in Fig 7.
First we introduce some auxiliary results. In stating and proving them, we will make use of the following **CBV redex table**:

R	R'	ξ
$(\lambda a^A.M)\, V$	$M\{V/a\}$	$\mathbf{ba}(\widehat{R})$
$let\ u^A \triangleq !_\tau V\ in\ N$	$N\{!_\tau V/u\}$	$\mathbf{bb}(\widehat{R}); \widehat{N}\{\tau/u\}$
ι_A	$\mathtt{iter}_{\mathsf{can}(\rho)}$	$\mathbf{ti}_A(\rho)$

E.2 Reduction

The CBV reduction is defined as follows:

$$\begin{array}{l} \mathcal{F} ::= \Box \mid \mathcal{F}\, M \mid (\lambda a^A.M)\, \mathcal{F} \mid let\ u^A \triangleq \mathcal{F}\ in\ M \\ \mathcal{E} ::= \Box \mid !_\rho \mathcal{F}\langle \mathcal{E}\rangle \end{array} \qquad \frac{M \mapsto N}{\mathcal{E}\langle M\rangle \rightsquigarrow \mathcal{E}\langle N\rangle}\ \mathsf{R\text{-}Ctxt}$$

where we use CBV shallow contexts in the evaluation contexts and that $\mapsto$ is defined in Fig. 8:

$$\frac{R = (\lambda a^A.M)\,V}{!_\rho \mathcal{F}\langle R\rangle \mapsto !_{\rho;\widehat{\mathcal{F}}\langle \mathbf{ba}(\widehat{R})\rangle}\mathcal{F}\langle M\{a/V\}\rangle}\ \mathsf{R}\text{-}\beta\text{-}\mathsf{V} \qquad \frac{R = let\ u^A \triangleq !_\sigma V\ in\ N}{!_\rho \mathcal{F}\langle R\rangle \mapsto !_{\rho;\widehat{\mathcal{F}}\langle \mathbf{bb}(\widehat{R});\widehat{N}\{\sigma/u\}\rangle}\mathcal{F}\langle N\{!_\sigma V/u\}\rangle}\ \mathsf{R}\text{-}\beta_{\square}$$

$$\frac{R = \iota_A}{!_\rho \mathcal{F}\langle R\rangle \mapsto !_{\rho;\widehat{\mathcal{F}}\langle \mathbf{ti}_A(\rho)\rangle}\mathcal{F}\langle \mathtt{iter}_{\mathsf{can}(\rho)}\rangle}\ \mathsf{R}\text{-}\mathsf{TI}$$

Fig. 8. CBV Reduction Semantics

E.3 Results

Decompilation for shallow contexts is defined as follows:

$$\widehat{\square} := \square \tag{21}$$

$$\widehat{(\mathcal{F}\,M)} := \widehat{\mathcal{F}}\,\widehat{M} \tag{22}$$

$$\widehat{(V\,\mathcal{F})} := \widehat{V}\,\widehat{\mathcal{F}} \tag{23}$$

$$(let\ u^{\widehat{A \triangleq \mathcal{F}}}\ in\ M) := let\ u^A \triangleq \widehat{\mathcal{F}}\ in\ \widehat{M} \tag{24}$$

Lemma 13. $\widehat{\mathcal{F}\langle M\rangle} = \widehat{\mathcal{F}}\langle\widehat{M}\rangle$.

Proof. By induction on $\mathcal{F}$.

Lemma 14. $(\widehat{M\{V/a\}}) = \widehat{M}\{\widehat{V}/a\}$.

Proof. By induction on M.

Lemma 15. *If* $\pi\Big(M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} V \shortmid \sigma\Big)$ *and* $M \shortmid \rho \shortmid \mathcal{F} \simeq M' \shortmid \rho' \shortmid \mathcal{F}'$, *then there exists* $V' \shortmid \sigma'$ *and* π' *such that* $\pi'\Big(M' \shortmid \rho' \shortmid \mathcal{F}' \Downarrow^{\mathsf{cbv}} V' \shortmid \sigma'\Big)$ *and* $V \shortmid \sigma \simeq V' \shortmid \sigma'$.

Proof. By induction on π.

Lemma 16. $M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} V \shortmid \sigma$ *and* $M \shortmid \rho \shortmid \mathcal{F}$ *well-formed implies*

(a) ρ *is composable with* $\widehat{\mathcal{F}}\langle\sigma\rangle$ (i.e. $\widehat{\mathcal{F}}\langle\sigma\rangle^{src} = \rho^{tgt}$); *and*
(b) $!_{\rho;\widehat{\mathcal{F}}\langle\sigma\rangle}\mathcal{F}\langle V\rangle$ *is a well-formed configuration.*

Proof. By induction on the derivation of $M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} V \shortmid \sigma$.

– $\mathsf{E}\text{-}\mathsf{V}$

$$\frac{}{V \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} V \shortmid \widehat{V}}\ \mathsf{E}\text{-}\mathsf{V}$$

(a) For the first item we reason as follows: $(\widehat{\mathcal{F}}\langle\widehat{V}\rangle)^{src} = (\widehat{\mathcal{F}\langle V\rangle})^{src} = \widehat{\mathcal{F}\langle V\rangle} = \rho^{tgt}$. The last equality is from the hypothesis that $M \shortmid \rho \shortmid \mathcal{F}$ well-formed.

(b) For the second item we must show that $!_{\rho;\widehat{\mathcal{F}\langle V\rangle}}\mathcal{F}\langle V\rangle$ is well-formed. Note that $!_{\rho;\widehat{\mathcal{F}\langle V\rangle}}\mathcal{F}\langle V\rangle$ is consistent: $(\rho;\widehat{\mathcal{F}\langle V\rangle})^{tgt} = (\widehat{\mathcal{F}\langle V\rangle})^{tgt} = \widehat{\mathcal{F}\langle V\rangle}$. Moreover, every subterm of V and $\mathcal{F}$ of the form $!_\rho N$ is consistent by the hypothesis that $V \shortmid \rho \shortmid \mathcal{F}$ is well-formed.

– E-!

$$\frac{M \shortmid \tau \shortmid \Box \Downarrow^{\mathsf{cbv}} V \shortmid \mu}{!_\tau M \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} !_{\tau;\mu} V \shortmid !\tau^{src}}\ \mathsf{E\text{-}!}$$

(a) For the first item we reason as follows: $\widehat{\mathcal{F}}\langle\sigma\rangle^{src} = (\widehat{\mathcal{F}}\langle !\tau^{src}\rangle)^{src} = \widehat{\mathcal{F}}\langle !\tau^{src}\rangle = \rho^{tgt}$. The last equality is from the hypothesis that $!_\tau M \shortmid \rho \shortmid \mathcal{F}$ is well-formed.

(b) For the second item we must verify that: $!_{\rho;\widehat{\mathcal{F}}\langle !\tau^{src}\rangle}\mathcal{F}\langle !_{\tau;\mu}V\rangle$ is well-formed. We check two things:

- First we check that $!_{\rho;\widehat{\mathcal{F}}\langle !\tau^{src}\rangle}\mathcal{F}\langle !_{\tau;\mu}V\rangle$ is consistent. That is, $(\rho;\widehat{\mathcal{F}}\langle !\tau^{src}\rangle)^{tgt} = (\widehat{\mathcal{F}}\langle !\tau^{src}\rangle)^{tgt} = \widehat{\mathcal{F}\langle !_{\tau;\mu}V\rangle}$. For the LHS we use the definition of decompilation and target:

$$(\widehat{\mathcal{F}}\langle !\tau^{src}\rangle)^{tgt} = \widehat{\mathcal{F}}\langle !\tau^{src}\rangle$$

For the RHS we have

$$\mathcal{F}\langle\widehat{(!_{\tau;\mu}V)}\rangle =_{Lem.\ 13} \widehat{\mathcal{F}}\langle\widehat{(!_{\tau;\mu}V)}\rangle = \widehat{\mathcal{F}}\langle !(\tau;\mu)^{src}\rangle = \widehat{\mathcal{F}}\langle !\tau^{src}\rangle$$

- Moreover, every bang subterm of V and $\mathcal{F}$ is consistent from the hypothesis that $M \shortmid \rho \shortmid \mathcal{F}$ is well-formed. Finally, $!_{\tau;\mu}V$ is consistent from the i.h. on the derivation of $M \shortmid \tau \shortmid \Box \Downarrow^{\mathsf{cbv}} V \shortmid \mu$.

– E-β

$$\frac{\begin{array}{c}\pi_1\Big(M \shortmid \rho \shortmid \mathcal{F}\langle\Box\, N\rangle \Downarrow^{\mathsf{cbv}} \lambda a^A.P \shortmid \mu\Big)\\ \pi_2\Big(N \shortmid \rho;\widehat{\mathcal{F}}\langle\mu\,\widehat{N}\rangle \shortmid \mathcal{F}\langle(\lambda a^A.P)\,\Box\rangle \Downarrow^{\mathsf{cbv}} V \shortmid \tau\Big)\\ \pi_3\Big(P\{V/a\} \shortmid \rho;\widehat{\mathcal{F}}\langle(\mu\,\tau);\mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{V})\rangle \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} W \shortmid \upsilon\Big)\end{array}}{M\,N \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} W \shortmid (\mu\,\tau);\mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{V});\upsilon}\ E-\beta$$

(a) For the first item we reason as follows:

$$\widehat{\mathcal{F}}\langle\sigma\rangle^{src} = \widehat{\mathcal{F}}\langle(\mu\,\tau);\mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{V});\upsilon\rangle^{src} = \widehat{\mathcal{F}}\langle\mu\,\tau\rangle^{src} = \widehat{\mathcal{F}}\langle\mu^{src}\,\tau^{src}\rangle = \widehat{\mathcal{F}}\langle\widehat{M}\,\widehat{N}\rangle$$

Note that $\mu^{src} = \widehat{M}$ and $\tau^{src} = \widehat{N}$, follows from the i.h.. By hypothesis

$$\rho^{tgt} = \widehat{\mathcal{F}\langle M\,N\rangle}$$

(b) We must verify that $!_{\rho;((\mu\,\tau);\mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{V});\upsilon)}\mathcal{F}\langle W\rangle$ is well-formed.

- First we check that $!_{\rho;((\mu\,\tau);\mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{V});\upsilon)}\mathcal{F}\langle W\rangle$ is consistent. This implies checking that $(\rho;\widehat{\mathcal{F}}\langle(\mu\,\tau);\mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{V});\upsilon\rangle)^{tgt} = \upsilon^{tgt} = \widehat{\mathcal{F}\langle W\rangle}$. This follows from the i.h. applied to π_2, then to π_2 and then to π_3, from which we conclude.

- Moreover, every bang subterm of V and $\mathcal{F}$ is consistent from the hypothesis that $M \shortmid \rho \shortmid \mathcal{F}$ is well-formed.

– $\mathsf{E}\text{-}\beta_{\square}$

$$\frac{\pi_1\Big(M \shortmid \rho \shortmid \mathcal{F}\langle let\ u^A \triangleq \square\ in\ N\rangle \Downarrow^{\mathsf{cbv}} !_\tau W \shortmid \mu\Big) \quad \pi_2\Big(N\{!_\tau W/u\} \shortmid \rho; \widehat{\mathcal{F}}\langle let\ u^A \triangleq \mu\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau W)}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}\rangle \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} V \shortmid \upsilon\Big)}{let\ u^A \triangleq M\ in\ N \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} V \shortmid let\ u^A \triangleq \mu\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau W)}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon}\ E-\beta_{\square}$$

(a) For the first case we reason as follows:

$$\begin{aligned} &\widehat{\mathcal{F}}\langle\sigma\rangle^{src} \\ &= \widehat{\mathcal{F}}\langle let\ u^A \triangleq \mu\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau W)}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon\rangle^{src} \\ &= \widehat{\mathcal{F}}\langle let\ u^A \triangleq \mu\ in\ \widehat{N}\rangle^{src} \\ &= \widehat{\mathcal{F}}\langle let\ u^A \triangleq \mu^{src}\ in\ \widehat{N}\rangle \end{aligned}$$

By the i.h. on $M \shortmid \rho \shortmid \mathcal{F}\langle let\ u^A \triangleq \square\ in\ Q\rangle \Downarrow^{\mathsf{cbn}} !_\tau W \shortmid \mu$,

$$\rho^{tgt} = \widehat{\mathcal{F}}\langle let\ u^A \triangleq \mu\ in\ \widehat{N}\rangle^{src} = \widehat{\mathcal{G}\langle M\rangle}$$

for $\mathcal{G} = \mathcal{F}\langle let\ u^A \triangleq \square\ in\ N\rangle$. This concludes the case since $\rho^{tgt} = \mathcal{F}\langle \widehat{let\ u^A \triangleq M\ in\ N}\rangle = \widehat{\mathcal{G}\langle M\rangle}$.

(b) We must verify that $!_{\rho; let\ u^A \triangleq \mu\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau W)}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon} \mathcal{F}\langle V\rangle$ is well-formed.

- First we check that $!_{\rho; let\ u^A \triangleq \mu\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau W)}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon} \mathcal{F}\langle V\rangle$ is compatible. This implies checking $\rho; let\ u^A \triangleq \mu\ in\ \widehat{N}; \mathbf{bb}(let\ u^A \triangleq \widehat{(!_\tau W)}\ in\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon^{tgt} = \upsilon^{tgt} = \widehat{\mathcal{F}\langle V\rangle}$. This follows from the i.h. on π_1 and then from the i.h. on π_2.
- Moreover, every bang subterm of V and $\mathcal{F}$ is consistent from the hypothesis that $M \shortmid \rho \shortmid \mathcal{F}$ is well-formed.

– $\mathsf{E}\text{-}\mathsf{TI}$. Then $\sigma = \mathbf{ti}_A(\rho)$ and the derivation ends:

$$\frac{}{\iota_A \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} \mathtt{iter}_{\mathsf{can}(\rho)} \shortmid \mathbf{ti}_A(\rho)}\ \mathsf{E}\text{-}\mathsf{TI}$$

(a) For the first case we reason as follows: $\widehat{\mathcal{F}}\langle\sigma\rangle^{src} = \widehat{\mathcal{F}}\langle\mathbf{ti}_A(\rho)\rangle^{src} = \widehat{\mathcal{F}}\langle\iota_A\rangle = \rho^{tgt}$. The last equality is from the hypothesis that $M \shortmid \rho \shortmid \mathcal{F}$ well-formed.

(b) For the second item we have to prove that $\widehat{\mathcal{F}}\langle\sigma\rangle^{tgt} = (\widehat{\mathcal{F}}\langle\mathbf{ti}_A(\rho)\rangle)^{tgt} = \widehat{\mathcal{F}}\langle\mathtt{iter}_{\mathsf{can}(\rho)}\rangle$. We reason as follows:

$$\begin{aligned} &(\widehat{\mathcal{F}}\langle\mathbf{ti}_A(\rho)\rangle)^{tgt} \\ &= \widehat{\mathcal{F}}\langle\mathbf{ti}_A(\rho)^{tgt}\rangle \\ &= \widehat{\mathcal{F}}\langle\mathtt{iter}_{\mathsf{can}(\rho)}\rangle \end{aligned}$$

Proof of Prop. 4 (Reduction simulates evaluation).

Proof. By induction on π.

– $\mathsf{E\text{-}V}$. Then $M = V$ and π is:

$$\frac{}{V \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F} \Downarrow^{\mathsf{cbv}} V \mathbin{\imath} \widehat{V}}\ \mathsf{E\text{-}V}$$

Since $V \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F}$ is well-formed, $\rho^{tgt} = \widehat{\mathcal{F}\langle V\rangle}$ and therefore ρ and $\widehat{\mathcal{F}\langle V\rangle}$ are composable. We conclude from $\rho \simeq \rho; \widehat{\mathcal{F}\langle V\rangle}$.

– $\mathsf{E\text{-}!}$. Then $M = !_\tau N$ and π ends in:

$$\frac{N \mathbin{\imath} \tau \mathbin{\imath} \Box \Downarrow^{\mathsf{cbv}} V \mathbin{\imath} \mu}{!_\tau N \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F} \Downarrow^{\mathsf{cbv}} !_{\tau;\mu} V \mathbin{\imath} !\tau^{src}}\ \mathsf{E\text{-}!}$$

Since $M \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F}$ is well-formed, so is $N \mathbin{\imath} \tau \mathbin{\imath} \Box$. By the i.h., $!_\tau N \rightsquigarrow^*_{\mathsf{cbv}} !_{\tau;\mu} V$. We therefore have $!_\rho \mathcal{F}\langle !_\tau N\rangle \rightsquigarrow^*_{\mathsf{cbv}} !_\rho \mathcal{F}\langle !_{\tau;\mu} V\rangle \simeq !_{\rho;\widehat{\mathcal{F}\langle !\tau^{src}\rangle}} \mathcal{F}\langle !_{\tau;\mu} V\rangle$.

– $M = P\,Q$ and π ends in an application of E-β:

$$\frac{\begin{array}{c}\pi_1\Big(P \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F}\langle \Box\, Q\rangle \Downarrow^{\mathsf{cbv}} \lambda a^A.N \mathbin{\imath} \mu\Big) \\ \pi_2\Big(Q \mathbin{\imath} \rho; \widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle \mathbin{\imath} \mathcal{F}\langle (\lambda a^A.N)\, \Box\rangle \Downarrow^{\mathsf{cbv}} W \mathbin{\imath} \tau\Big) \\ \pi_3\Big(N\{W/a\} \mathbin{\imath} \rho; \widehat{\mathcal{F}}\langle (\mu\,\tau); \mathbf{ba}((\lambda a^A.\widehat{N})\,\widehat{W})\rangle \mathbin{\imath} \mathcal{F} \Downarrow^{\mathsf{cbv}} V \mathbin{\imath} \upsilon\Big)\end{array}}{P\,Q \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F} \Downarrow^{\mathsf{cbv}} V \mathbin{\imath} (\mu\,\tau); \mathbf{ba}((\lambda a^A.\widehat{N})\,\widehat{W}); \upsilon}\ \mathsf{E}\text{-}\beta$$

Since $P\,Q \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F}$ is well-formed, then so is $P \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F}\langle \Box\, Q\rangle$. Thus we can apply the i.h. to π_1:

$$!_\rho \mathcal{F}\langle P\,Q\rangle \rightsquigarrow^*_{\mathsf{cbv}} !_{\rho;\widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle} \mathcal{F}\langle (\lambda a^A.N)\, Q\rangle \tag{25}$$

By Lem. 16(2) on π_1 we also know that

$$!_{\rho;\widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle} \mathcal{F}\langle (\lambda a^A.N)\, Q\rangle \text{ is well-formed} \tag{26}$$

From this and the hypothesis that $M \mathbin{\imath} \rho \mathbin{\imath} \mathcal{F}$ is well-formed, we deduce that the triple

$$Q \mathbin{\imath} \rho; \widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle \mathbin{\imath} \mathcal{F}\langle (\lambda a^A.N)\, \Box\rangle$$

is well-formed. This allows us to apply the i.h. on π_2 and obtain

$$!_{\rho;\widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle} \mathcal{F}\langle (\lambda a^A.N)\, Q\rangle \rightsquigarrow^*_{\mathsf{cbv}} !_{\rho;\widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle;\widehat{\mathcal{F}}\langle \widehat{(\lambda a^A.N)}\, \tau\rangle} \mathcal{F}\langle (\lambda a^A.N)\, W\rangle \tag{27}$$

An additional application of R-β produces

$$\begin{array}{rl} & !_{\rho;\widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle} \mathcal{F}\langle (\lambda a^A.N)\, Q\rangle \\ \rightsquigarrow^*_{\mathsf{cbv}} & !_{\rho;\widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle;\widehat{\mathcal{F}}\langle \widehat{(\lambda a^A.N)}\, \tau\rangle} \mathcal{F}\langle (\lambda a^A.N)\, W\rangle \\ \rightsquigarrow & !_{\rho;\widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle;\widehat{\mathcal{F}}\langle \widehat{(\lambda a^A.N)}\, \tau\rangle;\widehat{\mathcal{F}}\langle \mathbf{ba}(\widehat{R})\rangle} \mathcal{F}\langle N\{W/a\}\rangle \end{array} \tag{28}$$

From Lem. 16, (26) and $Q \shortmid \rho; \widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle \shortmid \mathcal{F}\langle (\lambda a^A.R)\,\square\rangle \Downarrow^{\mathsf{cbv}} W \shortmid \tau$, we know that $!_{\rho;\widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle;\widehat{\mathcal{F}}\langle \widehat{(\lambda a^A.N)\,\tau}\rangle}\mathcal{F}\langle (\lambda a^A.N)\, W\rangle$ is well-formed. But then so is

$$!_{\rho;\widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle;\widehat{\mathcal{F}}\langle \widehat{(\lambda a^A.N)\,\tau}\rangle;\widehat{\mathcal{F}}\langle \mathbf{ba}(\widehat{R})\rangle}\mathcal{F}\langle N\{W/a\}\rangle$$

where $R := (\lambda a^A.N)\, W$. We may then apply the i.h. on π_3 and deduce

$$!_{\rho;\widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle;\widehat{\mathcal{F}}\langle \widehat{(\lambda a^A.N)\,\tau}\rangle;\widehat{\mathcal{F}}\langle \mathbf{ba}(\widehat{R})\rangle}\mathcal{F}\langle N\{W/a\}\rangle \rightsquigarrow^*_{\mathsf{cbv}} !_{\rho;\widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle;\widehat{\mathcal{F}}\langle \widehat{(\lambda a^A.N)\,\tau}\rangle;\widehat{\mathcal{F}}\langle \mathbf{ba}(\widehat{R})\rangle;\upsilon}\mathcal{F}\langle V\rangle \tag{29}$$

Since

$$!_{\rho;\widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle;\widehat{\mathcal{F}}\langle \widehat{(\lambda a^A.N)\,\tau}\rangle}\mathcal{F}\langle (\lambda a^A.N)\, W\rangle \rightsquigarrow !_{\rho;\widehat{\mathcal{F}}\langle \mu\, \widehat{Q}\rangle;\widehat{\mathcal{F}}\langle \widehat{(\lambda a^A.N)\,\tau}\rangle;\widehat{\mathcal{F}}\langle \mathbf{ba}(\widehat{R})\rangle}\mathcal{F}\langle N\{W/a\}\rangle \tag{30}$$

we may conclude by adjoining 25, 28 and 30.

– $M = \mathit{let}\ u^A \triangleq P\ \mathit{in}\ N$ and π ends in an application of $\mathsf{E}\text{-}\beta_{\square}$:

$$\frac{\pi_1\Big(P \shortmid \rho \shortmid \mathcal{F}\langle \mathit{let}\ u^A \triangleq \square\ \mathit{in}\ N\rangle \Downarrow^{\mathsf{cbv}} !_\tau W \shortmid \mu\Big) \qquad \pi_2\Big(N\{!_\tau W/u\} \shortmid \rho; \widehat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}; \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{!_\tau W}\ \mathit{in}\ \widehat{N}); \widehat{N}\{\tau/u\}\rangle \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} V \shortmid \upsilon\Big)}{\mathit{let}\ u^A \triangleq P\ \mathit{in}\ N \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} V \shortmid \mathit{let}\ u^A \triangleq \tau\ \mathit{in}\ \widehat{N}; \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{!_\tau W}\ \mathit{in}\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon}\ \mathsf{E}\text{-}\beta_{\square}$$

By the i.h. on π_1:

$$!_\rho \mathcal{F}\langle \mathit{let}\ u^A \triangleq P\ \mathit{in}\ N\rangle \rightsquigarrow^*_{\mathsf{cbv}} !_{\rho;\widehat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}\rangle}\mathcal{F}\langle \mathit{let}\ u^A \triangleq !_\tau W\ \mathit{in}\ N\rangle \tag{31}$$

By Lem. 16 we also know that $!_{\rho;\widehat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}\rangle}\mathcal{F}\langle \mathit{let}\ u^A \triangleq !_\tau W\ \mathit{in}\ N\rangle$ is well-formed. But then $!_{\rho;\widehat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}\rangle;\widehat{\mathcal{F}}\langle \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{(!_\tau V)}\ \mathit{in}\ \widehat{N}); N\{\tau/u\}\rangle} N\{!_\tau W/u\}$ is well-formed too. This allows us to apply the i.h. on π_2 and deduce

$$!_{\rho;\widehat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}\rangle}\mathcal{F}\langle N\{!_\tau W/u\}\rangle \rightsquigarrow^*_{\mathsf{cbv}} !_{\rho;\widehat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}\rangle;\widehat{\mathcal{F}}\langle \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{!_\tau V}\ \mathit{in}\ N); N\{\tau/u\}\rangle}\mathcal{F}\langle V\rangle \tag{32}$$

From $\mathsf{R}\text{-}\beta_{\square}$ we know:

$$!_{\rho;\widehat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}\rangle}\mathcal{F}\langle \mathit{let}\ u^A \triangleq V\ \mathit{in}\ N\rangle \rightsquigarrow !_{\rho;\widehat{\mathcal{F}}\langle \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ \widehat{N}\rangle;\widehat{\mathcal{F}}\langle \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{!_\tau V}\ \mathit{in}\ N); N\{\tau/u\}\rangle}\mathcal{F}\langle N\{\tau/u\}\rangle \tag{33}$$

We conclude from 31, 32 and 33.

– $\mathsf{E}\text{-}\mathsf{TI}$. Then π is the derivation

$$\frac{}{\iota_A \shortmid \rho \shortmid \mathcal{F} \Downarrow^{\mathsf{cbv}} \mathtt{iter}_{\mathsf{can}(\rho)} \shortmid \mathbf{ti}(\rho)}\ \mathsf{E}\text{-}\mathsf{TI}$$

We conclude from $\mathsf{R}\text{-}\mathsf{TI}$: $!_\rho \mathcal{F}\langle \iota_A\rangle \rightsquigarrow !_{\rho;\widehat{\mathcal{F}}\langle \mathbf{ti}(\rho)\rangle}\mathcal{F}\langle \mathtt{iter}_{\mathsf{can}(\rho)}\rangle$.

Lemma 17 (Root Expansion). *For all (R, R', ξ) in the CBV redex table, $R' \shortmid \rho; \widehat{\mathcal{G}}\langle r\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \sigma$, implies $R \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \xi; \sigma$.*

Proof. We consider each of the possible three cases for R:

– $R = (\lambda a^A.M)\,V$, $R' = M\{V/a\}$, $r = \mathbf{ba}(\widehat{R})$. Then we reason as follows:

$$\frac{\begin{array}{c}\lambda a^A.M \mathbin{\mathsf{I}} \rho \mathbin{\mathsf{I}} \mathcal{G}\langle \Box\, V\rangle \Downarrow^{\mathsf{cbv}} \lambda a^A.M \mathbin{\mathsf{I}} \widehat{\lambda a^A.M} \\ V \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \widehat{R}\rangle \mathbin{\mathsf{I}} \mathcal{G}\langle (\lambda a^A.M)\,\Box\rangle \Downarrow^{\mathsf{cbv}} V \mathbin{\mathsf{I}} \widehat{V} \\ M\{V/a\} \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \widehat{R}; \mathbf{ba}(\widehat{R})\rangle \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \sigma\end{array}}{(\lambda a^A.M)\,V \mathbin{\mathsf{I}} \rho \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \widehat{R}; \mathbf{ba}(\widehat{R}); \sigma}\, E-\beta$$

The last judgment above follows from $\widehat{\mathcal{G}}\langle \widehat{R}; \mathbf{ba}(\widehat{R})\rangle \simeq \widehat{\mathcal{G}}\langle \mathbf{ba}(\widehat{R})\rangle$ and the hypothesis $R' \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \xi\rangle \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \sigma$.

– $R = \mathit{let}\ u^A \triangleq !_\tau V\ \mathit{in}\ N$, $R' = N\{!_\tau V/u\}$ and $r = \mathbf{bb}(\widehat{R}); N\{\tau/u\}$. Then we reason as follows:

$$\frac{\begin{array}{c}!_\tau V \mathbin{\mathsf{I}} \rho \mathbin{\mathsf{I}} \mathcal{G}\langle \mathit{let}\ u^A \triangleq \Box\ \mathit{in}\ N\rangle \Downarrow^{\mathsf{cbv}} !_\tau V \mathbin{\mathsf{I}} \widehat{!_\tau V} \\ N\{!_\tau V/u\} \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \widehat{R}; \mathbf{bb}(\widehat{R}); \widehat{N}\{\tau/u\}\rangle \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \sigma\end{array}}{\mathit{let}\ u^A \triangleq !_\tau V\ \mathit{in}\ N \mathbin{\mathsf{I}} \rho \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \widehat{R}; \mathbf{bb}(\widehat{R}); \widehat{N}\{\tau/u\}; \sigma}\, E-\beta_{\Box}$$

The judgement just above the line follows from the hypothesis $R' \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \xi\rangle \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \sigma$.

– $R = \iota_A$, $R' = \mathtt{iter}_{\mathsf{can}(\rho)}$ and $r = \mathbf{ti}_A(\rho)$. Note that $\sigma = \widehat{R'}$ since R' is a value. We reason as follows:

$$\frac{}{\iota_A \mathbin{\mathsf{I}} \rho \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} \mathtt{iter}_{\mathsf{can}(\rho)} \mathbin{\mathsf{I}} \mathbf{ti}_A(\rho)}\, \mathsf{E\text{-}TI}$$

Note that since $\mathtt{iter}_{\mathsf{can}(\rho)}$ is a value, the hypothesis $R' \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \xi\rangle \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \sigma$ reads $\mathtt{iter}_{\mathsf{can}(\rho)} \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \mathbf{ti}_A(\rho)\rangle \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} \mathtt{iter}_{\mathsf{can}(\rho)} \mathbin{\mathsf{I}} \widehat{\mathtt{iter}_\rho}$. Thus, $\sigma = \widehat{\mathtt{iter}_{\mathsf{can}(\rho)}}$ and $r; \sigma = \mathbf{ti}_A(\rho); \widehat{\mathtt{iter}_{\mathsf{can}(\rho)}} = \mathbf{ti}_A(\rho)$.

Lemma 18 (Shallow Expansion). *For all (R, R', r) in the redex table, $\mathcal{F}\langle R'\rangle \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \widehat{\mathcal{F}}\langle \xi\rangle\rangle \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \sigma$, implies $\mathcal{F}\langle R\rangle \mathbin{\mathsf{I}} \rho \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \widehat{\mathcal{F}}\langle \xi\rangle; \sigma$.*

Proof. By induction on $\mathcal{F}$.

– $\mathcal{F} = \Box$. We must prove that if $R' \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \xi\rangle \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \sigma$, then $R \mathbin{\mathsf{I}} \rho \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \xi; \sigma$. This is Lem. 17.

– $\mathcal{F} = \mathcal{F}'\,M$. We have to prove $\mathcal{F}'\langle R\rangle\, M \mathbin{\mathsf{I}} \rho \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} (\widehat{\mathcal{F}'}\langle \xi\rangle\, \widehat{M}); \sigma$. From the hypothesis $\mathcal{F}'\langle R'\rangle\, M \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \widehat{\mathcal{F}'}\langle \xi\rangle\, M\rangle \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \sigma$ we have the following, where $\sigma = \rho\,\tau; \mathbf{ba}(\widehat{S}); \sigma'$:

$$\frac{\begin{array}{c}\mathcal{F}'\langle R'\rangle \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \widehat{\mathcal{F}'}\langle \xi\rangle\, M\rangle \mathbin{\mathsf{I}} \mathcal{G}\langle \Box\, M\rangle \Downarrow^{\mathsf{cbv}} \lambda a^A.P \mathbin{\mathsf{I}} \tau \\ M \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \widehat{\mathcal{F}'}\langle \xi\rangle\, M\rangle; \widehat{\mathcal{G}}\langle \tau\, \widehat{M}\rangle \mathbin{\mathsf{I}} \mathcal{G}\langle (\lambda a^A.P)\,\Box\rangle \Downarrow^{\mathsf{cbv}} V \mathbin{\mathsf{I}} \mu \\ P\{V/a\} \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \widehat{\mathcal{F}'}\langle \xi\rangle\, M\rangle; \widehat{\mathcal{G}}\langle \tau\,\mu; \mathbf{ba}(\widehat{S})\rangle \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \nu\end{array}}{\mathcal{F}'\langle R'\rangle\, M \mathbin{\mathsf{I}} \rho; \widehat{\mathcal{G}}\langle \widehat{\mathcal{F}'}\langle \xi\rangle\, M\rangle \mathbin{\mathsf{I}} \mathcal{G} \Downarrow^{\mathsf{cbv}} W \mathbin{\mathsf{I}} \tau\,\mu; \mathbf{ba}(\widehat{S}); \nu}\, E-\beta \tag{34}$$

where $S := (\lambda a^A.P)\,V$. If we set $\mathcal{G}' := \mathcal{G}\langle\Box\, M\rangle$, then we may rewrite the topmost judgement in (34) as:

$$\mathcal{F}'\langle R'\rangle \shortmid \rho; \widehat{\mathcal{G}}'\langle\widehat{\mathcal{F}'}\langle\xi\rangle\rangle \shortmid \mathcal{G}' \Downarrow^{\mathsf{cbv}} \lambda a^A.P \shortmid \tau \tag{35}$$

From the i.h. on (35), we deduce:

$$\mathcal{F}'\langle R\rangle \shortmid \rho \shortmid \mathcal{G}' \Downarrow^{\mathsf{cbv}} \lambda a^A.P \shortmid \widehat{\mathcal{F}'}\langle\xi\rangle; \tau$$

We now prove the judgement $\mathcal{F}'\langle R\rangle\, M \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid (\widehat{\mathcal{F}'}\langle\xi\rangle\, \widehat{M}); \sigma$.

$$\frac{\begin{array}{c}\mathcal{F}'\langle R\rangle \shortmid \rho \shortmid \mathcal{G}\langle\Box\, M\rangle \Downarrow^{\mathsf{cbv}} \lambda a^A.P \shortmid \widehat{\mathcal{F}'}\langle\xi\rangle; \tau \\ M \shortmid \rho; \widehat{\mathcal{G}}\langle(\widehat{\mathcal{F}'}\langle\xi\rangle\,; \tau)\, M\rangle \shortmid \mathcal{G}\langle(\lambda a^A.P)\,\Box\rangle \Downarrow^{\mathsf{cbv}} V \shortmid \mu \\ P\{V/a\} \shortmid \rho; \widehat{\mathcal{G}}\langle(\widehat{\mathcal{F}'}\langle\xi\rangle; \tau)\,\mu; \mathbf{ba}(\widehat{S})\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \nu\end{array}}{\mathcal{F}'\langle R\rangle\, \widehat{M} \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid (\widehat{\mathcal{F}'}\langle\xi\rangle; \tau)\,\mu; \mathbf{ba}(\widehat{S}); \nu}\, E-\beta$$

Since

$$\widehat{\mathcal{G}}\langle\widehat{\mathcal{F}'}\langle\xi\rangle\, \widehat{M}\rangle; \widehat{\mathcal{G}}\langle\tau\, \widehat{M}\rangle \simeq \widehat{\mathcal{G}}\langle(\widehat{\mathcal{F}'}\langle\xi\rangle; \tau)\, \widehat{M}\rangle$$

and

$$\widehat{\mathcal{G}}\langle\widehat{\mathcal{F}'}\langle\xi\rangle\, \widehat{M}\rangle; \widehat{\mathcal{G}}\langle\tau\,\mu; \mathbf{ba}(\widehat{S})\rangle \simeq \widehat{\mathcal{G}}\langle(\widehat{\mathcal{F}'}\langle\xi\rangle; \tau)\,\mu; \mathbf{ba}(\widehat{S})\rangle$$

we conclude.

– $\mathcal{F} = (\lambda a^A.P)\,\mathcal{F}'$. Let $V := \lambda a^A.P$. From the hypothesis:

$$\frac{\begin{array}{c}V \shortmid \rho; \widehat{\mathcal{G}}\langle V\, \widehat{\mathcal{F}'}\langle\xi\rangle\rangle \shortmid \mathcal{G}\langle\Box\, \mathcal{F}'\langle R'\rangle\rangle \Downarrow^{\mathsf{cbv}} V \shortmid \widehat{V} \\ \mathcal{F}'\langle R'\rangle \shortmid \rho; \widehat{\mathcal{G}}\langle V\, \widehat{\mathcal{F}'}\langle\xi\rangle\rangle; \widehat{\mathcal{G}}\langle\widehat{V}\, \widehat{\mathcal{F}'\langle R'\rangle}\rangle \shortmid \mathcal{G}\langle V\,\Box\rangle \Downarrow^{\mathsf{cbv}} U \shortmid \mu \\ P\{U/a\} \shortmid \rho; \widehat{\mathcal{G}}\langle V\, \widehat{\mathcal{F}'}\langle\xi\rangle\rangle; \widehat{\mathcal{G}}\langle\widehat{V}\,\mu; \mathbf{ba}(\widehat{S})\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \nu\end{array}}{V\, \mathcal{F}'\langle R'\rangle \shortmid \rho; \widehat{\mathcal{G}}\langle V\, \widehat{\mathcal{F}'}\langle\xi\rangle\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \widehat{V}\mu\,; \mathbf{ba}(\widehat{S}); \nu}\, E-\beta \tag{36}$$

where $S = (\lambda a^A.P)\,U$. If we set $\mathcal{G}' := \mathcal{G}\langle V\,\Box\rangle$, and noting that $\rho; \widehat{\mathcal{G}}\langle V\, \widehat{\mathcal{F}'}\langle\xi\rangle\rangle; \widehat{\mathcal{G}}\langle\widehat{V}\, \widehat{\mathcal{F}'\langle R'\rangle}\rangle \simeq \rho; \widehat{\mathcal{G}}\langle V\, \widehat{\mathcal{F}'}\langle\xi\rangle\rangle$, we can rewrite the second topmost judgement in (36) as:

$$\mathcal{F}'\langle R'\rangle \shortmid \rho; \widehat{\mathcal{G}}'\langle\widehat{\mathcal{F}'}\langle\xi\rangle\rangle \shortmid \mathcal{G}' \Downarrow^{\mathsf{cbv}} U \shortmid \mu \tag{37}$$

From the i.h. on (37), we deduce:

$$\mathcal{F}'\langle R\rangle \shortmid \rho \shortmid \mathcal{G}' \Downarrow^{\mathsf{cbv}} U \shortmid \widehat{\mathcal{F}'}\langle\xi\rangle; \mu$$

We now prove the judgement $V\, \mathcal{F}'\langle R\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid (\widehat{V}\, \widehat{\mathcal{F}'}\langle\xi\rangle); \sigma$.

$$\frac{\begin{array}{c}V \shortmid \rho \shortmid \mathcal{G}\langle\Box\, \mathcal{F}'\langle R\rangle\rangle \Downarrow^{\mathsf{cbv}} V \shortmid \widehat{V} \\ \mathcal{F}'\langle R\rangle \shortmid \rho; \widehat{\mathcal{G}}\langle\widehat{V}\, \widehat{\mathcal{F}'\langle R\rangle}\rangle \shortmid \mathcal{G}\langle V\,\Box\rangle \Downarrow^{\mathsf{cbv}} U \shortmid \widehat{\mathcal{F}'}\langle\xi\rangle; \mu \\ P\{U/a\} \shortmid \rho; \widehat{\mathcal{G}}\langle(V\, (\widehat{\mathcal{F}'}\langle\xi\rangle; \mu)); \mathbf{ba}(\widehat{S})\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \nu\end{array}}{V\, \mathcal{F}'\langle R\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid (\widehat{V}\, (\widehat{\mathcal{F}'}\langle\xi\rangle; \mu)); \mathbf{ba}(\widehat{S}); \nu}\, E-\beta$$

where $S := (\lambda a^A.P)\,U$. We conclude from:

$$\rho; \widehat{\mathcal{G}}\langle V\ \widehat{\mathcal{F}'}\langle\xi\rangle\rangle; \widehat{\mathcal{G}}\langle\widehat{V}\ \mu; \mathbf{ba}(\widehat{S})\rangle \simeq \rho; \widehat{\mathcal{G}}\langle(V\ (\widehat{\mathcal{F}'}\langle\xi\rangle; \mu)); \mathbf{ba}(\widehat{S})\rangle$$

– $\mathcal{F} = \mathit{let}\ u^A \triangleq \mathcal{F}'\ \mathit{in}\ M$. We have to prove $\mathit{let}\ u^A \triangleq \mathcal{F}'\langle R\rangle\ \mathit{in}\ M \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid (\mathit{let}\ u^A \triangleq \mathcal{F}'\langle\xi\rangle\ \mathit{in}\ \widehat{M}); \sigma$. From the hypothesis $\mathcal{F}\langle R'\rangle \shortmid \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}}\langle\xi\rangle\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \sigma$ we have the following, where $\sigma = \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}; \nu$:

$$\frac{\mathcal{F}'\langle R'\rangle \shortmid \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}}\langle\xi\rangle\rangle \shortmid \mathcal{G}\langle\mathit{let}\ u^A \triangleq \Box\ \mathit{in}\ N\rangle \Downarrow^{\mathsf{cbv}} !_\tau V \shortmid \mu \qquad N\{!_\tau V/u\} \shortmid \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}}\langle\xi\rangle; \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \nu}{\mathit{let}\ u^A \triangleq \mathcal{F}'\langle R'\rangle\ \mathit{in}\ N \shortmid \rho; \widehat{\mathcal{G}}\langle\widehat{\mathcal{F}}\langle\xi\rangle\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}; \nu}\ E - \beta_{\Box} \tag{38}$$

where $S := \mathit{let}\ u^A \triangleq !_\tau V\ \mathit{in}\ N$
If we set $\mathcal{G}' := \mathit{let}\ u^A \triangleq \Box\ \mathit{in}\ N$, then we may rewrite the topmost judgement in (38) as:

$$\mathcal{F}'\langle R'\rangle \shortmid \rho; \widehat{\mathcal{G}'}\langle\widehat{\mathcal{F}'}\langle\xi\rangle\rangle \shortmid \mathcal{G}' \Downarrow^{\mathsf{cbv}} !_\tau V \shortmid \mu \tag{39}$$

From the i.h. on (39), we deduce:

$$\mathcal{F}'\langle R\rangle \shortmid \rho \shortmid \mathcal{G}' \Downarrow^{\mathsf{cbv}} !_\tau V \shortmid \widehat{\mathcal{F}'}\langle\xi\rangle; \mu$$

We now prove the judgement $\mathit{let}\ u^A \triangleq \mathcal{F}'\langle R\rangle\ \mathit{in}\ N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \mathit{let}\ u^A \triangleq \widehat{\mathcal{F}'}\langle\xi\rangle\ \mathit{in}\ \widehat{N}; \sigma$.

$$\frac{\mathcal{F}'\langle R\rangle \shortmid \rho \shortmid \widehat{\mathcal{G}}\langle\mathit{let}\ u^A \triangleq \Box\ \mathit{in}\ N\rangle \Downarrow^{\mathsf{cbv}} !_\tau V \shortmid \widehat{\mathcal{F}'}\langle\xi\rangle; \mu \qquad N\{!_\tau V/u\} \shortmid \rho; \widehat{\mathcal{G}}\langle\mathit{let}\ u^A \triangleq (\widehat{\mathcal{F}}\langle\xi\rangle; \mu)\ \mathit{in}\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \nu}{\mathit{let}\ u^A \triangleq \mathcal{F}'\langle R\rangle\ \mathit{in}\ N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \mathit{let}\ u^A \triangleq (\widehat{\mathcal{F}}\langle\xi\rangle; \mu)\ \mathit{in}\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}; \nu}\ E - \beta_{\Box}$$

Note that

$$\begin{aligned} &\mathit{let}\ u^A \triangleq (\widehat{\mathcal{F}}\langle\xi\rangle; \mu)\ \mathit{in}\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}; \nu \\ \simeq\ &\mathit{let}\ u^A \triangleq \widehat{\mathcal{F}'}\langle\xi\rangle\ \mathit{in}\ \widehat{N}; \mathit{let}\ u^A \triangleq \mu\ \mathit{in}\ N; \mathbf{bb}(\widehat{S}); \widehat{N}\{\tau/u\}; \nu \\ =\ &\mathit{let}\ u^A \triangleq \widehat{\mathcal{F}'}\langle\xi\rangle\ \mathit{in}\ \widehat{N}; \sigma \end{aligned}$$

Lemma 19 (Projection). *If* $\pi\Big(\mathcal{F}\langle M\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} U \shortmid \sigma\Big)$, *then there exists* V *and* τ *s.t.* $\pi\mid_p\Big(M \shortmid \rho \shortmid \mathcal{G}\langle\mathcal{F}\rangle \Downarrow^{\mathsf{cbv}} V \shortmid \tau\Big)$, *where* p *is the position of the hole in* $\mathcal{F}$.

Proof. By induction on $\mathcal{F}$. If $\mathcal{F} = \Box$, the result is immediate; we develop the inductive cases below:

– $\mathcal{F} = \mathcal{F}'\,N$. Then π ends as follows:

$$\frac{\mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G}\langle\Box\,N\rangle \Downarrow^{\mathsf{cbv}} \lambda a^A.P \shortmid \sigma \qquad N \shortmid \rho; \widehat{\mathcal{G}}\langle\sigma\ \widehat{N}\rangle \shortmid \mathcal{G}\langle(\lambda a^A.P)\,\Box\rangle \Downarrow^{\mathsf{cbv}} V \shortmid \tau \qquad P\{V/a\} \shortmid \rho; \widehat{\mathcal{G}}\langle(\sigma\,\tau); \mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{V})\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \upsilon}{\mathcal{F}'\langle M\rangle\,N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid (\sigma\,\tau); \mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{V}); \upsilon}\ E - \beta$$

We conclude from the i.h. applied to the derivation of $\mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G}\langle\Box\, N\rangle \Downarrow^{\mathsf{cbv}} \lambda a^A.P \shortmid \sigma$.

– $\mathcal{F} = (\lambda a^A.P)\,\mathcal{F}'$. Let $V := \lambda a^A.P$. Then the derivation π ends in:

$$\dfrac{\begin{array}{c} V \shortmid \rho \shortmid \mathcal{G}\langle\Box\, N\rangle \Downarrow^{\mathsf{cbv}} \lambda a^A.P \shortmid \widehat{V} \\ \mathcal{F}'\langle M\rangle \shortmid \rho; \widehat{\mathcal{G}}\langle\widehat{V}\ \widehat{\mathcal{F}'\langle M\rangle}\rangle \shortmid \mathcal{G}\langle(\lambda a^A.P)\,\Box\rangle \Downarrow^{\mathsf{cbv}} U \shortmid \tau \\ P\{U/a\} \shortmid \rho; \widehat{\mathcal{G}}\langle(\sigma\,\tau); \mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{U})\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \upsilon \end{array}}{V\,\mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid (\sigma\,\tau); \mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{U}); \upsilon}\, E-\beta$$

Then we note that $\rho; \widehat{\mathcal{G}}\langle\widehat{V}\ \widehat{\mathcal{F}'\langle M\rangle}\rangle \simeq \rho$ and we can apply the i.h. to the derivation ending in the judgement $\mathcal{F}'\langle M\rangle \shortmid \rho; \widehat{\mathcal{G}}\langle\widehat{V}\ \widehat{\mathcal{F}'\langle M\rangle}\rangle \shortmid \mathcal{G}\langle(\lambda a^A.P)\,\Box\rangle \Downarrow^{\mathsf{cbv}} U \shortmid \tau$ to conclude.

– $\mathcal{F} = \mathit{let}\ u^A \triangleq \mathcal{F}'\ \mathit{in}\ M$. Then π ends in

$$\dfrac{\begin{array}{c} \mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G}\langle \mathit{let}\ u^A \triangleq \Box\ \mathit{in}\ N\rangle \Downarrow^{\mathsf{cbv}} !_\tau V \shortmid \sigma \\ N\{!_\tau V/u\} \shortmid \rho; \widehat{\mathcal{G}}\langle \mathit{let}\ u^A \triangleq \sigma\ \mathit{in}\ \widehat{N}; \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{(!_\tau V)}\ \mathit{in}\ \widehat{N}); \widehat{N}\{\tau/u\}\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \upsilon \end{array}}{\mathit{let}\ u^A \triangleq \mathcal{F}'\langle M\rangle\ \mathit{in}\ N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \mathit{let}\ u^A \triangleq \sigma\ \mathit{in}\ \widehat{N}; \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{(!_\tau V)}\ \mathit{in}\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon}\, E-\beta_{\Box}$$

We conclude from the i.h. on the derivation ending in the topmost judgement.

Lemma 20 (Substitution). *If*

– $\pi\Big(\mathcal{F}\langle M\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} U \shortmid \sigma\Big)$, *and*
– $\pi \mid_p \Big(M \shortmid \rho \shortmid \mathcal{G}\langle\mathcal{F}\rangle \Downarrow^{\mathsf{cbv}} V \shortmid \tau\Big)$, *for p the position of the hole in $\mathcal{F}$ and for some V and τ, and*
– $\pi_N\Big(N \shortmid \rho \shortmid \mathcal{G}\langle\mathcal{F}\rangle \Downarrow^{\mathsf{cbv}} V \shortmid \tau\Big)$.

Then $\pi \mid_p^{\pi_N} \Big(\mathcal{F}\langle N\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} U \shortmid \sigma\Big)$.

Proof. By induction on $\mathcal{F}$. If $\mathcal{F} = \Box$, then $U = V$ and $\sigma = \tau$ and the result holds immediately; we develop the inductive cases below:

– $\mathcal{F} = \mathcal{F}'\,N$. Then $p = 1.p'$, for p' the position of the hole in $\mathcal{F}'$, and π ends as follows:

$$\dfrac{\begin{array}{c} \mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G}\langle\Box\, N\rangle \Downarrow^{\mathsf{cbv}} \lambda a^A.P \shortmid \sigma \\ N \shortmid \rho; \widehat{\mathcal{G}}\langle\sigma\ \widehat{N}\rangle \shortmid \mathcal{G}\langle(\lambda a^A.P)\,\Box\rangle \Downarrow^{\mathsf{cbv}} V \shortmid \tau \\ P\{V/a\} \shortmid \rho; \widehat{\mathcal{G}}\langle(\sigma\,\tau); \mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{V})\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \upsilon \end{array}}{\mathcal{F}'\langle M\rangle\, N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid (\sigma\,\tau); \mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{V}); \upsilon}\, \mathsf{E}\text{-}\beta$$

We conclude from the i.h. applied to the derivation of $\mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G}\langle\Box\, N\rangle \Downarrow^{\mathsf{cbv}} \lambda a^A.P \shortmid \sigma$ and then an application of E-β.

– $\mathcal{F} = (\lambda a^A.P)\,\mathcal{F}'$. Let $V := \lambda a^A.P$. Then $p = 2.p'$, for p' the position of the hole in $\mathcal{F}'$, and the derivation π ends in:

$$\frac{\begin{array}{c} V \shortmid \rho \shortmid \mathcal{G}\langle \Box\, N\rangle \Downarrow^{\mathsf{cbv}} \lambda a^A.P \shortmid \widehat{V} \\ \mathcal{F}'\langle M\rangle \shortmid \rho; \widehat{\mathcal{G}}\langle \widehat{V}\, \widehat{\mathcal{F}'\langle M\rangle}\rangle \shortmid \mathcal{G}\langle (\lambda a^A.P)\,\Box\rangle \Downarrow^{\mathsf{cbv}} V \shortmid \tau \\ P\{V/a\} \shortmid \rho; \widehat{\mathcal{G}}\langle (\sigma\,\tau); \mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{V})\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \upsilon \end{array}}{V\,\mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid (\sigma\,\tau); \mathbf{ba}((\lambda a^A.\widehat{P})\,\widehat{V}); \upsilon}\, E-\beta$$

Then we note that $\rho; \widehat{\mathcal{G}}\langle \widehat{V}\, \widehat{\mathcal{F}'\langle M\rangle}\rangle \simeq \rho$ and we can apply the i.h. to the derivation ending in the judgement $\mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G}\langle (\lambda a^A.P)\,\Box\rangle \Downarrow^{\mathsf{cbv}} V \shortmid \tau$ and then apply E-β.

– $\mathcal{F} = \mathit{let}\ u^A \triangleq \mathcal{F}'\ \mathit{in}\ M$.

$$\frac{\begin{array}{c} \mathcal{F}'\langle M\rangle \shortmid \rho \shortmid \mathcal{G}\langle \mathit{let}\ u^A \triangleq \Box\ \mathit{in}\ N\rangle \Downarrow^{\mathsf{cbv}} !_\tau V \shortmid \sigma \\ N\{!_\tau V/u\} \shortmid \rho; \widehat{\mathcal{G}}\langle \mathit{let}\ u^A \triangleq \sigma\ \mathit{in}\ \widehat{N}; \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{(!_\tau V)}\ \mathit{in}\ \widehat{N}); \widehat{N}\{\tau/u\}\rangle \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \upsilon \end{array}}{\mathit{let}\ u^A \triangleq \mathcal{F}'\langle M\rangle\ \mathit{in}\ N \shortmid \rho \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \mathit{let}\ u^A \triangleq \sigma\ \mathit{in}\ \widehat{N}; \mathbf{bb}(\mathit{let}\ u^A \triangleq \widehat{(!_\tau V)}\ \mathit{in}\ \widehat{N}); \widehat{N}\{\tau/u\}; \upsilon}\, \mathsf{E}\text{-}\beta_{\Box}$$

We conclude from the i.h. on the derivation ending in the topmost judgement and then an application of E-$\beta_{\Box}$.

Lemma 21 (Expansion). *For all (R, R', r) in the redex table, if $\mathcal{E}\langle !_{\rho;\widehat{\mathcal{F}}\langle\xi\rangle}\mathcal{F}\langle R'\rangle\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \tau$, then $\mathcal{E}\langle !_\rho \mathcal{F}\langle R\rangle\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \tau$.*

Proof. By induction on $\mathcal{E}$.

– If $\mathcal{E} = \Box$, then by hypothesis:

$$\frac{\mathcal{F}\langle R'\rangle \shortmid \rho; \widehat{\mathcal{F}}\langle\xi\rangle \shortmid \Box \Downarrow^{\mathsf{cbv}} V \shortmid \mu}{!_{\rho;\widehat{\mathcal{F}}\langle\xi\rangle}\mathcal{F}\langle R'\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} !_{(\rho;\widehat{\mathcal{F}}\langle\xi\rangle);\mu} V \shortmid \tau}\, \mathsf{E}\text{-}!$$

and $W = !_{(\rho;\widehat{\mathcal{F}}\langle\xi\rangle);\mu} V$. By Shallow Expansion (Lem. 21) applied to $\mathcal{F}\langle R'\rangle \shortmid \rho; \widehat{\mathcal{F}}\langle\xi\rangle \shortmid \Box \Downarrow^{\mathsf{cbv}} V \shortmid \mu$, we deduce $\mathcal{F}\langle R\rangle \shortmid \rho \shortmid \Box \Downarrow^{\mathsf{cbv}} W \shortmid \widehat{\mathcal{F}}\langle\xi\rangle; \mu$. We conclude using E-Bang:

$$\frac{\mathcal{F}\langle R\rangle \shortmid \rho \shortmid \Box \Downarrow^{\mathsf{cbv}} W \shortmid \widehat{\mathcal{F}}\langle\xi\rangle; \mu}{!_\rho \mathcal{F}\langle R\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} !_{\rho;(\widehat{\mathcal{F}}\langle\xi\rangle;\mu)} V \shortmid \tau}\, \mathsf{E}\text{-}!$$

Note that $(\rho; \widehat{\mathcal{F}}\langle\xi\rangle); \mu \simeq \rho; (\widehat{\mathcal{F}}\langle\xi\rangle; \mu)$.

– Suppose $\mathcal{E} = !_{\rho'}\mathcal{F}'\langle\mathcal{E}'\rangle$. Then

$$\frac{\mathcal{F}'\langle\mathcal{E}'\langle !_{\rho;\widehat{\mathcal{F}}\langle\xi\rangle}\mathcal{F}\langle R'\rangle\rangle\rangle \shortmid \rho' \shortmid \Box \Downarrow^{\mathsf{cbv}} V' \shortmid \mu}{!_{\rho'}\mathcal{F}'\langle\mathcal{E}'\langle !_{\rho;\widehat{\mathcal{F}}\langle\xi\rangle}\mathcal{F}\langle R'\rangle\rangle\rangle \shortmid \sigma \shortmid \mathcal{G} \Downarrow^{\mathsf{cbv}} W \shortmid \tau}\, \mathsf{E}\text{-}!$$

By Projection (Lem. 19), there exists U, ν s.t.

$$\pi \mid_p \Big(\mathcal{E}'\langle !_{\rho;\widehat{\mathcal{F}}\langle\xi\rangle} \mathcal{F}\langle R'\rangle\rangle \intercal \rho' \intercal \mathcal{F}' \Downarrow^{\mathsf{cbv}} U \intercal \nu \Big)$$

where p is the position of the hole in $\mathcal{F}'$. By the i.h. ($\sigma := \rho'$ and $\mathcal{G} := \mathcal{F}'$) there exists π'

$$\pi' \Big(\mathcal{E}'\langle !_{\rho} \mathcal{F}\langle R\rangle\rangle \intercal \rho' \intercal \mathcal{F}' \Downarrow^{\mathsf{cbv}} U \intercal \nu \Big)$$

By Substitution (Lem. 20),

$$\pi \mid_p^{\pi'} \Big(\mathcal{F}'\langle \mathcal{E}'\langle !_{\rho} \mathcal{F}\langle R\rangle\rangle\rangle \intercal \rho' \intercal \Box \Downarrow^{\mathsf{cbv}} V' \intercal \mu \Big)$$

We then conclude using E-Bang:

$$\frac{\mathcal{F}'\langle \mathcal{E}'\langle !_{\rho} \mathcal{F}\langle R\rangle\rangle\rangle \intercal \rho' \intercal \Box \Downarrow^{\mathsf{cbv}} V' \intercal \mu}{!_{\rho'} \mathcal{F}'\langle \mathcal{E}'\langle !_{\rho} \mathcal{F}\langle R\rangle\rangle\rangle \intercal \sigma \intercal \mathcal{G} \Downarrow^{\mathsf{cbv}} W \intercal \tau}\ \mathsf{E\text{-}!}$$

Proof of Prop. 5 (Evaluation simulates reduction).

Proof. By induction on the length n of the derivation sequence. If $n = 0$, then $M = V$ and $V \intercal \rho \intercal \mathcal{G} \Downarrow^{\mathsf{cbv}} V \intercal \sigma$ holds by taking $\sigma = \widehat{V}$. Suppose $M \rightsquigarrow_{\mathsf{cbv}} P \rightsquigarrow_{\mathsf{cbv}}^{n} V$. By the i.h., for all $\rho, \mathcal{G}$ there exists σ such that:

$$P \intercal \rho \intercal \mathcal{G} \Downarrow^{\mathsf{cbv}} V \intercal \sigma \tag{40}$$

Since $M \rightsquigarrow_{\mathsf{cbv}} P$, then $M = \mathcal{E}\langle !_{\tau} \mathcal{F}\langle R\rangle\rangle$ and $P = \mathcal{E}\langle !_{\tau;\widehat{\mathcal{F}}\langle\xi\rangle} \mathcal{F}\langle R'\rangle\rangle$, for some (R, R', r) in the redex table. Then (40) reads $\mathcal{E}\langle !_{\tau;\widehat{\mathcal{F}}\langle\xi\rangle} \mathcal{F}\langle R'\rangle\rangle \intercal \rho \intercal \mathcal{G} \Downarrow^{\mathsf{cbv}} V \intercal \sigma$ and from Expansion (Lem. 21) we deduce $\mathcal{E}\langle !_{\tau} \mathcal{F}\langle R\rangle\rangle \intercal \rho \intercal \mathcal{G} \Downarrow^{\mathsf{cbv}} V \intercal \sigma$.