Compositional Security Definitions for Higher-Order Where Declassification - Technical Appendix

March 1, 2023

1 Structure of the document:

This document might be updated from time to time to make it more readable. If you are using an old version, consider getting checking if there is a new version at `https://gitlab.mpi-sws.org/Quarkbeast/lambda-where-fullproofs/-/raw/main/Technical_Appendix.pdf`.

1. In the section Structure of the document: we present the structure of this document.
2. Some proofs were still done with paralocks in mind. In the section Flow locks and Paralocks we talk about the relationship between Flow Locks and Paralocks. In particular we show that for Flow Locks policies important definitions coincide with the corresponding Paralocks definitions which allows us to freely switch between them.
3. In the section The language we formally present the language we use.
4. In section Properties of the policy ordering we prove properties of the policy language. In particular we prove that paralocks policies and therefore also flow locks policies have a lattice structure.
5. In section Weakening we prove weakening.
6. In section Type Safety we prove type safety.
7. In section Logical relations we present the logical relations model. Note that the binary relation presented in this section is a logical relation already restricted to firstorder state which we do not present in the paper. The model of the logical relation from the paper can be found in section Higher order observations:.
8. In section Proofs we prove the fundamental theorem of the logical relations presented in the previous section. Some of the proofs differ slightly for the version of the logical relation presented in the paper. These proofs can be found in section Higher order observations:.
9. In section Higher order observations: we extend the logical relation presented in section 7 to deal with higher-order observations. This is the logical relation presented in the paper. We also present updated versions of the proofs from Proofs which deal with the changes in the definition where necessary.
10. In section Knowledge based security we prove that the knowledge based Flow Lock security property follows from our notion of security.

2 Flow locks and Paralocks

While the paper only uses Flow locks [2, 4] we originally based our work on paralocks [4]. Consequently some of the proofs in this document, mainly those relating to the lattice structure of the policy language in section 4, still use this more general setting. In this section we prove that the ordering on flow locks and paralocks policies, which are defined differently, coincide. If nothing else is specified every definition related to policies is identical to [4].

The main difference between full paralocks policies and flow locks policies is that paralocks policies can use locks that are parameterised by actors. Therefore paralocks clauses have the form $\forall\vec{x}.\Sigma \Rightarrow a$ where the locks in the lock set Σ may use some of the actor variables in $\vec{x}$ and a may itself be an actor variable from $\vec{x}$.

Flow-locks clauses can be characterised as a subset of paralocks clauses. They are paralocks clauses where locks ($\sigma, \sigma_1, \sigma'$, etc.) are not parameterised and clauses remain unquantified.

For the proofs we use the characterisation of flow-lock policy ordering from the paralocks paper [4]. There the ordering on flow lock policies is defined as logical implication of the policies when interpreted as horn formulas. That is a flow lock policy $p = (p_1, \dots p_n)$ is below a flow lock policy $q = (q_1, \dots, q_m)$ (written $p \sqsubseteq q$) where for all $1 \leqslant i \leqslant n$ and $1 \leqslant j \leqslant m$ the clauses p_i (or q_j) have the form $\Sigma_{p_i} \Rightarrow a_i$ and $\Sigma_{q_j} \Rightarrow a_j$ respectively, if $\bigwedge_i p_i \rightarrow \bigwedge_j p_j$ when $\Rightarrow$ is read as logical implication.

We will show that this notion of a policy ordering coincides with the policy ordering for paralocks policies. The ordering on paralocks policies is defined based on an ordering on clauses $\sqsubseteq$. A paralocks policy p is below a paralocks policy q (written $p \sqsubseteq q$) if for every clause c_q in q there is a clause c_p in p such that

$c_p \sqsubseteq c_q$. The ordering $\sqsubseteq$ on clauses is the least partial order containing the proto-inclusion $\sqsubset$ which is defined as

$$\frac{c = c' \text{ up to } \alpha\text{-renaming of } \forall\text{-bound actors, deletion of unused quantifiers, reordering of quantifiers}}{c \sqsubset c'} \textbf{ refl}$$

$$\frac{\Sigma_1 \subseteq \Sigma_2}{\forall a_1, \ldots, a_n.\Sigma_1 \Rightarrow a \sqsubset \forall a_1, \ldots, a_n.\Sigma_2 \Rightarrow a} \textbf{ subset}$$

$$\frac{}{\forall a_0, a_1, \ldots, a_n.\Sigma \Rightarrow a \sqsubset \forall a_1, \ldots, a_n.(\Sigma \Rightarrow a)[a_0 := b]} \textbf{ subst}$$

We know that the least reflexive, transitive relation containing a relation R is the relation R^* defined as

$$\frac{}{R^* \; x \; x} \textbf{ refl-*} \qquad \frac{R \; x \; y \qquad R^* \; y \; z}{R^* \; x \; z} \textbf{ trans-*}$$

Hence $\sqsubseteq = \sqsubset^*$. We will use both of these characterisations in the future.

Note that for flow locks policies, which do not contain quantifiers and actor variables, only the rule **subset** is relevant. Therefore for flow locks the ordering on clauses simplifies to the following rule:

$$\frac{\Sigma_1 \subseteq \Sigma_2}{\Sigma_1 \Rightarrow a \sqsubseteq \Sigma_2 \Rightarrow a} \textbf{ subset-FlowLocks}$$

.

With this rule in mind this ordering on paralocks policies corresponds exactly to the ordering of flow locks policies we present in the paper which is how Broberg and Sands define ordering on flow locks policies in [2, 3] as well. In the following we show that this definition coincides with the logical interpretation.

Lemma 2.1. If $c = \Sigma \Rightarrow b$ and $c' = \Sigma' \Rightarrow b'$ are flow lock clauses and $c \sqsubseteq c'$, then $c \to c'$

Proof. By assumption $\Sigma \subseteq \Sigma'$ and $b = b'$. Assume Σ'. We have to show b. By c it suffices to show Σ. We already know Σ' which is a superset of assumptions of Σ. □

Lemma 2.2. Let p, q be flow lock policies with $p \sqsubseteq q$. Then for all clauses q_i in q, there is a clause p_j in p such that $p_j \sqsubseteq q_i$.

Proof. Assume this is not the case. Then for all p_j, p_j must be true. Otherwise the implication $p_j \to q_i$ would trivially hold for all q_i. Because all p_j are true we get that all q_i must be true from $p \sqsubseteq q$. But then for all i, j $p_j \to q_i$ is true as q_i is true. Contradiction. □

The converse direction is easy.

Lemma 2.3. Let p and q be flow lock policies such that for all clauses $q_i \in q$ there is a clause $p_i \in p$ such that $p_i \sqsubseteq q_i$. Then $p \sqsubseteq q$

Proof. As we know for all i that $p_i \sqsubseteq q_i$ we have that $p_i \to q_i$. Hence we have for all i that $p \to q_i$. Hence $p \to \bigwedge_i q_i$ which is the same as $p \sqsubseteq q$. □

This also means that join and meet of normal paralocks policies are also join an meet for flow lock policies.

Finally we look at specialization: For a flow lock policy p and a set of flow locks Σ we have $p(\Sigma) := \{\Sigma' \backslash \Sigma \Rightarrow a \mid \Sigma' \Rightarrow a \in p\}$.

We will consider a different than the standard equality relation on policies and clauses. Instead of syntactic equality we consider a notion of equality $\approx$ that characterises equal information flow restrictions. It is defined as $x \approx y := x \sqsubseteq y \wedge y \sqsubseteq x$.

Lemma 2.4. Flow lock specialization is identical to normal paralocks specialization on flow lock policies modulo $\approx$.

Proof. Let p be a flow lock policy and Σ a set of flow lock. Then all clauses $c \in p$ have the form $\Sigma_c \Rightarrow b_c$ where b_c is not bound because there are no quantifiers in flow lock policies. Let $\Sigma_1 \subseteq \Sigma$. Then the only set matching Σ_1 with any substitution is Σ_1 and the substitution is $\emptyset$. Because there are no bound actors in Σ, there are no bound actors in Σ_1 and hence the domain of any substitution used for matching Σ_1 is

empty. The only substitution with an empty domain is $\emptyset$. For a set Σ_m to match Σ_1 with $\emptyset$ we need to have $\Sigma_m(\emptyset) = \Sigma_1$. $\Sigma_m(\emptyset) = \Sigma_m$ and hence $\Sigma_m = \Sigma_1$.

Hence $p(\Sigma) := \{\Sigma_2 \Rightarrow b \,|\, \Sigma_1 \subseteq \Sigma, \Sigma' = \Sigma_1 \cup \Sigma_2, \Sigma' \Rightarrow b \in p\} = \{\Sigma' \backslash \Sigma_1 \Rightarrow b \,|\, \Sigma_1 \subseteq \Sigma, \Sigma' \Rightarrow b \in p\}$.

All that remains to be shown is $\{\Sigma' \backslash \Sigma \Rightarrow a \,|\, \Sigma' \Rightarrow a \in p\} \approx \{\Sigma' \backslash \Sigma_1 \Rightarrow b \,|\, \Sigma_1 \subseteq \Sigma, \Sigma' \Rightarrow b \in p\}$.

As $\Sigma \subseteq \Sigma$ we have $\{\Sigma' \backslash \Sigma \Rightarrow a \,|\, \Sigma' \Rightarrow a \in p\} \subseteq \{\Sigma' \backslash \Sigma_1 \Rightarrow b \,|\, \Sigma_1 \subseteq \Sigma, \Sigma' \Rightarrow b \in p\}$. Hence for all $c \in \{\Sigma' \backslash \Sigma \Rightarrow a \,|\, \Sigma' \Rightarrow a \in p\}$ there is a $c' \in \{\Sigma' \backslash \Sigma_1 \Rightarrow b \,|\, \Sigma_1 \subseteq \Sigma, \Sigma' \Rightarrow b \in p\}$ (namely c), such that $c' \to c$. Hence $\{\Sigma' \backslash \Sigma_1 \Rightarrow b \,|\, \Sigma_1 \subseteq \Sigma, \Sigma' \Rightarrow b \in p\} \sqsubseteq \{\Sigma' \backslash \Sigma \Rightarrow a \,|\, \Sigma' \Rightarrow a \in p\}$.

On the other hand when $c = \Sigma_c \backslash \Sigma_1 \Rightarrow b_c \in \{\Sigma' \backslash \Sigma_1 \Rightarrow b \,|\, \Sigma_1 \subseteq \Sigma, \Sigma' \Rightarrow b \in p\}$, then $c' = \Sigma_c \backslash \Sigma \Rightarrow b_c \in \{\Sigma' \backslash \Sigma \Rightarrow a \,|\, \Sigma' \Rightarrow a \in p\}$ where $\Sigma_1 \subseteq \Sigma$. Hence $\Sigma_c \backslash \Sigma \subseteq \Sigma_c \backslash \Sigma_1$ and therefore $c' \sqsubseteq c$. Hence $\{\Sigma' \backslash \Sigma \Rightarrow a \,|\, \Sigma' \Rightarrow a \in p\} \sqsubseteq \{\Sigma' \backslash \Sigma_1 \Rightarrow b \,|\, \Sigma_1 \subseteq \Sigma, \Sigma' \Rightarrow b \in p\}$. □

Because the flow lock policy and the paralocks policy viewpoint are equivalent for flow lock policies we will switch freely between these to viewpoints. In particular we will use some theorems proved for paralocks policies for flow lock policies.

3 The language

The language we are working with has two sets of types that are mutually inductively defined. We have a set of normal types (normally denoted by $A, B, A', A_1, \ldots$, etc.) and annotated types ($\tau, \tau_1, \tau', \ldots$, etc.) which are normal types annotated with a policy as described in the previous section. This is essentially the same setup as in the FG Type system [5].

Definition 3.1 (Types)**.**

$$\begin{array}{llll} \text{Types} & A & ::= & \mathsf{unit} \,|\, \tau_1 + \tau_2 \,|\, \tau_1 \times \tau_2 \,|\, \mathsf{ref}\ \tau \,|\, \tau_1 \xrightarrow{\Sigma, p} \tau_2 \,|\, \mathcal{N} \\ \text{Annotated Types} & \tau, \tau_1, \tau_2 & ::= & A^p \end{array}$$

where p is a policy and Σ is a set of locks.

We lift the ordering $\sqsubseteq$ on policies to an ordering on policy annotated types and paralocks policies in the following way:

Definition 3.2.

$$A^p \sqsubseteq p'^{\,} \triangleq p \sqsubseteq p'$$
$$p \sqsubseteq A^{p'} \triangleq p \sqsubseteq p'$$
$$A^p \sqsubseteq B^{p'} \triangleq p \sqsubseteq p'$$

For $\tau = A^p$ we define $\tau(\Sigma) \triangleq A^{p(\Sigma)}$.

Definition 3.3 (Expressions and values)**.** Assume a countable infinite set of memory locations $\mathcal{L}$ and a countable infinite set of variables $\mathbb{V}$. Source expressions are defined as follows:

$$\begin{array}{llll} \text{Variables} & x & \in & \mathbb{V} \\ \text{Numbers} & n & \in & \mathbb{N} \\ \text{Expressions} & e, e', e'' & ::= & x \,|\, () \,|\, n \,|\, \lambda x.\, e \,|\, (e, e') \,|\, \mathsf{fst}\ (e) \,|\, \mathsf{snd}\ (e) \\ & & | & \mathsf{inl}\ (e) \,|\, \mathsf{inr}\ (e) \,|\, \mathsf{case}\ e\ \mathsf{of}\ |\, \mathsf{inl}\ (x) \Rightarrow e' \,|\, \mathsf{inr}\ (y) \Rightarrow e'' \\ & & | & e\ e' \,|\, \mathsf{new}\ (e, \tau) \,|\, !\, e \,|\, e := e' \\ & & | & \mathsf{open}\ \sigma\ \mathsf{in}\ e \,|\, \mathsf{close}\ \sigma\ \mathsf{in}\ e \,|\, \mathsf{when}\ \sigma\ \mathsf{then}\ e\ \mathsf{else}\ e' \end{array}$$

We extend source expressions with some intermediate expressions to get runtime expressions:

$$\begin{array}{llll} \text{Locations} & l & \in & \mathcal{L} \\ \text{exp} & e, e', e'' & ::= & \ldots \,|\, l \,|\, e\ \mathsf{then\ unopen}\ \sigma \,|\, e\ \mathsf{then\ unclose}\ \sigma \end{array}$$

We also define a set $\mathcal{V}$ of values:

$$\mathcal{V} \quad v, v' \quad ::= \quad \lambda x.\, e \,|\, (v, v') \,|\, \mathsf{fst}\ (v) \,|\, \mathsf{snd}\ (v) \,|\, \mathsf{inl}\ (v) \,|\, \mathsf{inr}\ (v) \,|\, () \,|\, l \,|\, n$$

Note: We sometimes use the short version $\mathsf{Case}(e, x.e_1, y.e_2)$ instead of $\mathsf{case}\ e\ \mathsf{of}\ |\, \mathsf{inl}\ (x) \Rightarrow e_1 \,|\, \mathsf{inr}\ (y) \Rightarrow e_2$.

We also sometimes use the old notations $\mathsf{opened}(\sigma)\ \mathsf{in}\ e$ and $\mathsf{closed}(\sigma)\ \mathsf{in}\ e$ instead of $e\ \mathsf{then\ unopen}\ \sigma$ and $e\ \mathsf{then\ unclose}\ \sigma$.

We define substitutions on expressions:

Definition 3.4 (Capture avoiding substitutions)**.**

$$
\begin{aligned}
x[x \mapsto e] &\triangleq e \\
n[x \mapsto e] &\triangleq n \\
y[x \mapsto e] &\triangleq y && \text{if } x \neq y \\
(\lambda y.\, e')[x \mapsto e] &\triangleq \lambda y.\, e'[x \mapsto e] && \text{if } y \neq x \\
(\lambda x.\, e')[x \mapsto e] &\triangleq \lambda x.\, e' \\
(e'\ e'')[x \mapsto e] &\triangleq (e'[x \mapsto e])\ (e''[x \mapsto e]) \\
()[x \mapsto e] &\triangleq () \\
l[x \mapsto e] &\triangleq l \\
(\mathsf{inl}\,(e'))[x \mapsto e] &\triangleq \mathsf{inl}\,(e'[x \mapsto e]) \\
(\mathsf{inr}\,(e'))[x \mapsto e] &\triangleq \mathsf{inr}\,(e'[x \mapsto e]) \\
(e', e'')[x \mapsto e] &\triangleq (e'[x \mapsto e], e''[x \mapsto e]) \\
(\mathsf{fst}\,(e'))[x \mapsto e] &\triangleq \mathsf{fst}\,(e'[x \mapsto e]) \\
(\mathsf{snd}\,(e'))[x \mapsto e] &\triangleq \mathsf{snd}\,(e'[x \mapsto e]) \\
\left(\begin{array}{l}\mathsf{case}\ e'\ \mathsf{of} \\ \mid \mathsf{inl}\,(y) \Rightarrow e_1 \\ \mid \mathsf{inr}\,(y') \Rightarrow e_2\end{array}\right)[x \mapsto e] &\triangleq \begin{array}{l}\mathsf{case}\ e'[x \mapsto e]\ \mathsf{of} \\ \mid \mathsf{inl}\,(y) \Rightarrow e_1[x \mapsto e] \\ \mid \mathsf{inr}\,(y') \Rightarrow e_2[x \mapsto e]\end{array} && \text{if } y \neq x \neq y' \\
\left(\begin{array}{l}\mathsf{case}\ e'\ \mathsf{of} \\ \mid \mathsf{inl}\,(x) \Rightarrow e_1 \\ \mid \mathsf{inr}\,(y) \Rightarrow e_2\end{array}\right)[x \mapsto e] &\triangleq \begin{array}{l}\mathsf{case}\ e'[x \mapsto e]\ \mathsf{of} \\ \mid \mathsf{inl}\,(x) \Rightarrow e_1 \\ \mid \mathsf{inr}\,(y) \Rightarrow e_2[x \mapsto e]\end{array} && \text{if } y \neq x \\
\left(\begin{array}{l}\mathsf{case}\ e'\ \mathsf{of} \\ \mid \mathsf{inl}\,(y) \Rightarrow e_1 \\ \mid \mathsf{inr}\,(x) \Rightarrow e_2\end{array}\right)[x \mapsto e] &\triangleq \begin{array}{l}\mathsf{case}\ e'[x \mapsto e]\ \mathsf{of} \\ \mid \mathsf{inl}\,(y) \Rightarrow e_1[x \mapsto e] \\ \mid \mathsf{inr}\,(x) \Rightarrow e_2\end{array} && \text{if } y \neq x \\
(\mathsf{new}\,(e', \tau))[x \mapsto e] &\triangleq \mathsf{new}\,(e'[x \mapsto e], \tau) \\
(!\,e')[x \mapsto e] &\triangleq !(e'[x \mapsto e]) \\
(e' := e'')[x \mapsto e] &\triangleq (e'[x \mapsto e]) := e''[x \mapsto e] \\
(\mathsf{open}\ \sigma\ \mathsf{in}\ e')[x \mapsto e] &\triangleq \mathsf{open}\ \sigma\ \mathsf{in}\ e'[x \mapsto e] \\
(\mathsf{close}\ \sigma\ \mathsf{in}\ e')[x \mapsto e] &\triangleq \mathsf{close}\ \sigma\ \mathsf{in}\ e'[x \mapsto e] \\
(e'\ \mathsf{then\ unopen}\ \sigma)[x \mapsto e] &\triangleq e'[x \mapsto e]\ \mathsf{then\ unopen}\ \sigma \\
(e'\ \mathsf{then\ unclose}\ \sigma)[x \mapsto e] &\triangleq e'[x \mapsto e]\ \mathsf{then\ unclose}\ \sigma \\
(\mathsf{when}\ \sigma\ \mathsf{then}\ e'\ \mathsf{else}\ e'')[x \mapsto e] &\triangleq \mathsf{when}\ \sigma\ \mathsf{then}\ e'[x \mapsto e]\ \mathsf{else}\ e''[x \mapsto e]
\end{aligned}
$$

As is customary we regard α-equivalent terms as equal. Hence we can freely rename bound variables. In particular this means that we can assume that bound variables are different from other bound variables. We also work with Barendregt's variable convention:

> *"If $M_1, \ldots, M_n$ occur in a certain mathematical context (e.g. definition, proof), then in these terms all bound variables are chosen to be different from the free variables."*[1, page 26]

Definition 3.5 (Free Variables)**.**

$$
\begin{aligned}
\mathsf{FV}(x) &\triangleq x \\
\mathsf{FV}(n) &\triangleq \emptyset \\
\mathsf{FV}(\lambda x.\, e') &\triangleq \mathsf{FV}(e') \backslash \{x\} \\
\mathsf{FV}(e'\ e'') &\triangleq \mathsf{FV}(e') \cup \mathsf{FV}(e'') \\
\mathsf{FV}(()) &\triangleq \emptyset \\
\mathsf{FV}(l) &\triangleq \emptyset \\
\mathsf{FV}(\mathsf{inl}\,(e')) &\triangleq \mathsf{FV}(e') \\
\mathsf{FV}(\mathsf{inr}\,(e')) &\triangleq \mathsf{FV}(e') \\
\mathsf{FV}((e', e'')) &\triangleq \mathsf{FV}(e') \cup \mathsf{FV}(e'') \\
\mathsf{FV}(\mathsf{fst}\,(e')) &\triangleq \mathsf{FV}(e') \\
\mathsf{FV}(\mathsf{snd}\,(e')) &\triangleq \mathsf{FV}(e') \\
\mathsf{FV}(\mathsf{case}\ e'\ \mathsf{of} \mid \mathsf{inl}\,(y) \Rightarrow e_1 \mid \mathsf{inr}\,(y') \Rightarrow e_2) &\triangleq \mathsf{FV}(e') \cup (\mathsf{FV}(e_1) \backslash \{y\}) \cup (\mathsf{FV}(e_2) \backslash \{y'\}) \\
\mathsf{FV}(\mathsf{new}\,(e', \tau)) &\triangleq \mathsf{FV}(e') \\
\mathsf{FV}(!\,e') &\triangleq \mathsf{FV}(e') \\
\mathsf{FV}(e' := e'') &\triangleq \mathsf{FV}(e') \cup \mathsf{FV}(e'') \\
\mathsf{FV}(\mathsf{open}\ \sigma\ \mathsf{in}\ e') &\triangleq \mathsf{FV}(e') \\
\mathsf{FV}(\mathsf{close}\ \sigma\ \mathsf{in}\ e') &\triangleq \mathsf{FV}(e') \\
\mathsf{FV}(e'\ \mathsf{then\ unopen}\ \sigma) &\triangleq \mathsf{FV}(e') \\
\mathsf{FV}(e'\ \mathsf{then\ unclose}\ \sigma) &\triangleq \mathsf{FV}(e') \\
\mathsf{FV}(()\mathsf{when}\ \sigma\ \mathsf{then}\ e'\ \mathsf{else}\ e'') &\triangleq \mathsf{FV}(e') \cup \mathsf{FV}(e'')
\end{aligned}
$$

Lemma 3.1. If $x \notin \mathsf{FV}(e')$, then $e'[x \mapsto e] = e'$.

Proof. By induction on e'.

- $e' = y$: By assumption $x \notin \mathsf{FV}(y)$, so $x \notin \{y\}$, so $x \neq y$. So $[e/x]y = y$.
- $e' = n$. We have $[e/x]n = n$ anyway.
- $e' = \lambda y.e''$. Due to our assumptions about variables we can assume that $y \neq x$. Hence $[e/x](\lambda y.e'') = \lambda\, y.[e/x]e''$. We know $x \notin \mathsf{FV}(\lambda y.\ e'')$. Hence $x \notin \mathsf{FV}(e'') \backslash \{y\}$. Since $x \neq y$, $x \notin \mathsf{FV}(e'')$. By induction $[e/x]e'' = e''$. Hence $[e/x](\lambda y.e'') = \lambda\, y.[e/x]e'' = \lambda y.\ e''$.
- $e' = e_1\ e_2$. Since $x \notin \mathsf{FV}(e_1\ e_2)$ we know $x \notin \mathsf{FV}(e_1)$ and $x \notin \mathsf{FV}(e_2)$. By induction therefore $[e/x]e_1 = e_1$ and $[e/x]e_2 = e_2$. Hence $[e/x](e_1\ e_2) = ([e/x]e_1)\ ([e/x]e_2) = e_1\ e_2$.
- $e' = ()$: $[e/x]() = ()$ anyway.
- $e' = l$: $[e/x]l = l$ anyway.
- $e' = \mathtt{inl}\ e''$: By assumption $x \notin \mathsf{FV}(\mathtt{inl}\ e'')$. Hence $x \notin \mathsf{FV}(e'')$. Hence by induction $[e/x]e'' = e''$. Consequently $[e/x](\mathtt{inl}\ e'') = \mathtt{inl}\ ([e/x]e'') = \mathtt{inl}\ e''$.
- $e' = \mathtt{inr}\ e''$: By assumption $x \notin \mathsf{FV}(\mathtt{inr}\ e'')$. Hence $x \notin \mathsf{FV}(e'')$. Hence by induction $[e/x]e'' = e''$. Consequently $[e/x](\mathtt{inr}\ e'') = \mathtt{inr}\ ([e/x]e'') = \mathtt{inr}\ e''$.
- $e' = (e_1, e_2)$. Since $x \notin \mathsf{FV}((e_1, e_2))$ we know $x \notin \mathsf{FV}(e_1)$ and $x \notin \mathsf{FV}(e_2)$. By induction therefore $[e/x]e_1 = e_1$ and $[e/x]e_2 = e_2$. Hence $[e/x]((e_1, e_2)) = ([e/x]e_1, [e/x]e_2) = (e_1, e_2)$.
- $e' = \mathtt{fst}(e'')$: By assumption $x \notin \mathsf{FV}(\mathtt{fst}(e''))$. Hence $x \notin \mathsf{FV}(e'')$. Hence by induction $[e/x]e'' = e''$. Consequently $[e/x](\mathtt{fst}(e'')) = \mathtt{fst}([e/x]e'') = \mathtt{fst}(e'')$.
- $e' = \mathtt{snd}(e'')$: By assumption $x \notin \mathsf{FV}(\mathtt{snd}(e''))$. Hence $x \notin \mathsf{FV}(e'')$. Hence by induction $[e/x]e'' = e''$. Consequently $[e/x](\mathtt{snd}(e'')) = \mathtt{snd}([e/x]e'') = \mathtt{snd}(e'')$.

- $e' = \mathsf{case}(e_0, y.e_1, y'.e_2)$. Due to our assumptions about variables we can assume that $y \neq x \neq y'$. Hence $[e/x](\mathsf{case}(e_0, y.e_1, y'.e_2)) = \mathsf{case}([e/x]e_0, y.[e/x]e_1, y'.[e/x]e_2)$. We know $x \notin \mathsf{FV}(\mathsf{case}(e_0, y.e_1, y'.e_2))$. Hence $x \notin \mathsf{FV}(e_0) \cup \mathsf{FV}(e_1)\backslash\{y\} \cup \mathsf{FV}(e_2)\backslash\{y'\}$. Since $x \neq y$ and $x \neq y'$, $x \notin \mathsf{FV}(e_0)$,$x \notin \mathsf{FV}(e_1)$,$x \notin \mathsf{FV}(e_2)$. Consequently by induction $[e/x]e_0 = e_0$, $[e/x]e_1 = e_1$, and $[e/x]e_2 = e_2$. Thus $[e/x](\mathsf{case}(e_0, y.e_1, y'.e_2)) = \mathsf{case}([e/x]e_0, y.[e/x]e_1, y'.[e/x]e_2) = \mathsf{case}(e_0, y.e_1, y'.e_2)$.
- $e' = \mathsf{new}(e'', \tau)$. $\mathsf{FV}(\mathsf{new}(e', \tau)) = \mathsf{FV}(e'')$. Hence $x \notin \mathsf{FV}(e'')$. Therefore by induction $[e/x]e'' = e''$. Consequently $[e/x]\mathsf{new}(e', \tau) = \mathsf{new}([e/x]e'', \tau) = \mathsf{new}(e', \tau)$.
- $e' = !e''$: By assumption $x \notin \mathsf{FV}(!e'')$. Hence $x \notin \mathsf{FV}(e'')$. Hence by induction $[e/x](e'') = e''$. Consequently $[e/x](!e'') = !([e/x]e'') = !e''$.
- $e' = e_1 := e_2$. Since $x \notin \mathsf{FV}(e_1 := e_2)$ we know $x \notin \mathsf{FV}(e_1)$ and $x \notin \mathsf{FV}(e_2)$. By induction therefore $[e/x]e_1 = e_1$ and $[e/x]e_2 = e_2$. Hence $[e/x](e_1 := e_2) = ([e/x]e_1) := ([e/x]e_2) = e_1 := e_2$.
- $e' = \mathsf{open}\ \sigma\ \mathsf{in}\ e''$: By assumption $x \notin \mathsf{FV}(\mathsf{open}\ \sigma\ \mathsf{in}\ e'')$. Hence $x \notin \mathsf{FV}(e'')$. Hence by induction $[e/x]e'' = e''$. Consequently $[e/x](\mathsf{open}\ \sigma\ \mathsf{in}\ e'') = \mathsf{open}\ \sigma\ \mathsf{in}\ [e/x]e'' = \mathsf{open}\ \sigma\ \mathsf{in}\ e''$.
- $e' = \mathsf{close}\ \sigma\ \mathsf{in}\ e''$: By assumption $x \notin \mathsf{FV}(\mathsf{close}\ \sigma\ \mathsf{in}\ e'')$. Hence $x \notin \mathsf{FV}(e'')$. Hence by induction $[e/x]e'' = e''$. Consequently $[e/x](\mathsf{close}\ \sigma\ \mathsf{in}\ e'') = \mathsf{close}\ \sigma\ \mathsf{in}\ [e/x]e'' = \mathsf{close}\ \sigma\ \mathsf{in}\ e''$.
- $e' = \mathsf{opened}\ \sigma\ \mathsf{in}\ e''$: By assumption $x \notin \mathsf{FV}(\mathsf{opened}\ \sigma\ \mathsf{in}\ e'')$. Hence $x \notin \mathsf{FV}(e'')$. Hence by induction $[e/x]e'' = e''$. Consequently $[e/x](\mathsf{opened}\ \sigma\ \mathsf{in}\ e'') = \mathsf{opened}\ \sigma\ \mathsf{in}\ [e/x]e'' = \mathsf{opened}\ \sigma\ \mathsf{in}\ e''$.
- $e' = \mathsf{closed}\ \sigma\ \mathsf{in}\ e''$: By assumption $x \notin \mathsf{FV}(\mathsf{closed}\ \sigma\ \mathsf{in}\ e'')$. Hence $x \notin \mathsf{FV}(e'')$. Hence by induction $[e/x]e'' = e''$. Consequently $[e/x](\mathsf{closed}\ \sigma\ \mathsf{in}\ e'') = \mathsf{closed}\ \sigma\ \mathsf{in}\ [e/x]e'' = \mathsf{closed}\ \sigma\ \mathsf{in}\ e''$.
- $e' = \mathsf{when}\ \sigma\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2$. Since $x \notin \mathsf{FV}(\mathsf{when}\ \sigma\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2)$ we know $x \notin \mathsf{FV}(e_1)$ and $x \notin \mathsf{FV}(e_2)$. By induction therefore $[e/x]e_1 = e_1$ and $[e/x]e_2 = e_2$. Hence $[e/x](\mathsf{when}\ \sigma\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2) = \mathsf{when}\ \sigma\ \mathsf{then}\ [e/x]e_1\ \mathsf{else}\ [e/x]e_2 = \mathsf{when}\ \sigma\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2$.

□

3.1 Evaluation and traces

Definition 3.6.

$$\text{Observations} \quad \omega \quad ::= \quad \mathsf{open}(\sigma) \mid \mathsf{close}(\sigma) \mid \mathsf{unopen}(\sigma) \mid \mathsf{unclose}(\sigma) \mid l_\tau(v)$$

where σ is a lock, l is a memory location and $v \in \mathcal{V}$.

The judgement $\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'$ (or in some of the proofs still $e, \Sigma, S \succ e', S', \omega, \Sigma'$) means that expression e evaluates in one step to expression e' in lock-set Σ and state S resulting in state S' and observable output ω. Σ' is the effective lock set at the point of reduction. The state S is a finite partial function from heap locations to pairs of values and types. If for a heap S we have $(l \rightarrowtail (v, \tau)) \in S$ we say that $S(l) = v$. We also define $\mathsf{type}(S, l) = \tau$.

3.1.1 Small step evaluation

NOTE: For the paper we made a change in notation. In most of the proofs we still use a different notation for small-step evaluation, namely $\succ$. So $\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'$ and $e, \Sigma, S \succ e', S', \omega, \Sigma$ mean the same thing. We are working on updating this document with the new notation and apologize for this inconsistency.

$$\frac{\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e'', S'}{\Sigma \vdash e\ e', S \xrightarrow{\omega;\Sigma'} e''\ e', S'}\ \textbf{EAppl} \qquad \frac{\Sigma \vdash e', S \xrightarrow{\omega;\Sigma'} e'', S'}{\Sigma \vdash (\lambda x.e)\ e', S \xrightarrow{\omega;\Sigma'} (\lambda x.e)\ e'', S'}\ \textbf{EAppr}$$

$$\frac{}{\Sigma \vdash (\lambda x.e)\ v, S \xrightarrow{\epsilon;\Sigma} [v/x]e, S}\ \textbf{EAppBeta} \qquad \frac{\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e'', S'}{\Sigma \vdash (e, e'), S \xrightarrow{\omega;\Sigma'} (e'', e'), S'}\ \textbf{EPairl}$$

$$\frac{\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'}{\Sigma \vdash (v, e), S \xrightarrow{\omega;\Sigma'} (v, e'), S'}\ \textbf{EPairr} \qquad \frac{\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'}{\Sigma \vdash \mathsf{fst}(e), S \xrightarrow{\omega;\Sigma'} \mathsf{fst}(e'), S'}\ \textbf{EFst}$$

$$\frac{}{\Sigma \vdash \mathsf{fst}((v, v')), S \xrightarrow{\epsilon;\Sigma} v, S}\ \textbf{EFstBeta} \qquad \frac{\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'}{\Sigma \vdash \mathsf{snd}(e), S \xrightarrow{\omega;\Sigma'} \mathsf{snd}(e'), S'}\ \textbf{ESnd}$$

$$\frac{}{\Sigma \vdash \mathsf{snd}((v, v')), S \xrightarrow{\epsilon;\Sigma} v', S}\ \textbf{ESndBeta} \qquad \frac{\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'}{\Sigma \vdash \mathsf{inl}(e), S \xrightarrow{\omega;\Sigma'} \mathsf{inl}(e'), S'}\ \textbf{EInl}$$

$$\frac{\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'}{\Sigma \vdash \mathsf{inr}(e), S \xrightarrow{\omega;\Sigma'} \mathsf{inr}(e'), S'}\ \textbf{EInr}$$

$$\frac{\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e''', S'}{\Sigma \vdash \mathsf{case}\ e\ \mathsf{of}\ |\ \mathsf{inl}\,(x) \Rightarrow e'\ |\ \mathsf{inr}\,(y) \Rightarrow e'', S \xrightarrow{\omega;\Sigma'} \mathsf{case}\ e'''\ \mathsf{of}\ |\ \mathsf{inl}\,(x) \Rightarrow e'\ |\ \mathsf{inr}\,(y) \Rightarrow e'', S'}\ \textbf{ECase}$$

$$\frac{}{\Sigma \vdash \mathsf{case}\ \mathsf{inl}(v)\ \mathsf{of}\ |\ \mathsf{inl}\,(x) \Rightarrow e'\ |\ \mathsf{inr}\,(y) \Rightarrow e'', S \xrightarrow{\epsilon;\Sigma} [v/x]e', S}\ \textbf{ECasel}$$

$$\frac{}{\Sigma \vdash \mathsf{case}\ \mathsf{inr}(v)\ \mathsf{of}\ |\ \mathsf{inl}\,(x) \Rightarrow e'\ |\ \mathsf{inr}\,(y) \Rightarrow e'', S \xrightarrow{\epsilon;\Sigma} [v/x]e'', S}\ \textbf{ECaser}$$

$$\frac{\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'}{\Sigma \vdash \mathsf{new}(e, \tau), S \xrightarrow{\omega;\Sigma'} \mathsf{new}(e', \tau), S'}\ \textbf{ENew} \qquad \frac{l \notin \mathrm{dom}(S)}{\Sigma \vdash \mathsf{new}(v, \tau), S \xrightarrow{l_\tau(v);\Sigma} l, S \cup \{l \rightarrowtail (v, \tau)\}}\ \textbf{ENewBeta}$$

$$\frac{\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'}{\Sigma \vdash\, !\, e, S \xrightarrow{\omega;\Sigma'} !\, e', S'}\ \textbf{EDeref} \qquad \frac{(l \rightarrowtail (v, \tau)) \in S}{\Sigma \vdash\, !\, l, S \xrightarrow{\epsilon;\Sigma} v, S}\ \textbf{EDerefBeta}$$

$$\frac{\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e'', S'}{\Sigma \vdash e := e', S \xrightarrow{\omega;\Sigma'} e'' := e', S'}\ \textbf{Eassignl} \qquad \frac{\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'}{\Sigma \vdash l := e, S \xrightarrow{\omega;\Sigma'} l := e', S'}\ \textbf{Eassignr}$$

$$\frac{l \in \mathrm{dom}(S) \qquad \mathrm{type}(S, l) = \tau}{\Sigma \vdash l := v, S \xrightarrow{l_\tau(v);\Sigma} (), S[l \rightarrowtail (v, \tau)]}\ \textbf{Eassign}$$

$$\frac{}{\Sigma \vdash \mathsf{open}\ \sigma\ \mathsf{in}\ e, S \xrightarrow{\mathsf{open}(\sigma);\Sigma} e\ \mathsf{then\ unopen}\ \sigma, S}\ \textbf{Eopen}$$

$$\frac{\Sigma \cup \{\sigma\} \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'}{\Sigma \vdash e\ \mathsf{then\ unopen}\ \sigma, S \xrightarrow{\omega;\Sigma'} e'\ \mathsf{then\ unopen}\ \sigma, S'}\ \textbf{Eopened}$$

$$\frac{}{\Sigma \vdash v\ \mathsf{then\ unopen}\ \sigma, S \xrightarrow{\mathsf{unopen}(\sigma);\Sigma} v, S}\ \textbf{EopenedBeta}$$

$$\frac{}{\Sigma \vdash \mathsf{close}\ \sigma\ \mathsf{in}\ e, S \xrightarrow{\mathsf{close}(\sigma);\Sigma} e\ \mathsf{then\ unclose}\ \sigma, S}\ \textbf{Eclose}$$

$$\frac{\Sigma \setminus \{\sigma\} \vdash e,\ S \xrightarrow{\omega;\Sigma'} e',\ S'}{\Sigma \vdash e \text{ then unclose } \sigma,\ S \xrightarrow{\omega;\Sigma'} e' \text{ then unclose } \sigma,\ S'}\ \textbf{EclosedBeta}$$

$$\frac{}{\Sigma \vdash v \text{ then unclose } \sigma,\ S \xrightarrow{\text{unclose}(\sigma);\Sigma} v,\ S}$$

$$\frac{\sigma \in \Sigma \qquad \Sigma \vdash e,\ S \xrightarrow{\omega;\Sigma'} e'',\ S'}{\Sigma \vdash \text{when } \sigma \text{ then } e \text{ else } e',\ S \xrightarrow{\omega;\Sigma'} \text{when } \sigma \text{ then } e'' \text{ else } e',\ S'}\ \textbf{EWhenOpen}$$

$$\frac{\sigma \notin \Sigma \qquad \Sigma \vdash e',\ S \xrightarrow{\omega;\Sigma'} e'',\ S'}{\Sigma \vdash \text{when } \sigma \text{ then } e \text{ else } e',\ S \xrightarrow{\omega;\Sigma'} \text{when } \sigma \text{ then } e \text{ else } e'',\ S'}\ \textbf{EWhenClosed}$$

$$\frac{\sigma \in \Sigma}{\Sigma \vdash \text{when } \sigma \text{ then } v \text{ else } e',\ S \xrightarrow{\epsilon;\Sigma} v,\ S}\ \textbf{EWhenOpenBeta}$$

$$\frac{\sigma \notin \Sigma}{\Sigma \vdash \text{when } \sigma \text{ then } e \text{ else } v,\ S \xrightarrow{\epsilon;\Sigma} v,\ S}\ \textbf{EWhenClosedBeta}$$

3.2 Typing

3.2.1 Subtyping

Subtyping defined as in [5].

$$\frac{p \sqsubseteq p' \qquad A <: B}{A^p <: B^{p'}}\ \textbf{sub-policy} \qquad \frac{}{\text{ref } \tau <: \text{ref } \tau}\ \textbf{sub-ref} \qquad \frac{\tau_0 <: \tau_1 \qquad \tau_2 <: \tau_3}{\tau_0 \times \tau_2 <: \tau_1 \times \tau_3}\ \textbf{sub-prod}$$

$$\frac{\tau_0 <: \tau_1 \qquad \tau_2 <: \tau_3}{\tau_0 + \tau_2 <: \tau_1 + \tau_3}\ \textbf{sub-sum} \qquad \frac{\tau_0 <: \tau_1 \qquad \tau_2 <: \tau_3 \qquad p' \sqsubseteq p \qquad \Sigma \subseteq \Sigma'}{\tau_1 \xrightarrow{\Sigma,p} \tau_2 <: \tau_0 \xrightarrow{\Sigma',p'} \tau_3}\ \textbf{sub-arrow}$$

$$\frac{}{\text{unit} <: \text{unit}}\ \textbf{sub-unit} \qquad \frac{}{\mathbb{N} <: \mathbb{N}}\ \textbf{sub-nat}$$

We use state environments $\theta, \theta', \theta_0$ etc. to keep track of the heap. They are partial functions from heap locations to (annotated) types.

3.2.2 Typing

The typing judgements have the form $\Gamma; \Sigma; \theta \vdash_{pc} e : \tau$ which means that in environment Γ e has policy annotated type τ if at least the locks in Σ are open and locations have the types specified by θ. In this case the policy pc is an upper bound on the write effect of e.

NOTE:In the paper we do not have the subtyping premises in the case rule. The rule presented here can be derived from the rule in the paper using the subtyping rules and vice versa. All the proofs use the version presented here.

$$\frac{}{\Gamma, x : \tau, \Gamma'; \Sigma; \theta \vdash_{pc} x : \tau}\ \textbf{var} \qquad \frac{n \in \mathbb{N}}{\Gamma; \Sigma; \theta \vdash_{pc} n : \mathbb{N}^{\perp}}\ \textbf{nat} \qquad \frac{\Gamma; \Sigma \cup \{\sigma\}; \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq \text{pol}(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} \text{open } \sigma \text{ in } e : \tau}\ \textbf{open}$$

$$\frac{\Gamma; \Sigma \cup \{\sigma\}; \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq \text{pol}(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} e \text{ then unopen } \sigma : \tau}\ \textbf{opened} \qquad \frac{\Gamma, x : \tau_1; \Sigma'; \theta \vdash_{pc'} e : \tau_2}{\Gamma; \Sigma; \theta \vdash_{pc} \lambda x.\, e : (\tau_1 \xrightarrow{\Sigma', pc'} \tau_2)^{\perp}}\ \lambda$$

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e : (\text{ref } \tau)^p \qquad p \sqsubseteq \tau' \qquad \tau <: \tau'}{\Gamma; \Sigma; \theta \vdash_{pc} !\, e : \tau'}\ \textbf{deref} \qquad \frac{\Gamma; \Sigma; \theta \vdash_{pc} e_1 : \tau_1 \qquad \Gamma; \Sigma; \theta \vdash_{pc} e_2 : \tau_2}{\Gamma; \Sigma; \theta \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^{\perp}}\ \textbf{prod}$$

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\Sigma', pc'} \tau_2)^p \quad \Gamma;\Sigma;\theta \vdash_{pc} e_2 : \tau_1' \quad p \sqsubseteq \tau_2 \quad pc \sqcup p \sqsubseteq pc' \quad \tau_1' <: \tau_1 \quad \Sigma \supseteq \Sigma'}{\Gamma;\Sigma;\theta \vdash_{pc} e_1\ e_2 : \tau_2}\ \textbf{app}$$

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e : (\tau_1 \times \tau_2)^p \quad p \sqsubseteq \tau_1}{\Gamma;\Sigma;\theta \vdash_{pc} \mathsf{fst}\,(e) : \tau_1}\ \textbf{fst} \qquad \frac{\Gamma;\Sigma;\theta \vdash_{pc} e : (\tau_1 \times \tau_2)^p \quad p \sqsubseteq \tau_2}{\Gamma;\Sigma;\theta \vdash_{pc} \mathsf{snd}\,(e) : \tau_2}\ \textbf{snd}$$

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e : \tau_1}{\Gamma;\Sigma;\theta \vdash_{pc} \mathsf{inl}\,(e) : (\tau_1 + \tau_2)^\perp}\ \textbf{inl} \qquad \frac{\Gamma;\Sigma;\theta \vdash_{pc} e : \tau_2}{\Gamma;\Sigma;\theta \vdash_{pc} \mathsf{inr}\,(e) : (\tau_1 + \tau_2)^\perp}\ \textbf{inr}$$

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e : (\tau_1 + \tau_2)^p \quad p \sqsubseteq \tau \quad \Gamma, x : \tau_1';\Sigma;\theta \vdash_{pc \sqcup p} e_1 : \tau \quad \Gamma, y : \tau_2';\Sigma;\theta \vdash_{pc \sqcup p} e_2 : \tau \quad \tau_1 <: \tau_1' \quad \tau_2 <: \tau_2'}{\Gamma;\Sigma;\theta \vdash_{pc} \mathsf{case}\ e\ \mathsf{of}\ |\,\mathsf{inl}\,(x) \Rightarrow e_1\ |\,\mathsf{inr}\,(y) \Rightarrow e_2 : \tau}\ \textbf{case}$$

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e : \tau' \quad pc \sqsubseteq \tau \quad \tau'(\Sigma) <: \tau}{\Gamma;\Sigma;\theta \vdash_{pc} \mathsf{new}\,(e, \tau) : (\mathsf{ref}\ \tau)^\perp}\ \textbf{new} \qquad \frac{\theta(l) = \tau}{\Gamma;\Sigma;\theta \vdash_{pc} l : (\mathsf{ref}\ \tau)^\perp}\ \textbf{loc}$$

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc'} e : \tau' \quad pc \sqsubseteq pc' \quad \tau' <: \tau}{\Gamma;\Sigma;\theta \vdash_{pc} e : \tau}\ \textbf{sub} \qquad \frac{\Gamma;\Sigma\backslash\{\sigma\};\theta \vdash_{pc} e : \tau \quad pc \sqsubseteq pol(\sigma)}{\Gamma;\Sigma;\theta \vdash_{pc} e\ \mathsf{then\ unclose}\ \sigma : \tau}\ \textbf{closed}$$

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e : (\mathsf{ref}\ \tau')^p \quad \tau(\Sigma) <: \tau' \quad \Gamma;\Sigma;\theta \vdash_{pc} e' : \tau \quad pc \sqcup p \sqsubseteq \tau'}{\Gamma;\Sigma;\theta \vdash_{pc} e := e' : \mathsf{unit}^\perp}\ \textbf{assign}$$

$$\frac{}{\Gamma;\Sigma;\theta \vdash_{pc} () : \mathsf{unit}^\perp}\ \textbf{unit} \qquad \frac{\Gamma;\Sigma\backslash\{\sigma\};\theta \vdash_{pc} e : \tau \quad pc \sqsubseteq pol(\sigma)}{\Gamma;\Sigma;\theta \vdash_{pc} \mathsf{close}\ \sigma\ \mathsf{in}\ e : \tau}\ \textbf{close}$$

$$\frac{\Gamma;\Sigma \cup \{\sigma\};\theta \vdash_{pc \sqcup pol(\sigma)} e_1 : \tau \quad \Gamma;\Sigma;\theta \vdash_{pc \sqcup pol(\sigma)} e_2 : \tau \quad pol(\sigma) \sqsubseteq \tau}{\Gamma;\Sigma;\theta \vdash_{pc} \mathsf{when}\ \sigma\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2 : \tau}\ \textbf{when}$$

4 Properties of the policy ordering

Note that in this section we are using the full *paralocks* policy language including actor quantification and parameterised locks.

Lemma 4.1. The ordering $\sqsubseteq$ on policies is reflexive and transitive.

Proof.

reflexivity: Let p be a policy and $c \in p$. Then also $c \in p$ and $c \sqsubseteq c$ because the ordering $\sqsubseteq$ in clauses is reflexive by definition.

transitivity: Let p_0, p_1, p_2 be policies such that $p_0 \sqsubseteq p_1$ and $p_1 \sqsubseteq p_2$. We have to show $p_0 \sqsubseteq p_2$.

Let $c_2 \in p_2$. By assumption there is a $c_1 \in p_1$ such that $c_1 \sqsubseteq c_2$. By assumption there is also a $c_0 \in p_0$ such that $c_0 \sqsubseteq c_1$. By definition of the ordering $\sqsubseteq$ on clauses $\sqsubseteq$ is transitive. Hence $c_0 \sqsubseteq c_2$. Hence there is a clause c in p_0, namely c_0, such that $c \sqsubseteq c_2$. □

Lemma 4.2. $\forall A, p, p'.A^{p'} <: A^p \leftrightarrow p' \sqsubseteq p$.

Proof.

$\rightarrow$: Let $A^{p'} \leqslant: A^p$. This must have been derived using **sub-policy**. Hence $p' \sqsubseteq p$.

$\leftarrow$: Let $p' \leqslant p$. We have $A \leqslant: A$ by Lemma 5.1. So

$$\frac{p' \sqsubseteq p \quad A \leqslant: A}{A^{p'} \leqslant: A^p}\ \textbf{sub-policy}$$

□

Lemma 4.3. $\forall p, \Sigma, \Sigma'.\Sigma' \supseteq \Sigma \rightarrow p(\Sigma') \sqsubseteq p(\Sigma)$.

Proof. Let $\mathfrak{p}$ be a policy and Σ, Σ' lock-sets such that $\Sigma' \supseteq \Sigma$. We want to show $\mathfrak{p}(\Sigma') \sqsubseteq \mathfrak{p}(\Sigma)$. Since by definition $\mathfrak{p}(\Sigma') = \bigcup_{\mathfrak{c} \in \mathfrak{p}} \{\mathfrak{c} \cdot \Sigma'\}$ and $\mathfrak{p}(\Sigma) = \bigcup_{\mathfrak{c} \in \mathfrak{p}} \{\mathfrak{c} \cdot \Sigma\}$ it suffices to show

$$\mathfrak{c} \cdot \Sigma' \sqsubseteq \mathfrak{c} \cdot \Sigma$$

for all clauses $\mathfrak{c}$.

Let $\mathfrak{c}$ be a clause. This means $\mathfrak{c}$ is of the form $\forall \vec{x}.\Delta \Rightarrow \mathfrak{b}$. Then $\mathfrak{c} \cdot \Sigma$ only contains clauses of the form $\forall \vec{x}.\Delta_2(\theta) \Rightarrow \mathfrak{b}(\theta)$, were Δ_2 is a lockset such that there is a lockset Δ_1 such that $\Delta = \Delta_1 \cup \Delta_2$ and there is a $\Sigma'' \subseteq \Sigma$ such that Δ_1 matches Σ'' with θ.

Let $\forall \vec{x}.\Delta_2(\theta) \Rightarrow \mathfrak{b}(\theta) \in \mathfrak{c} \cdot \Sigma$ and let Σ'', Δ_1 be such that they fulfil the condition above. In that case $\Sigma'' \subseteq \Sigma'$ because $\Sigma' \supseteq \Sigma$ and still $\Delta = \Delta_1 \cup \Delta_2$ and Δ_1 matches Σ'' with θ. Hence $\forall \vec{x}.\Delta_2(\theta) \Rightarrow \mathfrak{b}(\theta) \in \mathfrak{c} \cdot \Sigma'$. This suffices to show $\mathfrak{c} \cdot \Sigma' \sqsubseteq \mathfrak{c} \cdot \Sigma$ because for all clauses $\mathfrak{c}$ we have $\mathfrak{c} \sqsubseteq \mathfrak{c}$. □

Lemma 4.4. For all policies $\mathfrak{p}$ we have $\mathfrak{p}(\emptyset) = \mathfrak{p}$.

Proof. First we show that for any clause $\mathfrak{c}$ we have $\mathfrak{c} \cdot \emptyset = \mathfrak{c}$. By definition of clauses $\mathfrak{c}$ has the form $\forall \vec{x}.\Delta \Rightarrow \mathfrak{b}$. In this case $\mathfrak{c} \cdot \emptyset = \{\forall \vec{x}.\Delta_2(\theta) \Rightarrow \mathfrak{b}(\theta) \mid \Delta = \Delta_1 \cup \Delta_2 \wedge \Sigma_1 \subseteq \emptyset \wedge \Delta_1 \text{ matches } \Sigma_1 \text{ with } \theta\}$.

Every subset of the empty set is the empty set, so the set simplifies to
$\{\forall \vec{x}.\Delta_2(\theta) \Rightarrow \mathfrak{b}(\theta) \mid \Delta = \Delta_1 \cup \Delta_2 \wedge \Delta_1 \text{ matches } \emptyset \text{ with } \theta\}$

For a set Δ_1 to match $\emptyset$ with a substitution θ among other things $\Delta_1(\theta) = \emptyset$ must be true. This is only the case if $\Delta_1 = \emptyset$. On the other hand we also need θ to be defined on exactly the free variables of Δ_1. When $\Delta_1 = \emptyset$ this is only the case of θ is the empty substitution. Hence the set simplifies to $\{\forall \vec{x}.\Delta_2 \Rightarrow \mathfrak{b} \mid \Delta = \emptyset \cup \Delta_2\}$.

Since for any set Δ_2 we have $\emptyset \cup \Delta_2 = \Delta_2$ this simplifies to $\{\forall \vec{x}.\Delta_2 \Rightarrow \mathfrak{b} \mid \Delta = \Delta_2\}$. Using the equality we get $\{\forall \vec{x}.\Delta \Rightarrow \mathfrak{b}\}$ which is exactly $\mathfrak{c}$.

Now we show the main goal: $\mathfrak{p}(\emptyset) = \bigcup_{\mathfrak{c} \in \mathfrak{p}} (\mathfrak{c} \cdot \emptyset) = \bigcup_{\mathfrak{c} \in \mathfrak{p}} (\mathfrak{c}) = \mathfrak{p}$. □

Corollary 4.5. $\forall \Sigma.\ \mathfrak{p}(\Sigma) \sqsubseteq \mathfrak{p}$.

Proof. Let Σ be a set of locks. By Lemma 4.4 it suffices to show $\mathfrak{p}(\Sigma) \sqsubseteq \mathfrak{p}(\emptyset)$. Since $\emptyset \subseteq \Sigma$ we have $\mathfrak{p}(\Sigma) \sqsubseteq \mathfrak{p}(\emptyset)$ by Lemma 4.3. □

Lemma 4.6. For all policies $\mathfrak{p}, \mathfrak{q}$, the policy $\mathfrak{p} \sqcup \mathfrak{q}$ is an upper bound on $\mathfrak{p}$ and $\mathfrak{q}$, respectively. And $\mathfrak{p} \sqcap \mathfrak{q}$ is the greatest lower bound on $\mathfrak{p}$ and $\mathfrak{q}$.

Proof. $\sqcap$: Let $\mathfrak{p}, \mathfrak{q}$ be paralocks policies. We show

- $\mathfrak{p} \sqcap \mathfrak{q} \sqsubseteq \mathfrak{p}$ and $\mathfrak{p} \sqcap \mathfrak{q} \sqsubseteq \mathfrak{q}$
- $\forall \mathfrak{r} : \mathfrak{r} \sqsubseteq \mathfrak{p} \wedge \mathfrak{r} \sqsubseteq \mathfrak{q} \to \mathfrak{r} \sqsubseteq \mathfrak{p} \sqcap \mathfrak{q}$.

$\mathfrak{p} \sqcap \mathfrak{q} = \mathfrak{p} \cup \mathfrak{q}$. Hence forall $\mathfrak{c} \in \mathfrak{p}$ also $\mathfrak{c} \in \mathfrak{p} \cup \mathfrak{q} = \mathfrak{p} \sqcap \mathfrak{q}$. Similarly forall $\mathfrak{c} \in \mathfrak{q}$ also $\mathfrak{c} \in \mathfrak{p} \cup \mathfrak{q} = \mathfrak{p} \sqcap \mathfrak{q}$. Hence $\mathfrak{p} \sqcap \mathfrak{q} \sqsubseteq \mathfrak{p}$ and $\mathfrak{p} \sqcap \mathfrak{q} \sqsubseteq \mathfrak{q}$ as for all clauses $\mathfrak{c}$ we have $\mathfrak{c} \sqsubseteq \mathfrak{c}$.

Let $\mathfrak{r}$ such that $\mathfrak{r} \sqsubseteq \mathfrak{p} \wedge \mathfrak{r} \sqsubseteq \mathfrak{q}$. Let $\mathfrak{c} \in \mathfrak{p} \cup \mathfrak{q} = \mathfrak{p} \sqcap \mathfrak{q}$. Then $\mathfrak{c} \in \mathfrak{p}$ or $\mathfrak{c} \in \mathfrak{q}$. W.l.o.g. assume $\mathfrak{c} \in \mathfrak{p}$. Then because $\mathfrak{r} \sqsubseteq \mathfrak{p}$ there is a clause $\mathfrak{c}' \in \mathfrak{r}$, such that $\mathfrak{c}' \sqsubseteq \mathfrak{c}$. Hence $\mathfrak{r} \sqsubseteq \mathfrak{p} \sqcap \mathfrak{q}$.

$\sqcup$: Let $\mathfrak{p}, \mathfrak{q}$ be paralocks policies. We show

- $\mathfrak{p} \sqcup \mathfrak{q} \sqsupseteq \mathfrak{p}$ and $\mathfrak{p} \sqcup \mathfrak{q} \sqsupseteq \mathfrak{q}$

Let $\mathfrak{c} \in \mathfrak{p} \sqcup \mathfrak{q}$. There are four possibilities:

1. $\mathfrak{c} = \forall \mathfrak{x}, \vec{\mathfrak{y}_\mathfrak{p}}, \vec{\mathfrak{y}_\mathfrak{q}}.\Sigma_\mathfrak{p} \cup \Sigma_\mathfrak{q} \Rightarrow \mathfrak{x}$, where $\forall \mathfrak{x}, \vec{\mathfrak{y}_\mathfrak{p}}.\Sigma_\mathfrak{p} \Rightarrow \mathfrak{x} \in \mathfrak{p}$ and $\forall \mathfrak{x}, \vec{\mathfrak{y}_\mathfrak{q}}.\Sigma_\mathfrak{q} \Rightarrow \mathfrak{x} \in \mathfrak{q}$ and $\vec{\mathfrak{y}_\mathfrak{p}}$ and $\vec{\mathfrak{y}_\mathfrak{q}}$ are disjoint sets of actor variables.
2. $\mathfrak{c} = \forall \vec{\mathfrak{y}_\mathfrak{p}}, \vec{\mathfrak{y}_\mathfrak{q}}.\Sigma_\mathfrak{p} \cup \Sigma_\mathfrak{q} \Rightarrow \mathfrak{a}$, where $\forall \vec{\mathfrak{y}_\mathfrak{p}}.\Sigma_\mathfrak{p} \Rightarrow \mathfrak{a} \in \mathfrak{p}$ and $\forall \vec{\mathfrak{y}_\mathfrak{q}}.\Sigma_\mathfrak{q} \Rightarrow \mathfrak{a} \in \mathfrak{q}$ and $\vec{\mathfrak{y}_\mathfrak{p}}$ and $\vec{\mathfrak{y}_\mathfrak{q}}$ are disjoint sets of actor variables and $\mathfrak{a}$ is free.
3. $\mathfrak{c} = \forall \vec{\mathfrak{y}_\mathfrak{p}}, \vec{\mathfrak{y}_\mathfrak{q}}.\Sigma_\mathfrak{p} \cup \Sigma_\mathfrak{q}[\mathfrak{x} := \mathfrak{a}] \Rightarrow \mathfrak{x}$, where $\forall \vec{\mathfrak{y}_\mathfrak{p}}.\Sigma_\mathfrak{p} \Rightarrow \mathfrak{a} \in \mathfrak{p}$ and $\forall \mathfrak{x}, \vec{\mathfrak{y}_\mathfrak{q}}.\Sigma_\mathfrak{q} \Rightarrow \mathfrak{x} \in \mathfrak{q}$ and $\vec{\mathfrak{y}_\mathfrak{p}}$ and $\vec{\mathfrak{y}_\mathfrak{q}}$ are disjoint sets of actor variables and $\mathfrak{a}$ is free.
4. $\mathfrak{c} = \forall \vec{\mathfrak{y}_\mathfrak{p}}, \vec{\mathfrak{y}_\mathfrak{q}}.\Sigma_\mathfrak{q} \cup \Sigma_\mathfrak{p}[\mathfrak{x} := \mathfrak{a}] \Rightarrow \mathfrak{x}$, where $\forall \vec{\mathfrak{y}_\mathfrak{q}}.\Sigma_\mathfrak{q} \Rightarrow \mathfrak{a} \in \mathfrak{q}$ and $\forall \mathfrak{x}, \vec{\mathfrak{y}_\mathfrak{p}}.\Sigma_\mathfrak{p} \Rightarrow \mathfrak{x} \in \mathfrak{p}$ and $\vec{\mathfrak{y}_\mathfrak{p}}$ and $\vec{\mathfrak{y}_\mathfrak{q}}$ are disjoint sets of actor variables and $\mathfrak{a}$ is free.

We will look at all of these cases separately.

1. $\forall x, \vec{y_p}, \vec{y_q}.\Sigma_p \Rightarrow x \sqsubseteq \forall x, \vec{y_p}, \vec{y_q}.\Sigma_p \cup \Sigma_q \Rightarrow x = c$ because $\Sigma_p \sqsubseteq \Sigma_p \cup \Sigma_q$. Because the variables from $\vec{y_q}$ do not appear in Σ_p, we also have $\forall x, \vec{y_p}.\Sigma_p \Rightarrow x \sqsubseteq \forall x, \vec{y_p}, \vec{y_q}.\Sigma_p \Rightarrow x$. Hence by transitivity $\forall x, \vec{y_p}.\Sigma_p \Rightarrow x \sqsubseteq c$. With the corresponing argument we get $\forall x, \vec{y_q}.\Sigma_q \Rightarrow x \sqsubseteq c$.

2. $\forall \vec{y_p}, \vec{y_q}.\Sigma_p \Rightarrow a \sqsubseteq \forall \vec{y_p}, \vec{y_q}.\Sigma_p \cup \Sigma_q \Rightarrow a = c$ because $\Sigma_p \sqsubseteq \Sigma_p \cup \Sigma_q$. Because the variables from $\vec{y_q}$ do not appear in Σ_p, we also have $\forall \vec{y_p}.\Sigma_p \Rightarrow a \sqsubseteq \forall \vec{y_p}, \vec{y_q}.\Sigma_p \Rightarrow a$. Hence by transitivity $\forall \vec{y_p}.\Sigma_p \Rightarrow a \sqsubseteq c$. With the corresponing argument we get $\forall \vec{y_q}.\Sigma_q \Rightarrow a \sqsubseteq c$.

3. We get $\forall \vec{y_p}.\Sigma_p \Rightarrow a \sqsubseteq c$ as in the previous case.

   We know $\forall x, \vec{y_q}.\Sigma_q \Rightarrow x \sqsubseteq \forall \vec{y_q}.\Sigma_q[x := a] \Rightarrow a$. We also know $\forall \vec{y_q}\Sigma_q[x := a] \Rightarrow a \sqsubseteq \forall \vec{y_p}, \vec{y_q}.\Sigma_q[x := a] \Rightarrow a$ because the variables of $\vec{y_p}$ do not appear in $\Sigma_q[x := a]$. Additionally $\forall \vec{y_p}, \vec{y_q}.\Sigma_q[x := a] \Rightarrow a \sqsubseteq \forall \vec{y_p}, \vec{y_q}.\Sigma_p \cup \Sigma_q[x := a] \Rightarrow a = c$ because $\Sigma_q[x := a] \subseteq \Sigma_p \cup \Sigma_q[x := a]$. We get $\forall x, \vec{y_q}.\Sigma_q \Rightarrow x \sqsubseteq c$ by transitivity of $\sqsubseteq$.

4. Symmetric to the previous case.

□

Lemma 4.7. Whenever $c \sqsubseteq c'$ and $c = \forall \vec{x}.\Sigma \Rightarrow a$ where $a \notin \vec{x}$ and $c' = \forall \vec{y}.\Sigma' \Rightarrow b$, then $a = b$ and $b \notin \vec{y}$.

Proof. By induction on the derivation of $c \sqsubset^* c'$.
Let $c \sqsubseteq c'$. Then $c \sqsubset^* c'$. We do induction in the derivation of $c \sqsubset^* c'$.

refl-*: In this case $c = c'$ and therefore trivially $a = b$.

trans-*: In this case there is a y such that $c \sqsubset y$ and $y \sqsubset^* c'$. We show that for $y = \forall \vec{z}.\Sigma'' \Rightarrow d$, $a = d$ by case distinction.

  refl: In this case clearly $a = d$, as renaming of bound variables in c does not change the free variable a. As no new bindings appear $a = d$ is free in y as well.

  - $a = d$ because otherwise the rule is not applicable. d is free because the quantifiers are the same in c and y.
  - Because a is free in c the substitution of a_0 does not change a. d is not bound as no new quantifiers appear in y.

  By induction we now get $b = d$. By transitivity $a = b$.

□

Lemma 4.8. Let $\vec{y} = y_0, \ldots, y_n$ and $\vec{x}$ be vectors of actor variables such that $\vec{y} \cap \vec{x} = \emptyset$ and Σ be a lock-set such that all the free variables of Σ are disjoint from the variables in $\vec{y}$. Then $c'_0 = \forall \vec{y_p}, \vec{x_p}.\Sigma \cup \Sigma[x_0 := y_0, x_1 := y_1, \ldots, x_n := y_n] \Rightarrow a \sqsubseteq \forall \vec{x}.\Sigma \Rightarrow a = c_o$ if $a \notin \vec{x}$ and $c'_1 = \forall x, \vec{y_p}, \vec{x_p}.\Sigma \cup \Sigma[x_0 := y_0, x_1 := y_1, \ldots, x_n := y_n] \Rightarrow x \sqsubseteq \forall \vec{x}.\Sigma \Rightarrow x = c_1$.

Proof. By induction on n.

If $n = 0$, then $c_0 = \Sigma \Rightarrow a$ and $c'_0 = \Sigma \cup \Sigma \Rightarrow a = \Sigma \Rightarrow a$. As $c_0 = c'_0$ clearly $c'_0 \sqsubseteq c_0$. $c_1 = \forall x.\Sigma \Rightarrow x$ and $c'_1 = \forall x.\Sigma \cup \Sigma \Rightarrow x = \forall x.\Sigma \Rightarrow x$. As $c_1 = c'_1$ clearly $c'_1 \sqsubseteq c_1$.

Case $n+1$: Then $c'_0 = \forall y_0, y_1, \ldots, y_n, \vec{x}.\Sigma \cup \Sigma[x_0 := y_0, x_1 := y_1, \ldots, x_n := y_n] \Rightarrow a \sqsubseteq \forall y_1, \ldots, y_n, \vec{x}.\Sigma \cup (\Sigma[x_0 := y_0, x_1 := y_1, \ldots, x_n := y_n] \Rightarrow a)[y_0 := x_0] = \forall y_1, \ldots, y_n, \vec{x}.\Sigma \cup \Sigma[x_1 := y_1, \ldots, x_n := y_n] \Rightarrow a$ as $a \neq y_0$ and the free variables of sigma are disjoint from y_0.
By induction $\forall y_1, \ldots, y_n, \vec{x}.\Sigma \cup \Sigma[x_1 := y_1, \ldots, x_n := y_n] \Rightarrow a \sqsubseteq \forall \vec{x}.\Sigma \Rightarrow a = c_0$. The case for c'_1 and c_1 works analogously. □

Definition 4.1. For two clauses c, c', we define $c \sqcup c'$ as the single element of $\{c\} \sqcup \{c'\}$ if such an element exists. If it does not exist $c \sqcup c'$ is undefined.

Lemma 4.9 (Monotonicity)**.** $\sqcup$ is monotone with regard to the ordering $\sqsubseteq$ on both clauses and policies. That is for all clauses c_0, c_1, c with $c_0 \sqsubseteq c_1$ we have $c_0 \sqcup c \sqsubseteq c_1 \sqcup c$ if $c_1 \sqcup c$ exists and for all polcies p, q, r with $p \sqsubseteq r$ we have $p \sqcup r \sqsubseteq q \sqcup r$.
$\sqcap$ is monotone with regard to the ordering $\sqsubseteq$ on policies, i.e. $\forall p, q.p \sqsubseteq q \rightarrow \forall r.p \sqcap r \sqsubseteq q \sqcap r$.

Proof. We first show this for the ordering $\sqsubset$ on clauses. That is we show for all c_0, c_1, c with $c_0 \sqsubset c_1$ that $c_0 \sqcup c \sqsubseteq c_1 \sqcup c$ if $c_1 \sqcup c$ exists.

We do case analysis on $c_0 \sqsubset c_1$.

refl: In this case $c_0 = c_1$ up to deletion of unused quantifiers, α-renaming and reordering of quantifiers. In particular this means that when $c_1 \sqcup c$ exists that $c_0 \sqcup c$ also exists and that these two clauses can be made to be equal by the same deletion of unused quantifiers, α-renaming and reordering of quantifiers. Hence $c_0 \sqcup c \sqsubseteq c_1 \sqcup c$.

subset: In this case c_0 has the form $\forall \vec{x}.\Sigma_0 \Rightarrow b$ and c_1 has the form $\forall \vec{x}.\Sigma_1 \Rightarrow b$ and $\Sigma_0 \subseteq \Sigma_1$. We do case analysis on the form of c

- $c = \forall \vec{x_c}.\Sigma \Rightarrow b$. Then $c_0 \sqcup c = \forall \vec{x}, \vec{x_c}.\Sigma_0 \cup \Sigma \Rightarrow b$ and $c_1 \sqcup c = \forall \vec{x}, \vec{x_c}.\Sigma_1 \cup \Sigma \Rightarrow b$. Because $\Sigma_0 \subseteq \Sigma_1$ also $\Sigma_0 \cup \Sigma \subseteq \Sigma_1 \cup \Sigma$. Hence by **subset** $c_0 \sqcup c \sqsubset c_1 \sqcup c$.
- $c = \forall x, \vec{x_c}.\Sigma \Rightarrow x$ and $b \notin \vec{x}$. Then $c_0 \sqcup c = \forall \vec{x}, \vec{x_c}.\Sigma_0 \cup \Sigma[x := b] \Rightarrow b$ and $c_1 \sqcup c = \forall \vec{x}, \vec{x_c}.\Sigma_1 \cup \Sigma[x := b] \Rightarrow b$. Because $\Sigma_0 \subseteq \Sigma_1$ also $\Sigma_0 \cup \Sigma[x := b] \subseteq \Sigma_1 \cup \Sigma[x := b]$. Hence by **subset** $c_0 \sqcup c \sqsubset c_1 \sqcup c$.
- $c = \forall \vec{x_c}.\Sigma \Rightarrow d$ and $d \notin \vec{x_c}$ and $\vec{x} = b, \vec{x'}$. Then $c_0 \sqcup c = \forall \vec{x'}, \vec{x_c}.\Sigma_0[b := d] \cup \Sigma \Rightarrow d$ and $c_1 \sqcup c = \forall \vec{x'}, \vec{x_c}.\Sigma_1[b := d] \cup \Sigma \Rightarrow d$. Because $\Sigma_0 \subseteq \Sigma_1$ also $\Sigma_0[b := d] \cup \Sigma \subseteq \Sigma_1[b := d] \cup \Sigma$. Hence by **subset** $c_0 \sqcup c \sqsubset c_1 \sqcup c$.
- The case where $c = \forall \vec{x_c}.\Sigma \Rightarrow d$ with $d \notin \vec{x_c}$, $d \neq b$ and $b \notin \vec{x}$ cannot happen because $c_\cdot \sqcup c$ exists.

subst: $c_0 = \forall x, \vec{x}.\Sigma \Rightarrow b$ and $c_1 = \forall \vec{x}.(\Sigma \Rightarrow b)[x := a]$. We do some further case analysis

- $b \neq x$ and $b \notin \vec{x}$.
  - $c = \forall \vec{x_c}.\Sigma_c \Rightarrow d$ with $d \notin \vec{x_c}$. In this case $d = b$ because $c_1 \sqcup c$ exists. Then $c_0 \sqcup c = \forall x, \vec{x}, \vec{x_c}.\Sigma \cup \Sigma_c \Rightarrow b$ and $c_1 \sqcup c = \forall \vec{x}, \vec{x_c}.\Sigma[x := a] \cup \Sigma_c \Rightarrow b = \forall \vec{x}, \vec{x_c}.(\Sigma \cup \Sigma_c \Rightarrow b)[x := a]$. Hence $c_0 \sqcup c \sqsubset c_1 \sqcup c$ by **subst**.
  - $c = \forall x, \vec{x_p}.\Sigma_c \Rightarrow x$. Then $c_0 \sqcup c = \forall x, \vec{x}, \vec{x_c}.\Sigma \cup \Sigma_c[x := b] \Rightarrow b$ and $c_1 \sqcup c = \forall \vec{x}, \vec{x_c}.\Sigma[x := a] \cup \Sigma_c[x := b] \Rightarrow b = \forall \vec{x}, \vec{x_c}.(\Sigma \cup \Sigma_c[x := b] \Rightarrow b)[x := a]$. Hence $c_0 \sqcup c \sqsubset c_1 \sqcup c$ by **subst**.
- $b = x$. Then $c_0 = \forall x, \vec{x}.\Sigma \Rightarrow x$ and $c_1 = \forall \vec{x}.\Sigma[x := a] \Rightarrow a$.
  - $c = \forall \vec{x_c}.\Sigma \Rightarrow d$. By assumption $c_1 \sqcup c$ exists. Hence $d = a$. Then $c_0 \sqcup c = \forall \vec{x}, \vec{x_c}.\Sigma[x := a] \cup \Sigma_c \Rightarrow a = c_1 \sqcup c$. Hence $c_0 \sqcup c \sqsubset c_1 \sqcup c$ by **refl**.
  - $c = \forall x, \vec{x_c}.\Sigma_c \Rightarrow x$. Then $c_0 \sqcup c = \forall x, \vec{x}, \vec{x_c}.\Sigma \cup \Sigma_p \Rightarrow x$ and $c_0 \sqcup c = \forall \vec{x}, \vec{x_p} \Rightarrow \Sigma[x := a] \cup \Sigma_c[x := a] \Rightarrow a = \forall \vec{x}, \vec{x_p}.(\Sigma \cup \Sigma_c \Rightarrow x)[x := a]$. Hence $c_0 \sqcup c \sqsubset c_1 \sqcup c$ by **subst**.

We continue with the proof for $\sqsubseteq = \sqsubset^*$. To show: $\forall c_0, c_1, c.c_0 \sqsubseteq c_1 \rightarrow \exists c'.c' = c_1 \sqcup c \rightarrow c_0 \sqcup c \sqsupseteq c_1 \sqcup c$. Let c_0, c_1, c be clauses and $c_0 \sqsupseteq c_1$.

Assume that $c_1 \sqcup c$ exists. We proceed by induction on $c_0 \sqsubseteq c_1$.

refl-*: In this case $c_0 = c_1$. Hence $c_0 \sqcup c = c_1 \sqcup c$ and consequently also $c_0 \sqcup c \sqsubseteq c_1 \sqcup c$ by reflexivity.

trans-*: We have some c_2, s.t. $c_0 \sqsubset c_2$ and $c_2 \sqsubseteq c_1$. By induction $c_2 \sqcup c$ exists and $c_2 \sqcup c \sqsubseteq c_1 \sqcup c$. By the previous proof $c_0 \sqcup c_1$ also exists and $c_0 \sqcup c \sqsubseteq c_2 \sqcup c$. We get the goal by transitivity.

Monotonicity for policies remains to be shown. Let p, q, r be policies such that $p \sqsubseteq q$. Let $c \in q \sqcup r$. This means that there must be clauses $c_q \in q$ and $c_r \in r$ such that $c_q \sqcup c_r = c$. In particular $c_q \sqcup c_r$ exists. Because $c_q \in q$ and $p \sqsubseteq q$ there is a clause $c_p \in p$, such that $c_p \sqsubseteq c_q$. By monotonicity for clauses which we have shown above $c_p \sqcup c_r$ exists and $c_p \sqcup c_r \sqsubseteq c_q \sqcup c_r$. Because $c_p \in p$ and $c_r \in r$ we know that $c_p \sqcup c_r \in p \sqcup r$. Hence there exists a clause $c' \in p \sqcup r$ such that $c' \sqsubseteq c$. Consequently $p \sqcup r \sqsubseteq q \sqcup r$.

Finally we prove monotonicity for $\sqcap$. Let p, q be policies and $p \sqsubseteq q$. Let r be a policy and let $c \in q \sqcap r = q \cup r$. Then $c \in q$ or $c \in r$. If $c \in q$, then there is a $c' \in p$, s. t. $c' \sqsubseteq c$. Since $c' \in p$, also $c' \in p \cup r = p \sqcap r$. If $c \in r$, then also $c \in p \cup r = p \sqcap r$ and $c \sqsubseteq c$ by reflexivity. ☐

Lemma 4.10. $\sqsubseteq$ together with $\sqcup$ and $\sqcap$ forms a lattice on paralocks policies.

Proof. It is clear that the meet $p \sqcap q = p \cup q$ of to policies p, q is associative, commutative and idempotent.

The join $p \sqcup q$ of two paralocks policies p, q is also clearly commutative.

Idempotence: We have to show $p \sqsubseteq p \sqcup p$(1) and $p \sqcup p \sqsubseteq p$ (2).

(1) As shown in Lemma 4.6, $\sqcup$ is an upper bound.

(2) Let $c \in p$. c has the form $\forall \vec{x_p}.\Sigma_p \Rightarrow a$, where a is either a bound or a free actor variable and $\vec{x_p} = x_0, \ldots, x_n$ is vector of bound actor variables. Because $c \in p$, there is a $\vec{y_p} = y_0, \ldots y_n$ such that $\vec{x_p}$ and $\vec{y_p}$ are disjoint and either $\vec{x_p} \not\ni a \notin \vec{y_p}$ or $x_0 = a = y_0$ and $c_j := \forall \vec{y_p}, \vec{x_p}.\Sigma_p \cup \Sigma_p[x_0 := y_0, \ldots x_n := y_0] \Rightarrow a \in p \sqcup p$ in the first case and $c_j := \forall a, y_1, \ldots, y_n, x_1, \ldots, x_n.\Sigma_p \cup \Sigma_p[x_1 := y_1, \ldots x_n := y_0] \Rightarrow a \in p \sqcup p$ in the second case. By Lemma 4.8 $c_j \sqsubseteq c$ and hence $p \sqcup p \sqsubseteq p$.

Associativity: We are using the same side conditions as in the definition of $\sqcup$. We show for policies p, q, r that

$p \sqcup (q \sqcup r) = (p \sqcup q) \sqcup r = \{\Sigma_p \cup \Sigma_q \cup \Sigma_r \Rightarrow x \mid \Sigma_p \Rightarrow x \in p \wedge \Sigma_q \Rightarrow x \in q \wedge \Sigma_r \Rightarrow x \in r\} \cup$
$\{\Sigma_p \cup \Sigma_q \cup \Sigma_r \Rightarrow a \mid \Sigma_p \Rightarrow a \in p \wedge \Sigma_q \Rightarrow a \in q \wedge \Sigma_r \Rightarrow a \in r\} \cup$
$\{\Sigma_p \cup \Sigma_q \cup \Sigma_r[x := a] \Rightarrow a \mid \Sigma_p \Rightarrow a \in p \wedge \Sigma_q \Rightarrow a \in q \wedge \Sigma_r \Rightarrow x \in r\} \cup$
$\{\Sigma_p \cup \Sigma_q[x := a] \cup \Sigma_r \Rightarrow a \mid \Sigma_p \Rightarrow a \in p \wedge \Sigma_q \Rightarrow x \in q \wedge \Sigma_r \Rightarrow a \in r\} \cup$
$\{\Sigma_p[x := a] \cup \Sigma_q \cup \Sigma_r \Rightarrow a \mid \Sigma_p \Rightarrow x \in p \wedge \Sigma_q \Rightarrow a \in q \wedge \Sigma_r \Rightarrow a \in r\} \cup$
$\{\Sigma_p[x := a] \cup \Sigma_q[x := a] \cup \Sigma_r \Rightarrow a \mid \Sigma_p \Rightarrow x \in p \wedge \Sigma_q \Rightarrow x \in q \wedge \Sigma_r \Rightarrow a \in r\} \cup$
$\{\Sigma_p[x := a] \cup \Sigma_q \cup \Sigma_r[x := a] \Rightarrow a \mid \Sigma_p \Rightarrow x \in p \wedge \Sigma_q \Rightarrow a \in q \wedge \Sigma_r \Rightarrow x \in r\} \cup$
$\{\Sigma_p \cup \Sigma_q[x := a] \cup \Sigma_r[x := a] \Rightarrow a \mid \Sigma_p \Rightarrow a \in p \wedge \Sigma_q \Rightarrow x \in q \wedge \Sigma_r \Rightarrow x \in r\}$

We call the long set on the right hand side of the equation $\bigsqcup p, q, r$.

$p \sqcup (q \sqcup r) \subseteq \bigsqcup p, q, r$: Let $c \in p \sqcup (q \sqcup r)$.

- $c = \Sigma_p \cup \Sigma_{q,r} \Rightarrow x$ where $\Sigma_p \Rightarrow x \in p$ and $\Sigma_{q,r} \Rightarrow x \in q \sqcup r$. In this case $\Sigma_{q,r}$ must have the form $\Sigma_q \cup \Sigma_r$ with $\Sigma_q \Rightarrow x \in q$ and $\Sigma_r \Rightarrow x \in r$. Hence $\Sigma_p \cup \Sigma_{q,r} = \Sigma_p \cup \Sigma_q \cup \Sigma_r \in \bigsqcup p, q, r$.
- $c = \Sigma_p \cup \Sigma_{q,r} \Rightarrow a$ where $\Sigma_p \Rightarrow a \in p$ and $\Sigma_{q,r} \Rightarrow a \in q \sqcup r$. There are 3 further cases:
  - $\Sigma_{q,r} = \Sigma_q \cup \Sigma_r$ with $\Sigma_q \Rightarrow a \in q$ and $\Sigma_r \Rightarrow a \in r$. Hence $\Sigma_p \cup \Sigma_{q,r} = \Sigma_p \cup \Sigma_q \cup \Sigma_r \in \bigsqcup p, q, r$.
  - $\Sigma_{q,r} = \Sigma_q \cup \Sigma_r[x := a]$ with $\Sigma_q \Rightarrow a \in q$ and $\Sigma_r \Rightarrow x \in r$. Hence $\Sigma_p \cup \Sigma_{q,r} = \Sigma_p \cup \Sigma_q \cup \Sigma_r[x := a] \in \bigsqcup p, q, r$.
  - $\Sigma_{q,r} = \Sigma_q[x := a] \cup \Sigma_r$ with $\Sigma_q \Rightarrow x \in q$ and $\Sigma_r \Rightarrow a \in r$. Hence $\Sigma_p \cup \Sigma_{q,r} = \Sigma_p \cup \Sigma_q[x := a] \cup \Sigma_r \in \bigsqcup p, q, r$.
- $c = \Sigma_p \cup \Sigma_{q,r}[x := a] \Rightarrow a$ where $\Sigma_p \Rightarrow a \in p$ and $\Sigma_{q,r} \Rightarrow x \in q \sqcup r$. In this case $\Sigma_{q,r}$ must have the form $\Sigma_q \cup \Sigma_r$ with $\Sigma_q \Rightarrow x \in q$ and $\Sigma_r \Rightarrow x \in r$. Hence $\Sigma_p \cup \Sigma_{q,r}[x := a] = \Sigma_p \cup \Sigma_q[x := a] \cup \Sigma_r[x := a] \in \bigsqcup p, q, r$.
- $c = \Sigma_p[x := a] \cup \Sigma_{q,r} \Rightarrow a$ where $\Sigma_p \Rightarrow x \in p$ and $\Sigma_{q,r} \Rightarrow a \in q \sqcup r$. There are 3 further cases:
  - $\Sigma_{q,r} = \Sigma_q \cup \Sigma_r$ with $\Sigma_q \Rightarrow a \in q$ and $\Sigma_r \Rightarrow a \in r$. Hence $\Sigma_p[x := a] \cup \Sigma_{q,r} = \Sigma_p[x := a] \cup \Sigma_q \cup \Sigma_r \in \bigsqcup p, q, r$.
  - $\Sigma_{q,r} = \Sigma_q \cup \Sigma_r[x := a]$ with $\Sigma_q \Rightarrow a \in q$ and $\Sigma_r \Rightarrow x \in r$. Hence $\Sigma_p[x := a] \cup \Sigma_{q,r} = \Sigma_p[x := a] \cup \Sigma_q \cup \Sigma_r[x := a] \in \bigsqcup p, q, r$.
  - $\Sigma_{q,r} = \Sigma_q[x := a] \cup \Sigma_r$ with $\Sigma_q \Rightarrow x \in q$ and $\Sigma_r \Rightarrow a \in r$. Hence $\Sigma_p[x := a] \cup \Sigma_{q,r} = \Sigma_p[x := a] \cup \Sigma_q[x := a] \cup \Sigma_r \in \bigsqcup p, q, r$.

$\bigsqcup p, q, r \subseteq p \sqcup (q \sqcup r)$: Let $c \in \bigsqcup p, q, r$.

- $c = \Sigma_p \cup \Sigma_q \cup \Sigma_r \Rightarrow x$ where $\Sigma_p \Rightarrow x \in p$, $\Sigma_q \Rightarrow x \in q$ and $\Sigma_r \Rightarrow x \in r$. Then $\Sigma_q \cup \Sigma_r \Rightarrow x \in q \sqcup r$ and hence $\Sigma_p \cup (\Sigma_q \cup \Sigma_r) \Rightarrow x \in p \sqcup (q \sqcup r)$.
- $c = \Sigma_p \cup \Sigma_q \cup \Sigma_r \Rightarrow a$ where $\Sigma_p \Rightarrow a \in p$, $\Sigma_q \Rightarrow a \in q$ and $\Sigma_r \Rightarrow a \in r$. Then $\Sigma_q \cup \Sigma_r \Rightarrow a \in q \sqcup r$ and hence $\Sigma_p \cup (\Sigma_q \cup \Sigma_r) \Rightarrow a \in p \sqcup (q \sqcup r)$.
- $c = \Sigma_p \cup \Sigma_q \cup \Sigma_r[x := a] \Rightarrow a$ where $\Sigma_p \Rightarrow a \in p$, $\Sigma_q \Rightarrow a \in q$ and $\Sigma_r \Rightarrow x \in r$. Then $\Sigma_q \cup \Sigma_r[x := a] \Rightarrow a \in q \sqcup r$ and hence $\Sigma_p \cup (\Sigma_q \cup \Sigma_r[x := a]) \Rightarrow a \in p \sqcup (q \sqcup r)$.
- $c = \Sigma_p \cup \Sigma_q[x := a] \cup \Sigma_r \Rightarrow a$ where $\Sigma_p \Rightarrow a \in p$, $\Sigma_q \Rightarrow x \in q$ and $\Sigma_r \Rightarrow a \in r$. Then $\Sigma_q[x := a] \cup \Sigma_r \Rightarrow a \in q \sqcup r$ and hence $\Sigma_p \cup (\Sigma_q[x := a] \cup \Sigma_r) \Rightarrow a \in p \sqcup (q \sqcup r)$.
- $c = \Sigma_p[x := a] \cup \Sigma_q \cup \Sigma_r \Rightarrow a$ where $\Sigma_p \Rightarrow x \in p$, $\Sigma_q \Rightarrow a \in q$ and $\Sigma_r \Rightarrow a \in r$. Then $\Sigma_q \cup \Sigma_r \Rightarrow a \in q \sqcup r$ and hence $\Sigma_p[x := a] \cup (\Sigma_q \cup \Sigma_r) \Rightarrow a \in p \sqcup (q \sqcup r)$.
- $c = \Sigma_p[x := a] \cup \Sigma_q[x := a] \cup \Sigma_r \Rightarrow a$ where $\Sigma_p \Rightarrow x \in p$, $\Sigma_q \Rightarrow x \in q$ and $\Sigma_r \Rightarrow a \in r$. Then $\Sigma_q[x := a] \cup \Sigma_r \Rightarrow a \in q \sqcup r$ and hence $\Sigma_p[x := a] \cup (\Sigma_q[x := a] \cup \Sigma_r) \Rightarrow a \in p \sqcup (q \sqcup r)$.

- $\mathfrak{c} = \Sigma_\mathfrak{p}[\mathfrak{x} := \mathfrak{a}] \cup \Sigma_\mathfrak{q} \cup \Sigma_\mathfrak{r}[\mathfrak{x} := \mathfrak{a}] \Rightarrow \mathfrak{a}$ where $\Sigma_\mathfrak{p} \Rightarrow \mathfrak{x} \in \mathfrak{p}$, $\Sigma_\mathfrak{q} \Rightarrow \mathfrak{a} \in \mathfrak{q}$ and $\Sigma_\mathfrak{r} \Rightarrow \mathfrak{x} \in \mathfrak{r}$. Then $\Sigma_\mathfrak{q} \cup \Sigma_\mathfrak{r}[\mathfrak{x} := \mathfrak{a}] \Rightarrow \mathfrak{a} \in \mathfrak{q} \sqcup \mathfrak{r}$ and hence $\Sigma_\mathfrak{p}[\mathfrak{x} := \mathfrak{a}] \cup (\Sigma_\mathfrak{q} \cup \Sigma_\mathfrak{r}[\mathfrak{x} := \mathfrak{a}]) \Rightarrow \mathfrak{a} \in \mathfrak{p} \sqcup (\mathfrak{q} \sqcup \mathfrak{r})$.
- $\mathfrak{c} = \Sigma_\mathfrak{p} \cup \Sigma_\mathfrak{q}[\mathfrak{x} := \mathfrak{a}] \cup \Sigma_\mathfrak{r}[\mathfrak{x} := \mathfrak{a}] \Rightarrow \mathfrak{a}$ where $\Sigma_\mathfrak{p} \Rightarrow \mathfrak{a} \in \mathfrak{p}$, $\Sigma_\mathfrak{q} \Rightarrow \mathfrak{x} \in \mathfrak{q}$ and $\Sigma_\mathfrak{r} \Rightarrow \mathfrak{x} \in \mathfrak{r}$. Then $\Sigma_\mathfrak{q} \cup \Sigma_\mathfrak{r} \Rightarrow \mathfrak{x} \in \mathfrak{q} \sqcup \mathfrak{r}$ and hence $\Sigma_\mathfrak{p} \cup (\Sigma_\mathfrak{q} \cup \Sigma_\mathfrak{r})[\mathfrak{x} := \mathfrak{a}] \Rightarrow \mathfrak{a} = \Sigma_\mathfrak{p} \cup (\Sigma_\mathfrak{q}[\mathfrak{x} := \mathfrak{a}] \cup \Sigma_\mathfrak{r}[\mathfrak{x} := \mathfrak{a}]) \Rightarrow \mathfrak{a} \in \mathfrak{p} \sqcup (\mathfrak{q} \sqcup \mathfrak{r})$.

The proofs of the inclusions involving $(\mathfrak{p} \sqcup \mathfrak{q}) \sqcup \mathfrak{r}$ work analogously.
Absorbtion:

$p \sqcup (p \sqcap q) \sqsubseteq p$: Let $\mathfrak{c} \in \mathfrak{p}$. Then $\mathfrak{c} \in \mathfrak{p}$ and because $\mathfrak{p} \sqcap \mathfrak{q} = \mathfrak{p} \cup \mathfrak{q}$, also $\mathfrak{c} \in \mathfrak{p} \sqcap \mathfrak{q}$. The rest of the proof is identical to part of the proof for idempotence.

$p \sqsubseteq p \sqcup (p \sqcap q)$: This is true by Lemma 4.6.

$p \sqcap (p \sqcup q) \sqsubseteq p$: This is true by Lemma 4.6.

$p \sqsubseteq p \sqcap (p \sqcup q)$: Let $\mathfrak{c} \in \mathfrak{p} \sqcap (\mathfrak{p} \sqcup \mathfrak{q}) = \mathfrak{p} \cup \mathfrak{p} \sqcup \mathfrak{q}$. We make a case distinction:

- $\mathfrak{c} \in \mathfrak{p}$. Then also $\mathfrak{c} \in \mathfrak{p}$ and $\mathfrak{c} \sqsubseteq \mathfrak{c}$.
- $\mathfrak{c} \in \mathfrak{p} \sqcup \mathfrak{q}$. By Lemma 4.6 $\mathfrak{p} \sqsubseteq \mathfrak{p} \sqcup \mathfrak{q}$. Hence there is a $\mathfrak{c}' \in \mathfrak{p}$ such that $\mathfrak{c}' \sqsubseteq \mathfrak{c}$.

Congruence: We have to show that $\approx$ is a congruence relation with regard to $\sqcup$ and $\sqcap$.
Let $\mathfrak{p} \approx \mathfrak{p}'$ and $\mathfrak{q} \approx \mathfrak{q}'$. Then $\mathfrak{p} \sqcup \mathfrak{q} \overset{\text{Lemma 4.9}}{\sqsubseteq} \mathfrak{p}' \sqcup \mathfrak{q} \overset{\text{commutativity}}{\sqsubseteq} \mathfrak{q} \sqcup \mathfrak{p}' \overset{\text{Lemma 4.9}}{\sqsubseteq} \mathfrak{q}' \sqcup \mathfrak{p}' \overset{\text{commutativity}}{\sqsubseteq} \mathfrak{p}' \sqcup \mathfrak{q}'$. Similarly $\mathfrak{p}' \sqcup \mathfrak{q}' \overset{\text{Lemma 4.9}}{\sqsubseteq} \mathfrak{p} \sqcup \mathfrak{q}' \overset{\text{commutativity}}{\sqsubseteq} \mathfrak{q}' \sqcup \mathfrak{p} \overset{\text{Lemma 4.9}}{\sqsubseteq} \mathfrak{q} \sqcup \mathfrak{p} \overset{\text{commutativity}}{\sqsubseteq} \mathfrak{p} \sqcup \mathfrak{q}$. Hence $\mathfrak{p} \sqcup \mathfrak{q} \approx \mathfrak{p}' \sqcup \mathfrak{q}'$.
Corresponding reasoning works for $\sqcap$. □

Corollary 4.11. For all policies $\mathfrak{p}, \mathfrak{q}$ with $\mathfrak{p} \sqsubseteq \mathfrak{q}$ we have $\mathfrak{p} \sqcup \mathfrak{q} \approx \mathfrak{q}$

Proof. Let $\mathfrak{p}, \mathfrak{q}$ be policies with $\mathfrak{p} \sqsubseteq \mathfrak{q}$. Then by $\mathfrak{p} \sqcup \mathfrak{q} \sqsubseteq \mathfrak{q} \sqcup \mathfrak{q}$ by Lemma 4.9 and $\mathfrak{q} \sqcup \mathfrak{q} \sqsubseteq \mathfrak{q}$ by idempotence 4.10. We have $\mathfrak{q} \sqsubseteq \mathfrak{p} \sqcup \mathfrak{q}$ by Lemma 4.6. □

Corollary 4.12. For policies $\mathfrak{p}, \mathfrak{q}$ the policy $\mathfrak{p} \sqcup \mathfrak{q}$ is the least upper bound of $\mathfrak{p}$ and $\mathfrak{q}$.

Proof. $\mathfrak{p} \sqcup \mathfrak{q}$ is an upper bound of $\mathfrak{p}$ and $\mathfrak{q}$ by Lemma 4.6.
Let $\mathfrak{r}$ be an upper bound of $\mathfrak{p}$ and $\mathfrak{q}$, i.e. $\mathfrak{p} \sqsubseteq \mathfrak{r}$ and $\mathfrak{q} \sqsubseteq \mathfrak{r}$. Then $\mathfrak{p} \sqcup \mathfrak{q} \sqsubseteq \mathfrak{r} \sqcup \mathfrak{q}$ by Lemma 4.9. By Corollary 4.11 $\mathfrak{r} \sqcup \mathfrak{q} \approx \mathfrak{r}$. Hence $\mathfrak{p} \sqcup \mathfrak{q} \sqsubseteq \mathfrak{r}$ by transitivity (4.1). □

Lemma 4.13. $\forall \mathfrak{p}, \mathfrak{q}, \mathfrak{r} : \mathfrak{p} \sqcup \mathfrak{q} \sqsubseteq \mathfrak{r} \leftrightarrow \mathfrak{p} \sqsubseteq \mathfrak{r} \wedge \mathfrak{q} \sqsubseteq \mathfrak{r}$.

Proof. Let $\mathfrak{p}, \mathfrak{q}$ and $\mathfrak{r}$ be policies.
$\rightarrow$: By definition of least upper bound $\mathfrak{p} \sqsubseteq \mathfrak{p} \sqcup \mathfrak{q}$ and $\mathfrak{q} \sqsubseteq \mathfrak{p} \sqcup \mathfrak{q}$. Hence by transitivity of $\sqsubseteq$ (4.1) $\mathfrak{p} \sqsubseteq \mathfrak{r}$ and $\mathfrak{q} \sqsubseteq \mathfrak{r}$.
$\leftarrow$: Because $\mathfrak{p} \sqsubseteq \mathfrak{r}$ and $\mathfrak{q} \sqsubseteq \mathfrak{r}$, $\mathfrak{r}$ is clearly an upper bound of $\mathfrak{p}$ and $\mathfrak{q}$. Because $\mathfrak{p} \sqcup \mathfrak{q}$ is the least upper bound of $\mathfrak{p}$ and $\mathfrak{q}$, we must have $\mathfrak{p} \sqcup \mathfrak{q} \sqsubseteq \mathfrak{r}$. □

Lemma 4.14. If $\mathfrak{c}_1 \sqsubset \mathfrak{c}_2$, then $\mathfrak{c}_1 \cdot \Sigma \sqsubseteq \mathfrak{c}_2 \cdot \Sigma$.

Proof. By case analysis on $\mathfrak{c}_1 \sqsubset \mathfrak{c}_2$.

- **refl**: In this case the same deletions, reorderings and renamings make $\mathfrak{c}_1 \cdot \Sigma$ and $\mathfrak{c}_2 \cdot \Sigma$ equal.
- **subset:** In this case $\mathfrak{c}_1 = \forall \vec{\mathfrak{x}}.\Sigma_1 \Rightarrow \mathfrak{b}$ and $\mathfrak{c}_2 = \forall \vec{\mathfrak{x}}.\Sigma_2 \Rightarrow \mathfrak{b}$ and $\Sigma_1 \subseteq \Sigma_2$. Let $\forall \vec{\mathfrak{x}}.\Sigma_2'(\theta) \Rightarrow \mathfrak{b}(\theta) \in \mathfrak{c}_2 \cdot \Sigma$. Then there are Σ_2'' and Σ' such that $\Sigma' \subseteq \Sigma$, Σ_2'' matches Σ' with θ and $\Sigma_2 = \Sigma_2' \cup \Sigma_2''$.
  Let $\Sigma_1' = \Sigma_1 \backslash \Sigma_2''$. Then $\forall \vec{\mathfrak{x}}.\Sigma_1'(\theta) \Rightarrow \mathfrak{b}(\theta) \in \mathfrak{c}_1 \cdot \Sigma$. Because $\Sigma_1 \subseteq \Sigma_2$ and $\Sigma_1' = \Sigma_1 \backslash \Sigma_2''$ and $\Sigma_2' \supseteq \Sigma_2 \backslash \Sigma_2''$ we have $\Sigma_1' \subseteq \Sigma_2'$ and hence $\forall \vec{\mathfrak{x}}.\Sigma_1'(\theta) \Rightarrow \mathfrak{b}(\theta) \sqsubseteq \forall \vec{\mathfrak{x}}.\Sigma_2'(\theta) \Rightarrow \mathfrak{b}(\theta)$. This shows the claim.
- **subst:** In this case $\mathfrak{c}_1 = \forall \mathfrak{x}_0, \mathfrak{x}_1, \ldots \mathfrak{x}_n.\Sigma_\mathfrak{c} \Rightarrow \mathfrak{a}$ and $\mathfrak{c}_1 = \forall \mathfrak{x}_1, \ldots \mathfrak{x}_n.\Sigma_\mathfrak{c}[\mathfrak{x}_0 := \mathfrak{b}] \Rightarrow \mathfrak{a}[\mathfrak{x}_0 := \mathfrak{b}]$. Let $\forall \mathfrak{x}_1, \ldots \mathfrak{x}_n.\Sigma_2'(\theta) \Rightarrow \mathfrak{a}[\mathfrak{x}_0 := \mathfrak{b}](\theta) \in \mathfrak{c}_2 \cdot \Sigma$. Then there are Σ_2'' and Σ' such that $\Sigma' \subseteq \Sigma$, Σ_2'' matches Σ' with θ and $\Sigma_\mathfrak{c}[\mathfrak{x}_0 := \mathfrak{b}] = \Sigma_2' \cup \Sigma_2''$. In this case there are $\Sigma_\mathfrak{c}'$ and $\Sigma_\mathfrak{c}''$ such that $\Sigma_\mathfrak{c} = \Sigma_\mathfrak{c}' \cup \Sigma_\mathfrak{c}''$ and both $\Sigma_\mathfrak{c}'[\mathfrak{x}_0 := \mathfrak{b}] = \Sigma_2'$ and $\Sigma_\mathfrak{c}''[\mathfrak{x}_0 := \mathfrak{b}] = \Sigma_2''$.
  There are two possibilities:

– $\Sigma_c''[x_0 := b] = \Sigma_c''$. In this case Σ_c'' matches Σ' with θ. Hence $\forall x_0, x_1, \ldots, x_n.\Sigma_c'(\theta) \Rightarrow a(\theta) \in c_1 \cdot \Sigma$. We know that $x_0(\theta) = x_0$ because x_0 is not bound in Σ_c'' By **subst** $\forall x_0, x_1, \ldots, x_n.\Sigma_c'(\theta) \Rightarrow a(\theta) \sqsubset \forall x_1, \ldots x_n.(\Sigma_c'(\theta) \Rightarrow a(\theta))[x_0 := b(\theta)] = \forall x_1, \ldots, x_n.\Sigma_c'(\theta)[x_0 := b(\theta)] \Rightarrow a(\theta)[x_0 := b(\theta)] = \forall x_1, \ldots, x_n.\Sigma_c'[x_0 := b](\theta) \Rightarrow a[x_0 := b](\theta) = \forall x_1, \ldots x_n.\Sigma_2'(\theta) \Rightarrow a[x_0 := b](\theta)$

– $\Sigma_c''[x_0 := b] \neq \Sigma_c''$ In this case x_0 is bound in Σ_c''. There are again two cases:

  * b is one of $x_1 \ldots x_n$ Say $b = x_i$. Because x_0 is bound in Σ_c'' and $\Sigma_c''[x_0 := b]\Sigma_2''$ we know that x_i is bound in Σ_2''. Because Σ_2'' matches Σ' with θ we know that $x_i \in \mathtt{dom}(\theta)$ and $\theta(x_i)$ is a free actor variable. Hence Σ_c'' matches Σ' with $(\theta(x_i)/x_0, \theta)$ because $\Sigma_c''(\theta(x_i)/x_0, \theta) = \Sigma_2''(\theta(x_i)/x_0)(\theta) = \Sigma_2''[x_0 := x_i](x_i/\theta(x_i))(\theta) = \Sigma_2''[x_0 := b](\theta)$ Hence $\forall x_0, x_1, \ldots, x_n.\Sigma_c'((\theta(x_i)/x_0), \theta) \Rightarrow a((\theta(x_i)/x_0), \theta) \in c_1 \cdot \Sigma$. By the same argument as above $\Sigma_c'((\theta(x_i)/x_0), \theta) = \Sigma_c'[x_0 := b](\theta)$ and $a((\theta(x_i)/x_0), \theta) = a[x_0 := b](\theta)$. Consequently $\forall x_0, x_1, \ldots, x_n.\Sigma_c'((\theta(x_i)/x_0), \theta) \Rightarrow a((\theta(x_i)/x_0), \theta) = \forall x_0, x_1, \ldots, x_n.\Sigma_c'[x_0 := b](\theta) \Rightarrow a[x_0 := b](\theta) \sqsubset \forall x_1, \ldots, x_n.\Sigma_c'[x_0 := b](\theta) \Rightarrow a[x_0 := b](\theta) = \forall x_1, \ldots, x_n.\Sigma_2'(\theta) \Rightarrow a[x_0 := b](\theta)$

  * b is a free actor variable. In this case $(b/x_0, \theta)$ is a substitution substituting free actor variables for bound variables and Σ_c'' matches Σ' with $(b/x_0, \theta)$ because $\Sigma_c''(b/x_0, \theta) = \Sigma_2''(b/x_0)(\theta) = \Sigma_2''[x_0 := b](\theta)$. By the same argument as above $\Sigma_c'((b/x_0), \theta) = \Sigma_c'[x_0 := b](\theta)$ and $a((b/x_0), \theta) = a[x_0 := b](\theta)$ Consequently $\forall x_0, x_1, \ldots, x_n.\Sigma_c'((b/x_0), \theta) \Rightarrow a((b/x_0), \theta) = \forall x_0, x_1, \ldots, x_n.\Sigma_c'[x_0 := b](\theta) \Rightarrow a[x_0 := b](\theta) \sqsubset \forall x_1, \ldots, x_n.\Sigma_c'[x_0 := b](\theta) \Rightarrow a[x_0 := b](\theta) = \forall x_1, \ldots, x_n.\Sigma_2'(\theta) \Rightarrow a[x_0 := b](\theta)$.

□

Lemma 4.15. If $p \sqsubseteq q$, then $p(\Sigma) \sqsubseteq q(\Sigma)$

Proof. By induction on the derivation of $p \sqsubset^* q$.

- **refl-***: In this case $p = q$. Hence also $p(\Sigma) = q(\Sigma)$. We get the claim by **refl-***.
- **trans-*** In this case by inversion there is an r such that $p \sqsubset r$ and $r \sqsubset *q$. We have $p(\Sigma) \sqsubseteq r(\Sigma)$ by Lemma 4.14 and $r(\Sigma) \sqsubseteq q(\Sigma)$ by induction. We get $p(\Sigma) \sqsubseteq q(\Sigma)$ by transitivity (4.1).

□

Lemma 4.16. $\forall p, \Sigma.p(\Sigma) \approx p(\Sigma)(\Sigma)$

Proof.

$p(\Sigma)(\Sigma) \sqsubseteq p(\Sigma)$: We have this by Corollary 4.5.

$p(\Sigma) \sqsubseteq p(\Sigma)(\Sigma)$: Let $\forall \vec{x}.\Delta_3(\theta) \Rightarrow a(\theta) \in p(\Sigma)(\Sigma)$. Then there is a $\Sigma' \subseteq \Sigma$ and a Δ_4 such that $\Delta_3 \cup \Delta_4 = \Delta'$ and Δ_4 matches Σ' with θ and $\forall \vec{x}.\Delta' \Rightarrow a \in p(\Sigma)$. This means in turn that there are $\Delta, \Delta_1, \Delta_2, \theta', \Sigma'', a'$ such that $\Delta' = \Delta_1(\theta')$, $\Delta = \Delta_1 \cup \Delta_2$, $a = a'(\theta')$, $\Sigma'' \subseteq \Sigma$ and Δ_2 matches Σ'' with θ' and $\forall \vec{x}.\Delta \Rightarrow a' \in p$.

Hence $\Delta_3 \cup \Delta_4 = \Delta_1(\theta')$. Therefore $\Delta_3' = \{x \mid x(\theta') \in \Delta_3\}$ and $\Delta_4' = \{x \mid x(\theta') \in \Delta_4\}$ are sets such that $\Delta_1 = \Delta_3' \cup \Delta_4'$ and $\Delta_3'(\theta') = \Delta_3$ and $\Delta_4'(\theta') = \Delta_4$. Hence $\Delta = \Delta_3' \cup \Delta_4' \cup \Delta_2$.

We show $\Delta_2 \cup \Delta_4'$ matches $\Sigma' \cup \Sigma'' \subseteq \Sigma$ with (θ', θ).
We have to show that the set of bound actors in $\Delta_2 \cup \Delta_4'$ is equal to $\mathtt{dom}(\theta', \theta) = \mathtt{dom}(\theta') \cup \mathtt{dom}(\theta)$. We know Δ_2 matches Σ'' with θ'. Hence $\mathtt{dom}(\theta')$ is equal to the set of bound actors in Δ_2. We also know $\Delta_4'(\theta')$ matches Σ' with θ. Hence $\mathtt{dom}(\theta)$ is equal to the set of bound actors in $\Delta_4'(\theta')$. The set of bound actors in $\Delta_4'(\theta')$ is equal to the set of bound actors in Δ_4' without $\mathtt{dom}(\theta')$. Hence the set of bound actors in Δ_4' is a subset of $\mathtt{dom}(\theta') \cup \mathtt{dom}(\theta)$.
We also have to show that $(\Delta_2 \cup \Delta_4')(\theta', \theta) = \Sigma' \cup \Sigma''$.

$(\Delta_2 \cup \Delta_4')(\theta', \theta) = \Delta_2(\mathtt{theta}', \theta) \cup \Delta_4'(\theta', \theta) = (\Delta_2(\theta'))(\theta) \cup (\Delta_4'(\theta'))(\theta) = \Sigma''(\theta) \cup \Delta_4(\theta) = \Sigma''(\theta) \cup \Sigma'$. Because Δ_2 matches Σ'' with θ' all the bound actor variables in Δ_2 are in the domain of θ'. Hence $\Sigma'' = \Delta_2(\theta')$ does not contain any bound actor variables anymore and $\Sigma''(\theta) = \Sigma''$. Hence indeed $(\Delta_2 \cup \Delta_4')(\theta', \theta) = \Sigma' \cup \Sigma''$.

Because $\Delta = \Delta_3' \cup \Delta_4' \cup \Delta_2$ and $\Delta_2 \cup \Delta_4'$ matches $\Sigma' \cup \Sigma'' \subseteq \Sigma$ with (θ', θ), we get $\forall \vec{x}.\Delta_3'(\theta', \theta) \Rightarrow a'(\theta', \theta) \in p(\Sigma)$. Using the equalities above this is simplifies as follows: $\forall \vec{x}.\Delta_3'(\theta', \theta) \Rightarrow a'(\theta', \theta) \in p(\Sigma) = \forall \vec{x}.(\Delta_3'(\theta'))(\theta) \Rightarrow (a'(\theta'))(\theta) \in p(\Sigma) = \forall \vec{x}.\Delta_3(\theta) \Rightarrow a(\theta) \in p(\Sigma)$.

Hence $\forall \vec{x}.\Delta_3(\theta) \Rightarrow a(\theta) \in p(\Sigma) \in p(\Sigma)$. We get the goal with **refl-***.

□

Corollary 4.17. If $p(\Sigma) \sqsubseteq q$, then $p(\Sigma) \sqsubseteq q(\Sigma)$.

Proof. By Lemma 4.15 $p(\Sigma)(\Sigma) \sqsubseteq q(\Sigma)$. By Lemma 4.16 $p(\Sigma) \sqsubseteq p(\Sigma)(\Sigma)$. Hence by transitivity (4.1) $p(\Sigma) \sqsubseteq q(\Sigma)$. □

Corollary 4.18. If $\tau <: \tau'$, then $\tau(\Sigma) <: \tau'$.

Proof. Let $\tau = A^p$ and $\tau' = A'^q$ be types such taht $\tau <: \tau'$. This must have been derived using **sub-policy**. Hence $A <: A'$ and $p \sqsubseteq q$. By 4.5 $p(\Sigma) \sqsubseteq p$. By transitivity $p(\Sigma) \sqsubseteq q$. Hence by **sub-policy** $A^{p(\Sigma)} <: A'^q$. □

Lemma 4.19 (Least and greatest policies)**.** $\bot = \forall x.x$ is the least policy and $\top = \emptyset$ is the greatest policy.

Proof. Let p be a policy. We show $p \sqsubseteq \top$. Let $c \in \top$. Since $\top = \emptyset$ this is a contradiction. Now we show $\bot \sqsubseteq p$. Let $c \in p$. Then c has the form $\forall \vec{x}.\Sigma \Rightarrow b$. There are two cases:

- $b = x$. Then $\bot = \forall x.x \approx \forall \vec{x}.x = \forall \vec{x}.\emptyset \Rightarrow x$. Since $\emptyset \subseteq \Sigma$ we have $\forall \vec{x}.\emptyset \Rightarrow x \sqsubseteq \forall \vec{x}.\Sigma \Rightarrow x$. We get the claim by transitivity.
- b is a free actor variable. In this case $\bot = \forall x.x \sqsubseteq b \approx \forall \vec{x}.b = \forall \vec{x}.\emptyset \Rightarrow b \sqsubseteq \forall \vec{x}.\Sigma \Rightarrow b$ for the same reasons as above.

□

5 Weakening

Lemma 5.1 (Subtyping reflexive)**.**

1. $\forall A.\ A <: A$
2. $\forall \tau.\ \tau <: \tau$

Proof. Almost identical to the proof in [5]. By mutual induction on the structure of the types.

$A^p <: A^p$: By induction $A <: A$ and $p \sqsubseteq p$ by the definition of $\sqsubseteq$. The claim follows by sub-policy.

$\mathtt{unit} <: \mathtt{unit}$: By sub-unit.

$\mathcal{N} <: \mathcal{N}$: By sub-nat.

$\mathtt{ref}\ \tau <: \mathtt{ref}\ \tau$: By sub-tau.

$\tau \times \tau' <: \tau \times \tau'$: By induction $\tau <: \tau$ and $\tau' <: \tau'$. The claim follows by sub-prod.

$\tau + \tau' <: \tau + \tau'$: By induction $\tau <: \tau$ and $\tau' <: \tau'$. The claim follows by sub-sum.

$\tau \xrightarrow{\Sigma;p} \tau' <: \tau \xrightarrow{\Sigma;p} \tau'$: By induction $\tau <: \tau$ and $\tau' <: \tau'$. We also have $\Sigma \subseteq \Sigma$ and $p \sqsubseteq p$. The claim follows by sub-arrow.

□

Note that due to the standard terminology for logical relations we also call state environments *worlds*. We need a notion of a larger state, that could exist at some point later in an execution. As we will mainly need this in the logical relation later on, we call this *world extension*. But the same notion is useful for some syntactic proofs as well, which is why we already define it here.

Definition 5.1 (World extension[5])**.** We say a world θ' extends a world θ written $\theta \sqsubseteq \theta'$ (or $\theta' \sqsupseteq \theta$) if $\forall l \in \mathtt{dom}(\theta).\ l \in \mathtt{dom}(\theta') \wedge \theta(l) = \theta'(l)$.

Lemma 5.2 (Weakening)**.** If $\Gamma; \Sigma; \theta \vdash_{pc} e : \tau$, then for all $\Gamma' \supseteq \Gamma$, $\Sigma' \supseteq \Sigma$, and $\theta' \sqsupseteq \theta$ we have $\Gamma'; \Sigma'; \theta' \vdash_{pc} e : \tau$.

Proof. By induction on the derivation. For the rules **var**, **nat** and **unit** the new judgements can be derived using the same rule. In most other rules we just replace the judgements in the premisses by the judgements we get from the induction hypothesis. Subtyping assumptions are usually not affected by the change. The same is mostly true for the orderings on policies.

In the case of **app** we also have to show, $\Sigma' \supseteq \Sigma''$, when e_1 has the type $\tau_1 \xrightarrow{\Sigma'', p} \tau_2$. We have this because the premiss of the rule is $\Sigma \supseteq \Sigma''$ and $\Sigma' \supseteq \Sigma$.

For **new** we also have to show $\tau'(\Sigma') <: \tau$. We already know $\tau'(\Sigma) <: \tau$. τ and τ' have the form A^p and B^q, respectively. By inversion we get $A <: B$ and $q(\Sigma) \sqsubseteq p$. By **sub-policy** it suffices to show $q(\Sigma') \sqsubseteq p$. We have $q(\Sigma') \sqsubseteq q(\Sigma)$ by Lemma 4.3. $q(\Sigma') \sqsubseteq p$ follows by transitivity (4.1).

For **assign** $\tau(\Sigma') <: \tau'$ follows with the same argument as above.

In **loc** we have to show $\theta'(l) = \tau$. We already know $\theta(l) = \tau$. This follows directly from the definition of $\theta' \sqsupseteq \theta$.

□

6 Type Safety

Lemma 6.1 (Subtyping transitive)**.** If $\tau_0 <: \tau_1$ and $\tau_1 <: \tau_2$, then $\tau_0 <: \tau_2$ and if $A_0 <: A_1$ and $A_1 <: A_2$, then $A_0 <: A_2$.

Proof. We are going to prove this by induction on the derivation of $\tau_0 <: \tau_1$ and $A_0 <: A_1$ respectively. To make the contravariant case in **sub-arrow** go through we will actually prove the following: If $\tau_0 <: \tau_1$, then $\forall \tau_2.(\tau_2 <: \tau_0 \to \tau_2 <: \tau_1) \wedge (\tau_1 <: \tau_2 \to \tau_0 <: \tau_2)$ and similarly for the unlabelled types.

- **sub-policy**. In this case $\tau_0 = A_0^{p_0}$, $\tau_1 = A_1^{p_1}$ with $p_0 \sqsubseteq p_1$ and $A_0 <: A_1$. There are two cases:
  - $\tau_1 <: \tau_2$ We find that the only rule with which this would be derivable is **sub-policy** and hence $\tau_2 = A_2^{p_2}$, $p_1 \sqsubseteq p_2$ and $A_1 <: A_2$. We show $A_0^{p_0} <: A_2^{p_2}$ with **subpolicy**. This means we have to show
    - $A_0 <: A_2$. We have this by induction.
    - $p_0 \sqsubseteq p_2$. We get this by transitivity of $\sqsubseteq$ (4.1).
  - $\tau_2 <: \tau_0$. We find that the only rule with which this would be derivable is **sub-policy** and hence $\tau_2 = A_2^{p_2}$, $p_2 \sqsubseteq p_0$ and $A_2 <: A_0$. We show $A_2^{p_2} <: A_1^{p_1}$ with **subpolicy**. This means we have to show
    - $A_2 <: A_1$. We have this by induction.
    - $p_2 \sqsubseteq p_1$. We get this by transitivity of $\sqsubseteq$ (4.1).
- **sub-ref:** In this case $A_0 = \mathtt{ref}\ \tau_0'$, $A_1 = \mathtt{ref}\ \tau_1'$. By inversion on $A_1 <: A_2$ and $A_2 <: A_0$, respectively, we find that the only rule with which this would be derivable is **sub-ref** and hence $A_2 = \mathtt{ref}\ \tau_2'$. We get $\mathtt{ref}\ \tau_0' <: \mathtt{ref}\ \tau_2'$ and $\mathtt{ref}\ \tau_2' <: \mathtt{ref}\ \tau_1'$, respectively, with **sub-ref**.
- **sub-prod:** In this case $A_0 = \tau_0' \times \tau_0''$, $A_1 = \tau_1' \times \tau_1''$ with $\tau_0' <: \tau_1'$ and $\tau_0'' <: \tau_1''$.

  There are two cases:
  - $A_1 <: A_2$: By inversion we find that the only rule with which this would be derivable is **sub-prod** and hence $A_2 = \tau_2' \times \tau_1''$, $\tau_1' <: \tau_2$ and $\tau_1'' <: \tau_2''$. By induction we have $\tau_0' <: \tau_2'$ and $\tau_0'' <: \tau_2''$. We get the claim with **sub-prod**.
  - $A_2 <: A_0$: By inversion we find that the only rule with which this would be derivable is **sub-prod** and hence $A_2 = \tau_2' \times \tau_1''$, $\tau_2' <: \tau_0$ and $\tau_2'' <: \tau_0''$. By induction we have $\tau_2' <: \tau_1'$ and $\tau_2'' <: \tau_1''$. We get the claim with **sub-prod**.
- **sub-sum:** In this case $A_0 = \tau_0' + \tau_0''$, $A_1 = \tau_1' + \tau_1''$ with $\tau_0' <: \tau_1'$ and $\tau_0'' <: \tau_1''$.

  There are two cases:
  - $A_1 <: A_2$: By inversion we find that the only rule with which this would be derivable is **sub-sum** and hence $A_2 = \tau_2' + \tau_1''$, $\tau_1' <: \tau_2$ and $\tau_1'' <: \tau_2''$. By induction we have $\tau_0' <: \tau_2'$ and $\tau_0'' <: \tau_2''$. We get the claim with **sub-sum**.
  - $A_2 <: A_0$: By inversion we find that the only rule with which this would be derivable is **sub-sum** and hence $A_2 = \tau_2' + \tau_1''$, $\tau_2' <: \tau_0$ and $\tau_2'' <: \tau_0''$. By induction we have $\tau_2' <: \tau_1'$ and $\tau_2'' <: \tau_1''$. We get the claim with **sub-sum**.

- **sub-arrow:** In this case $A_0 = \tau_0' \xrightarrow{\Sigma_0, p_0} \tau_0''$ and $A_1 = \tau_1' \xrightarrow{\Sigma_1, p_1} \tau_1''$ such that $\tau_1' <: \tau_0'$, $\tau_0'' <: \tau_1''$, $p_1 \sqsubseteq p_0$ and $\Sigma_0 \subseteq \Sigma_1$.

  There are two cases:

  - $A_1 <: A_2$: By inversion we find that the only rule with which this would be derivable is **sub-arrow** and hence $A_2 = \tau_2' \xrightarrow{\Sigma_2, p_2} \tau_2''$, $\tau_2' <: \tau_1'$, $\tau_1'' <: \tau_2''$, $p_2 \sqsubseteq p_1$ and $\Sigma_1 \subseteq \Sigma_2$.

    We show $\tau_0' \xrightarrow{\Sigma_0, p_0} \tau_0'' <: \tau_2' \xrightarrow{\Sigma_2, p_2} \tau_2''$ using **sub-arrow**. This means we have to show:

    * $\tau_2' <: \tau_0'$ which we get by induction.
    * $\tau_0'' <: \tau_2''$ which we get by induction.
    * $p_2 \sqsubseteq p_0$. We get this by transitivity of $\sqsubseteq$ (4.1).
    * $\Sigma_0 \subseteq \Sigma_2$. We get this by transitivity of $\subseteq$.
  - $A_2 <: A_0$: By inversion we find that the only rule with which this would be derivable is **sub-arrow** and hence $A_2 = \tau_2' \xrightarrow{\Sigma_2, p_2} \tau_2''$, $\tau_0' <: \tau_2'$, $\tau_2'' <: \tau_0''$, $p_0 \sqsubseteq p_2$ and $\Sigma_2 \subseteq \Sigma_0$.

    We show $\tau_2' \xrightarrow{\Sigma_2, p_2} \tau_2'' <: \tau_1' \xrightarrow{\Sigma_1, p_1} \tau_1''$ using **sub-arrow**. This means we have to show:

    * $\tau_1' <: \tau_2'$ which we get by induction.
    * $\tau_2'' <: \tau_1''$ which we get by induction.
    * $p_1 \sqsubseteq p_2$. We get this by transitivity of $\sqsubseteq$ (4.1).
    * $\Sigma_2 \subseteq \Sigma_1$. We get this by transitivity of $\subseteq$.

- **sub-unit:** In this case $A_0 = \mathtt{unit}$, $A_1 = \mathtt{unit}$. By inversion on $A_1 <: A_2$ and $A_2 <: A_0$, respectively, we find that the only rule with which this would be derivable is **sub-unit** and hence $A_2 = \mathtt{unit}$. We get $\mathtt{unit} <: \mathtt{unit}$ with **sub-unit**.

- **sub-nat:** In this case $A_0 = \mathcal{N}$, $A_1 = \mathcal{N}$. By inversion on $A_1 <: A_2$ and $A_2 <: A_0$, respectively, we find that the only rule with which this would be derivable is **sub-nat** and hence $A_2 = \mathcal{N}$. We get $\mathcal{N} <: \mathcal{N}$ with **sub-nat**.

□

Lemma 6.2 (World extension ordering)**.** World extension ($\sqsubseteq$) is an ordering.

Proof. Reflexivity: Let θ be a world and $l \in \mathtt{dom}(\theta)$. Then $l \in \mathtt{dom}(\theta)$ and $\theta(l) = \theta(l)$. Hence $\theta \sqsubseteq \theta$.
Transitivity: Let $\theta_0, \theta_1, \theta_2$ be worlds such that $\theta_0 \sqsubseteq \theta_1$ and $\theta_1 \sqsubseteq \theta_2$. Let $l \in \mathtt{dom}(\theta_0)$. Then by $\theta_0 \sqsubseteq \theta_1$ also $l \in \mathtt{dom}(\theta_1)$ and $\theta_0(l) = \theta_1(l)$. By $\theta_1 \sqsubseteq \theta_2$ also $l \in \mathtt{dom}(\theta_2)$ and $\theta_1(l) = \theta_2(l)$. Transitivity of $=$ gives us $\theta_0(l) = \theta_2(l)$. Hence $\theta_0 \sqsubseteq \theta_2$.
Antisymmetry: Let θ, θ' be worlds such that $\theta \sqsubseteq \theta'$ and $\theta' \sqsubseteq \theta$. We have to show $\theta = \theta'$.
$\subseteq$:
Let $(l, \tau) \in \theta$. This means that $l \in \mathtt{dom}(\theta)$ and $\theta(l) = \tau$. Because $\theta \sqsubseteq \theta'$ also $l \in \mathtt{dom}(\theta')$ and $\theta'(l) = \tau$. Hence $(l, \tau) \in \theta'$.
$\supseteq$:
Let $(l, \tau) \in \theta'$. This means that $l \in \mathtt{dom}(\theta')$ and $\theta(l') = \tau$. Because $\theta' \sqsubseteq \theta$ also $l \in \mathtt{dom}(\theta)$ and $\theta(l) = \tau$. Hence $(l, \tau) \in \theta$. □

Definition 6.1 (Syntactic state well-formedness)**.**
$S \triangleright_\Gamma (\theta) :=$

$$\mathtt{dom}(\theta) \subseteq \mathtt{dom}(S)$$

$$\wedge\ (\forall l \in \mathtt{dom}(\theta).\Gamma; \emptyset; \theta \vdash_\bot S(l) : \theta(l))$$

$$\wedge\ \forall l \in \mathtt{dom}(\theta).\theta(l) = \mathtt{type}(S, l)$$

$$\wedge\ \forall l \in \mathtt{dom}(S).S(l) \in \mathcal{V}.$$

Lemma 6.3. Whenever $\Gamma; \Sigma; \theta \vdash_{pc} v : \tau$, then we also have for any lock set Σ' that $\Gamma; \Sigma'; \theta \vdash_{pc} v : \tau$.

Proof. By induction on $\Gamma; \Sigma; \theta \vdash_{pc} v : \tau$.

1. **nat:** In this case $v = n$ and,$n \in \mathbb{N}$ and $\tau = \mathcal{N}^\bot$. We get $\Gamma; \Sigma'; \theta \vdash_{pc} n : \mathcal{N}^\bot$ by **nat**.

2. **λ:** In this case $v = \lambda\, x : \tau_1.e$ and $\tau = \tau_1 \xrightarrow{\Sigma'', p_e} \tau_2$. We know $\Gamma, x : \tau_1; \Sigma''; \theta \vdash_{p_e} e : \tau_2$ by inversion. Hence by $\lambda\ \Gamma; \Sigma; \theta \vdash_{pc} \lambda\, x.e : \tau_1 \xrightarrow{\Sigma'', p_e} \tau_2$.

3. **prod:** In this case $v = (v_1, v_2)$. We replace the assumptions of the rule by the judgements we get from the induction hypothesis. This gives us the new goal.

4. **inr:** In this case $v = \mathtt{inr}\ v'$. We replace the assumption of the rule by the judgement we get from the induction hypothesis. This gives us the new goal.

5. **inl:** In this case $v = \mathtt{inl}\ v'$. We replace the assumption of the rule by the judgement we get from the induction hypothesis. This gives us the new goal.

6. **loc:** In this case $v = l$. By inversion we know $\theta(l) = \tau$. We get $\Gamma; \Sigma'; \theta \vdash_{pc} l : \tau$ by **loc**.

7. **sub:** We replace the typing assumption of the rule by the judgement we get from the induction hypothesis. This gives us the new goal.

8. **unit:** In this case $v = ()$ and $\tau = \mathtt{unit}^{\perp}$. We get $\Gamma; \Sigma'; \theta \vdash_{pc} () : \mathtt{unit}^{\perp}$ by **unit**.

□

Lemma 6.4. If $\Gamma, x : \tau_1, \Gamma'; \Sigma; \theta \vdash_{pc} e : \tau_2$ and $\tau_1' <: \tau_1$, then $\Gamma, x : \tau_1', \Gamma'; \Sigma; \theta \vdash_{pc} e : \tau_2$.

Proof. By induction on the derivation of $\Gamma, x : \tau_1, \Gamma'; \Sigma; \theta \vdash_{pc} e : \tau_2$.
The most interesting case is the **var** rule. There are three cases:

- $$\frac{}{\Gamma_0, y : \tau, \Gamma_1, x : \tau_1, \Gamma'; \Sigma; \theta \vdash_{pc} y : \tau}\ \textbf{var}$$

  In this case we get $\Gamma_0, y : \tau, \Gamma_1, x : \tau_1', \Gamma'; \Sigma; \theta \vdash_{pc} y : \tau$ with **var**.

- $$\frac{}{\Gamma, x : \tau_1, \Gamma'; \Sigma; \theta \vdash_{pc} x : \tau_1}\ \textbf{var}$$

  In this case we get $\Gamma, x : \tau_1', \Gamma'; \Sigma\theta \vdash_{pc} x : \tau_1'$ with **var**. We get $\Gamma, x : \tau_1', \Gamma'; \Sigma\theta \vdash_{pc} x : \tau_1$ with **sub**.

- $$\frac{}{\Gamma, x : \tau_1, \Gamma_0, y : \tau, \Gamma_1; \Sigma; \theta \vdash_{pc} y : \tau}\ \textbf{var}$$

  In this case we get $\Gamma_0, x : \tau_1', \Gamma_0, y : \tau, \Gamma_1; \Sigma; \theta \vdash_{pc} y : \tau$ with **var**.

In all other rules we just replace the judgements in the assumptions by judgments we get from the induction hypothesis where $x : \tau_1$ is replaced by $x : \tau_1'$ in Γ. Then we can derive the goal with the same rule.
□

Lemma 6.5 (λ-inversion)**.** If $\Gamma; \Sigma; \theta \vdash_{pc} v : (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^p$, then $v = \lambda x.\, e$ and $\Gamma, x : \tau_1; \Sigma'; \theta \vdash_{p_e} e : \tau_2$.

Proof. By induction on the derivation of $\Gamma; \Sigma; \theta \vdash_{pc} v : (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^p$. There are only two cases:

- **λ:** In this case this is exactly what the rule says.

- **sub:** By inversion there is a $pc' \sqsupseteq pc$ and a τ' such that $\tau' \leqslant (\tau_1 \xrightarrow{\Sigma', q} \tau_2)^p$ and $\Gamma; \Sigma; \theta \vdash_{pc'} v : \tau'$. We do inversion on the derivation of $\tau' \leqslant (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^p$. The only applicable rule is **sub-policy**. Hence τ' has the form $A^{p'}$ and $p' \sqsubseteq p$ and $A <: \tau_1 \xrightarrow{\Sigma', p_e} \tau_2$. We do another inversion. The only applicable rule this time is **sub-arrow**. Hence A has the form $\tau_1' \xrightarrow{\Sigma'', p_e'} \tau_2'$ where $\Sigma'' \subseteq \Sigma'$ and $p_e \sqsubseteq p_e'$, $\tau_1 <: \tau_1'$, $\tau_2' <: \tau_2$. Hence by induction v has the form $\lambda\, x.e$ and $\Gamma, x : \tau_1'; \Sigma'; \theta \vdash_{p_e'} e : \tau_2'$. By Lemma 6.4 $\Gamma, x : \tau_1; \Sigma''; \theta \vdash_{p_e'} e : \tau_2'$. By weakening (5.2) $\Gamma, x : \tau_1; \Sigma'; \theta \vdash_{p_e'} e : \tau_2'$. Finally we get $\Gamma, x : \tau_1; \Sigma'; \theta \vdash_{p_e} e : \tau_2$ with **sub**.

□

Lemma 6.6 (Pair inversion)**.** If $\Gamma; \Sigma; \theta \vdash_{pc} (e, e') : (\tau_1 \times \tau_2)^p$, then $\Gamma; \Sigma; \theta \vdash_{pc} e : \tau_1$ and $\Gamma; \Sigma; \theta \vdash_{pc} e' : \tau_2$.

Proof. By induction on the derivation of $\Gamma; \Sigma; \theta \vdash_{pc} (e, e') : (\tau_1 \times \tau_2)^p$. There are only two cases:

- **prod:** The goals are assumptions of the rule.
- **sub:** By inversion there is a $\mathsf{pc}' \sqsupseteq \mathsf{pc}$ and a τ' such that $\tau' \leqslant (\tau_1 \times \tau_2)^{\mathsf{p}}$ and $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}'} (e, e') : \tau'$. We do inversion on the derivation of $\tau' \leqslant (\tau_1 \times \tau_2)^{\mathsf{p}}$. The only applicable rule is **sub-policy**. Hence τ' has the form $A^{\mathsf{p}'}$ and $\mathsf{p}' \sqsubseteq \mathsf{p}$ and $A <: \tau_1 \times \tau_2$. We do another inversion. The only applicable rule this time is **sub-prod**. Hence A has the form $\tau_1' \times \tau_2'$ where $\tau_1' <: \tau_1$ and $\tau_2' <: \tau_2$. Hence $\tau' = (\tau_1' \times \tau_2')^{\mathsf{p}'}$. Therefore we get $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}'} e : \tau_1'$ and $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}'} e' : \tau_2'$ by induction. We get $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau_1$ and $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} e' : \tau_2$ with **sub**.

□

Lemma 6.7 (Injection inversion)**.**

1. If $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} \mathsf{inl}\,(e) : (\tau_1 + \tau_2)^{\mathsf{p}}$, then $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau_1$.
2. If $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} \mathsf{inr}\,(e) : (\tau_1 + \tau_2)^{\mathsf{p}}$, then $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau_1$.

Proof. 1. By induction in the derivation of $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} \mathsf{inl}\,(e) : (\tau_1 + \tau_2)^{\mathsf{p}}$. There are two cases:

- **inl:** In this case the goal is an assumption of the rule.
- **sub:** By inversion there is a $\mathsf{pc}' \sqsupseteq \mathsf{pc}$ and a τ' such that $\tau' \leqslant (\tau_1 + \tau_2)^{\mathsf{p}}$ and $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}'} \mathtt{inl}\ e : \tau'$. We do inversion on the derivation of $\tau' \leqslant (\tau_1 + \tau_2)^{\mathsf{p}}$. The only applicable rule is **sub-policy**. Hence τ' has the form $A^{\mathsf{p}'}$ and $\mathsf{p}' \sqsubseteq \mathsf{p}$ and $A <: \tau_1 + \tau_2$. We do another inversion. The only applicable rule this time is **sub-sum**. Hence A has the form $\tau_1' + \tau_2'$ where $\tau_1' <: \tau_1$ and $\tau_2' <: \tau_2$. Hence $\tau' = (\tau_1' + \tau_2')^{\mathsf{p}'}$. Therefore we get $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}'} e : \tau_1'$ by induction. We get $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau_1$ with **sub**.

2. As in case 1. Just replace inl with inr and 1 with 2 in the appropriate places.

□

Lemma 6.8. If $\Gamma, x : \tau, \Gamma'; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau'$ and $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} e' : \tau$, then $\Gamma, \Gamma'; \Sigma; \theta \vdash_{\mathsf{pc}} e[x \mapsto e'] : \tau'$.

Proof. By induction on the derivation of $\Gamma, x : \tau, \Gamma'; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau'$.

In most cases we just replace the typing assumptions of a rule with the assumptions we get from the induction hypothesis and use the same rule to get the claim. We do, however, need to take a closer look at **var**. There are several cases:

- $\Gamma = \Gamma_1, y : \tau', \Gamma_2$ and we have

$$\frac{}{\Gamma_1, y : \tau', \Gamma_2, x : \tau, \Gamma'; \Sigma; \theta \vdash_{\mathsf{pc}} y : \tau'}\ \textbf{var}$$

  In this case $[e'/x]y = y$ and we get $\Gamma_1, y : \tau', \Gamma_2, \Gamma'; \Sigma; \theta \vdash_{\mathsf{pc}} y : \tau'$ by **var**.

- $\tau = \tau'$ and we have

$$\frac{}{\Gamma, x : \tau, \Gamma'; \Sigma; \theta \vdash_{\mathsf{pc}} x : \tau}\ \textbf{var}$$

  .

  In this case $[e'/x]x = e'$. We already know $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} e' : \tau$. We get $\Gamma, \Gamma'; \Sigma; \theta \vdash_{\mathsf{pc}} e' : \tau$ by Weakening.

- $\Gamma = \Gamma_1, y : \tau', \Gamma_2$ and we have

$$\frac{}{\Gamma, x : \tau, \Gamma_1, y : \tau', \Gamma_2; \Sigma; \theta \vdash_{\mathsf{pc}} y : \tau'}\ \textbf{var}$$

  In this case $[e'/x]y = y$ and we get $\Gamma, \Gamma_1, y : \tau', \Gamma_2; \Sigma; \theta \vdash_{\mathsf{pc}} y : \tau'$ by **var**.

□

Lemma 6.9 (location inversion)**.** If $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} l : (\mathsf{ref}\ \tau)^{\mathsf{p}}$, then $\theta(l) = \tau$.

Proof. By induction on the derivation of $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} l : (\mathsf{ref}\ \tau)^{\mathsf{p}}$. There are two cases:

- **loc:** By inversion we have $\theta(l) = \tau$.
- **sub** By inversion we have

– A $\mathsf{pc}' \sqsubseteq \mathsf{pc}$ such that $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}'} l : \tau'$
– $\tau' <: (\mathtt{ref}\ \tau)^{\mathsf{p}}$.

We do inversion on $\tau' <: (\mathtt{ref}\ \tau)^{\mathsf{p}}$. The only applicable rule is **sub-policy**. Hence $\tau' = A^{\mathsf{p}'}$ and $\mathsf{p}' \sqsubseteq \mathsf{p}$ and $A <: \mathtt{ref}\ \tau$. We do another inversion. The only applicable rule is **sub-ref**. Hence $A = \mathtt{ref}\ \tau$. Hence $\tau' = (\mathtt{ref}\ \tau)^{\mathsf{p}'}$. By induction we get $\theta(l) = \tau$.

□

Lemma 6.10. If $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} v : (\tau_1 \times \tau_2)^{\mathsf{p}}$, then there are v_1, v_2 s.t. $v = (v_1, v_2)$.

Proof. By induction on the derivation.

- **prod:** The rule gives us that $v = (e_1, e_2)$. For this to be a value both e_1 and e_2 need to be values.
- **sub:** By inversion there is a $\mathsf{pc}' \sqsupseteq \mathsf{pc}$ and a τ' such that $\tau' \leqslant (\tau_1 \times \tau_2)^{\mathsf{p}}$ and $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}'} v : \tau'$. We do inversion on the derivation of $\tau' \leqslant (\tau_1 \times \tau_2)^{\mathsf{p}}$. The only applicable rule is **sub-policy**. Hence τ' has the form $A^{\mathsf{p}'}$ and $\mathsf{p}' \sqsubseteq \mathsf{p}$ and $A <: \tau_1 \times \tau_2$. We do another inversion. The only applicable rule this time is **sub-prod**. Hence A has the form $\tau_1' \times \tau_2'$ where $\tau_1' <: \tau_1$ and $\tau_2' <: \tau_2$. Hence $\tau' = (\tau_1' \times \tau_2')^{\mathsf{p}'}$. By induction we get that there are v_1, v_2 s.t. $v = (v_1, v_2)$.

□

Lemma 6.11. If $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} v : (\tau_1 + \tau_2)^{\mathsf{p}}$, then there is a v' s.t. either $v = \mathsf{inl}\,(v')$ or $v = \mathsf{inr}\,(v')$.

Proof. By induction on the derivation.

- **inl:** The rule gives us that $v = \mathtt{inl}\ e$. For this to be a value e needs to be a value.
- **inr:** The rule gives us that $v = \mathtt{inr}\ e$. For this to be a value e needs to be a value.
- **sub:** By inversion there is a $\mathsf{pc}' \sqsupseteq \mathsf{pc}$ and a τ' such that $\tau' \leqslant (\tau_1 + \tau_2)^{\mathsf{p}}$ and $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}'} v : \tau'$. We do inversion on the derivation of $\tau' \leqslant (\tau_1 + \tau_2)^{\mathsf{p}}$. The only applicable rule is **sub-policy**. Hence τ' has the form $A^{\mathsf{p}'}$ and $\mathsf{p}' \sqsubseteq \mathsf{p}$ and $A <: \tau_1 + \tau_2$. We do another inversion. The only applicable rule this time is **sub-sum**. Hence A has the form $\tau_1' + \tau_2'$ where $\tau_1' <: \tau_1$ and $\tau_2' <: \tau_2$. Hence $\tau' = (\tau_1' + \tau_2')^{\mathsf{p}'}$. By induction we get that there are is a v' s.t. $v = \mathtt{inl}\ v'$ or $v = \mathtt{inr}\ v'$.

□

Lemma 6.12. If $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} v : (\mathsf{ref}\ \tau)^{\mathsf{p}}$, then $v = l$ for some l.

Proof. By induction in the derivation.

- **loc:** The rule gives us that $v = l$ for some l.
- **sub** By inversion we have
  – A $\mathsf{pc}' \sqsubseteq \mathsf{pc}$ such that $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}'} v : \tau'$
  – $\tau' <: (\mathtt{ref}\ \tau)^{\mathsf{p}}$.

  We do inversion on $\tau' <: (\mathtt{ref}\ \tau)^{\mathsf{p}}$. The only applicable rule is **sub-policy**. Hence $\tau' = A^{\mathsf{p}'}$ and $\mathsf{p}' \sqsubseteq \mathsf{p}$ and $A <: \mathtt{ref}\ \tau$. We do another inversion. The only applicable rule is **sub-ref**. Hence $A = \mathtt{ref}\ \tau$. Hence $\tau' = (\mathtt{ref}\ \tau)^{\mathsf{p}'}$. Hence we get the claim by induction.

□

Lemma 6.13. If $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} v : \mathsf{unit}^{\mathsf{p}}$, then $v = ()$.

Proof. By induction on the derivation of $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} v : \mathsf{unit}^{\mathsf{p}}$.

- **unit**: In this case $v = ()$.
- **sub:** By inversion we have
  – A $\mathsf{pc}' \sqsubseteq \mathsf{pc}$ such that $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}'} v : \tau'$
  – $\tau' <: \mathtt{unit}^{\mathsf{p}}$.

We do inversion on $\tau' <: \mathtt{unit}^{p}$. The only applicable rule is **sub-policy**. Hence $\tau' = A^{p'}$ and $p' \sqsubseteq p$ and $A <: \mathtt{unit}$. We do another inversion. The only applicable rule is **sub-unit**. Hence $A = \mathtt{unit}$. Hence $\tau' = \mathtt{unit}^{p'}$ and we get the claim by induction.

□

Lemma 6.14. If $\Gamma; \Sigma; \theta \vdash_{pc} v : \mathcal{N}^{p}$, then $v = n$ and $n \in \mathbb{N}$.

Proof. By induction on the derivation of $\Gamma; \Sigma; \theta \vdash_{pc} v : \mathcal{N}^{p}$.

- **unit**: In this case $v = n$ and $n \in \mathbb{N}$.
- **sub:** By inversion we have
  - A $pc' \sqsubseteq pc$ such that $\Gamma; \Sigma; \theta \vdash_{pc'} v : \tau'$
  - $\tau' <: \mathcal{N}^{p}$.

  We do inversion on $\tau' <: \mathcal{N}^{p}$. The only applicable rule is **sub-policy**. Hence $\tau' = A^{p'}$ and $p' \sqsubseteq p$ and $A <: \mathcal{N}$. We do another inversion. The only applicable rule is **sub-nat**. Hence $A = \mathcal{N}$. Hence $\tau' = \mathcal{N}^{p'}$ and we get the claim by induction.

□

Lemma 6.15. If $\Gamma; \Sigma; \theta \vdash_{pc} v : A^{p}$, then also $\forall pc'.\ \Gamma; \Sigma; \theta \vdash_{pc'} v : A^{\perp}$.

Proof. By induction in the derivation. In all cases but **sub** $p = \perp$ already and the pc is either arbitrary or we get the changed pc by induction. In the case for **sub** we get $\Gamma; \Sigma; \theta \vdash_{pc''} v : B^{q}$ by inversion for some $pc'' \sqsupseteq pc$ and $B^{q} <: A^{p}$. By inversion of **sub-policy**, which is the only applicable rule, we get $B <: A$ and $q \sqsubseteq p$. Induction gives us $\Gamma; \Sigma; \theta \vdash_{pc'} v : B^{\perp}$. By **sub-policy** and Lemma 4.1 we get $B^{\perp} <: A^{\perp}$ and $pc' \sqsubseteq pc'$. Finally we get $\Gamma; \Sigma; \theta \vdash_{pc'} v : A^{\perp}$ with **sub**. □

Corollary 6.16. If $\Gamma; \Sigma; \theta \vdash_{pc} v : A^{p}$, then for all policies q, pc' we have $\Gamma; \Sigma; \theta \vdash_{pc'} v : A^{q}$.

Proof. By Lemma 6.15 $\Gamma; \Sigma; \theta \vdash_{pc'} v : A^{\perp}$. As $\perp$ is the least policy (4.19) we have $A^{\perp} <: A^{q}$ by Lemma 5.1 and **sub-policy** and hence by Lemma 4.1 and **sub** $\Gamma; \Sigma; \theta \vdash_{pc'} v : A^{q}$. □

Definition 6.2 (Policy of an observation)**.** We define the policy of an observation:

$$\begin{aligned}
\mathrm{pol}(l_{A^{p}}(v)) &\triangleq p \\
\mathrm{pol}(\mathsf{open}(\sigma)) &\triangleq \mathrm{pol}(\sigma) \\
\mathrm{pol}(\mathsf{close}(\sigma)) &\triangleq \mathrm{pol}(\sigma) \\
\mathrm{pol}(\mathsf{unopen}(\sigma)) &\triangleq \mathrm{pol}(\sigma) \\
\mathrm{pol}(\mathsf{unclose}(\sigma)) &\triangleq \mathrm{pol}(\sigma)
\end{aligned}$$

In all other cases the policy is undefined.

Lemma 6.17 (Progress)**.** If $\cdot; \Sigma; \theta \vdash_{pc} e : \tau$, then either e is a value or $\forall S, \Sigma'. S \triangleright. (\theta) \to \exists e', \omega, S', \Sigma''.\ \Sigma' \vdash e, S \xrightarrow{\omega; \Sigma''} e', S'$

Proof. By induction on the derivation.

- **var:** This rule could not have been applied because the context is empty.
- **nat:** Numbers are values.
- **open:**

$$\frac{\cdot; \Sigma \cup \{\sigma\}; \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq \mathrm{pol}(\sigma)}{\cdot; \Sigma; \theta \vdash_{pc} \mathsf{open}\ \sigma\ \mathsf{in}\ e : \tau}\ \textbf{open}$$

  Let $S \triangleright. (\theta)$ and Σ' be a lock set.
  By **Eopen** $\Sigma' \vdash \mathsf{open}\ \sigma\ \mathsf{in}\ e, S \xrightarrow{\mathsf{open}(\sigma); \Sigma'} e\ \mathsf{then}\ \mathsf{unopen}\ \sigma, S$.

- **opened:**

$$\frac{\cdot; \Sigma \cup \{\sigma\}; \theta \vdash_{\mathsf{pc}} e : \tau \qquad \mathsf{pc} \sqsubseteq \mathrm{pol}(\sigma)}{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} e \text{ then unopen } \sigma : \tau}\ \textbf{opened}$$

  Let $S \triangleright (\theta)$ and Σ' be a lock set. By induction either e is a value v or there are e', ω, Σ'', S', s.t $\Sigma' \cup \{\sigma\} \vdash e, S \xrightarrow{\omega;\Sigma''} e', S'$.

  In the first case by **EopenedBeta** $\Sigma' \vdash v \text{ then unopen } \sigma, S \xrightarrow{\mathrm{unopen}(\sigma);\Sigma'} v, S$.

  In the second case $\Sigma' \vdash e \text{ then unopen } \sigma, S \xrightarrow{\omega;\Sigma''} e' \text{ then unopen } \sigma, S'$ by **Eopened**.

- **λ:** Functions are values.

- **prod:**

$$\frac{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} e_1 : \tau_1 \qquad \cdot; \Sigma; \theta \vdash_{\mathsf{pc}} e_2 : \tau_2}{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} (e_1, e_2) : (\tau_1 \times \tau_2)^{\perp}}\ \textbf{prod}$$

  By induction either e_1 is a value or $\forall S, \Sigma'. S \triangleright (\theta) \to \exists e_1', \omega_1, S_1', \Sigma_1.\ \Sigma' \vdash e_1, S \xrightarrow{\omega_1;\Sigma_1} e_1', S_1'$. Similarly by induction either e_2 is a value or $\forall S, \Sigma'. S \triangleright (\theta) \to \exists e_2', \omega_2, S_2', \Sigma_2.\ \Sigma' \vdash e_2, S \xrightarrow{\omega_2;\Sigma_2} e_2', S_2'$.

  There are several cases:

  - Both e_1 and e_2 are values. Then (e_1, e_2) is a value.
  - e_1 is not a value. Let Σ' be a lock set and $S \triangleright (\theta)$. Then $\exists e_1', \omega_1, S_1', \Sigma_1.\ \Sigma' \vdash e_1, S \xrightarrow{\omega_1;\Sigma_1} e_1', S_1'$. By **EPairl** $\Sigma' \vdash (e_1, e_2), S \xrightarrow{\omega_1;\Sigma_1} (e_1', e_2), S_1'$.
  - e_1 is a value v and e_2 is not a value. Let Σ' be a lock set and $S \triangleright (\theta)$. Then $\exists e_2', \omega_2, S_2', \Sigma_2.\ \Sigma' \vdash e_2, S \xrightarrow{\omega_2;\Sigma_2} e_2', S_2'$. By **EPairr** $\Sigma' \vdash (v, e_2), S \xrightarrow{\omega_2;\Sigma_2} (v, e_2'), S_2'$.

- **app:**

$$\frac{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} e_1 : (\tau_1 \xrightarrow{\Sigma'', \mathsf{pc}'} \tau_2)^{\mathsf{p}} \qquad \cdot; \Sigma; \theta \vdash_{\mathsf{pc}} e_2 : \tau_1' \qquad \mathsf{p} \sqsubseteq \tau_2 \qquad \mathsf{pc} \sqcup \mathsf{p} \sqsubseteq \mathsf{pc}' \qquad \tau_1' <: \tau_1 \qquad \Sigma \supseteq \Sigma''}{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} e_1\ e_2 : \tau_2}\ \textbf{app}$$

  By induction either e_1 is a value or $\forall S, \Sigma'.\ S \triangleright (\theta) \to \exists e_1', \omega_1, S_1', \Sigma_1.\ \Sigma' \vdash e_1, S \xrightarrow{\omega_1;\Sigma_1} e_1', S_1'$. Similarly by induction either e_2 is a value or $\forall S, \Sigma'. S \triangleright (\theta) \to \exists e_2', \omega_2, S_2', \Sigma_2.\ \Sigma' \vdash e_2, S \xrightarrow{\omega_2;\Sigma_2} e_2', S_2'$.

  There are several cases:

  - e_1 is not a value. Let Σ' be a lock set and $S \triangleright (\theta)$. Then $\exists e_1', \omega_1, S_1', \Sigma_1.\ \Sigma' \vdash e_1, S \xrightarrow{\omega_1;\Sigma_1} e_1', S_1'$. By **EAppl** $\Sigma' \vdash e_1\ e_2, S \xrightarrow{\omega_1;\Sigma_1} e_1'\ e_2, S_1'$.
  - e_1 is a value v and e_2 is not a value. Then by Lemma 6.5 e_1 has the form $\lambda x.\, e$. Let Σ' be a lock set and $S \triangleright (\theta)$. Then $\exists e_2', \omega_2, S_2', \Sigma_2.\ \Sigma' \vdash e_2, S \xrightarrow{\omega_2;\Sigma_2} e_2', S_2'$. By **EAppr** $\Sigma' \vdash (\lambda x.\, e)\ e_2, S \xrightarrow{\omega_2;\Sigma_2} (\lambda x.\, e)\ e_2', S_2'$.
  - Both e_1 and e_2 are values. Then by Lemma 6.5 e_1 has the form $\lambda x.\, e$. Say $e_2 = v$. Let Σ' be a lock set and $S \triangleright (\theta)$. Then by **EAppBeta** $\Sigma' \vdash (\lambda x.\, e)\ v, S \xrightarrow{\epsilon;\Sigma'} e[x \mapsto v], S$.

- **fst:**

$$\frac{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} e : (\tau_1 \times \tau_2)^{\mathsf{p}} \qquad \mathsf{p} \sqsubseteq \tau_1}{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} \mathsf{fst}\,(e) : \tau_1}\ \textbf{fst}$$

  Let $S \triangleright (\theta)$ and Σ' be a lock set. By induction either e is a value v or there are e', ω, Σ'', S', s.t $\Sigma' \vdash e, S \xrightarrow{\omega;\Sigma''} e', S'$.

  In the first case by Lemma 6.10 $v = (v_1, v_2)$. Hence by **EFstBeta** $\Sigma' \vdash \mathsf{fst}\,((v_1, v_2))\,, S \xrightarrow{\epsilon;\Sigma'} v_1, S$.

  In the second case by **EFst** $\Sigma' \vdash \mathsf{fst}\,(e)\,, S \xrightarrow{\omega;\Sigma''} \mathsf{fst}\,(e')\,, S'$.

- **snd:**

$$\frac{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} e : (\tau_1 \times \tau_2)^{\mathsf{p}} \qquad \mathsf{p} \sqsubseteq \tau_2}{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} \mathsf{snd}\,(e) : \tau_2}\ \textbf{snd}$$

  Let $S \triangleright. (\theta)$ and Σ' be a lock set. By induction either e is a value v or there are e', ω, Σ'', S', s.t $\Sigma' \vdash e, S \xrightarrow{\omega;\Sigma''} e', S'$.

  In the first case by Lemma 6.10 $v = (v_1, v_2)$. Hence by **ESndBeta** $\Sigma' \vdash \mathsf{snd}\,((v_1, v_2))\,, S \xrightarrow{\epsilon;\Sigma'} v_2, S$.

  In the second case by **ESnd** $\Sigma' \vdash \mathsf{snd}\,(e)\,, S \xrightarrow{\omega;\Sigma''} \mathsf{snd}\,(e')\,, S'$.

- **inl:**

$$\frac{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau_1}{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} \mathsf{inl}\,(e) : (\tau_1 + \tau_2)^{\perp}}\ \textbf{inl}$$

  By induction either e is a value v or $\forall S, \Sigma'.\ S \triangleright. (\theta) \to \exists e', \omega, S', \Sigma''.\ \Sigma' \vdash e, S \xrightarrow{\omega;\Sigma''} e', S'$.

  In the first case $\mathsf{inl}\,(v)$ is a value. In the second case let Σ' be a lock-set and S such that $S \triangleright. (\theta)$. Then there are e', Σ'', ω, S' such that $\Sigma' \vdash e, S \xrightarrow{\omega;\Sigma''} e', S'$. Hence by **EInl** $\Sigma' \vdash \mathsf{inl}\,(e)\,, S \xrightarrow{\omega;\Sigma''} \mathsf{inl}\,(e')\,, S'$.

- **inr:**

$$\frac{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau_2}{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} \mathsf{inr}\,(e) : (\tau_1 + \tau_2)^{\perp}}\ \textbf{inr}$$

  By induction either e is a value v or $\forall S, \Sigma'.\ S \triangleright. (\theta) \to \exists e', \omega, S', \Sigma''.\ \Sigma' \vdash e, S \xrightarrow{\omega;\Sigma''} e', S'$.

  In the first case $\mathsf{inr}\,(v)$ is a value. In the second case let Σ' be a lock-set and S such that $S \triangleright. (\theta)$. Then there are e', Σ'', ω, S' such that $\Sigma' \vdash e, S \xrightarrow{\omega;\Sigma''} e', S'$. Hence by **EInr** $\Sigma' \vdash \mathsf{inr}\,(e)\,, S \xrightarrow{\omega;\Sigma''} \mathsf{inr}\,(e')\,, S'$.

- **case:**

$$\frac{\begin{array}{c}\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} e : (\tau_1 + \tau_2)^{\mathsf{p}} \\ \mathsf{p} \sqsubseteq \tau \qquad x : \tau_1'; \Sigma; \theta \vdash_{\mathsf{pc} \sqcup \mathsf{p}} e_1 : \tau \qquad y : \tau_2'; \Sigma; \theta \vdash_{\mathsf{pc} \sqcup \mathsf{p}} e_2 : \tau \qquad \tau_1 <: \tau_1' \qquad \tau_2 <: \tau_2'\end{array}}{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} \mathsf{case}\ e\ \mathsf{of}\ |\,\mathsf{inl}\,(x) \Rightarrow e_1\ |\,\mathsf{inr}\,(y) \Rightarrow e_2 : \tau}\ \textbf{case}$$

  Let Σ' be a lock-set and S such that $S \triangleright. (\theta)$. By induction either e is a value v or there are e', S', ω, Σ'' such that $\Sigma' \vdash e, S \xrightarrow{\omega;\Sigma''} e', S'$.

  In the first case there are two options. Either $v = \mathsf{inl}\,(v')$ or $v = \mathsf{inr}\,(v')$ for some v' (see Lemma 6.11).

  - $v = \mathsf{inl}\,(v')$. Then by **ECasel**
    $\Sigma' \vdash (\mathsf{case}\ \mathsf{inl}\,(v')\ \mathsf{of}\ |\,\mathsf{inl}\,(x) \Rightarrow e_1\ |\,\mathsf{inr}\,(y) \Rightarrow e_2), S \xrightarrow{\epsilon;\Sigma'} e_1[x \mapsto v'], S$.
  - $v = \mathsf{inl}\,(v')$. Then by **ECaser**
    $\Sigma' \vdash (\mathsf{case}\ \mathsf{inr}\,(v')\ \mathsf{of}\ |\,\mathsf{inl}\,(x) \Rightarrow e_1\ |\,\mathsf{inr}\,(y) \Rightarrow e_2), S \xrightarrow{\epsilon;\Sigma'} e_2[x \mapsto v'], S$.

  In the second case by **ECase** $\Sigma' \vdash \mathsf{case}\ e\ \mathsf{of}\ |\,\mathsf{inl}\,(x) \Rightarrow e_1\ |\,\mathsf{inr}\,(y) \Rightarrow e_2, S \xrightarrow{\omega;\Sigma''} \mathsf{case}\ e'\ \mathsf{of}\ |\,\mathsf{inl}\,(x) \Rightarrow e_1\ |\,\mathsf{inr}\,(y) \Rightarrow e_2, S'$.

- **new:**

$$\frac{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau' \qquad \mathsf{pc} \sqsubseteq \tau \qquad \tau'(\Sigma) <: \tau}{\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} \mathsf{new}\,(e, \tau) : (\mathsf{ref}\ \tau)^{\perp}}\ \textbf{new}$$

  Let Σ' be a lock-set and S such that $S \triangleright. (\theta)$. By induction either e is a value v or $\Sigma' \vdash e, S \xrightarrow{\omega;\Sigma''} e', S'$.

In the first case let $l \notin \mathrm{dom}(S)$. Then by **ENewBeta** $\Sigma' \vdash \mathsf{new}\,(v, \tau)\,,\ S \xrightarrow{l_\tau(\nu);\Sigma'} l,\ S \cup \{l \rightarrowtail (v, \tau)\}$.

In the second case $\Sigma' \vdash \mathsf{new}\,(e, \tau)\,,\ S \xrightarrow{\omega;\Sigma''} \mathsf{new}\,(e', \tau)\,,\ S'$.

- **loc:** Locations are values.
- **sub:**

$$\frac{\cdot; \Sigma; \theta \vdash_{pc'} e : \tau' \qquad pc \sqsubseteq pc' \qquad \tau' <: \tau}{\cdot; \Sigma; \theta \vdash_{pc} e : \tau}\ \textbf{sub}$$

We get the claim from the induction hypothesis.

deref:

$$\frac{\cdot; \Sigma; \theta \vdash_{pc} e : (\mathsf{ref}\ \tau)^p \qquad p \sqsubseteq \tau' \qquad \tau <: \tau'}{\cdot; \Sigma; \theta \vdash_{pc} !\,e : \tau'}\ \textbf{deref}$$

Let Σ' be a lock-set and S such that $S \triangleright (\theta)$. By induction either e is a value v or there are e', S', ω, Σ'' such that $\Sigma' \vdash e,\ S \xrightarrow{\omega;\Sigma''} e',\ S'$.

In the first case there is some l such that $v = l$ by Lemma 6.12. Hence $\cdot; \Sigma; \theta \vdash_{pc} l : (\mathsf{ref}\ \tau)^p$. By Lemma 6.9 $\theta(l) = \tau$. In particular $l \in \mathrm{dom}(\theta)$ Because $S \triangleright (\theta)$ and $l \in \mathrm{dom}(\theta)$, $l \in \mathrm{dom}(S)$. Hence there are v, τ such that $(l \rightarrowtail (v, \tau)) \in S$. Therefore by **EDerefBeta** $\Sigma' \vdash !\,l,\ S \xrightarrow{\epsilon;\Sigma'} v,\ S$.

In the second case we have $\Sigma' \vdash !\,e,\ S \xrightarrow{\omega;\Sigma''} !\,e',\ S'$ by **EDeref**.

- **assign:**

$$\frac{\cdot; \Sigma; \theta \vdash_{pc} e : (\mathsf{ref}\ \tau')^p \qquad \tau(\Sigma) <: \tau' \qquad \cdot; \Sigma; \theta \vdash_{pc} e' : \tau \qquad pc \sqcup p \sqsubseteq \tau'}{\cdot; \Sigma; \theta \vdash_{pc} e := e' : \mathsf{unit}^\perp}\ \textbf{assign}$$

Let Σ' be a lock-set and S such that $S \triangleright (\theta)$. By induction either e is a value v or there are $e'', S', \omega, \Sigma''$ such that $\Sigma' \vdash e,\ S \xrightarrow{\omega;\Sigma''} e'',\ S'$. Similarly either e' is a value v' or there are $e''', S'', \omega', \Sigma''$ such that $\Sigma' \vdash e',\ S \xrightarrow{\omega';\Sigma''} e''',\ S''$.

There are several cases:

- $\Sigma' \vdash e,\ S \xrightarrow{\omega;\Sigma''} e'',\ S'$. In this case $\Sigma' \vdash e := e',\ S \xrightarrow{\omega;\Sigma''} e'' := e',\ S'$ by **Eassignl**.
- e is a value v and $\Sigma' \vdash e',\ S \xrightarrow{\omega';\Sigma''} e''',\ S''$. Then by Lemma 6.12 $v = l$ for some l. Hence $\Sigma' \vdash l := e',\ S \xrightarrow{\omega';\Sigma''} l := e''',\ S''$ by **Eassignr**.
- Both e and e' are values v and v' respectively. In that case $v = l$ for some l by Lemma 6.12. By Lemma 6.9 $\theta(l) = \tau'$. Hence $l \in \mathrm{dom}(\theta)$. Consequently we get $l \in \mathrm{dom}(S)$ from $S \triangleright (\theta)$. Let $\tau'' = \mathsf{type}(S, l)$. Then $\Sigma' \vdash l := v',\ S \xrightarrow{l_{\tau''}(v');\Sigma'} (),\ S[l \rightarrowtail (v', \tau'')]$ by **Eassign**.

- **unit:** $()$ is a value.
- **close**

$$\frac{\cdot; \Sigma \backslash \{\sigma\}; \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq \mathrm{pol}(\sigma)}{\cdot; \Sigma; \theta \vdash_{pc} \mathsf{close}\ \sigma\ \mathsf{in}\ e : \tau}\ \textbf{close}$$

Let $S \triangleright (\theta)$ and Σ' be a lock set. By **Eclose** $\Sigma' \vdash \mathsf{close}\ \sigma\ \mathsf{in}\ e,\ S \xrightarrow{\mathsf{close}(\sigma);\Sigma'} e\ \mathsf{then\ unclose}\ \sigma,\ S$.

- **closed:**

$$\frac{\cdot; \Sigma \backslash \{\sigma\}; \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq \mathrm{pol}(\sigma)}{\cdot; \Sigma; \theta \vdash_{pc} e\ \mathsf{then\ unclose}\ \sigma : \tau}\ \textbf{closed}$$

Let $S \triangleright (\theta)$ and Σ' be a lock set. By induction either e is a value v or there are e', ω, Σ'', S', s.t $\Sigma' \setminus \{\sigma\} \vdash e, S \xrightarrow{\omega;\Sigma''} e', S'$.

In the first case by **EclosedBeta** $\Sigma' \vdash v \text{ then unclose } \sigma, S \xrightarrow{\text{unclose}(\sigma);\Sigma'} v, S$.

In the second case $\Sigma' \vdash e \text{ then unclose } \sigma, S \xrightarrow{\omega;\Sigma''} e' \text{ then unclose } \sigma, S'$ by **Eclosed**.

- **when:**
$$\frac{\cdot; \Sigma \cup \{\sigma\}; \theta \vdash_{pc \sqcup pol(\sigma)} e_1 : \tau \qquad \cdot; \Sigma; \theta \vdash_{pc \sqcup pol(\sigma)} e_2 : \tau \qquad pol(\sigma) \sqsubseteq \tau}{\cdot; \Sigma; \theta \vdash_{pc} \text{when } \sigma \text{ then } e_1 \text{ else } e_2 : \tau} \textbf{ when}$$

  Let $S \triangleright (\theta)$ and Σ' be a lock set. We do case analysis on $\sigma \in \Sigma'$.

  – $\sigma \in \Sigma'$. By induction either e_1 is a value v_1 or there are $e_1', \omega_1, \Sigma_1', S_1'$, s.t $\Sigma' \vdash e_1, S \xrightarrow{\omega_1;\Sigma_1'} e_1', S_1'$.

  In the first case by **EWhenOpenBeta** $\Sigma' \vdash \text{when } \sigma \text{ then } v_1 \text{ else } e_2, S \xrightarrow{\epsilon;\Sigma'} v_1, S$.

  In the second case by **EWhenOpen**
  $\Sigma' \vdash \text{when } \sigma \text{ then } e_1 \text{ else } e_2, S \xrightarrow{\omega_1;\Sigma_1'} \text{when } \sigma \text{ then } e_1' \text{ else } e_2, S_1'$.

  – $\sigma \notin \Sigma'$. By induction either e_2 is a value v_2 or there are $e_2', \omega_2, \Sigma_2', S_2'$, s.t. $\Sigma' \vdash e_2, S \xrightarrow{\omega_2;\Sigma_2'} e_2', S_2'$. In the first case by **EWhenClosedBeta** $\Sigma' \vdash \text{when } \sigma \text{ then } e_1 \text{ else } v_2, S \xrightarrow{\epsilon;\Sigma'} v_2, S$.

  In the second case by **EWhenClosed**
  $\text{when } \sigma \text{ then } e_1 \text{ else } e_2, \Sigma', S, \text{when } \sigma \text{ then } e_1 \text{ else } e_2', S_2', \omega_2, \Sigma_2'$.

□

Lemma 6.18 (Preservation)**.** $\Gamma; \Sigma; \theta \vdash_{pc} e : \tau \to \forall \Sigma'.\ \Sigma' \vdash e, S \xrightarrow{\omega;\Sigma''} e', S' \wedge S \triangleright_\Gamma (\theta) \to \exists \theta'. \theta' \sqsupseteq \theta \wedge \Gamma; \Sigma; \theta' \vdash_{pc} e' : \tau \wedge S' \triangleright_\Gamma (\theta')$.

Proof. By induction on the typing derivation.

- **Var:** Variables don't reduce.
- **nat:** Numbers are values and don't reduce.
- **open:**
$$\frac{\Gamma; \Sigma \cup \{\sigma\}; \Delta, \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq pol(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} \text{open}(\sigma) \text{ in } e : \tau} \textbf{ open}$$

  The reduction could only have happened with **Eopen**:

$$\frac{}{\text{open } \sigma \text{ in } e, \Sigma', S \succ \text{opened } \sigma \text{ in } e, S, \text{open}(\sigma), \Sigma'} \textbf{ Eopen}$$

  It suffices to show $\Gamma; \Sigma; \theta \vdash_{pc} \text{opened } \sigma \text{ in } e : \tau$ which we get from **opened** using the premisses from the **open** rule.

- **opened:**
$$\frac{\Gamma; \Sigma \cup \{\sigma\}; \Delta, \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq pol(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} \text{opened}(\sigma) \text{ in } e : \tau} \textbf{ opened}$$

  There are two cases:

  – The reduction happened with **Eopened**:

$$\frac{e, \Sigma' \cup \{\sigma\}, S \succ e', S', \omega, \Sigma''}{\text{opened } \sigma \text{ in } e, \Sigma', S \succ \text{opened } \sigma \text{ in } e', S', \omega, \Sigma''} \textbf{ Eopened}$$

  By the assumptions of the rules **opened** and **Eopened** and by $S \triangleright (\theta)$ we get that there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma; \Sigma \cup \{\sigma\}; \theta' \vdash_{pc} e' : \tau$ using the induction hypothesis. As we already know $pc \sqsubseteq pol(\sigma)$, we get $\Gamma; \Sigma; \theta' \vdash_{pc} \text{open } \sigma \text{ in } e' : \tau$ using **opened**.

– The reduction happened with **EopenBeta**:

$$\frac{}{\mathtt{open}\ \sigma(\vec{a})\ \mathtt{in}\ v, \Sigma', S \succ v, S, \mathtt{unopen}(\sigma), \Sigma'}\ \textbf{EopenBeta}$$

In this case $e = v$. It suffices to show $\Gamma; \Sigma; \theta \vdash_{pc} v : \tau$.
We already know $\Gamma; \Sigma \cup \{\sigma\}; \theta \vdash_{pc} v : \tau$. The goal follows by Lemma 6.3.

- **λ:** Functions are values and don't reduce.
- **prod:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e_1 : \tau_1 \qquad \Gamma; \Sigma; \theta \vdash_{pc} e_2 : \tau_2}{\Gamma; \Sigma; \theta \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^{\perp}}\ \textbf{prod}$$

There are two cases:

– The reduction happened with **EPairl**:

$$\frac{e_1, \Sigma', S \succ e_1', S', \omega, \Sigma''}{(e_1, e_2), \Sigma', S \succ (e_1', e_2), S', \omega, \Sigma''}\ \textbf{EPairl}$$

We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma, \Sigma, \theta' \vdash_{pc} e_1' : \tau_1$. By Weakening also $\Gamma, \Sigma, \theta' \vdash_{pc} e_2 : \tau_2$. We get the claim by **prod**.

– The reduction happened with **EPairr**

$$\frac{e_2, \Sigma', S \succ e_2', S', \omega, \Sigma''}{(v, e_2), \Sigma', S \succ (v, e_2'), S', \omega, \Sigma''}\ \textbf{EPairr}$$

In this case $e_1 = v$. We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma, \Sigma, \theta' \vdash_{pc} e_2' : \tau_2$. By Weakening also $\Gamma, \Sigma, \theta' \vdash_{pc} v : \tau_1$. We get the claim by **prod**.

- **app:**

$$\frac{\begin{array}{c}\Gamma; \Sigma; \theta \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^{p} \\ \Gamma; \Sigma; \theta \vdash_{pc} e_2 : \tau_1' \qquad p \sqsubseteq \tau_2 \qquad pc \sqcup p \sqsubseteq p_e \qquad \tau_1' <: \tau_1 \qquad \Sigma \supseteq \Sigma'\end{array}}{\Gamma; \Sigma; \theta \vdash_{pc} e_1\ e_2 : \tau_2}\ \textbf{app}$$

There are three cases:

– The reduction happened with **EAppl**:

$$\frac{e_1, \Sigma'', S \succ e_1', S', \omega, \Sigma'''}{e_1\ e_2, \Sigma'', S \succ e_1'\ e_2, S', \omega, \Sigma'''}\ \textbf{EAppl}$$

We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma, \Sigma, \theta' \vdash_{pc} e_1' : (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^{p}$. By Weakening also $\Gamma, \Sigma, \theta' \vdash_{pc} e_2 : \tau_1'$. We get $\Gamma, \Sigma, \theta' \vdash_{pc} e_1'\ e_2 : \tau_2$ by **app**.

– The reduction happened with **EAppr**:

$$\frac{e_2, \Sigma'', S \succ e_2', S', \omega, \Sigma'''}{(\lambda\ x.e)\ e_2, \Sigma'', S \succ (\lambda\ x.e)\ e_2', S', \omega, \Sigma'''}\ \textbf{EAppr}$$

In this case $e_1 = \lambda\ x.e$. We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma, \Sigma, \theta' \vdash_{pc} e_2' : \tau_1'$. By Weakening also $\Gamma, \Sigma, \theta' \vdash_{pc} \lambda\ x.e : (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^{p}$. We get $\Gamma, \Sigma, \theta' \vdash_{pc} (\lambda\ x.e)\ e_2' : \tau_2$ by **app**.

– The reduction happened with **EAppBeta**:

$$\frac{}{(\lambda\ x.e)\ v, \Sigma'', S \succ [v/x]e, S, \epsilon, \Sigma''}\ \textbf{EAppBeta}$$

In this case $e_1 = \lambda\ x.e$ and $e_2 = v$. It suffices to show $\Gamma; \Sigma; \theta \vdash_{pc} [v/x]e : \tau_2$. By Lemma 6.5 $\Gamma, x : \tau_1; \Sigma'; \theta \vdash_{p_e} e : \tau_2$. By Weakening we get $\Gamma, x : \tau_1; \Sigma; \theta \vdash_{p_e} e : \tau_2$. With **sub** we get $\Gamma, x : \tau_1; \Sigma; \theta \vdash_{pc} e : \tau_2$ because $pc \sqcup p \sqsubseteq p_e$ and hence also $pc \sqsubseteq p_e$ by Lemma 4.13 and Lemma 4.1. With **sub** we get $\Gamma; \Sigma; \theta \vdash_{pc} v : \tau_1$. Hence by Lemma 6.8 $\Gamma; \Sigma; \theta \vdash_{pc} [v/x]e : \tau_2$ which is what needed to be shown.

- **fst:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} e : (\tau_1 \times \tau_2)^{\mathsf{p}} \qquad \mathsf{p} \sqsubseteq \tau_1}{\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} \mathtt{fst}(e) : \tau_1}\ \textbf{fst}$$

  There are two cases:

  – The reduction happened with **EFst**.

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{\mathtt{fst}(e), \Sigma', S \succ \mathtt{fst}(e'), S', \omega, \Sigma''}\ \textbf{EFst}$$

  We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma; \Sigma; \theta' \vdash_{\mathsf{pc}} e' : (\tau_1 \times \tau_2)^{\mathsf{p}}$. We obtain the goal with **fst**.

  – The reduction happened with **EFstBeta**

$$\frac{}{\mathtt{fst}((v, v')), \Sigma', S \succ v, S, \epsilon, \Sigma'}\ \textbf{EFstBeta}$$

  In this case $e = (v, v')$. By Lemma 6.6 we get $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} v : \tau_1$ which is sufficient to show the goal.

- **snd:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} e : (\tau_1 \times \tau_2)^{\mathsf{p}} \qquad \mathsf{p} \sqsubseteq \tau_2}{\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} \mathtt{snd}(e) : \tau_2}\ \textbf{snd}$$

  There are two cases:

  – The reduction happened with **ESnd**.

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{\mathtt{snd}(e), \Sigma', S \succ \mathtt{snd}(e'), S', \omega, \Sigma''}\ \textbf{ESnd}$$

  We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta'$ and $\Gamma; \Sigma; \theta' \vdash_{\mathsf{pc}} e' : (\tau_1 \times \tau_2)^{\mathsf{p}}$. We obtain the goal with **snd**.

  – The reduction happened with **ESndBeta**

$$\frac{}{\mathtt{snd}((v, v')), \Sigma', S \succ v', S, \epsilon, \Sigma'}\ \textbf{ESndBeta}$$

  In this case $e = (v, v')$. By Lemma 6.6 we get $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} v' : \tau_2$ which is sufficient to show the goal.

- **inl:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau_1}{\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} \mathtt{inl}(e) : (\tau_1 + \tau_2)^{\perp}}\ \textbf{inl}$$

  The reduction could only have happened with **EInl**.

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{\mathtt{inl}(e), \Sigma', S \succ \mathtt{inl}(e'), S', \omega, \Sigma''}\ \textbf{EInl}$$

  We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma; \Sigma; \theta' \vdash_{\mathsf{pc}} e' : \tau_1$. We obtain the goal with **inl**.

- **inr:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau_2}{\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} \mathtt{inr}(e) : (\tau_1 + \tau_2)^{\perp}}\ \textbf{inr}$$

  The reduction could only have happened with **EInr**

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{\mathtt{inr}(e), \Sigma', S \succ \mathtt{inr}(e'), S', \omega, \Sigma''}\ \textbf{EInr}$$

  We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there are is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma; \Sigma; \theta' \vdash_{\mathsf{pc}} e' : \tau_2$. We obtain the goal with **inr**.

- **case:**

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e : (\tau_1 + \tau_2)^p \qquad p \sqsubseteq \tau \qquad \Gamma, x : \tau_1'; \Sigma; \theta \vdash_{pc \sqcup p} e_1 : \tau \qquad \Gamma, y : \tau_2'; \Sigma; \theta \vdash_{pc \sqcup p} e_2 : \tau \qquad \tau_1 <: \tau_1' \qquad \tau_2 <: \tau_2'}{\Gamma;\Sigma;\theta \vdash_{pc} case(e, x.e_1, y.e_2) : \tau}\ \textbf{case}$$

  There are three cases:

  – The reduction happened with **ECase**:

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{case(e, x.e_1, y.e_2), \Sigma', S \succ case(e', x.e_1, y.e_2), S', \omega, \Sigma''}\ \textbf{ECase}$$

  We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma;\Sigma;\theta' \vdash_{pc} e' : (\tau_1 + \tau_2)^p$. We get $\Gamma, x : \tau_1'; \Sigma; \theta' \vdash_{pc \sqcup p} e_1 : \tau$ and $\Gamma, y : \tau_2'; \Sigma; \theta' \vdash_{pc \sqcup p} e_2 : \tau$ by Weakening. We get $\Gamma;\Sigma;\theta' \vdash_{pc} case(e', x.e_1, y.e_2) : \tau$ with **case**.

  – The reduction happened with **ECasel**:

$$\frac{}{case(inl\ v, x.e_1, y.e_2), \Sigma', S \succ [v/x]e_1, S, \epsilon, \Sigma'}\ \textbf{ECasel}$$

  In this case $e = inl\ v$. It suffices to show $\Gamma;\Sigma;\theta \vdash_{pc} [v/x]e_1 : \tau$. We already know $\Gamma, x : \tau_1'; \Sigma; \theta \vdash_{pc \sqcup p} e_1 : \tau$. We get $\Gamma;\Sigma;\theta \vdash_{pc} v : \tau_1$ by Lemma 6.7. From this we get $\Gamma, x : \tau_1'; \Sigma; \theta \vdash_{pc} e_1 : \tau$ and $\Gamma;\Sigma;\theta \vdash_{pc} v : \tau_1'$ with **sub** and Lemma 4.6. We get the goal by Lemma 6.8.

  – The reduction happened with **ECaser**:

$$\frac{}{case(inr\ v, x.e_1, y.e_2), \Sigma', S \succ [v/y]e_2, S, \epsilon, \Sigma'}\ \textbf{ECaser}$$

  In this case $e = inr\ v$. It suffices to show $\Gamma;\Sigma;\theta \vdash_{pc} [v/x]e_2 : \tau$. We already know $\Gamma, x : \tau_2'; \Sigma; \theta \vdash_{pc \sqcup p} e_2 : \tau$. We get $\Gamma;\Sigma;\theta \vdash_{pc} v : \tau_1$ by Lemma 6.7. From this we get $\Gamma, x : \tau_2'; \Sigma; \theta \vdash_{pc} e_2 : \tau$ and $\Gamma;\Sigma;\theta \vdash_{pc} v : \tau_2'$ with **sub** and Lemma 4.6. We get the goal by Lemma 6.8.

- **new:**

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e : \tau' \qquad pc \sqsubseteq \tau \qquad \tau'(\Sigma) <: \tau}{\Gamma;\Sigma;\theta \vdash_{pc} new\ (e, \tau) : (ref\ \tau)^\perp}\ \textbf{new}$$

  There are two cases:

  – The reduction happened with **ENew**:

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{new\ (e, \tau), \Sigma', S \succ new\ (e', \tau), S', \omega, \Sigma''}\ \textbf{ENew}$$

  We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma;\Sigma;\theta' \vdash_{pc} e' : \tau'$. We obtain the goal with **new**.

  – The reduction happened with **ENewBeta**:

$$\frac{l \notin dom(S)}{new\ (v, \tau), \Sigma', S \succ l, S \cup \{l \rightarrowtail (v, \tau)\}, l_\tau(v), \Sigma'}\ \textbf{ENewBeta}$$

  In this case $e = v$. Let $\theta' = \theta[l \rightarrowtail \tau]$. It is clear that θ' extends θ. We show $S \cup \{l \rightarrowtail (v, \tau)\} \triangleright_\Gamma (\theta')$. We have to show

  * $dom(\theta') \subseteq dom(S \cup \{l \rightarrowtail (v, \tau)\})$.

    Let $l' \in dom(\theta')$. There are two cases:
    · $l' \in dom(\theta)$. Then by $S \triangleright_\Gamma (\theta)$ we have $l' \in dom(S)$ and consequently $l' \in dom(S \cup \{l \rightarrowtail (v, \tau)\})$.
    · $l' = l$. In this case $l' \in dom(\{l \rightarrowtail (v, \tau)\})$ and consequently $l' \in dom(S \cup \{l \rightarrowtail (v, \tau)\})$.
  * $\forall l' \in dom(\theta').\Gamma;\emptyset;\theta' \vdash_\perp S \cup \{l \rightarrowtail (v, \tau)\}(l') : \theta'(l')$

    Let $l' \in dom(\theta')$. There are two cases:

· $l' \in \mathrm{dom}(\theta)$. Then by $S \triangleright_\Gamma (\theta)$ we have $\Gamma; \emptyset; \theta \vdash_\bot S(l') : \theta(l')$. Because $\theta' \sqsupseteq \theta$ we have $\theta(l') = \theta'(l')$ and we have $S(l') = S \cup \{l \rightarrowtail (v, \tau)\}(l')$. Hence we have $\Gamma; \emptyset; \theta \vdash_\bot S \cup \{l \rightarrowtail (v, \tau)\}(l') : \theta'(l')$. We get the claim by Weakening.

· $l' = l$. In this case we have to show $\Gamma; \emptyset; \theta' \vdash_\bot v : \tau$. We already have $\Gamma; \Sigma; \theta \vdash_{pc} v : \tau'$. By weakening we get $\Gamma; \Sigma; \theta' \vdash_{pc} v : \tau'$. There must be types A and B and policies q and p such that $B^q = \tau'$ and $A^p = \tau$. Then $B^{q(\Sigma)} <: A^p$. By inversion we get $B <: A$. By Corollary 6.16 we get $\Gamma; \Sigma; \theta' \vdash_{pc} v : B^p$. By **sub-policy** and Lemma 4.1 $B^p <: A^p$. Hence $\Gamma; \Sigma; \theta' \vdash_\bot v : A^p$ by **sub** and Lemma 4.1 as $\bot \sqsubseteq pc$ by Lemma 4.19. We get $\Gamma; \emptyset; \theta' \vdash_\bot v : A^p$ by Lemma 6.3.

* $\forall l' \in \mathrm{dom}(\theta').\theta'(l') = \mathtt{type}(S \cup \{l \rightarrowtail (v, \tau)\}, l')$.
Let $l' \in \mathrm{dom}(\theta')$. Again there are two cases:
  · $l' \in \mathrm{dom}(\theta)$. Then by $S \triangleright_\Gamma (\theta)$ we have $\theta(l') = \mathtt{type}(S, l')$. As $l \notin \mathrm{dom}(S)$ we know $l' \neq l$. Hence $\mathtt{type}(S, l') = \mathtt{type}(S \cup \{l \rightarrowtail (v, \tau)\}, l')$. Therefore $\theta(l') = \mathtt{type}(S \cup \{l \rightarrowtail (v, \tau)\}, l')$
  · $l' = l$. In this case $\theta'(l) = \tau = \mathtt{type}(S \cup \{l \rightarrowtail (v, \tau)\}, l)$ by construction.
* $\forall l' \in \mathrm{dom}(S \cup \{l \rightarrowtail (v, \tau)\}).S \cup \{l \rightarrowtail (v, \tau)\}(l') \in \mathcal{V}$. There are two cases:
  · $l' \in \mathrm{dom}(S)$. Then we have $S \cup \{l \rightarrowtail (v, \tau)\}(l') = S(l)$ and $S(l) \in \mathcal{V}$ by $S \triangleright_\Gamma \theta$.
  · $l' = l$. In this cases it suffices to show $v \in \mathcal{V}$. This is the case by assumption.

All that remains to be shown is $\Gamma; \Sigma; \theta' \vdash_{pc} l : (\mathtt{ref}\ (\tau))^\bot$ which we have using **loc**.

- **loc:** Locations are values and do not reduce.
- **sub:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc'} e : \tau' \qquad pc \sqsubseteq pc' \qquad \tau' <: \tau}{\Gamma; \Sigma; \theta \vdash_{pc} e : \tau}\ \textbf{sub}$$

By induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma; \Sigma; \theta' \vdash_{pc'} e' : \tau'$. We get $\Gamma; \Sigma; \theta \vdash_{pc} e' : \tau$ by **sub**.

- **deref:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e : (\mathtt{ref}\ \tau')^p \qquad p \sqsubseteq \tau \qquad \tau' <: \tau}{\Gamma; \Sigma; \theta \vdash_{pc} !\, e : \tau}\ \textbf{deref}$$

There are two cases:

– The reduction happened with **EDeref**:

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{!e, \Sigma', S \succ !(e'), S', \omega, \Sigma''}\ \textbf{EDeref}$$

We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma; \Sigma; \theta' \vdash_{pc} e' : (\mathtt{ref}\ \tau)^p$. We obtain the goal with **deref**.

– The reduction happened with **EDerefBeta**:

$$\frac{l \rightarrowtail (v, \tau'') \in S}{!l, \Sigma', S \succ v, S, \epsilon, \Sigma'}\ \textbf{EDerefBeta}$$

In this case $e = l$. It suffices to show $\Gamma; \Sigma; \theta \vdash_{pc} v : \tau'$. We know $\Gamma; \Sigma; \theta \vdash_{pc} l : (\mathtt{ref}\ \tau)^p$ already. By Lemma 6.9 $\theta(l) = \tau$. By assumption $S \triangleright_\Gamma (\theta)$. Since $l \in \mathrm{dom}(\theta)$, this gives us $\Gamma; \emptyset; \theta \vdash_\bot v : \tau$ and $v \in \mathcal{V}$. We already know $\tau <: \tau'$ We get $\Gamma; \emptyset; \theta \vdash_\bot v : \tau'$ by **sub** and Lemma 4.1. Finally we get the goal by Weakening and Corollary 6.16.

- **assign:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e : (\mathrm{ref}(\tau'))^p \qquad \tau(\Sigma) <: \tau' \qquad \Gamma; \Sigma; \theta \vdash_{pc} e' : \tau \qquad pc \sqcup p \sqsubseteq \tau'}{\Gamma; \Sigma; \theta \vdash_{pc} e := e' : \mathtt{unit}^\bot}\ \textbf{assign}$$

There are three cases:

– The reduction happened with **Eassignl**

$$\frac{e, \Sigma', S \succ e'', S', \omega, \Sigma''}{e := e', \Sigma', S \succ e'' := e', S', \omega, \Sigma''}\ \textbf{Eassignl}$$

We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma; \Sigma; \theta' \vdash_{pc} e'' : (\mathtt{ref}\ \tau')^p$. By Weakening also $\Gamma; \Sigma; \theta' \vdash_{pc} e' : \tau$. We get $\Gamma; \Sigma; \theta' \vdash_{pc} e'' := e' : \mathtt{unit}^\perp$ by **assign**.

– The reduction happened with **Eassignr**

$$\frac{e', \Sigma', S \succ e'', S', \omega, \Sigma''}{l := e', \Sigma', S \succ l := e'', S', \omega, \Sigma''}\ \textbf{Eassignr}$$

In this case $e = l$. We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma; \Sigma; \theta' \vdash_{pc} e'' : \tau$. By Weakening also $\Gamma; \Sigma; \theta' \vdash_{pc} l : (\mathtt{ref}\ \tau')^p$. We get $\Gamma; \Sigma; \theta' \vdash_{pc} l := e'' : \mathtt{unit}^\perp$ by **assign**.

– The reduction happened with **Eassign**

$$\frac{l \in \mathtt{dom}(S) \qquad \mathtt{type}(S, l) = \tau''}{l := v, \Sigma', S \succ (), S[l \rightarrowtail (v, \tau'')], l_{\tau''}(v), \Sigma'}\ \textbf{Eassign}$$

In this case $e = l$ and $e' = v$. It suffices to show $\Gamma; \Sigma; \theta \vdash_{pc} () : \mathtt{unit}^\perp$ and $S[l \rightarrowtail (v, \tau'')] \triangleright_\Gamma (\theta)$. We get the first with **unit**. For the second we have to show:

* $\mathtt{dom}(\theta) \subseteq \mathtt{dom}(S[l \rightarrowtail (v, \tau'')])$.

  Since $l \in \mathtt{dom}(S)$ we know $\mathtt{dom}(S[l \rightarrowtail (v, \tau'')]) = \mathtt{dom}(S)$. Hence it suffices to show $\mathtt{dom}(\theta) \subseteq \mathtt{dom}(S)$ which we already know from $S \triangleright_\Gamma (\theta)$.
* $\forall l' \in \mathtt{dom}(\theta).\Gamma; \emptyset; \theta \vdash_\perp S[l \rightarrowtail (v, \tau'')](l') : \theta(l')$.

  Let $l' \in \mathtt{dom}(\theta)$. There are two cases:

  $l' \neq l$: In this case $S[l \rightarrowtail (v, \tau'')](l') = S(l')$. We already know $\Gamma; \emptyset; \theta \vdash_\perp S(l') : \theta(l')$ from $S \triangleright_\Gamma (\theta)$.

  $l' = l$: In this case $S[l \rightarrowtail (v, \tau'')](l') = S[l \rightarrowtail (v, \tau'')](l) = v$. So we have to show $\Gamma; \emptyset; \theta \vdash_\perp v : \theta(l)$.
  We know $\Gamma; \Sigma; \theta \vdash_{pc} l : (\mathtt{ref}\ \tau')^p$. By Lemma 6.9 $\theta(l) = \tau'$. We already know $\Gamma; \Sigma; \theta \vdash_{pc} v : \tau$ and $\tau(\Sigma) <: \tau'$. There must be types A and B and policies q and r such that $A^q = \tau$ and $B^r = \tau'$. Then $A^{q(\Sigma)} <: B^r$. By inversion we get $A <: B$. By Corollary 6.16 we get $\Gamma; \Sigma; \theta \vdash_{pc} v : A^r$. By **sub-policy** and Lemma 4.1 $A^r <: B^r$. Hence $\Gamma; \Sigma; \theta \vdash_\perp v : B^r$ by **sub** and Lemma 4.1 as $\perp \sqsubseteq pc$ by Lemma 4.19. We get the goal by Lemma 6.3.
* $\forall l' \in \mathtt{dom}(\theta).\theta(l') = \mathtt{type}(S[l \rightarrowtail (v, \tau'')], l')$. Let $l' \in \mathtt{dom}(\theta)$. There are two cases.
  - $l' \neq l$ In that case $\mathtt{type}(S, l') = \mathtt{type}(S[l \rightarrowtail (v, \tau'')], l')$. We know $\theta(l') = \mathtt{type}(S, l')$ from $S \triangleright_\Gamma \theta$. Hence also $\theta(l') = \mathtt{type}(S[l \rightarrowtail (v, \tau'')], l')$
  - $l' = l$ By $S \triangleright_\Gamma \theta$ we know $\theta(l) = \mathtt{type}(S, l')$. We also know $\mathtt{type}(S, l) = \tau''$. Hence $\theta(l') = \theta(l) = \tau'' = \mathtt{type}(S[l \rightarrowtail (v, \tau'')], l)$ by construction.
* $\forall l' \in \mathtt{dom}(S[l \rightarrowtail (v, \tau'')]).S[l \rightarrowtail (v, \tau'')](l') \in \mathcal{V}$. There are two cases:
  - $l' \neq l$. In this case $S[l \rightarrowtail (v, \tau'')](l') = S(l')$. We have $S(l') \in \mathcal{V}$ by $S \triangleright_\Gamma \theta$.
  - $l' = l$. In this case we have to show $v \in \mathcal{V}$. We have this by assumption.

- **unit:** () is a value and does not reduce.
- **close:**

$$\frac{\Gamma; \Sigma \backslash \{\sigma\}; \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq \mathtt{pol}(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} \mathtt{close}(\sigma)\ \mathtt{in}\ e : \tau}\ \textbf{close}$$

The reduction could only have happened with **Eopen**:

$$\frac{}{\mathtt{close}\ \sigma\ \mathtt{in}\ e, \Sigma', S \succ \mathtt{closed}\ \sigma\ \mathtt{in}\ e, S, \mathtt{close}(\sigma), \Sigma'}\ \textbf{Eclose}$$

It suffices to show $\Gamma; \Sigma; \theta \vdash_{pc} \mathtt{closed}\ \sigma\ \mathtt{in}\ e : \tau$ which we get from **closed** using the premisses from the **close** rule.

- **closed**:

$$\frac{\Gamma; \Sigma\backslash\{\sigma\}; \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq pol(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} \text{closed}(\sigma)\ \text{in}\ e : \tau}\ \textbf{closed}$$

  There are two cases:

  – The reduction happened with **Eclosed**:

$$\frac{e, \Sigma'\backslash\{\sigma\}, S \succ e', S', \omega, \Sigma''}{\text{closed}\ \sigma\ \text{in}\ e, \Sigma', S \succ \text{closed}\ \sigma\ \text{in}\ e', S', \omega, \Sigma''}\ \textbf{Eclosed}$$

  By the assumptions of the rules **open** and **Eopen** and by $S \triangleright (\theta)$ we get that there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma; \Sigma\backslash\{\sigma\}; \theta' \vdash_{pc} e' : \tau$ using the induction hypothesis. As we already know $pc(\Sigma) \sqsubseteq pol(\sigma)$, we get $\Gamma; \Sigma; \theta' \vdash_{pc} \text{closed}\ \sigma\ \text{in}\ e' : \tau$ using **Eclosed**.

  – The reduction happened with **EclosedBeta**:

$$\frac{}{\text{closed}\ \sigma\ \text{in}\ v, \Sigma', S \succ v, S, \text{unclose}(\sigma), \Sigma'}\ \textbf{EclosedBeta}$$

  In this case $e = v$. It suffices to show $\Gamma; \Sigma; \theta \vdash_{pc} v : \tau$. We already know $\Gamma; \Sigma\backslash\{\sigma\}; \theta \vdash_{pc} v : \tau$ and get the goal by Weakening.

- **when:**

$$\frac{\Gamma; \Sigma \cup \{\sigma\}; \theta \vdash_{pc \sqcup pol(\sigma)} e_1 : \tau \qquad \Gamma; \Sigma; \theta \vdash_{pc \sqcup pol(\sigma)} e_2 : \tau \qquad pol(\sigma) \sqsubseteq \tau}{\Gamma; \Sigma; \theta \vdash_{pc} \text{when}\ (\sigma)\ \text{then}\ e_1\ \text{else}\ e_2 : \tau}\ \textbf{when}$$

  There are four cases:

  – The reduction happened with **EWhenOpen**:

$$\frac{\sigma \in \Sigma' \qquad e_1, \Sigma', S \succ e_1', S', \omega, \Sigma''}{\text{when}\ \sigma\ \text{then}\ e_1\ \text{else}\ e_2, \Sigma', S \succ \text{when}\ \sigma\ \text{then}\ e_1'\ \text{else}\ e_2, S', \omega, \Sigma''}\ \textbf{EWhenOpen}$$

  We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta')$ and $\Gamma; \Sigma \cup \{\sigma\}; \theta' \vdash_{pc \sqcup pol(\sigma)} e_1' : \tau$. By Weakening we also get $\Gamma; \Sigma; \theta' \vdash_{pc \sqcup pol(\sigma)} e_2 : \tau$. The goal follows with **when**.

  – The reduction happened with **EWhenClosed**:

$$\frac{\sigma \notin \Sigma' \qquad e_2, \Sigma', S \succ e_2', S', \omega, \Sigma''}{\text{when}\ \sigma\ \text{then}\ e_1\ \text{else}\ e_2, \Sigma', S \succ \text{when}\ \sigma\ \text{then}\ e_1\ \text{else}\ e_2', S', \omega, \Sigma''}\ \textbf{EWhenClosed}$$

  We already know $S \triangleright_\Gamma (\theta)$. Hence by induction there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \triangleright_\Gamma (\theta', \Delta')$ and $\Gamma; \Sigma; \theta' \vdash_{pc \sqcup pol(\sigma)} e_2' : \tau$. By Weakening we also get $\Gamma; \Sigma \cup \{\sigma\}; \theta' \vdash_{pc \sqcup pol(\sigma)} e_1 : \tau$. The goal follows with **when**.

  – The reduction happened with **EWhenOpenBeta**:

$$\frac{\sigma \in \Sigma'}{\text{when}\ \sigma\ \text{then}\ v\ \text{else}\ e', \Sigma', S \succ v, S, \epsilon, \Sigma'}\ \textbf{EWhenOpenBeta}$$

  In this case $e_1 = v$. It suffices to show $\Gamma; \Sigma; \theta \vdash_{pc} v : \tau$. We already know $\Gamma; \Sigma \cup \{\sigma\}; \theta \vdash_{pc \sqcup pol(\sigma)} v : \tau$. We get $\Gamma; \Sigma; \theta \vdash_{pc \sqcup pol(\sigma)} v : \tau$ by Lemma 6.3. Finally we get $\Gamma; \Sigma; \theta \vdash_{pc} v : \tau$ with **sub** and Lemma 4.6.

  – The reduction happened with **EWhenClosedBeta**:

$$\frac{\sigma \notin \Sigma'}{\text{when}\ \sigma\ \text{then}\ e\ \text{else}\ v, \Sigma', S \succ v, S, \epsilon, \Sigma'}\ \textbf{EWhenClosedBeta}$$

  In this case $e_1 = v$. It suffices to show $\Gamma; \Sigma; \theta \vdash_{pc} v : \tau$. We already know $\Gamma; \Sigma; \theta \vdash_{pc \sqcup pol(\sigma)} v : \tau$. We get the goal with **sub** and Lemma 4.6.

□

Lemma 6.19. If $\Gamma; \Sigma; \theta \vdash_{pc} e : \tau$, then $\forall \Sigma', S.\ S \triangleright_\Gamma \theta \to \Sigma' \vdash e, S \xrightarrow{\omega;\Sigma''} e', S' \to pol(\omega) = p \to pc \sqsubseteq p$.

Proof. By induction on the typing derivation.

- **Var:** Variables don't reduce.
- **nat:** Numbers are values and don't reduce.
- **open:**

$$\frac{\Gamma; \Sigma \cup \{\sigma\}; \Delta, \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq pol(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} open(\sigma)\ in\ e : \tau}\ \textbf{open}$$

  The reduction could only have happened with **Eopen**:

$$\frac{}{open\ \sigma\ in\ e, \Sigma', S \succ opened\ \sigma\ in\ e, S, open(\sigma), \Sigma'}\ \textbf{Eopen}$$

  $pol(open(\sigma)) = pol(\sigma) \sqsupseteq pc$.

- **opened:**

$$\frac{\Gamma; \Sigma \cup \{\sigma\}; \Delta, \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq pol(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} opened(\sigma)\ in\ e : \tau}\ \textbf{opened}$$

  There are two cases:

  - The reduction happened with **Eopened**:

$$\frac{e, \Sigma' \cup \{\sigma\}, S \succ e', S', \omega, \Sigma''}{opened\ \sigma\ in\ e, \Sigma', S \succ opened\ \sigma\ in\ e', S', \omega, \Sigma''}\ \textbf{Eopened}$$

    By induction $pol(\omega) = p \to pc \sqsubseteq p$.
  - The reduction happened with **EopenBeta**:

$$\frac{}{open\ \sigma(\vec{a})\ in\ v, \Sigma', S \succ v, S, unopen(\sigma), \Sigma'}\ \textbf{EopenBeta}$$

    In this case $e = v$. $pol(unopen(\sigma)) = pol(\sigma) \sqsupseteq pc$.

- **λ:** Functions are values and don't reduce.
- **prod:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e_1 : \tau_1 \qquad \Gamma; \Sigma; \theta \vdash_{pc} e_2 : \tau_2}{\Gamma; \Sigma; \theta \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^\perp}\ \textbf{prod}$$

  There are two cases:

  - The reduction happened with **EPairl**:

$$\frac{e_1, \Sigma', S \succ e_1', S', \omega, \Sigma''}{(e_1, e_2), \Sigma', S \succ (e_1', e_2), S', \omega, \Sigma''}\ \textbf{EPairl}$$

    By induction $pol(\omega) = p \to pc \sqsubseteq p$.
  - The reduction happened with **EPairr**

$$\frac{e_2, \Sigma', S \succ e_2', S', \omega, \Sigma''}{(v, e_2), \Sigma', S \succ (v, e_2'), S', \omega, \Sigma''}\ \textbf{EPairr}$$

    In this case $e_1 = v$. By induction $pol(\omega) = p \to pc \sqsubseteq p$.

- **app:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\Sigma'', p_e} \tau_2)^p \qquad \Gamma; \Sigma; \theta \vdash_{pc} e_2 : \tau_1' \qquad p \sqsubseteq \tau_2 \qquad pc \sqcup p \sqsubseteq p_e \qquad \tau_1' <: \tau_1 \qquad \Sigma \supseteq \Sigma''}{\Gamma; \Sigma; \theta \vdash_{pc} e_1\ e_2 : \tau_2}\ \textbf{app}$$

  There are three cases:

– The reduction happened with **EAppl**:

$$\frac{e_1, \Sigma', S \succ e_1', S', \omega, \Sigma'''}{e_1\ e_2, \Sigma', S \succ e_1'\ e_2, S', \omega, \Sigma'''}\ \textbf{EAppl}$$

By induction $\mathtt{pol}(\omega) = p \to pc \sqsubseteq p$.

– The reduction happened with **EAppr**:

$$\frac{e_2, \Sigma', S \succ e_2', S', \omega, \Sigma'''}{(\lambda\ x.e)\ e_2, \Sigma', S \succ (\lambda\ x.e)\ e_2', S', \omega, \Sigma'''}\ \textbf{EAppr}$$

In this case $e_1 = \lambda\ x.e$. By induction $\mathtt{pol}(\omega) = p \to pc \sqsubseteq p$.

– The reduction happened with **EAppBeta**:

$$\frac{}{(\lambda\ x.e)\ v, \Sigma'', S \succ [v/x]e, S, \epsilon, \Sigma''}\ \textbf{EAppBeta}$$

In this case $e_1 = \lambda\ x.e$ and $e_2 = v$. $\mathtt{pol}(\epsilon)$ is undefined. Hence there is nothing to show.

- **fst:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e : (\tau_1 \times \tau_2)^p \qquad p \sqsubseteq \tau_1}{\Gamma; \Sigma; \theta \vdash_{pc} \mathtt{fst}(e) : \tau_1}\ \textbf{fst}$$

There are two cases:

– The reduction happened with **EFst**.

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{\mathtt{fst}(e), \Sigma', S \succ \mathtt{fst}(e'), S', \omega, \Sigma''}\ \textbf{EFst}$$

By induction $\mathtt{pol}(\omega) = p \to pc \sqsubseteq p$.

– The reduction happened with **EFstBeta**

$$\frac{}{\mathtt{fst}((v, v')), \Sigma', S \succ v, S, \epsilon, \Sigma'}\ \textbf{EFstBeta}$$

In this case $e = (v, v')$. $\mathtt{pol}(\epsilon)$ is undefined. Hence there is nothing to show.

- **snd:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e : (\tau_1 \times \tau_2)^p \qquad p \sqsubseteq \tau_2}{\Gamma; \Sigma; \theta \vdash_{pc} \mathtt{snd}(e) : \tau_2}\ \textbf{snd}$$

There are two cases:

– The reduction happened with **ESnd**.

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{\mathtt{snd}(e), \Sigma', S \succ \mathtt{snd}(e'), S', \omega, \Sigma''}\ \textbf{ESnd}$$

By induction $\mathtt{pol}(\omega) = p \to pc \sqsubseteq p$.

– The reduction happened with **ESndBeta**

$$\frac{}{\mathtt{snd}((v, v')), \Sigma', S \succ v', S, \epsilon, \Sigma'}\ \textbf{ESndBeta}$$

In this case $e = (v, v')$. $\mathtt{pol}(\epsilon)$ is undefined. Hence there is nothing to show.

- **inl:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e : \tau_1}{\Gamma; \Sigma; \theta \vdash_{pc} \mathtt{inl}(e) : (\tau_1 + \tau_2)^\perp}\ \textbf{inl}$$

The reduction could only have happened with **EInl**.

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{\mathtt{inl}(e), \Sigma', S \succ \mathtt{inl}(e'), S', \omega, \Sigma''}\ \textbf{EInl}$$

By induction $\mathtt{pol}(\omega) = p \to pc \sqsubseteq p$.

- **inr:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e : \tau_2}{\Gamma; \Sigma; \theta \vdash_{pc} inr(e) : (\tau_1 + \tau_2)^{\perp}}\ \textbf{inr}$$

  The reduction could only have happened with **EInr**

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{inr(e), \Sigma', S \succ inr(e'), S', \omega, \Sigma''}\ \textbf{EInr}$$

  By induction $pol(\omega) = p \to pc \sqsubseteq p$.

- **case:**

$$\frac{p \sqsubseteq \tau \qquad \Gamma, x : \tau_1'; \Sigma; \theta \vdash_{pc \sqcup p} e_1 : \tau \qquad \Gamma, y : \tau_2'; \Sigma; \theta \vdash_{pc \sqcup p} e_2 : \tau \qquad \tau_1 <: \tau_1' \qquad \tau_2 <: \tau_2' \qquad \Gamma; \Sigma; \theta \vdash_{pc} e : (\tau_1 + \tau_2)^p}{\Gamma; \Sigma; \theta \vdash_{pc} case(e, x.e_1, y.e_2) : \tau}\ \textbf{case}$$

  There are three cases:

  – The reduction happened with **ECase**:

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{case(e, x.e_1, y.e_2), \Sigma', S \succ case(e', x.e_1, y.e_2), S', \omega, \Sigma''}\ \textbf{ECase}$$

    By induction $pol(\omega) = p \to pc \sqsubseteq p$.

  – The reduction happened with **ECasel**:

$$\frac{}{case(inl\ v, x.e_1, y.e_2), \Sigma', S \succ [v/x]e_1, S, \epsilon, \Sigma'}\ \textbf{ECasel}$$

    In this case $e = inl\ v$. $pol(\epsilon)$ is undefined. Hence there is nothing to show.

  – The reduction happened with **ECaser**:

$$\frac{}{case(inr\ v, x.e_1, y.e_2), \Sigma', S \succ [v/y]e_2, S, \epsilon, \Sigma'}\ \textbf{ECaser}$$

    In this case $e = inr\ v$. $pol(\epsilon)$ is undefined. Hence there is nothing to show.

- **new:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e : \tau' \qquad pc \sqsubseteq \tau \qquad \tau'(\Sigma) <: \tau}{\Gamma; \Sigma; \theta \vdash_{pc} new\ (e, \tau) : (ref\ \tau)^{\perp}}\ \textbf{new}$$

  There are two cases:

  – The reduction happened with **ENew**:

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{new\ (e, \tau), \Sigma', S \succ new\ (e', \tau), S', \omega, \Sigma''}\ \textbf{ENew}$$

    By induction $pol(\omega) = p \to pc \sqsubseteq p$.

  – The reduction happened with **ENewBeta**:

$$\frac{l \notin dom(S)}{new\ (v, \tau), \Sigma', S \succ l, S \cup \{l \rightarrowtail (v, \tau)\}, l_\tau(v), \Sigma'}\ \textbf{ENewBeta}$$

    In this case $e = v$. $pol(l_\tau(v)) = pol(\tau)$. We have $pc \sqsubseteq \tau$ as an assumption. Hence $pc \sqsubseteq pol(\tau)$.

- **loc:** Locations are values and do not reduce.

- **sub:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc'} e : \tau' \qquad pc \sqsubseteq pc' \qquad \tau' <: \tau}{\Gamma; \Sigma; \theta \vdash_{pc} e : \tau}\ \textbf{sub}$$

  By induction if $pol(\omega) = p$, then $pc' \sqsubseteq p$. We know $pc \sqsubseteq pc'$. We get the claim by Lemma 4.1.

- **deref:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e : (\mathsf{ref}\ \tau)^p \qquad p \sqsubseteq \tau' \qquad \tau <: \tau'}{\Gamma; \Sigma; \theta \vdash_{pc} !\, e : \tau'}\ \textbf{deref}$$

  There are two cases:

  – The reduction happened with **EDeref**:

$$\frac{e, \Sigma', S \succ e', S', \omega, \Sigma''}{!e, \Sigma', S \succ !(e'), S', \omega, \Sigma''}\ \textbf{EDeref}$$

  By induction $\mathtt{pol}(\omega) = p \to pc \sqsubseteq p$.

  – The reduction happened with **EDerefBeta**:

$$\frac{l \rightarrowtail (v, \tau'') \in S}{!l, \Sigma', S \succ v, S, \epsilon, \Sigma'}\ \textbf{EDerefBeta}$$

  In this case $e = l$. $\mathtt{pol}(\epsilon)$ is undefined. Therefore there is nothing to show.

- **assign:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e : (\mathrm{ref}(\tau'))^p \qquad \tau(\Sigma) <: \tau' \qquad \Gamma; \Sigma; \theta \vdash_{pc} e' : \tau \qquad pc \sqcup p \sqsubseteq \tau'}{\Gamma; \Sigma; \theta \vdash_{pc} e := e' : \mathrm{unit}^{\perp}}\ \textbf{assign}$$

  There are three cases:

  – The reduction happened with **Eassignl**

$$\frac{e, \Sigma', S \succ e'', S', \omega, \Sigma''}{e := e', \Sigma', S \succ e'' := e', S', \omega, \Sigma''}\ \textbf{Eassignl}$$

  By induction $\mathtt{pol}(\omega) = q \to pc \sqsubseteq q$.

  – The reduction happened with **Eassignr**

$$\frac{e', \Sigma', S \succ e'', S', \omega, \Sigma''}{l := e', \Sigma', S \succ l := e'', S', \omega, \Sigma''}\ \textbf{Eassignr}$$

  In this case $e = l$. By induction $\mathtt{pol}(\omega) = q \to pc \sqsubseteq q$.

  – The reduction happened with **Eassign**

$$\frac{l \in \mathrm{dom}(S) \qquad \mathtt{type}(S, l) = \tau''}{l := v, \Sigma', S \succ (), S[l \rightarrowtail (v, \tau'')], l_{\tau''}(v), \Sigma'}\ \textbf{Eassign}$$

  In this case $e = l$ and $e' = v$. $\mathtt{pol}(l_{\tau''}(v)) = \mathtt{pol}(\tau'')$. We know $\Gamma; \Sigma; \theta \vdash_{pc} l : \mathrm{ref}(\tau')^p$. Hence by Lemma 6.9 $\theta(l) = \tau'$. By $S \triangleright_\Gamma \theta$ $\theta(l) = \mathtt{type}(S, l)$. Because $\mathtt{type}(S, l) = \tau''$,we have $\tau' = \tau''$. We have $pc \sqcup p \sqsubseteq \tau'$. By Lemma 4.6, Lemma 4.1 and Definition 3.2 we have $pc \sqsubseteq \mathtt{pol}(\tau'')$ which is what we needed to show.

- **unit:** () is a value and does not reduce.

- **close:**

$$\frac{\Gamma; \Sigma \backslash \{\sigma\}; \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq \mathtt{pol}(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} \mathtt{close}(\sigma)\ \mathtt{in}\ e : \tau}\ \textbf{close}$$

  The reduction could only have happened with **Eopen**:

$$\frac{}{\mathtt{close}\ \sigma\ \mathtt{in}\ e, \Sigma', S \succ \mathtt{closed}\ \sigma\ \mathtt{in}\ e, S, \mathtt{close}(\sigma), \Sigma'}\ \textbf{Eclose}$$

  $\mathtt{pol}(\mathtt{close}(\sigma)) = \mathtt{pol}(\sigma)$ and we have $pc \sqsubseteq \mathtt{pol}(\sigma)$ by assumption.

- **closed**:

$$\frac{\Gamma; \Sigma \backslash \{\sigma\}; \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq pol(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} closed(\sigma)\ in\ e : \tau}\ \textbf{closed}$$

  There are two cases:

  – The reduction happened with **Eclosed**:

$$\frac{e, \Sigma' \backslash \{\sigma\}, S \succ e', S', \omega, \Sigma''}{closed\ \sigma\ in\ e, \Sigma', S \succ closed\ \sigma\ in\ e', S', \omega, \Sigma''}\ \textbf{Eclosed}$$

  By induction $pol(\omega) = p \to pc \sqsubseteq p$.

  – The reduction happened with **EclosedBeta**:

$$\frac{}{closed\ \sigma\ in\ v, \Sigma', S \succ v, S, unclose(\sigma), \Sigma'}\ \textbf{EclosedBeta}$$

  In this case $e = v$. $pol(unclose(\sigma)) = pol(\sigma)$. We know $pc \sqsubseteq pol(\sigma)$ by assumption.

- **when:**

$$\frac{\Gamma; \Sigma \cup \{\sigma\}; \theta \vdash_{pc \sqcup pol(\sigma)} e_1 : \tau \qquad \Gamma; \Sigma; \theta \vdash_{pc \sqcup pol(\sigma)} e_2 : \tau \qquad pol(\sigma) \sqsubseteq \tau}{\Gamma; \Sigma; \theta \vdash_{pc} when\ (\sigma)\ then\ e_1\ else\ e_2 : \tau}\ \textbf{when}$$

  There are four cases:

  – The reduction happened with **EWhenOpen**:

$$\frac{\sigma \in \Sigma' \qquad e_1, \Sigma', S \succ e_1', S', \omega, \Sigma''}{when\ \sigma\ then\ e_1\ else\ e_2, \Sigma', S \succ when\ \sigma\ then\ e_1'\ else\ e_2, S', \omega, \Sigma''}\ \textbf{EWhenOpen}$$

  By induction $pol(\omega) = p \to pc \sqcup pol(\sigma) \sqsubseteq p$. Because $pc \sqsubseteq pc \sqcup pol(\sigma)$ by Lemma 4.6, we get $pol(\omega) = p \to pc \sqsubseteq p$ by Lemma 4.1.

  – The reduction happened with **EWhenClosed**:

$$\frac{\sigma \notin \Sigma' \qquad e_2, \Sigma', S \succ e_2', S', \omega, \Sigma''}{when\ \sigma\ then\ e_1\ else\ e_2, \Sigma', S \succ when\ \sigma\ then\ e_1\ else\ e_2', S', \omega, \Sigma''}\ \textbf{EWhenClosed}$$

  By induction $pol(\omega = p) \to pc \sqcup pol(\sigma) \sqsubseteq p$. Because $pc \sqsubseteq pc \sqcup pol(\sigma)$ by Lemma 4.6, we get $pol(\omega = p) \to pc \sqsubseteq p$ by Lemma 4.1.

  – The reduction happened with **EWhenOpenBeta**:

$$\frac{\sigma \in \Sigma'}{when\ \sigma\ then\ v\ else\ e', \Sigma', S \succ v, S, \epsilon, \Sigma'}\ \textbf{EWhenOpenBeta}$$

  In this case $e_1 = v$. $pol(\epsilon)$ is undefined. Hence there is nothing to show.

  – The reduction happened with **EWhenClosedBeta**:

$$\frac{\sigma \notin \Sigma' \qquad \alpha = S(a)}{when\ \sigma\ then\ e\ else\ v, \Sigma', S \succ v, S, \epsilon, \Sigma'}\ \textbf{EWhenClosedBeta}$$

  In this case $e_1 = v$. $pol(\epsilon)$ is undefined. Hence there is nothing to show.

□

Theorem 6.1 (Type Safety)**.** If $\cdot; \Sigma; \theta \vdash_{pc} e : \tau$, then either e is a value, or for all states S such that $S \rhd \theta$ and for all lock sets Σ', there are $e', S', \omega, \Sigma'', \theta'$ such that

$$\Sigma' \vdash e, S \xrightarrow{\omega; \Sigma''} e', S'$$

where $\theta' \supseteq \theta$, $S' \rhd \theta'$, and $\cdot; \Sigma; \theta' \vdash_{pc} e' : \tau$. Also if $pol(\omega) = p$, then $pc \sqsubseteq p$.

Proof. There are two cases:

1. e is a value. This proves the goal.
2. e is not a value. In this case let S be a state such that $S \rhd (\theta)$ and let Σ' be a lock set. Then by Progress there are e', S', ω, Σ'' such that $\Sigma' \vdash e, S \xrightarrow{\omega; \Sigma''} e', S'$. Then by Preservation there is a θ' such that $\theta' \sqsupseteq \theta$, $S' \rhd (\theta')$ and $\cdot; \Sigma; \theta' \vdash_{pc} e' : \tau$ and by Lemma 6.19 if $pol(\omega) = p$, then $pc \sqsubseteq p$.

□

7 Logical relations

7.1 Unary relation

Definition 7.1 (Substitutions)**.** Substitutions $\delta, \delta', \delta_0$, etc. are partial functions from variables to values.

Definition 7.2 (Substitution usage)**.**

$$
\begin{aligned}
\delta(x) &\triangleq e && \text{if } \delta(x) = e \\
\delta(y) &\triangleq y && \text{if } y \notin \mathrm{dom}(\delta) \\
\delta(n) &\triangleq n \\
\delta(\lambda y.\, e') &\triangleq \lambda y.\, \delta|_{\mathrm{dom}(\delta)\setminus\{y\}}(e') \\
\delta(e'\ e'') &\triangleq (\delta(e'))\ (\delta(e'')) \\
\delta(()) &\triangleq () \\
\delta(l) &\triangleq l \\
\delta(\mathsf{inl}\,(e')) &\triangleq \mathsf{inl}\,(\delta(e')) \\
\delta(\mathsf{inr}\,(e')) &\triangleq \mathsf{inr}\,(\delta(e')) \\
\delta((e', e'')) &\triangleq (\delta(e'), \delta(e'')) \\
\delta(\mathsf{fst}\,(e')) &\triangleq \mathsf{fst}\,(\delta(e')) \\
\delta(\mathsf{snd}\,(e')) &\triangleq \mathsf{snd}\,(\delta(e')) \\
\delta\left(\begin{array}{l}\mathsf{case}\ e'\ \mathsf{of} \\ |\ \mathsf{inl}\,(y) \Rightarrow e_1 \\ |\ \mathsf{inr}\,(y') \Rightarrow e_2\end{array}\right) &\triangleq \begin{array}{l}\mathsf{case}\ \delta(e')\ \mathsf{of} \\ |\ \mathsf{inl}\,(y) \Rightarrow \delta|_{\mathrm{dom}(\delta)\setminus\{y\}}(e_1) \\ |\ \mathsf{inr}\,(y') \Rightarrow \delta|_{\mathrm{dom}(\delta)\setminus\{y'\}}(e_2)\end{array} \\
\delta(\mathsf{new}\,(e', \tau)) &\triangleq \mathsf{new}\,(\delta(e'), \tau) \\
\delta(!\,e') &\triangleq !(\delta(e')) \\
\delta(e' := e'') &\triangleq \delta(e') := \delta(e'') \\
\delta(\mathsf{open}\ \sigma\ \mathsf{in}\ e') &\triangleq \mathsf{open}\ \sigma\ \mathsf{in}\ \delta(e') \\
\delta(\mathsf{close}\ \sigma\ \mathsf{in}\ e') &\triangleq \mathsf{close}\ \sigma\ \mathsf{in}\ \delta(e') \\
\delta(e'\ \mathsf{then\ unopen}\ \sigma) &\triangleq \delta(e')\ \mathsf{then\ unopen}\ \sigma \\
\delta(e'\ \mathsf{then\ unclose}\ \sigma) &\triangleq \delta(e')\ \mathsf{then\ unclose}\ \sigma \\
\delta(\mathsf{when}\ \sigma\ \mathsf{then}\ e'\ \mathsf{else}\ e'') &\triangleq \mathsf{when}\ \sigma\ \mathsf{then}\ \delta(e')\ \mathsf{else}\ \delta(e'')
\end{aligned}
$$

Lemma 7.1. If $\forall y \in \mathrm{dom}(\delta).x \notin \mathrm{FV}(\delta(y))$, then $(\delta(e'))[x \mapsto e] = \delta \cup \{(x, e)\}(e')$.

Proof. By induction on e'.

- $e' = y$: There are several cases:
  - $y \in \mathrm{dom}(\delta)$. Then $[e/x]\delta(y) = [e/x]\delta(y) \overset{\text{Lemma 3.1}}{=} \delta(y) = \delta \cup \{(x, e)\}(y)$.
  - $y \notin \mathrm{dom}(\delta)$ and $x = y$. Then $[e/x]\delta(y) = [e/x]y = [e/y]y = e = \delta \cup \{(y, e)\}(y) = \delta \cup \{(x, e)\}(y)$.
  - $y \notin \mathrm{dom}(\delta)$ and $x \neq y$. Then $[e/x]\delta(y) = [e/x]y = y = \delta \cup \{(x, e)\}(y)$.
- $e' = \lambda y.e''$: By our assumptions about variables $y \notin \mathrm{dom}(\delta)$ and $y \neq x$. Hence $[e/x]\delta(\lambda\ y.\ e'') = \lambda y.\ [e/x]\delta(e'') \overset{\text{induction}}{=} \lambda y.\delta \cup \{(x, e)\}(e'') = \delta \cup \{(x, e)\}(\lambda y.\ e'')$.
- $e' = e_1\ e_2$: $[e/x]\delta(e_1\ e_2) = [e/x](\delta(e_1)\ \delta(e_2)) = [e/x]\delta(e_1)\ [e/x]\delta(e_2) \overset{\text{induction}}{=} (\delta \cup \{(x, e)\}(e_1))\ (\delta \cup \{(x, e)\}(e_2)) = \delta \cup \{(x, e)\}(e_1\ e_2)$.
- $e' = ()$: $[e/x]\delta(()) = [e/x]() = () = \delta \cup \{(x, e)\}(())$.
- $e' = l$: $[e/x]\delta(l) = [e/x]l = l = \delta \cup \{(x, e)\}(l)$.
- $e' = \mathtt{inl}\ e''$: $[e/x]\delta(\mathtt{inl}\ e'') = [e/x](\mathtt{inl}\ \delta(e'')) = \mathtt{inl}\ [e/x]\delta(e'') \overset{\text{induction}}{=} \mathtt{inl}\ \delta \cup \{(x, e)\}(e'') = \delta \cup \{(x, e)\}(\mathtt{inl}\ e'')$.

- $e' = \mathsf{inr}\ e''$: $[e/x]\delta(\mathsf{inr}\ e'') = [e/x](\mathsf{inr}\ \delta(e'')) = \mathsf{inr}\ [e/x]\delta(e'') \overset{\text{induction}}{=} \mathsf{inr}\ \delta \cup \{(x,e)\}(e'') = \delta \cup \{(x,e)\}(\mathsf{inr}\ e'')$.
- $e' = (e_1, e_2)$: $[e/x]\delta((e_1,e_2)) = [e/x]((\delta(e_1),\delta(e_2))) = ([e/x]\delta(e_1),[e/x]\delta(e_2)) \overset{\text{induction}}{=} ((\delta\cup\{(x,e)\}(e_1)),(\delta\cup\{(x,e)\}(e_2))) = \delta \cup \{(x,e)\}((e_1,e_2))$.
- $e' = \mathsf{fst}(e'')$: $[e/x]\delta(\mathsf{fst}\ e'') = [e/x](\mathsf{fst}\ \delta(e'')) = \mathsf{fst}\ ([e/x]\delta(e'')) \overset{\text{induction}}{=} \mathsf{fst}(\delta \cup \{(x,e)\}(e'')) = \delta \cup \{(x,e)\}(\mathsf{fst}\ e'')$.
- $e' = \mathsf{snd}(e'')$: $[e/x]\delta(\mathsf{snd}\ e'') = [e/x](\mathsf{snd}\ \delta(e'')) = \mathsf{snd}\ ([e/x]\delta(e'')) \overset{\text{induction}}{=} \mathsf{snd}(\delta\cup\{(x,e)\}(e'')) = \delta \cup \{(x,e)\}(\mathsf{snd}\ e'')$.
- $e' = \mathsf{case}(e_0, y.e_1, y'.e_2)$: By our assumptions about variables $y, y' \notin \mathrm{dom}(\delta)$ and $y \neq x \neq y'$. Hence $[e/x]\delta(\mathsf{case}(e_0,y.e_1,y'.e_2)) = [e/x](\mathsf{case}(\delta(e_0),y.\delta(e_1),y'.\delta(e_2))) = \mathsf{case}([e/x]\delta(e_0),y.[e/x]\delta(e_1),y'.[e/x]\delta(e_2)) \overset{\text{induction}}{=} \mathsf{case}(\delta\cup\{(x,e)\}(e_0),y.\delta\cup\{(x,e)\}(e_1),y'.\delta\cup\{(x,e)\}(e_2)) = \delta\cup\{(x,e)\}(\mathsf{case}(e_0,y.e_1,y'.e_2))$.
- $e' = \mathsf{new}(e'',\tau)$: $[e/x]\delta(\mathsf{new}(e'',\tau)) = [e/x](\mathsf{new}(\delta(e''),\tau)) = \mathsf{new}([e/x]\delta(e''),\tau) \overset{\text{induction}}{=} \mathsf{new}(\delta \cup \{(x,e)\}(e''),\tau) = \delta \cup \{(x,e)\}(\mathsf{new}(e'',\tau))$.
- $e' = e_1 := e_2$: $[e/x]\delta(e_1 := e_2) = [e/x](\delta(e_1) := \delta(e_2)) = [e/x]\delta(e_1) := [e/x]\delta(e_2) \overset{\text{induction}}{=} (\delta \cup \{(x,e)\}(e_1)) := (\delta \cup \{(x,e)\}(e_2)) = \delta \cup \{(x,e)\}(e_1 := e_2)$.
- $e' = \mathsf{open}\ \sigma\ \mathsf{in}\ e''$: $[e/x]\delta(\mathsf{open}\ \sigma\ \mathsf{in}\ e'') = [e/x](\mathsf{open}\ \sigma\ \mathsf{in}\ \delta(e'')) = \mathsf{open}\ \sigma\ \mathsf{in}\ [e/x]\delta(e'') \overset{\text{induction}}{=} \mathsf{open}\ \sigma\ \mathsf{in}\ \delta \cup \{(x,e)\}(e'') = \delta \cup \{(x,e)\}(\mathsf{open}\ \sigma\ \mathsf{in}\ e'')$.
- $e' = \mathsf{close}\ \sigma\ \mathsf{in}\ e''$: $[e/x]\delta(\mathsf{close}\ \sigma\ \mathsf{in}\ e'') = [e/x](\mathsf{close}\ \sigma\ \mathsf{in}\ \delta(e'')) = \mathsf{close}\ \sigma\ \mathsf{in}\ [e/x]\delta(e'') \overset{\text{induction}}{=} \mathsf{close}\ \sigma\ \mathsf{in}\ \delta \cup \{(x,e)\}(e'') = \delta \cup \{(x,e)\}(\mathsf{close}\ \sigma\ \mathsf{in}\ e'')$.
- $e' = \mathsf{opened}\ \sigma\ \mathsf{in}\ e''$: $[e/x]\delta(\mathsf{opened}\ \sigma\ \mathsf{in}\ e'') = [e/x](\mathsf{opened}\ \sigma\ \mathsf{in}\ \delta(e'')) = \mathsf{opened}\ \sigma\ \mathsf{in}\ [e/x]\delta(e'') \overset{\text{induction}}{=} \mathsf{opened}\ \sigma\ \mathsf{in}\ \delta \cup \{(x,e)\}(e'') = \delta \cup \{(x,e)\}(\mathsf{opened}\ \sigma\ \mathsf{in}\ e'')$.
- $e' = \mathsf{closed}\ \sigma\ \mathsf{in}\ e''$: $[e/x]\delta(\mathsf{closed}\ \sigma\ \mathsf{in}\ e'') = [e/x](\mathsf{closed}\ \sigma\ \mathsf{in}\ \delta(e'')) = \mathsf{closed}\ \sigma\ \mathsf{in}\ [e/x]\delta(e'') \overset{\text{induction}}{=} \mathsf{closed}\ \sigma\ \mathsf{in}\ \delta \cup \{(x,e)\}(e'') = \delta \cup \{(x,e)\}(\mathsf{closed}\ \sigma\ \mathsf{in}\ e'')$.
- $e' = \mathsf{when}\ \sigma\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2$: $[e/x]\delta(\mathsf{when}\ \sigma\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2) = [e/x](\mathsf{when}\ \sigma\ \mathsf{then}\ \delta(e_1)\ \mathsf{else}\ \delta(e_2)) = \mathsf{when}\ \sigma\ \mathsf{then}\ [e/x]\delta(e_1)\ \mathsf{else}\ [e/x]\delta(e_2) \overset{\text{induction}}{=} \mathsf{when}\ \sigma\ \mathsf{then}\ \delta\cup\{(x,e)\}(e_1)\ \mathsf{else}\ \delta\cup\{(x,e)\}(e_2) = \delta\cup\{(x,e)\}(\mathsf{when}\ \sigma\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2)$.

□

Definition 7.3 (State Well-Formedness). $(S,m) \triangleright (\theta) \triangleq$

$$\begin{aligned} &\mathrm{dom}(\theta) \subseteq \mathrm{dom}(S) \\ \wedge\ &(\forall l \in \mathrm{dom}(\theta).(S(l),\theta,m) \in \lceil \theta(l) \rceil_\nu) \\ \wedge\ &\forall l \in \mathrm{dom}(\theta).\theta(l) = \mathrm{type}(S,l) \end{aligned}$$

Definition 7.4 (Unary relation). We define the following sets

$$\begin{aligned}
\lceil \mathsf{unit} \rceil_\nu &\triangleq \{((),\theta,m)\} \\
\lceil \mathcal{N} \rceil_\nu &\triangleq \{(n,\theta,m) \mid n \in \mathbb{N}\} \\
\lceil \tau_1 \times \tau_2 \rceil_\nu &\triangleq \{((v_1,v_2),\theta,m) \mid (v_1,\theta,m) \in \lceil \tau_1 \rceil_\nu \wedge (v_2,\theta,m) \in \lceil \tau_2 \rceil_\nu\} \\
\lceil \tau_1 + \tau_2 \rceil_\nu &\triangleq \{(\mathsf{inl}\,(v),\theta,m) \mid (v,\theta,m) \in \lceil \tau_1 \rceil_\nu\} \cup \{(\mathsf{inr}\,(v),\theta,m) \mid (v,\theta,m) \in \lceil \tau_2 \rceil_\nu\} \\
\lceil \tau_1 \xrightarrow{\Sigma,\mathsf{pc}} \tau_2 \rceil_\nu &\triangleq \left\{ (\lambda x.e,\theta,m) \;\middle|\; \begin{array}{l} \forall \theta', v, m'.\theta' \sqsupseteq \theta \wedge m' < m \wedge \\ (v,\theta',m') \in \lceil \tau_1 \rceil_\nu \rightarrow (e[x \mapsto v],\theta',m') \in \lceil \tau_2 \rceil_E^{\mathsf{pc}} \end{array} \right\} \\
\lceil \mathsf{ref}\ \tau \rceil_\nu &\triangleq \{(l,\theta,m) \mid \theta(l) = \tau\} \\
\lceil A^p \rceil_\nu &\triangleq \lceil A \rceil_\nu \\
\lceil \Gamma \rceil_\nu &\triangleq \{(\delta,\theta,m) \mid \mathrm{dom}(\Gamma) \subseteq \mathrm{dom}(\delta) \wedge \forall x \in \mathrm{dom}(\Gamma).(\delta(x),\theta,m) \in \lceil \Gamma(x) \rceil_\nu\}
\end{aligned}$$

$$\lceil\tau\rceil^{pc}_{E_\beta} \triangleq \left\{ (e,\theta,m) \;\middle|\; \begin{array}{l} e \notin \mathcal{V} \wedge \forall S,\theta',m',e',S',\omega,\Sigma,\Sigma'.\ \theta' \sqsupseteq \theta \wedge m' < m \wedge (S,m') \triangleright (\theta') \rightarrow \\ \Sigma \vdash e,\ S \xrightarrow{\omega;\Sigma'} e',\ S' \ \rightarrow \\ (\forall p.(pol(\omega) = p) \rightarrow pc \sqsubseteq p) \wedge \\ (\exists \theta''.\ \theta'' \sqsupseteq \theta' \wedge (S',m') \triangleright (\theta'') \wedge (e',\theta'',m') \in \lceil\tau\rceil^{pc}_{E}) \end{array} \right\}$$

$$\lceil\tau\rceil^{pc}_{E_\nu} \triangleq \lceil\tau\rceil_\nu$$

$$\lceil\tau\rceil^{pc}_{E} \triangleq \lceil\tau\rceil^{pc}_{E_\beta} \cup \lceil\tau\rceil^{pc}_{E_\nu}$$

7.2 Binary relation

Note: In this section we only define the logical relation for firstorder state, so that we will only have firstorder observations. The changes needed to obtain the more general logical relation, that we present in the paper, are described in section 9.

This restriction means we assume that the locations only point to data of firstorder types. We define firstorder types inductively in the following way

Definition 7.5 (Firstorder types)**.**

$$\frac{}{\text{firstorder}(\text{unit})}\ \textbf{Funit} \qquad \frac{}{\text{firstorder}(\mathbb{N})}\ \textbf{Fnat} \qquad \frac{\text{firstorder}(A)}{\text{firstorder}(A^p)}\ \textbf{FPol}$$

$$\frac{\text{firstorder}(\tau_1) \qquad \text{firstorder}(\tau_2)}{\text{firstorder}(\tau_1 \times \tau_2)}\ \textbf{FProd} \qquad \frac{\text{firstorder}(\tau_1) \qquad \text{firstorder}(\tau_2)}{\text{firstorder}(\tau_1 + \tau_2)}\ \textbf{FSum}$$

$$\frac{\text{firstorder}(\tau)}{\text{firstorder}(\text{ref}\ \tau)}\ \textbf{FRef}$$

Definition 7.6 (Worlds)**.** A world W is a tuple $(\theta_1,\theta_2,\beta)$ where θ_1 and θ_2 are state environments and β is a partial bijection $\text{dom}(\theta_1) \rightharpoonup \text{dom}(\theta_2)$.

For $W = (\theta,\theta',\beta)$, we define the projections $W.\theta_1 \triangleq \theta$, $W.\theta_2 \triangleq \theta'$ and $W.\beta \triangleq \beta'$.

We also define world extension:

$$W' \sqsubseteq W \triangleq \begin{array}{l} (W'.\theta_1 \sqsubseteq W.\theta_1) \\ \wedge\ (W'.\theta_2 \sqsubseteq W.\theta_2) \\ \wedge\ (W'.\beta \subseteq W.\beta) \end{array}$$

Definition 7.7 (Binary State Well-Formedness)**.**

$(S_1,S_2,m) \overset{\mathcal{A}}{\triangleright} (W) \triangleq$

$$(S_1,m) \triangleright W.\theta_1 \wedge (S_2,m) \triangleright W.\theta_2$$

$$\wedge\ W.\beta \subseteq \text{dom}(W.\theta_1) \times \text{dom}(W.\theta_2)$$

$$\wedge\ \left(\forall (l,l') \in W.\beta.\ \begin{array}{l} W.\theta_1(l) = W.\theta_2(l') \wedge \\ (S_1(l),S_2(l'),W,m) \in [\![W.\theta_1(l)]\!]^{\mathcal{A}}_{\mathcal{V}} \end{array} \right)$$

Lemma 7.2 (World-extension-ordering)**.** World extension ($\sqsubseteq$) is an ordering

Proof. This is true because $\subseteq$ and $\sqsubseteq$ on unary worlds are both orderings 6.2. □

Definition 7.8 (Attacker policy)**.** For a policy p and an attacker $\mathcal{A} = (a, \Sigma^{\mathcal{A}})$ we write $p \sqsubseteq \mathcal{A} \triangleq p \sqsubseteq \Sigma^{\mathcal{A}} \Rightarrow a$. Similarly for $\tau = A^p$ we write $\tau \sqsubseteq \mathcal{A} \triangleq p \sqsubseteq \mathcal{A}$. We also write $\Sigma' \sqsubseteq \mathcal{A}$ to mean $\Sigma' \subseteq \Sigma^{\mathcal{A}}$.

Definition 7.9 (Observational equivalence)**.** For observations and values we inductively define observational equivalence.

$$\frac{\forall l,\tau,v.\ \omega \neq l_\tau(v)}{\omega \approx^{\mathcal{A}}_\beta \omega}\ \textbf{refl} \qquad \frac{\neg(pol(\omega) \sqsubseteq \mathcal{A}) \vee \neg(pol(\omega') \sqsubseteq \mathcal{A})}{\omega \approx^{\mathcal{A}}_\beta \omega'}\ \textbf{high} \qquad \frac{v\ {}^{\beta}\!\simeq^{\mathcal{A}}_\tau\ v'}{l_\tau(v) \approx^{\mathcal{A}}_\beta l'_\tau(v')}\ \textbf{extend-}\tau$$

and

$$\frac{\mathsf{pol}(\omega) \not\sqsubseteq \mathcal{A} \qquad \mathsf{pol}(\omega') \not\sqsubseteq \mathcal{A}}{\omega \approx^{\mathcal{A}}_{\beta} \omega'}\ \textbf{high} \qquad \frac{\nu \,{}^{\beta}\!\simeq^{\mathcal{A}}_{\tau} \nu' \qquad (l, l') \in \beta}{l_\tau(\nu) \approx^{\mathcal{A}}_{\beta} l'_\tau(\nu')}\ \textbf{extend-}\tau \qquad \frac{\forall l, \tau, \nu. \omega \neq l_\tau(\nu)}{\omega \approx^{\mathcal{A}}_{\beta} \omega}\ \textbf{refl}$$

$$\frac{}{() \,{}^{\beta}\!\simeq^{\mathcal{A}}_{\mathsf{unit}} ()}\ \textbf{eqUnit} \qquad \frac{}{n \,{}^{\beta}\!\simeq^{\mathcal{A}}_{\mathbb{N}} n}\ \textbf{eqNat} \qquad \frac{\nu \,{}^{\beta}\!\simeq^{\mathcal{A}}_{\tau_1} \nu'}{\mathsf{inl}\,(\nu) \,{}^{\beta}\!\simeq^{\mathcal{A}}_{\tau_1+\tau_2} \mathsf{inl}\,(\nu')}\ \textbf{eqInl}$$

$$\frac{\nu \,{}^{\beta}\!\simeq^{\mathcal{A}}_{\tau_2} \nu'}{\mathsf{inr}\,(\nu) \,{}^{\beta}\!\simeq^{\mathcal{A}}_{\tau_1+\tau_2} \mathsf{inr}\,(\nu')}\ \textbf{eqInr} \qquad \frac{\nu_1 \,{}^{\beta}\!\simeq^{\mathcal{A}}_{\tau_1} \nu_1' \qquad \nu_2 \,{}^{\beta}\!\simeq^{\mathcal{A}}_{\tau_2} \nu_2'}{(\nu_1, \nu_2) \,{}^{\beta}\!\simeq^{\mathcal{A}}_{\tau_1\times\tau_2} (\nu_1', \nu_2')}\ \textbf{eqPair} \qquad \frac{(l, l') \in \beta}{l \,{}^{\beta}\!\simeq^{\mathcal{A}}_{\mathsf{ref}\,\tau} l'}\ \textbf{eqRef}$$

$$\frac{p \not\sqsubseteq \mathcal{A}}{\nu \,{}^{\beta}\!\simeq^{\mathcal{A}}_{A^p} \nu'}\ \textbf{eqHigh} \qquad \frac{p \sqsubseteq \mathcal{A} \qquad \nu \,{}^{\beta}\!\simeq^{\mathcal{A}}_{A} \nu'}{\nu \,{}^{\beta}\!\simeq^{\mathcal{A}}_{A^p} \nu'}\ \textbf{eqLow}$$

Definition 7.10 (Binary substitutions)**.** A binary substitution γ is a pair (δ_1, δ_2) of substitutions. When $\gamma = (\delta_1, \delta_2)$, then $\gamma_1 = \delta_1$ and $\gamma_2 = \delta_2$ and we define $\mathrm{dom}(\gamma) := \mathrm{dom}(\delta_1) \cap \mathrm{dom}(\delta_2)$.

Definition 7.11 (Low locks and lock equivalence)**.**
We define the set of locks in Σ visible to an attacker $\mathcal{A}$ as $\Sigma_{\mathcal{A}} := \{\sigma \in \Sigma \mid \mathsf{pol}(\sigma) \sqsubseteq \mathcal{A}\}$. We say that two lock sets Σ and Σ' are low equivalent for attacker $\mathcal{A}$ ($\Sigma \approx_{\mathcal{A}} \Sigma'$) if ${\Sigma_{\mathcal{A}}} = {\Sigma'}_{\mathcal{A}}$.

$$\begin{aligned}
\llbracket \mathsf{unit} \rrbracket^{\mathcal{A}}_{\mathcal{V}} &\triangleq \{((), (), W, m)\} \\
\llbracket \mathbb{N} \rrbracket^{\mathcal{A}}_{\mathcal{V}} &\triangleq \{(n, n, W, m) \mid n \in \mathbb{N}\} \\
\llbracket \tau_1 \times \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}} &\triangleq \left\{((\nu_1, \nu_2), (\nu_1', \nu_2'), W, m) \,\middle|\, (\nu_1, \nu_1', W, m) \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_{\mathcal{V}} \wedge (\nu_2, \nu_2', W, m) \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}}\right\} \\
\llbracket \tau_1 + \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}} &\triangleq \left\{(\mathsf{inl}\,(\nu), \mathsf{inl}\,(\nu'), W, m) \,\middle|\, (\nu, \nu', W, m) \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_{\mathcal{V}}\right\} \cup \left\{(\mathsf{inr}\,(\nu), \mathsf{inr}\,(\nu'), W, m) \,\middle|\, (\nu, \nu', W, m) \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}}\right\} \\
\llbracket \tau_1 \xrightarrow{\Sigma, \mathsf{pc}} \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}} &\triangleq \left\{ (\lambda x.\, e, \lambda x.\, e', W, m) \;\middle|\; \begin{array}{l} (\forall W'. W' \sqsupseteq W \to \forall m'. m' < m \to \forall \nu, \nu'. (\nu, \nu', W', m') \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_{\mathcal{V}} \to \\ \forall \Sigma_1, \Sigma_2. \Sigma_1 \supseteq \Sigma \subseteq \Sigma_2 \wedge \Sigma_1 \approx_{\mathcal{A}} \Sigma_2 \to \\ (e[x \mapsto \nu], e'[x \mapsto \nu'], W', \Sigma_1, \Sigma_2, m') \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_{\mathsf{E}}) \wedge \\ (\lambda x.\, e, W.\theta_1, m) \in \lceil \tau_1 \xrightarrow{\Sigma, \mathsf{pc}} \tau_2 \rceil_{\mathcal{V}} \wedge (\lambda e.\, e', W.\theta_2, m) \in \lceil \tau_1 \xrightarrow{\Sigma, \mathsf{pc}} \tau_2 \rceil_{\mathcal{V}} \end{array} \right\} \\
\llbracket \mathsf{ref}\,\tau \rrbracket^{\mathcal{A}}_{\mathcal{V}} &\triangleq \{(l, l', W, m) \mid W.\theta_1(l) = \tau = W.\theta_2(l') \wedge (l, l') \in W.\beta\} \\
\llbracket A^p \rrbracket^{\mathcal{A}}_{\mathcal{V}} &\triangleq \left\{ (\nu, \nu', W, m) \;\middle|\; \begin{array}{l} (p \sqsubseteq \mathcal{A} \to (\nu, \nu', W, m) \in \llbracket A \rrbracket^{\mathcal{A}}_{\mathcal{V}}) \wedge \\ (p \not\sqsubseteq \mathcal{A} \to (\nu, W.\theta_1, m) \in \lceil A \rceil_{\mathcal{V}} \wedge (\nu', W.\theta_2, m) \in \lceil A \rceil_{\mathcal{V}}) \end{array} \right\}
\end{aligned}$$

$$\llbracket \Gamma \rrbracket^{\mathcal{A}}_{\mathcal{V}} \triangleq \left\{(\gamma, W, m) \,\middle|\, \mathrm{dom}(\Gamma) \subseteq \mathrm{dom}(\gamma) \wedge \forall x \in \mathrm{dom}(\Gamma). (\gamma_1(x), \gamma_2(x), W, m) \in \llbracket \Gamma(x) \rrbracket^{\mathcal{A}}_{\mathcal{V}}\right\}$$

Note: Note that we are working with a different, but equivalent definition in the technical report. Instead of the disjunction "relevant declassification or continued indistinguishability" presented in the paper, we work with the equivalent implication "no relevant declassification implies continued indistinguishability" here. Also note that the logical relation below is only for first-order state. The logical relation for higher-order state can be found in section 9.

$\llbracket \tau \rrbracket^{\mathcal{A}}_{\mathsf{E}} \triangleq \llbracket \tau \rrbracket^{\mathcal{A}}_{\mathsf{E}_\beta} \cup \left\{ (v, v', W, \Sigma, \Sigma', m) \,\middle|\, (v, v', W, m) \in \llbracket \tau \rrbracket^{\mathcal{A}}_{\mathcal{V}} \right\}$, where:

$$
\llbracket \tau \rrbracket^{\mathcal{A}}_{\mathsf{E}_\beta} \triangleq \left\{ (e_1, e_2, W, \Sigma, \Sigma', m) \;\middle|\; \begin{array}{l}
\Sigma \approx_{\mathcal{A}} \Sigma' \wedge \forall \Sigma_1, \Sigma_2. \Sigma \subseteq \Sigma_1 \wedge \Sigma' \subseteq \Sigma_2 \wedge \Sigma_1 \approx_{\mathcal{A}} \Sigma_2 \rightarrow \\
\\
\forall W', m', S_1, S_2. m' < m \wedge W' \sqsupseteq W \wedge (S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W' \rightarrow (e_1, e_2) \in \\
\\
\left(\begin{array}{l}
C_{\mathrm{sym}} = \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l}
e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\
\forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\
\Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \wedge \\
\Sigma_2 \vdash e_2, S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2', S_2' \rightarrow \\
(\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\
\exists W''. W'' \sqsupseteq W' \wedge\; (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\
\omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', m') \in \llbracket \tau \rrbracket^{\mathcal{A}}_{\mathsf{E}}
\end{array} \right\} \cup \\
C_{\mathrm{L}} = \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l}
e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\
\Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\
(\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\
(e_1', e_2, W'', \Sigma, \Sigma', m') \in \llbracket \tau \rrbracket^{\mathcal{A}}_{\mathsf{E}})
\end{array} \right\} \cup \\
C_{\mathrm{R}} = \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l}
e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\
\Sigma_2 \vdash e_2, S_2 \overset{\omega;\Sigma_2'}{\Longrightarrow} e_2', S_2' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\
(\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\
(e_1, e_2', W'', \Sigma, \Sigma', m') \in \llbracket \tau \rrbracket^{\mathcal{A}}_{\mathsf{E}})
\end{array} \right\}
\end{array} \right)
\end{array} \right\}
$$

8 Proofs

8.1 General properties

Lemma 8.1 (Substitution extension unary)**.** Let $(\delta, \theta, m) \in \lceil \Gamma \rceil_{\mathcal{V}}$ and $(v, \theta, m) \in \lceil \tau \rceil_{\mathcal{V}}$. Then $(\delta \cup \{x, v\}, \theta, m) \in \lceil \Gamma, x : \tau \rceil_{\mathcal{V}}$.

Proof. We have to show

- $\mathrm{dom}(\Gamma, x : \tau) \subseteq \mathrm{dom}(\delta \cup \{x, v\})$.

$$\mathrm{dom}(\Gamma, x : \tau) = \mathrm{dom}(\Gamma) \cup \{x\} \overset{(\delta,\theta,m) \in \lceil \Gamma \rceil_{\mathcal{V}}}{\subseteq} \mathrm{dom}(\delta) \cup x = \mathrm{dom}(\delta \cup \{(x, v)\})$$

- $\forall y \in \mathrm{dom}(\Gamma, x : \tau). (\delta \cup \{(x, v)\}(y), \theta, m) \in \lceil \Gamma, x : \tau(y) \rceil_{\mathcal{V}}$

  Let $y \in \mathrm{dom}(\Gamma, x : \tau)$. There are two cases:

  1. $y \neq x$. In this case
     - $y \in \mathrm{dom}(\Gamma)$
     - $\Gamma, x : \tau(y) = \Gamma(y)$
     - $(\delta \cup \{(x, v)\})(y) = \delta(y)$

So we have to show $(\delta(y), \theta, m) \in \lceil \Gamma(y) \rceil_\nu$ which we get from $(\delta, \theta, m) \in \lceil \Gamma \rceil_\nu$.

2. $y = x$ In this case the goal simplifies to $(\nu, \theta, m) \in \lceil \tau \rceil_\nu$ which we already know.

□

Lemma 8.2 (Substitution extension binary)**.** Let $(\gamma, W, m) \in [\![\Gamma]\!]^{\mathcal{A}}_{\mathcal{V}}$ and $(\nu, \nu', W, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$, then $((\{(x,\nu)\} \cup \gamma_1, \{x, \nu'\} \cup \gamma_2), W, m) \in [\![\Gamma, x : \tau]\!]^{\mathcal{A}}_{\mathcal{V}}$.

Proof. We have to show

- $\mathrm{dom}(\Gamma, x : \tau) \subseteq \mathrm{dom}((\gamma_1 \cup \{(x,\nu)\}, \gamma_2 \cup \{(x,\nu')\}))$.
  $\mathrm{dom}((\gamma_1 \cup \{(x,\nu)\}, \gamma_2 \cup \{(x,\nu')\})) = \mathrm{dom}(\gamma_1 \cup \{(x,\nu)\}) \cap \mathrm{dom}(\gamma_2 \cup \{(x,\nu')\}) = (\mathrm{dom}(\gamma_1) \cup \{x\}) \cap (\mathrm{dom}(\gamma_2) \cup \{x\}) = (\mathrm{dom}(\gamma_1) \cap \mathrm{dom}(\gamma_2)) \cup \{x\} = \mathrm{dom}(\gamma) \cup \{x\}$. Also $\mathrm{dom}(\Gamma, x : \tau) = \mathrm{dom}(\Gamma) \cup \{x\}$. Since we already know $(\gamma, W, m) \in \lceil \Gamma \rceil_\nu$, we also know $\mathrm{dom}(\Gamma) \subseteq \mathrm{dom}(\gamma)$. Hence also $\mathrm{dom}(\Gamma) \cup \{x\} \subseteq \mathrm{dom}(\gamma) \cup \{x\}$ which suffices to prove the goal.
- $\forall y \in \mathrm{dom}(\Gamma, x : \tau).(\gamma_1 \cup \{(x,\nu)\}(y), \gamma_2 \cup \{(x,\nu')\}(y), W, m) \in [\![\Gamma, x : \tau_1(y)]\!]^{\mathcal{A}}_{\mathcal{V}}$.

  Let $y \in \mathrm{dom}(\Gamma, x : \tau)$. There are two options

  - $y \in \mathrm{dom}(\Gamma)$. In this case $(\gamma_1 \cup \{(x,\nu)\}(y), \gamma_2 \cup \{(x,\nu')\}(y), W, m) \in [\![\Gamma, x : \tau(y)]\!]^{\mathcal{A}}_{\mathcal{V}}$ simplifies to $(\gamma_1(y), \gamma_2(y), W, m) \in [\![\Gamma(y)]\!]^{\mathcal{A}}_{\mathcal{V}}$. We already know $(\gamma, W, m) \in [\![\Gamma]\!]^{\mathcal{A}}_{\mathcal{V}}$ which implies the goal.
  - $y = x$. In this case $(\gamma_1 \cup \{(x,\nu)\}(y), \gamma_2 \cup \{(x,\nu')\}(y), W, m) \in [\![\Gamma, x : \tau(y)]\!]^{\mathcal{A}}_{\mathcal{V}}$ simplifies to $(\nu, \nu', W, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$ which we already know.

□

Lemma 8.3 (Policy of updated locations)**.** If $\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'$, then for all $l \in \mathrm{dom}(S')$ we have $S'(l) = S(l) \vee \mathrm{pol}(\omega) = \mathrm{pol}(\mathrm{type}(S', l))$

Proof. By induction on the derivation of $\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'$. In most cases either $S = S'$ which makes the statement trivial or we get the claim by induction. The only interesting cases are the following:

- **ENewBeta**:

$$\frac{l \notin \mathrm{dom}(S)}{\Sigma \vdash \mathsf{new}\,(\nu, \tau)\,, S \xrightarrow{l_\tau(\nu);\Sigma} l, S \cup \{l \rightarrowtail (\nu, \tau)\}}\ \textbf{ENewBeta}$$

  Let $l' \in \mathrm{dom}(S \cup \{l \rightarrowtail (\nu, \tau)\})$. There are two cases:

  - $l' \in \mathrm{dom}(S)$. In that case $S \cup \{l \rightarrowtail (\nu, \tau)\}(l') = S(l')$ because $l \notin \mathrm{dom}(S)$, so $l' \neq l$.
  - $l' = l$. In this case $\mathrm{pol}(\mathrm{type}(S \cup \{l \rightarrowtail (\nu, \tau)\}, l')) = \mathrm{pol}(\mathrm{type}(S \cup \{l \rightarrowtail (\nu, \tau)\}, l)) = \mathrm{pol}(\tau) = \mathrm{pol}(l_\tau(\nu))$.

- **Eassign**:

$$\frac{l \in \mathrm{dom}(S) \qquad \mathrm{type}(S, l) = \tau}{\Sigma \vdash l := \nu, S \xrightarrow{l_\tau(\nu);\Sigma} (), S[l \rightarrowtail (\nu, \tau)]}\ \textbf{Eassign}$$

  Let $l' \in \mathrm{dom}(S[l \rightarrowtail (\nu, \tau)])$. There are two cases:

  - $l' \neq l$. In this case $l' \in \mathrm{dom}(S)$ and $S(l') = S[l \rightarrowtail (\nu, \tau)](l')$.
  - $l' = l$. In this case $\mathrm{pol}(\mathrm{type}(S[l \rightarrowtail (\nu, \tau)], l')) = \mathrm{pol}(\mathrm{type}(S[l \rightarrowtail (\nu, \tau)], l)) = \tau = \mathrm{pol}(l_\tau(\nu))$.

□

Lemma 8.4. For all τ, ν, θ, m. $(\nu, \theta, m) \in \lceil \tau \rceil_\nu \to \forall \theta', m'.\theta \sqsubseteq \theta' \wedge m' \leqslant m \to (\nu, \theta', m') \in \lceil \tau \rceil_\nu$ and for all $A, \nu, \theta, m.(\nu, \theta, m) \in \lceil A \rceil_\nu \to \forall \theta', m'.\theta \sqsubseteq \theta' \wedge m' < m \to (\nu, \theta', m') \in \lceil A \rceil_\nu$.

Proof. By mutual induction on the structure of A and τ.

- $\mathtt{unit}$: Then $\nu = n$ and $n \in \mathbb{N}$. Hence $(n, \theta', m') \in \lceil \mathcal{N} \rceil_\nu$ anyway.
- $\mathcal{N}$: Then $\nu = ()$ and $((), \theta', m') \in \lceil \mathtt{unit} \rceil_\nu$ anyway.

- $\tau_1 \times \tau_2$: Then $v = (v_1, v_2)$ and $(v_1, \theta, m) \in \lceil \tau_1 \rceil_\mathcal{V}$ and $(v_2, \theta, m) \in \lceil \tau_2 \rceil_\mathcal{V}$. By induction also $(v_1, \theta', m') \in \lceil \tau_1 \rceil_\mathcal{V}$ and $(v_2, \theta', m') \in \lceil \tau_2 \rceil_\mathcal{V}$. This suffices to show the goal.
- $\tau_1 + \tau_2$: W.l.o.g. assume $v = \mathtt{inl}\ v'$. Then $(v', \theta, m) \in \lceil \tau_1 \rceil_\mathcal{V}$. By induction $(v', \theta', m') \in \lceil \tau_1 \rceil_\mathcal{V}$. This proofs the goal.
- $\tau_1 \xrightarrow{\Sigma,p} \tau_2$: In this case $v = \lambda x.e$. Let $\theta'' \sqsupseteq \theta', m'', v'$ s.t. $m'' < m'$ and $(v', \theta'', m'') \in \lceil \tau_1 \rceil_\mathcal{V}$. We have to show $([v'/x]e, \theta'', m'') \in \lceil \tau_2 \rceil^p_\mathsf{E}$. By transitivity (Lemma 6.2) we have $\theta \sqsubseteq \theta''$ and $m'' < m$. Since we already know$(v', \theta'', m'') \in \lceil \tau_1 \rceil_\mathcal{V}$ we get $([v'/x]e, \theta'', m'') \in \lceil \tau_2 \rceil^p_\mathsf{E}$ from $(\lambda x.e, \theta) \in \lceil \tau_1 \xrightarrow{\Sigma,p} \tau_2 \rceil_\mathcal{V}$.
- $\mathtt{ref}\ \tau'$: In this case $v = l$ and $\theta(l) = \tau'$. Because $\theta' \sqsupseteq \theta$ also $\theta'(l) = \tau'$ and hence $(l, \theta', m') \in \lceil \mathtt{ref}\ \tau' \rceil_\mathcal{V}$.
- A^l: In this case $(v, \theta, m) \in \lceil A \rceil_\mathcal{V}$ By induction $(v, \theta', m') \in \lceil A \rceil_\mathcal{V}$ and hence $(v, \theta', m') \in \lceil A^l \rceil_\mathcal{V}$.

□

Lemma 8.5. For all m, τ, e, θ, pc. $(e, \theta, m) \in \lceil \tau \rceil^{pc}_\mathsf{E} \to \forall \theta', m', pc'. \theta \sqsubseteq \theta' \wedge m' \leqslant m \wedge pc' \sqsubseteq pc \to (e, \theta', m') \in \lceil \tau \rceil^{pc'}_\mathsf{E}$.

Proof. By induction on m. There are two cases:

1. $(e, \theta, m) \in \lceil \tau \rceil^{pc}_{\mathsf{E}_\beta}$. It suffices to show $(e, \theta', m') \in \lceil \tau \rceil^{pc'}_{\mathsf{E}_\beta}$. We get $e \notin \mathcal{V}$ from $(e, \theta, m) \in \lceil \tau \rceil^{pc}_{\mathsf{E}_\beta}$.
   So let S, θ'', m'' such that
   - $\theta'' \sqsupseteq \theta'$
   - $(S, m'') \triangleright \theta''$
   - $m'' < m'$

   and $e', S', \omega, \Sigma, \Sigma'$ such that
   - $e, \Sigma, S \succ e', S', \omega, \Sigma'$

   By transitivity $\theta'' \sqsupseteq \theta$ (Lemma 6.2), and $m'' < m$.
   Hence by $(e, \theta, m) \in \lceil \tau \rceil^{pc}_{\mathsf{E}_\beta}$
   - $(\forall p. \mathtt{pol}(\omega) = p \to pc \sqsubseteq p)$

   and there is a θ''' such that
   - $\theta''' \sqsupseteq \theta''$
   - $(S', m'') \triangleright \theta'''$
   - $(e', \theta''', m'') \in \lceil \tau \rceil^{pc}_\mathsf{E}$

   It suffices to show
   - $\forall p. (\mathtt{pol}(\omega = p)) \to pc' \sqsubseteq p$. Let p be a policy and $\mathtt{pol}(\omega) = p$. Then $pc \sqsubseteq p$. We also know $pc' \sqsubseteq pc$. We get $pc' \sqsubseteq p$ by transitivity (Lemma 4.1).
   - $\theta''' \sqsupseteq \theta''$. We already know that.
   - $(S', m'') \triangleright \theta'''$. We already know that.
   - $(e', \theta''', m'') \in \lceil \tau \rceil^{pc'}_\mathsf{E}$. We get this by induction.
2. $(e, \theta, m) \in \lceil \tau \rceil^{pc}_{\mathsf{E}_\nu}$. In that case $(e, \theta, m) \in \lceil \tau \rceil_\mathcal{V}$. We get $(e, \theta', m') \in \lceil \tau \rceil_\mathcal{V}$ by Lemma 8.4. The goal follows directly from the definition of $\lceil \tau \rceil^{pc'}_\mathsf{E}$.

□

Lemma 8.6 (Unary Semantic subtyping)**.** [5]

1. $\forall A, A'.\ A <: A' \to \lceil A \rceil_\mathcal{V} \subseteq \lceil A' \rceil_\mathcal{V}$
2. $\forall \tau, \tau'.$
   (a) $\tau <: \tau' \to \lceil \tau \rceil_\mathcal{V} \subseteq \lceil \tau' \rceil_\mathcal{V}$

(b) $\tau <: \tau' \to \forall \mathsf{pc}.\ \lceil \tau \rceil_{\mathsf{E}}^{\mathsf{pc}} \subseteq \lceil \tau' \rceil_{\mathsf{E}}^{\mathsf{pc}}$

Proof. By mutual induction on $A <: A'$ and $\tau <: \tau'$.

1.
   - **sub-ref**. In this case $A = \mathtt{ref}\ \tau_A = A'$. Hence $\lceil A \rceil \nu = \lceil A' \rceil \nu$ and we get the claim by reflexivity.
   - **sub-prod** In this case
     - $A = \tau_0 \times \tau_0'$
     - $A' = \tau_1 \times \tau_1'$
     - $\tau_0 <: \tau_1$
     - $\tau_0' <: \tau_1'$

     Let $((v_0, v_0'), \theta, m) \in \lceil \tau_0 \times \tau_0' \rceil \nu$. In this case
     - $(v_0, \theta, m) \in \lceil \tau_0 \rceil \nu$
     - $(v_0', \theta, m) \in \lceil \tau_0' \rceil \nu$.

     By induction also
     - $(v_0, \theta, m) \in \lceil \tau_1 \rceil \nu$
     - $(v_0', \theta, m) \in \lceil \tau_1' \rceil \nu$.

     Hence $(v_0, v_0', \theta, m) \in \lceil \tau_1 \times \tau_1' \rceil \nu$.
   - **sub-sum**: In this case $A = \mathtt{ref}\ \tau_A = A'$. Hence $\lceil A \rceil \nu = \lceil A' \rceil \nu$ and we get the claim by reflexivity.
   - **sub-prod** In this case
     - $A = \tau_0 + \tau_0'$
     - $A' = \tau_1 + \tau_1'$
     - $\tau_0 <: \tau_1$
     - $\tau_0' <: \tau_1'$

     Let $(v, \theta, m) \in \lceil \tau_0 \times \tau_0' \rceil \nu$. W.l.o.g. assume $v = \mathtt{inl}\ v'$. In this case
     - $(v', \theta, m) \in \lceil \tau_0 \rceil \nu$

     By induction also
     - $(v', \theta, m) \in \lceil \tau_1 \rceil \nu$

     Hence $(\mathtt{inl}\ v', \theta, m) \in \lceil \tau_1 + \tau_1' \rceil \nu$.
   - **sub-arrow** In this case
     - $A = \tau_0 \xrightarrow{\Sigma, p} \tau_1$
     - $A' = \tau_0' \xrightarrow{\Sigma', p'} \tau_1'$
     - $\tau_0' <: \tau_0$
     - $\tau_1 <: \tau_1'$
     - $p' \sqsubseteq p$
     - $\Sigma \subseteq \Sigma'$

     Let $(\lambda x.\ e, \theta, m) \in \lceil \tau_0 \xrightarrow{\Sigma, p} \tau_1 \rceil \nu$ We need to show $(\lambda x.\ e, \theta, m) \in \lceil \tau_0' \xrightarrow{\Sigma', p'} \tau_1' \rceil \nu$. So let θ', v, m' such that
     - $\theta' \sqsupseteq \theta$
     - $m' < m$
     - $(v, \theta', m') \in \lceil \tau_0' \rceil \nu$

     Then by induction
     - $(v, \theta', m') \in \lceil \tau_0 \rceil \nu$

     Therefore
     - $([v/x]e, \theta', m') \in \lceil \tau_1 \rceil_{\mathsf{E}}^{p}$

     By induction
     - $([v/x]e, \theta', m') \in \lceil \tau_1' \rceil_{\mathsf{E}}^{p'}$

     We get $([v/x]e, \theta', m') \in \lceil \tau_1' \rceil_{\mathsf{E}}^{p'}$ by Lemma 8.5.
   - **sub-unit** In this case $A = \mathtt{unit} = A'$ Hence $\lceil A \rceil \nu = \lceil A' \rceil \nu$ and we get the claim by reflexivity.

- **sub-nat** In this case $A = \mathcal{N} = A'$ Hence $\lceil A \rceil_\mathcal{V} = \lceil A' \rceil_\mathcal{V}$ and we get the claim by reflexivity.

2. (a) The only applicable rule is **sub-policy**. In this case
   - $\tau = A^p$
   - $\tau' = B^{p'}$
   - $p \sqsubseteq p'$
   - $A <: B$

   Let $(v, \theta, m) \in \lceil A^p \rceil_\mathcal{V}$. Then
   - $(v, \theta, m) \in \lceil A \rceil_\mathcal{V}$

   By induction therefore
   - $(v, \theta, m) \in \lceil B \rceil_\mathcal{V}$

   This directly gives us $(v, \theta, m) \in \lceil B^{p'} \rceil_\mathcal{V}$.

   (b) The only applicable rule is **sub-policy**. In this case
   - $\tau = A^p$
   - $\tau' = B^{p'}$
   - $p \sqsubseteq p'$
   - $A <: B$

   To show $\lceil A^p \rceil^{pc}_E \subseteq \lceil B^{p'} \rceil^{pc}_E$ we have to show $\forall m, e, \theta.(e, \theta, m) \in \lceil A^p \rceil^{pc}_E \to (e, \theta, m) \in \lceil B^{p'} \rceil^{pc}_E$. We do this by induction on m. So let $(e, \theta, m) \in \lceil \tau \rceil^{pc}_E$. There are two cases:
   - $(e, \theta, m) \in \lceil A^p \rceil^{pc}_{E_\mathcal{V}}$. In this case e is a value v and $(v, \theta, m) \in \lceil A^p \rceil_\mathcal{V}$. Then also $(v, \theta, m) \in \lceil A \rceil_\mathcal{V}$. By induction $(v, \theta, m) \in \lceil B \rceil_\mathcal{V}$. This gives us $(v, \theta, m) \in \lceil B^{p'} \rceil_\mathcal{V}$ which implies the goal.
   - $(e, \theta, m) \in \lceil A^p \rceil^{pc}_{E_\beta}$. It suffices to show $(e, \theta, m) \in \lceil B^{p'} \rceil^{pc}_{E_\beta}$. By assumption e is not a value. So let S, θ', m' such that
     - $\theta' \sqsupseteq \theta$,
     - $(S, m') \triangleright \theta'$,
     - $m' < m$

     Also let $e', S', \omega, \Sigma, \Sigma'$ such that
     - $e, \Sigma, S \succ e', S', \omega, \Sigma'$

     Then
     - $\forall q.\mathtt{pol}(\omega) = q \to pc \sqsubseteq q$

     And there is a θ'' such that
     - $\theta'' \sqsupseteq \theta'$
     - $(S', m') \triangleright \theta''$
     - $(e', \theta'', m') \in \lceil A^p \rceil^{pc}_E$

     It suffices to show
     - $\forall q.\mathtt{pol}(\omega) = q \to pc \sqsubseteq q$. We already know that.
     - $\theta'' \sqsupseteq \theta'$. We already know that.
     - $(S', m') \triangleright \theta''$. We already know that.
     - $(e', \theta'', m') \in \lceil B^{p'} \rceil^{pc}_E$. We get this from the induction hypothesis from the inner induction.

□

8.2 Fundamental lemma for the unary relation

Lemma 8.7.
If $(e, \theta, m) \in [\![\tau]\!]^\mathcal{A}_E$ and $\mathsf{pc} \sqsubseteq \mathrm{pol}(\sigma)$, then $(e \ \mathtt{then\ unopen}\ \sigma, \theta, m) \in \lceil \tau \rceil^{pc}_E$.

Proof. By induction on m. There are two cases:

1. $(e, \theta, m) \in \lceil \tau \rceil^{pc}_{E_\beta}$. In this case it suffices to show $(\mathtt{opened}\ \sigma\ \mathtt{in}\ e, \theta, m) \in \lceil \tau \rceil^{pc}_{E_\beta}$. It is clear that $\mathtt{opened}\ \sigma\ \mathtt{in}\ e$ is not a value. So let S, θ', m' such that

- $\theta' \sqsupseteq \theta$,
- $(S, m') \triangleright \theta'$ and
- $m' < m$.

Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

- $\mathtt{opened}\ \sigma\ \mathtt{in}\ e, \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

By assumption e is not a value. Hence the reduction must have happened with **Eopened**. Hence we know there is a e' such that

- $e, \Sigma \cup \{\sigma\}, S \succ e', S', \omega, \Sigma'$ and
- $e_\beta = \mathtt{opened}\ \sigma\ \mathtt{in}\ e'$.

Because $(e, \theta, m) \in \lceil\tau\rceil^{pc}_{E_\beta}$ therefore

- $\forall p.\mathtt{pol}(\omega) = p \to pc \sqsubseteq p$

and there is a θ'' such that

- $\theta'' \sqsupseteq \theta'$,
- $(S', m') \triangleright \theta''$,
- $(e', \theta'', m') \in \lceil\tau\rceil^{pc}_{E}$.

It suffices to show

- $\forall p.\mathtt{pol}(\omega) = p \to pc \sqsubseteq p$. We already know that.
- $\theta'' \sqsupseteq \theta'$. We already know that
- $(S', m') \triangleright \theta''$. We already know that.
- $(\mathtt{opened}\ \sigma\ \mathtt{in}\ e', \theta'', m') \in \lceil\tau\rceil^{pc}_{E}$. We get this by induction.

2. $(e, \theta, m) \in \lceil\tau\rceil^{pc}_{E_v}$. In this case $(e, \theta, m) \in \lceil\tau\rceil_v$. So there is a value v such that $v = e$. It suffices to show $(\mathtt{opened}\ \sigma\ \mathtt{in}\ v, \theta, m) \in \lceil\tau\rceil^{pc}_{E_\beta}$. It is clear that $\mathtt{opened}\ \sigma\ \mathtt{in}\ e$ is not a value. So let S, θ', m' such that

   - $\theta' \sqsupseteq \theta$,
   - $(S, m') \triangleright \theta'$ and
   - $m' < m$.

   Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

   - $\mathtt{opened}\ \sigma\ \mathtt{in}\ v, \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

   Because v is a value, the reduction must have happened with **EopenedBeta**. Hence we know that

   - $S' = S$,
   - $e_\beta = v$,
   - $\omega = \mathtt{unopen}(\sigma)$ and
   - $\Sigma' = \Sigma$.

   So the reduction is really

   - $\mathtt{opened}\ \sigma\ \mathtt{in}\ v, \Sigma, S \succ v, S, \mathtt{unopen}(\sigma), \Sigma$.

   It suffices to show

   - $pc \sqsubseteq \mathtt{pol}(\sigma)$. This is one of our assumptions.
   - $\theta' \sqsupseteq \theta'$. We have this by Lemma 6.2.
   - $(S, m') \triangleright \theta'$. We already know that.
   - $(v, \theta', m') \in \lceil\tau\rceil^{pc}_{E}$. We get this by Lemma 8.5.

□

Lemma 8.8.
If $(e, \theta, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$ and $pc \sqsubseteq pol(\sigma)$, then $(\mathsf{open}\ \sigma\ \mathsf{in}\ e, \theta, m) \in \lceil \tau \rceil^{pc}_{E}$.

Proof. By induction on m. It suffices to show $(\mathsf{open}\ \sigma\ \mathsf{in}\ e, \theta, m) \in \lceil \tau \rceil^{pc}_{E_\beta}$. It is clear that $\mathsf{open}\ \sigma\ \mathsf{in}\ e$ is not a value. So let S, θ', m' such that

- $\theta' \sqsupseteq \theta$,
- $(S, m') \triangleright \theta'$ and
- $m' < m$.

Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

- $\mathsf{open}\ \sigma\ \mathsf{in}\ e, \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

The reduction must have happened with **Eopen**. Hence we know

- $S' = S$,
- $e_\beta = \mathsf{opened}\ \sigma\ \mathsf{in}\ e$,
- $\Sigma' = \Sigma$, and
- $\omega = \mathsf{open}(\sigma)$.

So the reduction is really

- $\mathsf{open}\ \sigma\ \mathsf{in}\ e, \Sigma, S \succ \mathsf{opened}\ \sigma\ \mathsf{in}\ e, S, \mathsf{open}(\sigma), \Sigma$.

It suffices to show

- $pc \sqsubseteq \mathsf{pol}(\sigma)$. We already know that.
- $\theta' \sqsupseteq \theta'$. We already know that
- $(S, m') \triangleright \theta'$. We already know that.
- $(\mathsf{opened}\ \sigma\ \mathsf{in}\ e, \theta', m') \in \lceil \tau \rceil^{pc}_{E}$. We get $(e, \theta', m') \in \lceil \tau \rceil^{pc}_{E}$ by Lemma 8.5. The goal follows by Lemma 8.7.

□

Lemma 8.9. If $(e_1, \theta, m) \in \lceil \tau_1 \rceil^{pc}_{E}$ and $(e_2, \theta, m) \in \lceil \tau_2 \rceil^{pc}_{E}$, then $((e_1, e_2), \theta, m) \in \lceil (\tau_1 \times \tau_2)^p \rceil^{pc}_{E}$.

Proof. By induction on m. There are several cases:

1. $(e_1, \theta, m) \in \lceil \tau_1 \rceil^{pc}_{E_\beta}$. It suffices to show $((e_1, e_2), \theta, m) \in \lceil (\tau_1 \times \tau_2)^p \rceil^{pc}_{E_\beta}$. By assumption e_1 is not a value. Hence (e_1, e_2) is not a value either. So let S, θ', m' such that

   - $\theta' \sqsupseteq \theta$,
   - $(S, m') \triangleright \theta'$ and
   - $m' < m$.

   Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

   - $(e_1, e_2), \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

   By assumption e_1 is not a value. Hence the reduction must have happened with **EPairl**. Hence we know there is a e_1' such that

   - $e_1, \Sigma, S \succ e_1', S', \omega, \Sigma'$ and
   - $e_\beta = (e_1', e_2)$.

   Because $(e_1, \theta, m) \in \lceil \tau_1 \rceil^{pc}_{E_\beta}$ therefore

   - $\forall p. \mathsf{pol}(\omega) = p \to pc \sqsubseteq p$

   and there is a θ'' such that

- $\theta'' \sqsupseteq \theta'$,
- $(S', m') \triangleright \theta''$,
- $(e_1', \theta'', m') \in \lceil \tau_1 \rceil^{pc}_E$.

It suffices to show

- $\forall p.\mathrm{pol}(\omega) = p \to pc \sqsubseteq p$. We already know that.
- $\theta'' \sqsupseteq \theta'$. We already know that
- $(S', m') \triangleright \theta''$. We already know that.
- $((e_1', e_2), \theta'', m') \in \lceil (\tau_1 \times \tau_2)^p \rceil^{pc}_E$. By Lemma 6.2 we have $\theta'' \sqsupseteq \theta$. Hence we get $(e_2, \theta'', m') \in \lceil \tau_2 \rceil^{pc}_E$ by Lemma 8.5 . The claim follows by induction.

2. $(e_1, \theta, m) \in \lceil \tau_1 \rceil^{pc}_{E_\nu}$. In this case there is a value ν_1 such that $e_1 = \nu_1$ and $(\nu_1, \theta, m) \in \lceil \tau_1 \rceil_\nu$. There are two further cases:

   (a) $(e_2, \theta, m) \in \lceil \tau_2 \rceil^{pc}_{E_\beta}$. It suffices to show $((\nu_1, e_2), \theta, m) \in \lceil (\tau_1 \times \tau_2)^p \rceil^{pc}_{E_\beta}$. By assumption e_2 is not a value. Hence (ν_1, e_2) is not a value either. So let S, θ', m' such that

   - $\theta' \sqsupseteq \theta$,
   - $(S, m') \triangleright \theta'$ and
   - $m' < m$.

   Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

   - $(\nu_1, e_2), \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

   By assumption ν_1 is a value and e_2 is not. Hence the reduction must have happened with **EPairr**. Hence we know there is a e_2' such that

   - $e_2, \Sigma, S \succ e_2', S', \omega, \Sigma'$ and
   - $e_\beta = (\nu_1, e_2')$.

   Because $(e_2, \theta, m) \in \lceil \tau_2 \rceil^{pc}_{E_\beta}$

   - $\forall p.\mathrm{pol}(\omega) = p \to pc \sqsubseteq p$

   and there is a θ'' such that

   - $\theta'' \sqsupseteq \theta'$,
   - $(S', m') \triangleright \theta''$,
   - $(e_2', \theta'', m') \in \lceil \tau_2 \rceil^{pc}_E$.

   It suffices to show

   - $\forall p.\mathrm{pol}(\omega) = p \to pc \sqsubseteq p$. We already know that.
   - $\theta'' \sqsupseteq \theta'$. We already know that
   - $(S', m') \triangleright \theta''$. We already know that.
   - $((\nu_1, e_2'), \theta'', m') \in \lceil (\tau_1 \times \tau_2)^p \rceil^{pc}_E$. By Lemma 6.2 we have $\theta'' \sqsupseteq \theta$. Hence we get $(\nu_1, \theta'', m') \in \lceil \tau_1 \rceil^{pc}_E$ by Lemma 8.5 . The claim follows by induction.

   (b) $e_2, \theta, m) \in \lceil \tau_2 \rceil^{pc}_{E_\nu}$. Then there is a value ν_2 such that $e_2 = \nu_2$ and $(\nu_2, \theta, m) \in \lceil \tau_2 \rceil_\nu$. It suffices to show $((\nu_1, \nu_2), \theta, m) \in \lceil (\tau_1 \times \tau_2)^p \rceil^{pc}_{E_\nu}$. For that it suffices to show $((\nu_1, \nu_2), \theta, m) \in \lceil (\tau_1 \times \tau_2)^p \rceil_\nu$. By definition it suffices to show $((\nu_1, \nu_2), \theta, m) \in \lceil \tau_1 \times \tau_2 \rceil_\nu$. To show this we need to show

   - $(\nu_1, \theta, m) \in \lceil \tau_1 \rceil_\nu$
   - $(\nu_2, \theta, m) \in \lceil \tau_2 \rceil_\nu$.

   We know both of this already.

□

Lemma 8.10. If $(e_1, \theta, m) \in \lceil (\tau_1 \xrightarrow{\Sigma_m, p} \tau_2)^q \rceil^{pc}_E$ and $(e_2, \theta, m) \in \lceil \tau_1 \rceil^{pc}_E$ and $pc \sqsubseteq p$, then $(e_1\ e_2, \theta, m) \in \lceil \tau_2 \rceil^{pc}_E$.

Proof. By induction on m. There are several cases:

1. $(e_1, \theta, m) \in \lceil (\tau_1 \xrightarrow{\Sigma_m, p} \tau_2)^q \rceil^{pc}_{E_\beta}$. It suffices to show $(e_1\ e_2, \theta, m) \in \lceil \tau_2 \rceil^{pc}_{E_\beta}$. Clearly $e_1\ e_2$ is not a value. So let S, θ', m' such that

- $\theta' \sqsupseteq \theta$,
- $(S, m') \triangleright \theta'$ and
- $m' < m$.

Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

- $e_1\ e_2, \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

By assumption e_1 is not a value. Hence the reduction must have happened with **EAppl**. Hence we know there is a e_1' such that

- $e_1, \Sigma, S \succ e_1', S', \omega, \Sigma'$ and
- $e_\beta = e_1'\ e_2$.

Because $(e_1, \theta, m) \in \lceil(\tau_1 \overset{\Sigma_m, p}{\to} \tau_2)^q\rceil^{pc}_{E_\beta}$ we know

- $\forall p.pol(\omega) = p \to pc \sqsubseteq p$

and there is a θ'' such that

- $\theta'' \sqsupseteq \theta'$,
- $(S', m') \triangleright \theta''$,
- $(e_1', \theta'', m') \in \lceil(\tau_1 \overset{\Sigma_m, p}{\to} \tau_2)^q\rceil^{pc}_{E}$.

It suffices to show

- $\forall p.pol(\omega) = p \to pc \sqsubseteq p$. We already know that.
- $\theta'' \sqsupseteq \theta'$. We already know that
- $(S', m') \triangleright \theta''$. We already know that.
- $(e_1'\ e_2, \theta'', m') \in \lceil\tau_2\rceil^{pc}_{E}$. By Lemma 6.2 we have $\theta'' \sqsupseteq \theta$. Hence we get $(e_2, \theta'', m') \in \lceil\tau_1\rceil^{pc}_{E}$ by Lemma 8.5 . The claim follows by induction.

2. $(e_1, \theta, m) \in \lceil(\tau_1 \overset{\Sigma_m, p}{\to} \tau_2)^q\rceil^{pc}_{E_\nu}$. In this case there is a value ν_1 such that $e_1 = \nu_1$ and $(\nu_1, \theta, m) \in \lceil(\tau_1 \overset{\Sigma_m, p}{\to} \tau_2)^q\rceil_\nu$. In this case $(\nu_1, \theta, m) \in \lceil\tau_1 \overset{\Sigma_m, p}{\to} \tau_2\rceil_\nu$. Hence ν_1 has the form $\lambda x.e$. There are two further cases:

   (a) $(e_2, \theta, m) \in \lceil\tau_1\rceil^{pc}_{E_\beta}$. It suffices to show $((\lambda x.e)\ e_2, \theta, m) \in \lceil\tau_2\rceil^{pc}_{E_\beta}$. Clearly $(\lambda x.e)\ e_2$ is not a value. So let S, θ', m' such that

   - $\theta' \sqsupseteq \theta$,
   - $(S, m') \triangleright \theta'$ and
   - $m' < m$.

   Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

   - $(\lambda x.e)\ e_2, \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

   By assumption e_2 is not a value. Hence the reduction must have happened with **EAppr**. Hence we know there is a e_2' such that

   - $e_2, \Sigma, S \succ e_2', S', \omega, \Sigma'$ and
   - $e_\beta = (\lambda x.e)\ e_2'$.

   Because $(e_2, \theta, m) \in \lceil\tau_1\rceil^{pc}_{E_\beta}$

   - $\forall p.pol(\omega) = p \to pc \sqsubseteq p$

   and there is a θ'' such that

   - $\theta'' \sqsupseteq \theta'$,
   - $(S', m') \triangleright \theta''$,
   - $(e_2', \theta'', m') \in \lceil\tau_1\rceil^{pc}_{E}$.

   It suffices to show

   - $\forall p.pol(\omega) = p \to pc \sqsubseteq p$. We already know that.

- $\theta'' \sqsupseteq \theta'$. We already know that
- $(S', m') \triangleright \theta''$. We already know that.
- $((\lambda x.e)\ e_2', \theta'', m') \in \lceil \tau_2 \rceil^{pc}_E$. By Lemma 6.2 we have $\theta'' \sqsupseteq \theta$. Hence we get $((\lambda x.e), \theta'', m') \in \lceil (\tau_1 \xrightarrow{\Sigma_m; p} \tau_2)^q \rceil^{pc}_E$ by Lemma 8.5 . The claim follows by induction.

(b) $(e_2, \theta, m) \in \lceil \tau_1 \rceil^{pc}_{E_\nu}$. Then there is a value ν_2 such that $e_2 = \nu_2$ and $(\nu_2, \theta, m) \in \lceil \tau_1 \rceil_\nu$. It suffices to show $((\lambda x.e)\ \nu_2, \theta, m) \in \lceil \tau_2 \rceil^{pc}_{E_\beta}$. It is clear that $(\lambda x.e)\ \nu_2$ is not a value. So let S, θ', m' such that

- $\theta' \sqsupseteq \theta$,
- $(S, m') \triangleright \theta'$ and
- $m' < m$.

Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

- $(\lambda x.e)\ \nu_2, \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

By assumption ν_2 is a value. Hence the reduction must have happened with **EAppBeta**. Therefore

- $e_\beta = [\nu_2/x]e$
- $S' = S$
- $\Sigma' = \Sigma$
- $\omega = \epsilon$

So the reduction is really

- $(\lambda x.e)\ \nu_2, \Sigma, S \succ [\nu_2/x]e, S, \epsilon, \Sigma$.

It suffices to show

- $\forall p.(pol(\epsilon) = p) \to pc \sqsubseteq p$. $pol(\epsilon)$ is undefined, so there is no p such that $pol(\epsilon) = p$. So there is nothing to show.
- $\theta' \sqsupseteq \theta'$. We get this by Lemma 6.2.
- $(S, m') \triangleright \theta$. We already know this.
- $([\nu_2/x]e, \theta', m') \in \lceil \tau_2 \rceil^{pc}_E$. Because $pc \sqsubseteq p$, it suffices to show $([\nu_2/x]e, \theta', m') \in \lceil \tau_2 \rceil^{p}_E$ by Lemma 8.5. By assumption $(\lambda x.e, \theta, m) \in \lceil (\tau_1 \xrightarrow{\Sigma_m; p} \tau_2)^q \rceil_\nu$. Hence we get the goal if we can show
  - $\theta' \sqsupseteq \theta$. We already know this.
  - $m' < m$. We already know this.
  - $(\nu_2, \theta', m') \in \lceil \tau_1 \rceil_\nu$. We get this by Lemma 8.4.

□

Lemma 8.11. If $(e, \theta, m) \in \lceil (\tau_1 \times \tau_2)^p \rceil^{pc}_E$, then $(\mathsf{fst}\,(e), \theta, m) \in \lceil \tau_1 \rceil^{pc}_E$.

Proof. By induction on m. It suffices to show $(\mathtt{fst}(e), \theta, m) \in \lceil \tau_1 \rceil^{pc}_{E_\beta}$. It is clear that $\mathtt{fst}(e)$ is not a value. So let S, θ', m' such that

- $\theta' \sqsupseteq \theta$,
- $(S, m') \triangleright \theta'$ and
- $m' < m$.

Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

- $\mathtt{fst}(e), \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

There are two cases:

1. $(e, \theta, m) \in \lceil (\tau_1 \times \tau_2)^p \rceil^{pc}_{E_\beta}$. In this case e is not a value. Hence the reduction must have happened with **EFst**. Hence we know there is a e' such that
   - $e, \Sigma, S \succ e', S', \omega, \Sigma'$ and
   - $e_\beta = \mathtt{fst}(e')$.

Because $(e, \theta, m) \in \lceil (\tau_1 \times \tau_2)^p \rceil^{pc}_{E_\beta}$,

- $\forall p.pol(\omega) = p \to pc \sqsubseteq p$

and there is a θ'' such that

- $\theta'' \sqsupseteq \theta'$,
- $(S', m') \triangleright \theta''$,
- $(e', \theta'', m') \in \lceil (\tau_1 \times \tau_2)^p \rceil^{pc}_{E}$.

It suffices to show

- $\forall p.pol(\omega) = p \to pc \sqsubseteq p$. We already know that.
- $\theta'' \sqsupseteq \theta'$. We already know that
- $(S', m') \triangleright \theta''$. We already know that.
- $(fst(e'), \theta'', m') \in \lceil \tau \rceil^{pc}_{E}$. We get this by induction.

2. $(e, \theta, m) \in \lceil (\tau_1 \times \tau_2)^p \rceil^{pc}_{E_\nu}$. In this case $(e, \theta, m) \in \lceil (\tau_1 \times \tau_2)^p \rceil_\nu$. So there is a value ν such that $\nu = e$ and $(\nu, \theta, m) \in \lceil \tau_1 \times \tau_2 \rceil_\nu$. Hence $\nu = (\nu_1, \nu_2)$ and $(\nu_1, \theta, m) \in \lceil \tau_1 \rceil_\nu$. Because (ν_1, ν_2) is a value, the reduction must have happened with **EFstBeta**. Hence we know that

   - $S' = S$,
   - $e_\beta = \nu_1$,
   - $\omega = \epsilon$ and
   - $\Sigma' = \Sigma$.

   So the reduction is really

   - $fst(\nu_1, \nu_2), \Sigma, S \succ \nu, S, \epsilon, \Sigma$.

   It suffices to show

   - $\forall p.pol(\epsilon) = p \to pc \sqsubseteq pol(\sigma)$. There is no such p so there is nothing to show.
   - $\theta' \sqsupseteq \theta'$. We have this by Lemma 6.2.
   - $(S, m') \triangleright \theta'$. We already know that.
   - $(\nu_1, \theta', m') \in \lceil \tau_1 \rceil^{pc}_{E}$. It suffices to show $(\nu_1, \theta', m') \in \lceil \tau_1 \rceil_\nu$. We get this by Lemma 8.4.

□

Lemma 8.12. If $(e, \theta, m) \in \lceil (\tau_1 \times \tau_2)^p \rceil^{pc}_{E}$, then $(\mathsf{snd}\,(e), \theta, m) \in \lceil \tau_2 \rceil^{pc}_{E}$.

Proof. Analogous to the proof of Lemma 8.11. □

Lemma 8.13. If $(e, \theta, m) \in \lceil \tau_1 \rceil^{pc}_{E}$, then $\forall \tau_2.(\mathsf{inl}\,(e), \theta, m) \in \lceil (\tau_1 + \tau_2)^p \rceil^{pc}_{E}$.

Proof. By induction on m. There are two cases:

1. $(e, \theta, m) \in \lceil \tau_1 \rceil^{pc}_{E_\beta}$. In this case it suffices to show $(\mathtt{inl}\ e, \theta, m) \in \lceil (\tau_1 + \tau_2)^p \rceil^{pc}_{E_\beta}$. It is clear that $fst(e)$ is not a value. So let S, θ', m' such that

   - $\theta' \sqsupseteq \theta$,
   - $(S, m') \triangleright \theta'$ and
   - $m' < m$.

   Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

   - $\mathtt{inl}\ e, \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

   The reduction must have happened with **EInl**. Hence we know there is a e' such that

   - $e, \Sigma, S \succ e', S', \omega, \Sigma'$ and
   - $e_\beta = \mathtt{inl}\ e'$.

Because $(e, \theta, m) \in \lceil \tau_1 \rceil^{pc}_{E_\beta}$,

- $\forall p.pol(\omega) = p \to pc \sqsubseteq p$

and there is a θ'' such that

- $\theta'' \sqsupseteq \theta'$,
- $(S', m') \triangleright \theta''$,
- $(e', \theta'', m') \in \lceil \tau_1 \rceil^{pc}_{E}$.

It suffices to show

- $\forall p.pol(\omega) = p \to pc \sqsubseteq p$. We already know that.
- $\theta'' \sqsupseteq \theta'$. We already know that
- $(S', m') \triangleright \theta''$. We already know that.
- $(\mathsf{inl}\ e', \theta'', m') \in \lceil (\tau_1 + \tau_2)^p \rceil^{pc}_{E}$. We get this by induction.

2. $(e, \theta, m) \in \lceil \tau_1 \rceil^{pc}_{E_v}$. In this case e is a value v and $(v, \theta, m) \in \lceil \tau_1 \rceil_v$. It suffices to show $(\mathsf{inl}\ v, \theta, m) \in \lceil (\tau_1 + \tau_2)^p \rceil_v$. For this is suffices to show $(\mathsf{inl}\ v, \theta, m) \in \lceil \tau_1 + \tau_2 \rceil_v$. We get this by definition because $(v, \theta, m) \in \lceil \tau_1 \rceil_v$.

□

Lemma 8.14. If $(e, \theta, m) \in \lceil \tau_2 \rceil^{pc}_{E}$, then $\forall \tau_1.(\mathsf{inr}\,(e), \theta, m) \in \lceil (\tau_1 + \tau_2)^p \rceil^{pc}_{E}$.

Proof. Analogous to the proof of Lemma 8.14. □

Lemma 8.15. If

- $(e, \theta, m) \in \lceil (\tau_1 + \tau_2)^p \rceil^{pc}_{E}$,
- $\forall \theta', m'.\theta' \sqsupseteq \theta \wedge m' \leqslant m \to \forall v.(v, \theta', m') \in \lceil \tau_1 \rceil_v \to ([v/x]e_1, \theta', m') \in \lceil \tau \rceil^{pc \sqcup p}_{E}$ and
- $\forall \theta'', m'.\theta' \sqsupseteq \theta \wedge m' \leqslant m \to \forall v.(v, \theta', m') \in \lceil \tau_2 \rceil_v \to ([v/y]e_2, \theta', m') \in \lceil \tau \rceil^{pc \sqcup p}_{E}$,

then $(\mathsf{case}\ e\ \mathsf{of}\ |\,\mathsf{inl}\,(x) \Rightarrow e_1\ |\,\mathsf{inr}\,(y) \Rightarrow e_2, \theta, m) \in \lceil \tau \rceil^{pc}_{E}$.

Proof. By induction on m. It suffices to show $(case(e, x.e_1, y.e_2), \theta, m) \in \lceil \tau \rceil^{pc}_{E_\beta}$. It is clear that $case(e, x.e_1, y.e_2)$ is not a value. So let S, θ', m' such that

- $\theta' \sqsupseteq \theta$,
- $(S, m') \triangleright \theta'$ and
- $m' < m$.

Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

- $case(e, x.e_1, y.e_2), \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

There are two cases:

1. $(e, \theta, m) \in \lceil (\tau_1 + \tau_2)^p \rceil^{pc}_{E_\beta}$. In this case e is not a value. Hence the reduction must have happened with **ECase**. Hence we know there is a e' such that

   - $e, \Sigma, S \succ e', S', \omega, \Sigma'$ and
   - $e_\beta = case(e', x.e_1, y.e_2)$.

   Because $(e, \theta, m) \in \lceil (\tau_1 + \tau_2)^p \rceil^{pc}_{E_\beta}$,

   - $\forall p.pol(\omega) = p \to pc \sqsubseteq p$

   and there is a θ'' such that

   - $\theta'' \sqsupseteq \theta'$,
   - $(S', m') \triangleright \theta''$,

- $(e', \theta'', m') \in \lceil (\tau_1 + \tau_2)^p \rceil_E^{pc}$.

It suffices to show

- $\forall p.pol(\omega) = p \to pc \sqsubseteq p$. We already know that.
- $\theta'' \sqsupseteq \theta'$. We already know that
- $(S', m') \triangleright \theta''$. We already know that.
- $(case(e', x.e_1, y.e_2), \theta'', m') \in \lceil \tau \rceil_E^{pc}$. We get this by induction, if we can show
  - $(e', \theta'', m') \in \lceil (\tau_1 + \tau_2)^p \rceil_E^{pc}$. We already know this.
  - $\forall \theta''', m''.\theta''' \sqsupseteq \theta'' \wedge m'' \leqslant m' \to \forall v.(v, \theta''', m'') \in \lceil \tau_1 \rceil_{\mathcal{V}} \to ([v/x]e_1, \theta''', m'') \in \lceil \tau \rceil_E^{pc \sqcup p}$. Let $\theta''' \sqsupseteq \theta''$ and $m'' < m'$. Then by transitivity (Lemma 6.2) we have $\theta''' \sqsupseteq \theta$ and $m'' < m$. Hence we get $\forall v.(v, \theta''', m'') \in \lceil \tau_1 \rceil_{\mathcal{V}} \to ([v/x]e_1, \theta''', m'') \in \lceil \tau \rceil_E^{pc \sqcup p}$ from our assumption.
  - $\forall \theta''', m''.\theta''' \sqsupseteq \theta'' \wedge m'' \leqslant m' \to \forall v.(v, \theta''', m'') \in \lceil \tau_2 \rceil_{\mathcal{V}} \to ([v/y]e_2, \theta''', m'') \in \lceil \tau \rceil_E^{pc \sqcup p}$. Let $\theta''' \sqsupseteq \theta''$ and $m'' < m'$. Then by transitivity (Lemma 6.2) we have $\theta''' \sqsupseteq \theta$ and $m'' < m$. Hence we get $\forall v.(v, \theta''', m'') \in \lceil \tau_2 \rceil_{\mathcal{V}} \to ([v/y]e_2, \theta''', m'') \in \lceil \tau \rceil_E^{pc \sqcup p}$ from our assumption.

.

2. $(e, \theta, m) \in \lceil (\tau_1 + \tau_2)^p \rceil_{E_v}^{pc}$. In this case $(e, \theta, m) \in \lceil (\tau_1 + \tau_2)^p \rceil_{\mathcal{V}}$. So there is a value v such that $v = e$ and $(v, \theta, m) \in \lceil \tau_1 + \tau_2 \rceil_{\mathcal{V}}$. Hence there is a value v' such that $v = inl\ v'$ or $v = inr\ v'$ and $(v', \theta, m) \in \lceil \tau_1 \rceil_{\mathcal{V}}$ or $(v', \theta, m) \in \lceil \tau_2 \rceil_{\mathcal{V}}$, respectively. We do case analysis

   (a) $e = inl\ v'$ and $(v', \theta, m) \in \lceil \tau_1 \rceil_{\mathcal{V}}$. The reduction must have happened with **ECasel**. Hence we know that
   - $S' = S$,
   - $e_\beta = [v'/x]e_1$,
   - $\omega = \epsilon$ and
   - $\Sigma' = \Sigma$.

   So the reduction is really
   - $case(inl\ v', x.e_1, y.e_2), \Sigma, S \succ [v'/x]e_1, S, \epsilon, \Sigma$.

   It suffices to show
   - $\forall p.pol(\epsilon) = p \to pc \sqsubseteq pol(\sigma)$. There is no such p so there is nothing to show.
   - $\theta' \sqsupseteq \theta'$. We have this by Lemma 6.2.
   - $(S, m') \triangleright \theta'$. We already know that.
   - $([v'/x]e_1, \theta', m') \in \lceil \tau_1 \rceil_E^{pc}$. Because $\theta' \sqsupseteq \theta$, $m' < m$ and $(v', \theta', m') \in \lceil \tau \rceil_{\mathcal{V}}$ by Lemma 8.4, we get this by assumption.

   (b) $e = inr\ v'$ and $(v', \theta, m) \in \lceil \tau_2 \rceil_{\mathcal{V}}$. The reduction must have happened with **ECaser**. Hence we know that
   - $S' = S$,
   - $e_\beta = [v'/x]e_2$,
   - $\omega = \epsilon$ and
   - $\Sigma' = \Sigma$.

   So the reduction is really
   - $case(inr\ v', x.e_1, y.e_2), \Sigma, S \succ [v'/x]e_2, S, \epsilon, \Sigma$.

   It suffices to show
   - $\forall p.pol(\epsilon) = p \to pc \sqsubseteq pol(\sigma)$. There is no such p so there is nothing to show.
   - $\theta' \sqsupseteq \theta'$. We have this by Lemma 6.2.
   - $(S, m') \triangleright \theta'$. We already know that.
   - $([v'/x]e_2, \theta', m') \in \lceil \tau \rceil_E^{pc}$. Because $\theta' \sqsupseteq \theta$, $m' < m$ and $(v', \theta', m') \in \lceil \tau_2 \rceil_{\mathcal{V}}$ by Lemma 8.4, we get this by assumption.

□

Lemma 8.16. If $(e, \theta, m) \in \lceil A^p \rceil^{pc}_E$, $pc \sqsubseteq q$ and $A <: B$, then $(\mathsf{new}\,(e, B^q), \theta, m) \in \lceil (\mathsf{ref}\ B^q)^r \rceil^{pc}_E$.

Proof. By induction on m. It suffices to show $(new(e, B^q), \theta, m) \in \lceil (\mathsf{ref}\ B^q)^r \rceil^{pc}_{E_\beta}$. It is clear that $new(e, B^q)$ is not a value. So let S, θ', m' such that

- $\theta' \sqsupseteq \theta$,
- $(S, m') \triangleright \theta'$ and
- $m' < m$.

Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

- $new(e, B^q), \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

There are two cases:

1. $(e, \theta, m) \in \lceil A^p \rceil^{pc}_{E_\beta}$. In this case e is not a value. Hence the reduction must have happened with **ENew**. Hence we know there is a e' such that

   - $e, \Sigma, S \succ e', S', \omega, \Sigma'$ and
   - $e_\beta = new(e', B^q)$.

   Because $(e, \theta, m) \in \lceil A^p \rceil^{pc}_{E_\beta}$,

   - $\forall p.pol(\omega) = p \to pc \sqsubseteq p$

   and there is a θ'' such that

   - $\theta'' \sqsupseteq \theta'$,
   - $(S', m') \triangleright \theta''$,
   - $(e', \theta'', m') \in \lceil A^p \rceil^{pc}_E$.

   It suffices to show

   - $\forall p.pol(\omega) = p \to pc \sqsubseteq p$. We already know that.
   - $\theta'' \sqsupseteq \theta'$. We already know that
   - $(S', m') \triangleright \theta''$. We already know that.
   - $(new(e', B^q), \theta'', m') \in \lceil (\mathsf{ref}\ B^q)^r \rceil^{pc}_E$. We get this by induction.

2. $(e, \theta, m) \in \lceil A^p \rceil^{pc}_{E_\nu}$. In this case $(e, \theta, m) \in \lceil A^p \rceil_\nu$. So there is a value ν such that $\nu = e$ and $(\nu, \theta, m) \in \lceil A \rceil_\nu$. Because ν is a value, the reduction must have happened with **ENewBeta**. Hence we know that there is an l such that

   - $l \notin dom(S)$
   - $S' = S \cup \{l \rightarrowtail (\nu, B^q)\}$,
   - $e_\beta = l$,
   - $\omega = l_{B^q}(\nu)$ and
   - $\Sigma' = \Sigma$.

   So the reduction is really

   - $new(\nu, B^q), \Sigma, S \succ l, S \cup \{l \rightarrowtail (\nu, B^q)\}, l_{B^q}(\nu), \Sigma$.

   It suffices to show

   - $pc \sqsubseteq q$. We have this by assumption.
   - $\theta' \cup \{(l, B^q)\} \sqsupseteq \theta'$. We have this because $\theta' \cup \{(l, B^q)\}$ is a superset of θ.
   - $(S \cup \{l \rightarrowtail (\nu, B^q)\}, m') \triangleright \theta' \cup \{(l, B^q)\}$. We have to show
     - $dom(\theta' \cup \{(l, B^q)\}) \subseteq dom(S \cup \{l \rightarrowtail (\nu, B^q)\})$.

$$dom(\theta' \cup \{(l, B^q)\}) = dom(\theta') \cup \{l\} \overset{(S, m') \triangleright \theta'}{\subseteq} dom(S) \cup \{l\} = dom(S \cup \{l \rightarrowtail (\nu, B^q)\})$$

- $\forall l' \in \mathsf{dom}(\theta' \cup \{(l, B^q)\}).(S \cup \{l \rightarrowtail (v, B^q)\}(l'), \theta' \cup \{(l, B^q)\}, m') \in \lceil \theta' \cup \{(l, B^q)\}(l') \rceil_{\mathcal{V}}$. Let $l' \in \mathsf{dom}(\theta' \cup \{(l, B^q)\})$. There are two cases
  (a) $l' \neq l$. In this case $l' \in \mathsf{dom}(\theta')$. Because $(S, m') \triangleright \theta'$, this gives us $(S(l'), \theta', m') \in \lceil \theta'(l') \rceil_{\mathcal{V}}$. Because $l' \neq l$, this is equivalent to $(S \cup \{l \rightarrowtail (v, B^q)\}(l'), \theta', m') \in \lceil \theta' \cup \{(l, B^q)\}(l') \rceil_{\mathcal{V}}$. We get the goal by Lemma 8.4.
  (b) $l' = l$. In this case we have to show $(v, \theta' \cup \{(l, B^q)\}, m') \in \lceil B^q \rceil_{\mathcal{V}}$. It suffices to show $(v, \theta' \cup \{(l, B^q)\}, m') \in \lceil B \rceil_{\mathcal{V}}$. By Lemma 8.6 it suffices to show $(v, \theta' \cup \{(l, B^q)\}, m') \in \lceil A \rceil_{\mathcal{V}}$. We get this by Lemma 8.4.
- $\forall l' \in \mathsf{dom}(\theta' \cup \{(l, B^q)\}).\theta' \cup \{(l, B^q)\}(l') = \mathsf{type}(S \cup \{l \rightarrowtail (v, B^q)\}, l')$. Let $l' \in \mathsf{dom}(\theta' \cup \{(l, B^q)\})$. There are two cases
  (a) $l' \neq l$. In this case $l \in \mathsf{dom}(\theta')$. By $(S, m) \triangleright \theta'$ this gives us $\theta'(l') = \mathsf{type}(S, l')$. Because $l' \neq l$ this is equivalent to the goal.
  (b) $l' = l$. In this case we have to show that $B^q = B^q$. This is clearly the case.

- $(l, \theta' \cup \{(l, B^q)\}, m') \in \lceil (\mathsf{ref}\ B^q)^r \rceil^{pc}_E$. It suffices to show $(l, \theta' \cup \{(l, B^q)\}, m') \in \lceil \mathsf{ref}\ B^q \rceil_{\mathcal{V}}$. It suffices to show that $\theta' \cup \{(l, B^q)\}(l) = B^q$. This is clearly the case.

□

Lemma 8.17. If $(e, \theta, m) \in \lceil (\mathsf{ref}\ \tau)^p \rceil^{pc}_E$ and $\tau <: \tau'$, then $(!\,e, \theta, m) \in \lceil \tau' \rceil^{pc}_E$.

Proof. By induction on m. It suffices to show $(!e, \theta, m) \in \lceil \tau' \rceil^{pc}_{E_\beta}$. It is clear that $!e$ is not a value. So let S, θ', m' such that

- $\theta' \sqsupseteq \theta$,
- $(S, m') \triangleright \theta'$ and
- $m' < m$.

Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

- $!e, \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

There are two cases:

1. $(e, \theta, m) \in \lceil (\mathsf{ref}\ \tau)^p \rceil^{pc}_{E_\beta}$. Then e is not a value and the reduction must have happened with **EDeref**. Hence we know there is a e' such that
   - $e, \Sigma, S \succ e', S', \omega, \Sigma'$ and
   - $e_\beta = !e'$.

   Because $(e, \theta, m) \in \lceil (\mathsf{ref}\ \tau)^p \rceil^{pc}_{E_\beta}$,
   - $\forall p.\mathsf{pol}(\omega) = p \to pc \sqsubseteq p$

   and there is a θ'' such that
   - $\theta'' \sqsupseteq \theta'$,
   - $(S', m') \triangleright \theta''$,
   - $(e', \theta'', m') \in \lceil (\mathsf{ref}\ \tau)^p \rceil^{pc}_E$.

   It suffices to show
   - $\forall p.\mathsf{pol}(\omega) = p \to pc \sqsubseteq p$. We already know that.
   - $\theta'' \sqsupseteq \theta'$. We already know that
   - $(S', m') \triangleright \theta''$. We already know that.
   - $(!e', \theta'', m') \in \lceil \tau' \rceil^{pc}_E$. We get this by induction.
2. $(e, \theta, m) \in \lceil (\mathsf{ref}\ \tau)^p \rceil^{pc}_{E_\nu}$. In this case $(e, \theta, m) \in \lceil (\mathsf{ref}\ \tau)^p \rceil_{\mathcal{V}}$. So there is a value v such that $v = e$ and $(v, \theta, m) \in \lceil \mathsf{ref}\ \tau \rceil_{\mathcal{V}}$. In particular this means that there is a location l such that $v = l$ and $\theta(l) = \tau$. Hence the reduction must have happened with **EDerefBeta**. This means that there there are v' and q such that

- $l \rightarrowtail (v', \tau'') \in S$
- $S = S$,
- $e_\beta = v'$,
- $\omega = \epsilon$ and
- $\Sigma' = \Sigma$.

So the reduction is really

- $!l, \Sigma, S \succ v', S, \epsilon, \Sigma$.

It suffices to show

- $\forall p.\mathtt{pol}(\epsilon) = p \to pc \sqsubseteq p$. As the policy of ϵ is undefined, no such policy exists. Hence there is nothing to show.
- $\theta' \sqsupseteq \theta'$. We get this by Lemma 6.2.
- $(S, m') \triangleright \theta'$. We already know this.
- $(v', \theta, m') \in \lceil \tau' \rceil^{pc}_E$.
  From $(S, m') \triangleright \theta'$ we get $(S(l), \theta', m') \in \lceil \theta'(l) \rceil v$. Because $\theta' \sqsupseteq \theta$ we have $\theta'(l) = \tau$. Because $l \rightarrowtail (v', q) \in S$ we have $S(l) = v'$. Hence $(v', \theta', m') \in \tau$. We get the claim by Lemma 8.6.

□

Lemma 8.18. If $(e_1, \theta, m) \in \lceil (\mathsf{ref}\ \tau')^p \rceil^{pc}_E$, $(e_2, \theta, m) \in \lceil \tau \rceil^{pc}_E$, $\tau(\Sigma) <: \tau'$ and $pc \sqsubseteq \tau'$, then $(e_1 := e_2, \theta, m) \in \lceil \mathsf{unit}^\perp \rceil^{pc}_E$.

Proof. By induction on m. It suffices to show $(e_1 := e_2, \theta, m) \in \lceil \mathtt{unit}^\perp \rceil^{pc}_{E_\beta}$. It is clear that $e_1 := e_2$ is not a value. So let S, θ', m' such that

- $\theta' \sqsupseteq \theta$,
- $(S, m') \triangleright \theta'$ and
- $m' < m$.

Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

- $e_1 := e_2, \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

There are two cases:

1. $(e_1, \theta, m) \in \lceil (\mathtt{ref}\ \tau')^p \rceil^{pc}_{E_\beta}$. In this case e_1 is not a value. Hence the reduction must have happened with **Eassignl**. Hence we know there is a e_1' such that

   - $e_1, \Sigma, S \succ e_1', S', \omega, \Sigma'$ and
   - $e_\beta = e_1' := e_2$.

   Because $(e_1, \theta, m) \in \lceil (\mathtt{ref}\ \tau')^p \rceil^{pc}_{E_\beta}$ we know

   - $\forall p.\mathtt{pol}(\omega) = p \to pc \sqsubseteq p$

   and there is a θ'' such that

   - $\theta'' \sqsupseteq \theta'$,
   - $(S', m') \triangleright \theta''$,
   - $(e_1', \theta'', m') \in \lceil (\mathtt{ref}\ \tau')^p \rceil^{pc}_E$.

   It suffices to show

   - $\forall p.\mathtt{pol}(\omega) = p \to pc \sqsubseteq p$. We already know that.
   - $\theta'' \sqsupseteq \theta'$. We already know that
   - $(S', m') \triangleright \theta''$. We already know that.

- $(e_1' := e_2, \theta'', m') \in \lceil \mathtt{unit}^{\perp} \rceil^{pc}_{E}$. By Lemma 6.2 we have $\theta'' \sqsupseteq \theta$. Hence we get $(e_2, \theta'', m') \in \lceil \tau \rceil^{pc}_{E}$ by Lemma 8.5 . The claim follows by induction.

2. $(e_1, \theta, m) \in \lceil (\mathtt{ref}\ \tau')^p \rceil^{pc}_{E_\nu}$. In this case there is a value ν_1 such that $e_1 = \nu_1$ and $(\nu_1, \theta, m) \in \lceil (\mathtt{ref}\ \tau')^p \rceil_\nu$. In this case $(\nu_1, \theta, m) \in \lceil \mathtt{ref}\ \tau' \rceil_\nu$. Hence ν_1 has the form l and $\theta(l) = \tau'$. There are two further cases:

   (a) $(e_2, \theta, m) \in \lceil \tau \rceil^{pc}_{E_\beta}$. By assumption e_2 is not a value. Hence the reduction must have happened with **Eassignr**. Hence we know there is a e_2' such that

   - $e_2, \Sigma, S \succ e_2', S', \omega, \Sigma'$ and
   - $e_\beta = l := e_2'$.

   Because $(e_2, \theta, m) \in \lceil \tau \rceil^{pc}_{E_\beta}$

   - $\forall p. pol(\omega) = p \to pc \sqsubseteq p$

   and there is a θ'' such that

   - $\theta'' \sqsupseteq \theta'$,
   - $(S', m') \triangleright \theta''$,
   - $(e_2', \theta'', m') \in \lceil \tau \rceil^{pc}_{E}$.

   It suffices to show

   - $\forall p. pol(\omega) = p \to pc \sqsubseteq p$. We already know that.
   - $\theta'' \sqsupseteq \theta'$. We already know that
   - $(S', m') \triangleright \theta''$. We already know that.
   - $(l := e_2', \theta'', m') \in \lceil \mathtt{unit}^{\perp} \rceil^{pc}_{E}$. By Lemma 6.2 we have $\theta'' \sqsupseteq \theta$. Hence we get $(l, \theta'', m') \in \lceil (\mathtt{ref}\ \tau')^p \rceil^{pc}_{E}$ by Lemma 8.5 . The claim follows by induction.

   (b) $(e_2, \theta, m) \in \lceil \tau \rceil^{pc}_{E_\nu}$. Then there is a value ν_2 such that $e_2 = \nu_2$ and $(\nu_2, \theta, m) \in \lceil \tau \rceil_\nu$. By assumption ν_2 is a value. Hence the reduction must have happened with **Eassign**. Therefore

   - $l \in dom(S)$
   - $e_\beta = ()$
   - $S' = S[l \rightarrowtail (\nu_2, \tau'')]$
   - $\Sigma' = \Sigma$
   - $\omega = l_{\tau''}(\nu_2)$
   - $\tau'' = type(S, l)$

   So the reduction is really

   - $l := \nu_2, \Sigma, S \succ (), S[l \rightarrowtail (\nu_2, \tau'')], l_{\tau''}(\nu), \Sigma$.

   We know $\theta' \sqsupseteq \theta$ and $\theta(l) = \tau'$. Hence also $\theta'(l) = \tau'$. It suffices to show

   - $pc \sqsubseteq pol(\tau'')$. We know $(S, m') \triangleright \theta'$. In particular this means that $l \in dom(\theta')$. Because $\theta'(l) = \tau'$, this means $\tau' = \theta'(l) = type(S, l) = \tau''$. By assumption also $pc \sqsubseteq \tau'$. Hence $pc \sqsubseteq pol(\tau'')$.
   - $\theta' \sqsupseteq \theta'$. We get this by Lemma 6.2.
   - $(S[l \rightarrowtail (\nu_2, \tau'')], m') \triangleright \theta'$. We have to show
     - $dom(\theta') \subseteq dom(S[l \rightarrowtail (\nu_2, \tau'')])$.

       $$dom(\theta') \overset{(S, m') \triangleright \theta'}{\subseteq} dom(S) \subseteq dom(S[l \rightarrowtail (\nu_2, \tau'')])$$

     - $\forall l' \in dom(\theta').(S[l \rightarrowtail (\nu_2, \tau'')](l'), \theta', m') \in \lceil \theta'(l') \rceil_\nu$. Let $l' \in dom(\theta')$. There are two cases
       i. $l' \neq l$. Because $(S, m') \triangleright \theta'$, this gives us $(S(l'), \theta', m') \in \lceil \theta'(l') \rceil_\nu$. Because $l' \neq l$, this is equivalent to $(S[l \rightarrowtail (\nu_2, \tau'')](l'), \theta', m') \in \lceil \theta'(l') \rceil_\nu$.
       ii. $l' = l$. In this case we have to show $(\nu_2, \theta', m') \in \lceil \tau' \rceil_\nu$. By Lemma 8.6 it suffices to show $(\nu_2, \theta', m') \in \lceil \tau(\Sigma) \rceil_\nu$. τ must have the form B^r for some type B and policy r. We already know $(\nu_2, \theta, m) \in \lceil \tau \rceil_\nu$. Hence $(\nu_2, \theta, m) \in \lceil B \rceil_\nu$. $(\nu, \theta, m) \in \lceil B^{r(\Sigma)} \rceil_\nu$ follows directly from the definition. We get the goal by Lemma 8.4.

– $\forall l' \in \mathrm{dom}(\theta').\theta'(l') = \mathrm{type}(S[l \rightarrowtail (v_2, \tau'')], l')$. By assumption $\tau'' = \mathrm{type}(S, l)$. Hence

$$\mathrm{type}(S[l \rightarrowtail (v_2, q)], l') = \mathrm{type}(S[l \rightarrowtail (v_2, \mathrm{type}(S, l))], l') = \mathrm{type}(S, l')$$

Hence the goal follows from $(S, m') \triangleright \theta'$.

- $((), \theta', m') \in \lceil \mathtt{unit}^{\perp} \rceil_E^{pc}$. It suffices to show $((), \theta', m') \in \lceil \mathtt{unit} \rceil_v$. This is trivially true.

□

Lemma 8.19. If $(e_1, \theta, m) \in \lceil \tau \rceil_E^{pc \sqcup pol(\sigma)}$ and $(e_2, \theta, m) \in \lceil \tau \rceil_E^{pc \sqcup pol(\sigma)}$, then $(\mathtt{when}\ \sigma\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2, \theta, m) \in \lceil \tau \rceil_E^{pc}$.

Proof. By induction on m. It suffices to show $(\mathtt{when}\ \sigma\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2, \theta, m) \in \lceil pc \rceil_{E_\beta}^{\tau}$. It is clear that $\mathtt{when}\ \sigma\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2$ is not a value.
So let S, θ', m' such that

- $\theta' \sqsupseteq \theta$,
- $(S, m') \triangleright \theta'$,
- $m' < m$

and $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

- $\mathtt{when}\ \sigma\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2, \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

We do case analysis on the derivation of the reduction:

1. The derivation happened with **EWhenOpen**. In this case e_1 is not a value and there is an e_1' such that

   - $\sigma \in \Sigma$,
   - $e_1, \Sigma, S \succ e_1', S', \omega, \Sigma'$,
   - $e_\beta = \mathtt{when}\ \sigma\ \mathtt{then}\ e_1'\ \mathtt{else}\ e_2$

   So the reduction is really

   - $\mathtt{when}\ \sigma\ \mathtt{then}\ e_1\ \mathtt{else}\ e_2, \Sigma, S \succ \mathtt{when}\ \sigma\ \mathtt{then}\ e_1'\ \mathtt{else}\ e_2, S', \omega, \Sigma'$.

   Because $(e_1, \theta, m) \in \lceil \tau \rceil_E^{pc \sqcup pol(\sigma)}$ and because e_1 is not a value we must have $(e_1, \theta, m) \in \lceil \tau \rceil_{E_\beta}^{pc \sqcup pol(\sigma)}$. Hence we have

   - $\forall p.(pol(\omega) = p) \rightarrow pc \sqcup pol(\sigma) \sqsubseteq p$.

   and there is a θ'' such that

   - $\theta'' \sqsupseteq \theta'$,
   - $(S', m') \triangleright \theta''$ and
   - $(e_1', \theta'', m') \in \lceil \tau \rceil_E^{pc \sqcup pol(\sigma)}$.

   It suffices to show

   - $\forall p.(pol(\omega) = p) \rightarrow pc \sqsubseteq p$. Let p such that $pol(\omega) = p$. In this case we know $pc \sqcup pol(\sigma) \sqsubseteq p$. We get $pc \sqsubseteq p$ by Lemma 4.13.
   - $\theta'' \sqsupseteq \theta'$. We already know that.
   - $(S', m') \triangleright \theta''$. We already know that.
   - $(\mathtt{when}\ \sigma\ \mathtt{then}\ e_1'\ \mathtt{else}\ e_2, \theta'', m') \in \lceil \tau \rceil_E^{pc}$. By induction it suffices to show
     – $(e_1', \theta'', m') \in \lceil \tau \rceil_E^{pc \sqcup pol(\sigma)}$. We already know this.
     – $(e_2, \theta'', m') \in \lceil \tau \rceil_E^{pc \sqcup pol(\sigma)}$. By transitivity (Lemma 6.2) we have $\theta'' \sqsupseteq \theta$. We get the goal by Lemma 8.5 from $(e_2, \theta, m) \in \lceil \tau \rceil_E^{pc \sqcup pol(\sigma)}$.

2. The derivation happened with **EWhenClosed**. In this case e_2 is not a value and there is an e_2' such that

- $\sigma \notin \Sigma$,
- $e_2, \Sigma, S \succ e_2', S', \omega, \Sigma'$,
- $e_\beta = \mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2'$

So the reduction is really

- $\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2, \Sigma, S \succ \mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2', S', \omega, \Sigma'$.

Because $(e_2, \theta, m) \in \lceil\tau\rceil_E^{pc \sqcup pol(\sigma)}$ and because e_2 is not a value we must have $(e_2, \theta, m) \in \lceil\tau\rceil_{E_\beta}^{pc \sqcup pol(\sigma)}$. Hence we have

- $\forall p.(pol(\omega) = p) \to pc \sqcup pol(\sigma) \sqsubseteq p$.

and there is a θ'' such that

- $\theta'' \sqsupseteq \theta'$,
- $(S', m') \triangleright \theta''$ and
- $(e_2', \theta'', m') \in \lceil\tau\rceil_E^{pc \sqcup pol(\sigma)}$.

It suffices to show

- $\forall p.(pol(\omega) = p) \to pc \sqsubseteq p$. Let p such that $pol(\omega) = p$. In this case we know $pc \sqcup pol(\sigma) \sqsubseteq p$. We get $pc \sqsubseteq p$ by Lemma 4.13.
- $\theta'' \sqsupseteq \theta'$. We already know that.
- $(S', m') \triangleright \theta''$. We already know that.
- $(\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2', \theta'', m') \in \lceil\tau\rceil_E^{pc}$. By induction it suffices to show
  - $(e_1, \theta'', m') \in \lceil\tau\rceil_E^{pc \sqcup pol(\sigma)}$. By transitivity (Lemma 6.2) we have $\theta'' \sqsupseteq \theta$. We get the goal by Lemma 8.5 from $(e_1, \theta, m) \in \lceil\tau\rceil_E^{pc \sqcup pol(\sigma)}$.
  - $(e_2', \theta'', m') \in \lceil\tau\rceil_E^{pc \sqcup pol(\sigma)}$. We already know this.

3. The derivation happened with **EWhenOpenBeta**. In this case e_1 is a value v_1 and

   - $\sigma \in \Sigma$,
   - $e_\beta = v_1$,
   - $S' = S$,
   - $\Sigma' = \Sigma$,
   - $\omega = \epsilon$

   So the reduction is really

   - $\mathit{when}\ \sigma\ \mathit{then}\ v_1\ \mathit{else}\ e_2, \Sigma, S \succ v_1, S, \epsilon, \Sigma$.

   It suffices to show

   - $\forall p.(pol(\epsilon) = p) \to pc \sqsubseteq p$. There is no p such that $pol(\epsilon) = p$. So the statement is trivially true.
   - $\theta' \sqsupseteq \theta'$. We get this by Lemma 6.2.
   - $(S, m') \triangleright \theta'$. We already know that.
   - $(v_1, \theta', m') \in \lceil\tau\rceil_E^{pc}$. We already know $(v_1, \theta, m) \in \lceil\tau\rceil_E^{pc \sqcup pol(\sigma)}$. By Lemma 4.6 $pc \sqsubseteq pc \sqcup pol(\sigma)$. Hence we get the goal by Lemma 8.5.

4. The derivation happened with **EWhenClosedBeta**. In this case e_2 is a value v_2 and

   - $\sigma \notin \Sigma$,
   - $e_\beta = v_2$,
   - $S' = S$,
   - $\Sigma' = \Sigma$,
   - $\omega = \epsilon$

So the reduction is really

- $\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ v_2, \Sigma, S \succ v_2, S, \epsilon, \Sigma$.

It suffices to show

- $\forall p.(\mathtt{pol}(\epsilon) = p) \to pc \sqsubseteq p$. There is no p such that $\mathtt{pol}(\epsilon) = p$. So the statement is trivially true.
- $\theta' \sqsupseteq \theta'$. We get this by Lemma 6.2.
- $(S, m') \triangleright \theta'$. We already know that.
- $(v_2, \theta', m') \in \lceil\tau\rceil_E^{pc}$. We already know $(v_2, \theta, m) \in \lceil\tau\rceil_E^{pc \sqcup \mathtt{pol}(\sigma)}$. By Lemma 4.6 $pc \sqsubseteq pc \sqcup \mathtt{pol}(\sigma)$. Hence we get the goal by Lemma 8.5.

□

Lemma 8.20. If $(e, \theta, m) \in [\![\tau]\!]_E^{\mathcal{A}}$ and $pc \sqsubseteq \mathrm{pol}(\sigma)$, then $(e\ \mathsf{then\ unclose}\ \sigma, \theta, m) \in \lceil\tau\rceil_E^{pc}$.

Proof. By induction on m. It suffices to show $(\mathtt{closed}\ \sigma\ \mathtt{in}\ e, \theta, m) \in \lceil\tau\rceil_{E_\beta}^{pc}$. It is clear that $\mathtt{closed}\ \sigma\ \mathtt{in}\ e$ is not a value. So let S, θ', m' such that

- $\theta' \sqsupseteq \theta$,
- $(S, m') \triangleright \theta'$ and
- $m' < m$.

Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

- $\mathtt{closed}\ \sigma\ \mathtt{in}\ e, \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

There are two cases:

1. $(e, \theta, m) \in \lceil\tau\rceil_{E_\beta}^{pc}$ In this case e is not a value. Hence the reduction must have happened with **Eclosed**. Hence we know there is a e' such that

   - $e, \Sigma\backslash\{\sigma\}, S \succ e', S', \omega, \Sigma'$ and
   - $e_\beta = \mathtt{closed}\ \sigma\ \mathtt{in}\ e'$.

   Because $(e, \theta, m) \in \lceil\tau\rceil_{E_\beta}^{pc}$ we have

   - $\forall p.\mathtt{pol}(\omega) = p \to pc \sqsubseteq p$

   and there is a θ'' such that

   - $\theta'' \sqsupseteq \theta'$,
   - $(S', m') \triangleright \theta''$,
   - $(e', \theta'', m') \in \lceil\tau\rceil_E^{pc}$.

   It suffices to show

   - $\forall p.\mathtt{pol}(\omega) = p \to pc \sqsubseteq p$. We already know that.
   - $\theta'' \sqsupseteq \theta'$. We already know that
   - $(S', m') \triangleright \theta''$. We already know that.
   - $(\mathtt{closed}\ \sigma\ \mathtt{in}\ e', \theta'', m') \in \lceil\tau\rceil_E^{pc}$. We get this by induction.

2. $(e, \theta, m) \in \lceil\tau\rceil_{E_v}^{pc}$. In this case $(e, \theta, m) \in \lceil\tau\rceil_v$. So there is a value v such that $v = e$. Because v is a value, the reduction must have happened with **EclosedBeta**. Hence we know that

   - $S' = S$,
   - $e_\beta = v$,
   - $\omega = \mathtt{unclose}(\sigma)$ and
   - $\Sigma' = \Sigma$.

So the reduction is really

- $\mathtt{closed}\ \sigma\ \mathtt{in}\ v, \Sigma, S \succ v, S, \mathtt{unclose}(\sigma), \Sigma$.

It suffices to show

- $\mathtt{pc} \sqsubseteq \mathtt{pol}(\sigma)$. This is one of our assumptions.
- $\theta' \sqsupseteq \theta'$. We have this by Lemma 6.2.
- $(S, m') \triangleright \theta'$. We already know that.
- $(v, \theta', m') \in \lceil \tau \rceil^{pc}_{E}$. We get this by Lemma 8.5.

□

Lemma 8.21. If $(e, \theta, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$ and $pc \sqsubseteq pol(\sigma)$, then $(\mathsf{close}\ \sigma\ \mathsf{in}\ e, \theta, m) \in \lceil \tau \rceil^{pc}_{E}$.

Proof. By induction on m. It suffices to show $(\mathtt{close}\ \sigma\ \mathtt{in}\ e, \theta, m) \in \lceil \tau \rceil^{pc}_{E_\beta}$. It is clear that $\mathtt{close}\ \sigma\ \mathtt{in}\ e$ is not a value. So let S, θ', m' such that

- $\theta' \sqsupseteq \theta$,
- $(S, m') \triangleright \theta'$ and
- $m' < m$.

Also let $e_\beta, S', \omega, \Sigma, \Sigma'$ such that

- $\mathtt{close}\ \sigma\ \mathtt{in}\ e, \Sigma, S \succ e_\beta, S', \omega, \Sigma'$.

The reduction must have happened with **Eclose**. Hence we know

- $S' = S$,
- $e_\beta = \mathtt{closed}\ \sigma\ \mathtt{in}\ e$,
- $\Sigma' = \Sigma$, and
- $\omega = \mathtt{close}(\sigma)$.

So the reduction is really

- $\mathtt{close}\ \sigma\ \mathtt{in}\ e, \Sigma, S \succ \mathtt{closed}\ \sigma\ \mathtt{in}\ e, S, \mathtt{close}(\sigma), \Sigma$.

It suffices to show

- $\mathtt{pc} \sqsubseteq \mathtt{pol}(\sigma)$. We already know that.
- $\theta' \sqsupseteq \theta'$. We already know that
- $(S, m') \triangleright \theta'$. We already know that.
- $(\mathtt{closed}\ \sigma\ \mathtt{in}\ e, \theta', m') \in \lceil \tau \rceil^{pc}_{E}$. We get $(e, \theta', m') \in \lceil \tau \rceil^{pc}_{E}$ by Lemma 8.5. The goal follows by Lemma 8.20.

□

Theorem 8.1 (Unary Fundamental Lemma)**.**
If $\Gamma; \Sigma; \theta \vdash_{pc} \bar{e} : \tau$ and $\theta' \sqsupseteq \theta$ and $(\delta, \theta', m) \in \lceil \Gamma \rceil_{\mathcal{V}}$, then $(\delta(\bar{e}), \theta', m) \in \lceil \tau \rceil^{pc}_{E}$.

Proof. By induction on $\Gamma; \Sigma; \theta \vdash_{pc} e : \tau$.

- **var:**

$$\frac{}{\Gamma', x : \tau, \Gamma''; \Sigma; \theta \vdash_{pc} x : \tau}\ \textbf{var}$$

In this case $\bar{e} = x$ and $\Gamma = \Gamma', x : \tau, \Gamma''$. We have to show $(\delta(x), \theta', m) \in \lceil \tau \rceil^{pc}_{E}$. By assumption $(\delta, \theta', m) \in \lceil \Gamma', x : \tau, \Gamma'' \rceil_{\mathcal{V}}$. Therefore since $x \in \mathrm{dom}(\Gamma', x : \tau, \Gamma'')$ we have $(\delta(x), \theta', m) \in \lceil \tau \rceil_{\mathcal{V}}$. The goal follows directly from the construction of $\lceil \tau \rceil^{pc}_{E}$.

- **nat:**

$$\frac{n \in \mathbb{N}}{\Gamma; \Sigma; \theta \vdash_{pc} n : \mathcal{N}^{\perp}} \textbf{ nat}$$

In this case $\bar{e} = n$. We have to show $(\delta(n), \theta', m) \in \lceil \mathcal{N}^{\perp} \rceil^{pc}_{E}$. It suffices to show $(n, \theta', m) \in \lceil \mathcal{N} \rceil_{\mathcal{V}}$. This is trivially true.

- **open:**

$$\frac{\Gamma; \Sigma \cup \{\sigma\}; \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq pol(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} \mathsf{open}\ \sigma\ \mathsf{in}\ e : \tau} \textbf{ open}$$

In this case $\bar{e} = \mathsf{open}(\sigma)\ \mathsf{in}\ e$. We have to show $(\delta(\mathsf{open}(\sigma)\ \mathsf{in}\ e), \theta', m) \in \lceil \tau \rceil^{pc}_{E}$ which is equivalent to showing $(\mathsf{open}(\sigma)\ \mathsf{in}\ \delta(e), \theta', m) \in \lceil \tau \rceil^{pc}_{E}$. By induction $(\delta(e), \theta', m) \in \lceil \tau \rceil^{pc}_{E}$.
Hence by Lemma 8.8 $(\mathsf{open}(\sigma)\ \mathsf{in}\ \delta(e), \theta', m) \in \lceil \tau \rceil^{pc}_{E}$.

- **opened:**

$$\frac{\Gamma; \Sigma \cup \{\sigma\}; \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq pol(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} e\ \mathsf{then\ unopen}\ \sigma : \tau} \textbf{ opened}$$

In this case $\bar{e} = \mathsf{opened}(\sigma)\ \mathsf{in}\ e$. We have to show $(\delta(\mathsf{opened}(\sigma)\ \mathsf{in}\ e), \theta', m) \in \lceil \tau \rceil^{pc}_{E}$ which is equivalent to showing $(\mathsf{opened}(\sigma)\ \mathsf{in}\ \delta(e), \theta', m) \in \lceil \tau \rceil^{pc}_{E}$. By induction $(\delta(e), \theta', m) \in \lceil \tau \rceil^{pc}_{E}$.
Hence by Lemma 8.7 $(\mathsf{opened}(\sigma)\ \mathsf{in}\ \delta(e), \theta', m) \in \lceil \tau \rceil^{pc}_{E}$.

- **λ:**

$$\frac{\Gamma, x : \tau_1; \Sigma'; \theta \vdash_{pc'} e : \tau_2}{\Gamma; \Sigma; \theta \vdash_{pc} \lambda x.e : (\tau_1 \xrightarrow{\Sigma', pc'} \tau_2)^{\perp}} \lambda$$

In this case $\bar{e} = \lambda x.e$ and $\tau = (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^{\perp}$. We have to show $(\delta(\lambda x.e), \theta', m) \in \lceil (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^{\perp} \rceil^{pc}_{E}$. It suffices to show $(\lambda x.\delta(e), \theta', m) \in \lceil \tau_1 \xrightarrow{\Sigma', p_e} \tau_2 \rceil_{\mathcal{V}}$ (remember we assume that x is distinct from the variables replaced by δ). So let θ'', m' such that

- $\theta'' \sqsupseteq \theta'$,
- $m' < m$ and
- $(v, \theta'', m') \in \lceil \tau_1 \rceil_{\mathcal{V}}$.

. We have to show $([v/x]\delta(e), \theta'', m') \in \lceil \tau_2 \rceil^{p_e}_{E}$. Because we assume that x is distinct from all free variables, in particular those in the codomain of δ by Lemma 7.1 it suffices to show $(\delta \cup \{(x, v)\}(e), \theta'', m') \in \lceil \tau_2 \rceil^{p_e}_{E}$. By Lemma 8.23 $(\delta, \theta'', m') \in \lceil \Gamma \rceil_{\mathcal{V}}$. Hence by Lemma 8.1 $(\delta \cup \{(x, v)\}, \theta'', m') \in \lceil \Gamma, x : \tau_1 \rceil_{\mathcal{V}}$. By Lemma 6.2 $\theta'' \sqsupseteq \theta$. Hence by induction $(\delta \cup \{(x, v)\}(e), \theta'', m') \in \lceil \tau_2 \rceil^{p_e}_{E}$.

- **prod:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e_1 : \tau_1 \qquad \Gamma; \Sigma; \theta \vdash_{pc} e_2 : \tau_2}{\Gamma; \Sigma; \theta \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^{\perp}} \textbf{ prod}$$

In this case $\bar{e} = (e_1, e_2)$. We have to show $(\delta((e_1, e_2)), \theta', m) \in \lceil (\tau_1 \times \tau_2)^{\perp} \rceil^{pc}_{E}$ which is equivalent to showing $((\delta(e_1), \delta(e_2)), \theta', m) \in \lceil (\tau_1 \times \tau_2)^{\perp} \rceil^{pc}_{E}$. By induction $(\delta(e_1), \theta', m) \in \lceil \tau_1 \rceil^{pc}_{E}$ and $(\delta(e_2), \theta', m) \in \lceil \tau_2 \rceil^{pc}_{E}$.
Hence by Lemma 8.9 $((\delta(e_1), \delta(e_2)), \theta', m) \in \lceil (\tau_1 \times \tau_2)^{\perp} \rceil^{pc}_{E}$.

- **app**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\Sigma', pc'} \tau_2)^{p} \qquad \Gamma; \Sigma; \theta \vdash_{pc} e_2 : \tau_1' \qquad p \sqsubseteq \tau_2 \qquad pc \sqcup p \sqsubseteq pc' \qquad \tau_1' <: \tau_1 \qquad \Sigma \supseteq \Sigma'}{\Gamma; \Sigma; \theta \vdash_{pc} e_1\ e_2 : \tau_2} \textbf{ app}$$

In this case $\bar{e} = e_1\ e_2$. We have to show $(\delta(e_1\ e_2), \theta', m) \in \lceil \tau_2 \rceil^{pc}_{E}$ which is equivalent to showing $((\delta(e_1)\ \delta(e_2)), \theta', m) \in \lceil \tau_2 \rceil^{pc}_{E}$. By induction $(\delta(e_1), \theta', m) \in \lceil (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^{p} \rceil^{pc}_{E}$ and $(\delta(e_2), \theta', m) \in \lceil \tau_1 \rceil^{pc}_{E}$.
By Lemma 4.13 $pc \sqsubseteq p_e$. Hence by Lemma 8.10 $(\delta(e_1)\ \delta(e_2), \theta', m) \in \lceil \tau_2 \rceil^{pc}_{E}$.

- **fst**

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e : (\tau_1 \times \tau_2)^p \qquad p \sqsubseteq \tau_1}{\Gamma;\Sigma;\theta \vdash_{pc} \mathsf{fst}\,(e) : \tau_1}\ \textbf{fst}$$

  In this case $\bar{e} = \mathtt{fst}(e)$. We have to show $(\delta(\mathtt{fst}(e)), \theta', m) \in \lceil \tau_1 \rceil^{pc}_E$ which is equivalent to showing $(\mathtt{fst}(\delta(e)), \theta', m) \in \lceil \tau_1 \rceil^{pc}_E$. By induction $(\delta(e), \theta', m) \in \lceil (\tau_1 \times \tau_2)^p \rceil^{pc}_E$.
  Hence by Lemma 8.11 $(\mathtt{fst}(\delta(e)), \theta', m) \in \lceil \tau_1 \rceil^{pc}_E$.

- **snd** Analogous to the case for **fst**.

- **inl:**

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e : \tau_1}{\Gamma;\Sigma;\theta \vdash_{pc} \mathsf{inl}\,(e) : (\tau_1 + \tau_2)^\perp}\ \textbf{inl}$$

  In this case $\bar{e} = \mathtt{inl}\ e$. We have to show $(\delta(\mathtt{inl}(e)), \theta', m) \in \lceil (\tau_1 + \tau_2)^\perp \rceil^{pc}_E$ which is equivalent to showing $(\mathtt{inl}(\delta(e)), \theta', m) \in \lceil (\tau_1 + \tau_2)^\perp \rceil^{pc}_E$. By induction $(\delta(e), \theta', m) \in \lceil \tau_1 \rceil^{pc}_E$.
  Hence by Lemma 8.13 $(\mathtt{inl}(\delta(e)), \theta', m) \in \lceil (\tau_1 + \tau_2)^\perp \rceil^{pc}_E$.

- **inr:** Analogous to the case for **inr**.

- **case:**

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e : (\tau_1 + \tau_2)^p \qquad p \sqsubseteq \tau \qquad \Gamma, x : \tau_1';\Sigma;\theta \vdash_{pc \sqcup p} e_1 : \tau \qquad \Gamma, y : \tau_2';\Sigma;\theta \vdash_{pc \sqcup p} e_2 : \tau \qquad \tau_1 <: \tau_1' \qquad \tau_2 <: \tau_2'}{\Gamma;\Sigma;\theta \vdash_{pc} \mathsf{case}\ e\ \mathsf{of}\ |\,\mathsf{inl}\,(x) \Rightarrow e_1\ |\,\mathsf{inr}\,(y) \Rightarrow e_2 : \tau}\ \textbf{case}$$

  In this case $\bar{e} = \mathtt{case}(e, x.e_1, y.e_2)$. We have to show $(\delta(\mathtt{case}(e, x.e_1, y.e_2)), \theta', m) \in \lceil \tau \rceil^{pc}_E$. By our assumptions about variables $x \notin \mathtt{dom}(\delta)$ and $y \notin \mathtt{dom}(\delta)$. Hence this is equivalent to showing $(\mathtt{case}(\delta(e), x.\delta(e_1), y.\delta(e_2))), \theta', m) \in \lceil \tau \rceil^{pc}_E$. We get the goal by Lemma 8.15 if we can show

  - $(\delta(e), \theta', m) \in \lceil (\tau_1 + \tau_2)^\perp \rceil^{pc}_E$. We get this by induction.
  - $\forall \theta'', m'.\theta'' \sqsupseteq \theta' \wedge m' < m \to \forall v.(v, \theta'', m') \in \lceil \tau_1 \rceil_{\mathcal{V}} \to ([v/x]\delta(e_1), \theta'', m') \in \lceil \tau \rceil^{pc \sqcup p}_E$. Let θ'', m' such that $\theta'' \sqsupseteq \theta'$, $m' < m$ and let v such that $(v, \theta'', m') \in \lceil \tau_1 \rceil_{\mathcal{V}}$. By Lemma 7.1 it suffices to show $(\delta \cup \{x, v\}(e_1), \theta'', m') \in \lceil \tau \rceil_{\mathcal{V}}$. We get this by induction if we can show
    - $\theta'' \sqsupseteq \theta$. We get this by transitivity (Lemma 6.2).
    - $(\delta \cup \{x, v\}, \theta'', m') \in \lceil \Gamma, x : \tau_1' \rceil_{\mathcal{V}}$. By Lemma 8.1 this is the case if
      - $(\delta, \theta'', m') \in \lceil \Gamma \rceil_{\mathcal{V}}$. We get this by Lemma 8.23.
      - $(v, \theta'', m') \in \lceil \tau_1' \rceil_{\mathcal{V}}$. We get this by Lemma 8.6.
  - $\forall \theta'', m'.\theta'' \sqsupseteq \theta' \wedge m' < m \to \forall v.(v, \theta'', m') \in \lceil \tau_2 \rceil_{\mathcal{V}} \to ([v/y]\delta(e_2), \theta'', m') \in \lceil \tau \rceil^{pc \sqcup p}_E$. Let θ'', m' such that $\theta'' \sqsupseteq \theta'$, $m' < m$ and let v such that $(v, \theta'', m') \in \lceil \tau_2 \rceil_{\mathcal{V}}$. By Lemma 7.1 it suffices to show $(\delta \cup \{y, v\}(e_2), \theta'', m') \in \lceil \tau \rceil_{\mathcal{V}}$. We get this by induction if we can show
    - $\theta'' \sqsupseteq \theta$. We get this by transitivity (Lemma 6.2).
    - $(\delta \cup \{y, v\}, \theta'', m') \in \lceil \Gamma, x : \tau_2' \rceil_{\mathcal{V}}$. By Lemma 8.1 this is the case if
      - $(\delta, \theta'', m') \in \lceil \Gamma \rceil_{\mathcal{V}}$. We get this by Lemma 8.23.
      - $(v, \theta'', m') \in \lceil \tau_2' \rceil_{\mathcal{V}}$. We get this by Lemma 8.6.

- **new:**

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e : \tau' \qquad pc \sqsubseteq \tau \qquad \tau'(\Sigma) <: \tau}{\Gamma;\Sigma;\theta \vdash_{pc} \mathsf{new}\,(e, \tau) : (\mathsf{ref}\ \tau)^\perp}\ \textbf{new}$$

  In this case $\bar{e} = \mathtt{new}(e, \tau)$. We have to show $(\delta(\mathtt{new}(e, \tau)), \theta', m) \in \lceil (\mathtt{ref}\ \tau)^\perp \rceil^{pc}_E$. This is equivalent to showing $(\mathtt{new}(\delta(e), \tau), \theta', m) \in \lceil (\mathtt{ref}\ \tau)^\perp \rceil^{pc}_E$. τ and τ' must have the forms A^p and B^q. By inversion of $\tau'(\Sigma) <: \tau$ with **sub-policy** we get $B <: A$. Because $pc \sqsubseteq \tau$ we get $pc \sqsubseteq p$. We get $(\delta(e), \theta', m) \in \lceil B^q \rceil^{pc}_E$ by induction. The goal follows by Lemma 8.16.

- **loc**: We have to show $(\delta(l), \theta', m) \in \lceil (\mathtt{ref}\ \tau)^\perp \rceil^{pc}_E$. It suffices to show $(l, \theta', m) \in \lceil \mathtt{ref}\ \tau \rceil^{pc}_E$. We have this by the definition of $\lceil \mathtt{ref}\ \tau \rceil^{pc}_E$ because $pc \sqsubseteq \tau$.

- **sub:**

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc'} e : \tau' \qquad pc \sqsubseteq pc' \qquad \tau' <: \tau}{\Gamma;\Sigma;\theta \vdash_{pc} e : \tau}\ \textbf{sub}$$

  In this case $\bar{e} = e$. By induction we get $(e, \theta', m) \in \lceil \tau' \rceil^{pc'}_E$. We get the goal by Lemma 8.5 and Lemma 8.6.

- **deref:**

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e : (\text{ref } \tau)^p \qquad p \sqsubseteq \tau' \qquad \tau <: \tau'}{\Gamma;\Sigma;\theta \vdash_{pc} !\,e : \tau'}\ \textbf{deref}$$

In this case $\bar{e} = !e$. We have to show $(\delta(!e), \theta', m) \in \lceil \tau' \rceil_E^{pc}$ which is equivalent to showing $(!(\delta(e)), \theta', m) \in \lceil \tau' \rceil_E^{pc}$. By induction $(\delta(e), \theta', m) \in \lceil (\text{ref } \tau)^p \rceil_E^{pc}$.
Hence by Lemma 8.17 $(!(\delta(e)), \theta', m) \in \lceil \tau' \rceil_E^{pc}$.

- **assign:**

$$\frac{\Gamma;\Sigma;\theta \vdash_{pc} e : (\text{ref } \tau')^p \qquad \tau(\Sigma) <: \tau' \qquad \Gamma;\Sigma;\theta \vdash_{pc} e' : \tau \qquad pc \sqcup p \sqsubseteq \tau'}{\Gamma;\Sigma;\theta \vdash_{pc} e := e' : \text{unit}^\perp}\ \textbf{assign}$$

In this case $\bar{e} = e := e'$. We have to show $(\delta((e := e')), \theta', m) \in \lceil \text{unit}^\perp \rceil_E^{pc}$ which is equivalent to showing $(\delta(e) := \delta(e'), \theta', m) \in \lceil \text{unit}^\perp \rceil_E^{pc}$. By induction $(\delta(e), \theta', m) \in \lceil (\text{ref}\tau')^p \rceil_E^{pc}$ and $(\delta(e'), \theta', m) \in \lceil \tau \rceil_E^{pc}$.
We get $pc \sqsubseteq \tau'$ by Lemma 4.13. Hence we get $(\delta(e) := \delta(e'), \theta', m) \in \lceil \text{unit}^\perp \rceil_E^{pc}$ by Lemma 8.18.

- **unit:**

$$\frac{}{\Gamma;\Sigma;\theta \vdash_{pc} () : \text{unit}^\perp}\ \textbf{unit}$$

In this case $\bar{e} = ()$. We have to show $(\delta(()), \theta', m) \in \lceil \text{unit}^\perp \rceil_E^{pc}$. It suffices to show $((), \theta', m) \in \lceil \text{unit} \rceil_\nu$. This is trivially true.

- **close:**

$$\frac{\Gamma;\Sigma\backslash\{\sigma\};\theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq pol(\sigma)}{\Gamma;\Sigma;\theta \vdash_{pc} \text{close } \sigma \text{ in } e : \tau}\ \textbf{close}$$

In this case $\bar{e} = \text{close}(\sigma)\ \text{in}\ e$. We have to show $(\delta(\text{close}(\sigma)\ \text{in}\ e), \theta', m) \in \lceil \tau \rceil_E^{pc}$ which is equivalent to showing $(\text{close}(\sigma)\ \text{in}\ \delta(e), \theta', m) \in \lceil \tau \rceil_E^{pc}$. By induction $(\delta(e), \theta', m) \in \lceil \tau \rceil_E^{pc}$.
Hence by Lemma 8.21 $(\text{close}(\sigma)\ \text{in}\ \delta(e), \theta', m) \in \lceil \tau \rceil_E^{pc}$.

- **closed:**

$$\frac{\Gamma;\Sigma\backslash\{\sigma\};\theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq pol(\sigma)}{\Gamma;\Sigma;\theta \vdash_{pc} e \text{ then unclose } \sigma : \tau}\ \textbf{closed}$$

In this case $\bar{e} = \text{closed}(\sigma)\ \text{in}\ e$. We have to show $(\delta(\text{closed}(\sigma)\ \text{in}\ e), \theta', m) \in \lceil \tau \rceil_E^{pc}$ which is equivalent to showing $(\text{closed}(\sigma)\ \text{in}\ \delta(e), \theta', m) \in \lceil \tau \rceil_E^{pc}$. By induction $(\delta(e), \theta', m) \in \lceil \tau \rceil_E^{pc}$.
Hence by Lemma 8.20 $(\text{closed}(\sigma)\ \text{in}\ \delta(e), \theta', m) \in \lceil \tau \rceil_E^{pc}$.

- **when:**

$$\frac{\Gamma;\Sigma \cup \{\sigma\};\theta \vdash_{pc \sqcup pol(\sigma)} e_1 : \tau \qquad \Gamma;\Sigma;\theta \vdash_{pc \sqcup pol(\sigma)} e_2 : \tau \qquad pol(\sigma) \sqsubseteq \tau}{\Gamma;\Sigma;\theta \vdash_{pc} \text{when } \sigma \text{ then } e_1 \text{ else } e_2 : \tau}\ \textbf{when}$$

In this case $\bar{e} = \text{when}\ \sigma\ \text{then}\ e_1\ \text{else}\ e_2$. We have to show $(\delta(\text{when}\ \sigma\ \text{then}\ e_1\ \text{else}\ e_2), \theta', m) \in \lceil \tau \rceil_E^{pc}$ which is equivalent to showing $(\text{when}\ \sigma\ \text{then}\ \delta(e_1)\ \text{else}\ \delta(e_2), \theta', m) \in \lceil \tau \rceil_E^{pc}$.

By induction $(\delta(e_1), \theta', m) \in \lceil \tau \rceil_E^{pc \sqcup pol(\sigma)}$ and $(\delta(e_2), \theta', m) \in \lceil \tau \rceil_E^{pc \sqcup pol(\sigma)}$.
Hence by Lemma 8.19 $(\text{when}\ \sigma\ \text{then}\ \delta(e_1)\ \text{else}\ \delta(e_2), \theta', m) \in \lceil \tau \rceil_E^{pc}$.

□

8.3 Properties of the binary relation

Lemma 8.22. For all $v, v', \mathcal{A}, W, \tau, m$ if $(v, v', W, m) \in [\![\tau]\!]_{\mathcal{V}}^{\mathcal{A}}$, then $(v, W.\theta_1, m) \in \lceil \tau \rceil_\nu$ and $(v', W.\theta_2, m) \in \lceil \tau \rceil_\nu$ and for all $v, v', \mathcal{A}, W, A, m$ if $(v, v', W, m) \in [\![A]\!]_{\mathcal{V}}^{\mathcal{A}}$, then $(v, W.\theta_1, m) \in \lceil A \rceil_\nu$ and $(v', W.\theta_2, m) \in \lceil A \rceil_\nu$.

Proof. By mutual induction on the structure of τ and A.

- unit: Then v=v'=(). $((), W.\theta_1, m) \in \lceil \text{unit} \rceil_\nu$ and $((), W.\theta_2, m) \in \lceil \text{unit} \rceil_\nu$ by the definition of $\lceil \text{unit} \rceil_\nu$.

- $\mathbb{N}$: Then v=v'=n and $n \in \mathbb{N}$. $(n, W.\theta_1, m) \in \lceil \mathbb{N} \rceil_\nu$ and $(n, W.\theta_2, m) \in \lceil \mathbb{N} \rceil_\nu$ by the definition of $\lceil \mathbb{N} \rceil_\nu$.
- $\tau_1 \times \tau_2$. Then $\nu = (\nu_1, \nu_2)$ and $\nu' = (\nu_1', \nu_2')$ and $(\nu_1, \nu_1', W, m) \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$ and $(\nu_2, \nu_2', W, m) \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$. By induction $(\nu_1, W.\theta_1, m) \in \lceil \tau_1 \rceil_\nu, (\nu_1', W.\theta_2, m) \in \lceil \tau_1 \rceil_\nu, (\nu_2, W.\theta_1, m) \in \lceil \tau_2 \rceil_\nu$ and $(\nu_2', W.\theta_2, m) \in \lceil \tau_2 \rceil_\nu$. Hence by the definition of $\lceil \tau_1 \times \tau_2 \rceil_\nu$ we have $((\nu_1, \nu_2), W.\theta_1, m) \in \lceil \tau_1 \times \tau_2 \rceil_\nu$ and $((\nu_1', \nu_2'), W.\theta_2, m) \in \lceil \tau_1 \times \tau_2 \rceil_\nu$.
- $\tau_1 + \tau_2$. W.l.o.g. assume that $\nu = \mathtt{inl}\ \nu_1$ and $\nu' = \mathtt{inl}\ \nu_2$. Then $(\nu_1, \nu_2, W, m) \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$. By induction $(\nu_1, W.\theta_1, m) \in \lceil \tau_1 \rceil_\nu$ and $(\nu_2, W.\theta_2, m) \in \lceil \tau_1 \rceil_\nu$. Hence $(\mathtt{inl}\ \nu_1, W.\theta_1, m) \in \lceil \tau_1 + \tau_2 \rceil_\nu$ and $(\mathtt{inl}\ \nu_2, W.\theta_2, m.) \in \lceil \tau_1 + \tau_2 \rceil_\nu$.
- $\tau_1 \xrightarrow{\Sigma,p} \tau_2$: In this case $\nu = \lambda x.e$ and $\nu' = \lambda x.e'$ for some expressions e and e'. We get the claim by the definition of $\llbracket \tau_1 \xrightarrow{\Sigma,p} \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$.
- ref τ: The $\nu = l$ and $\nu' = l'$ and $W.\theta_1(l) = \tau = W.\theta_2(l')$. Hence $(l, W.\theta_1, m) \in \lceil \mathtt{ref}\ \tau \rceil_\nu$ and $(l', W.\theta_2, m) \in \lceil \mathtt{ref}\ \tau \rceil_\nu$.
- A^l: There are two cases:
  - $l(\Sigma) \sqsubseteq \mathcal{A}$: In this case $(\nu, \nu', W, m) \in \llbracket A \rrbracket^{\mathcal{A}}_{\mathcal{V}}$. We get $(\nu, W.\theta_1, m) \in \lceil A \rceil_\nu$ and $(\nu', W.\theta_2, m) \in \lceil A \rceil_\nu$ by induction. $(\nu, W.\theta_1, m) \in \lceil A^l \rceil_\nu$ and $(\nu', W.\theta_2, m) \in \lceil A^l \rceil_\nu$ follows directly from the definition of $\lceil A^l \rceil_\nu$.
  - $l(\Sigma) \not\sqsubseteq \mathcal{A}$: In this case $(\nu, W.\theta_1, m) \in \lceil A \rceil_\nu$ and $(\nu', W.\theta_2, m) \in \lceil A \rceil_\nu$. $(\nu, W.\theta_1, m) \in \lceil A^l \rceil_\nu$ and $(\nu', W.\theta_2, m) \in \lceil A^l \rceil_\nu$ follows directly from the definition of $\lceil A^l \rceil_\nu$.

□

Lemma 8.23 (Context monotonicity)**.** For all $\Gamma, m, \theta, \theta', \delta, m'.(\delta, \theta, m) \in \lceil \Gamma \rceil_\nu \ \wedge \theta \sqsubseteq \theta' \wedge m' \leqslant m \rightarrow (\delta, \theta', m') \in \lceil \Gamma \rceil_\nu$.

Proof. Let $\Gamma, \theta, \theta', \delta, m, m'$ such that $(\delta, \theta, m) \in \lceil \Gamma \rceil_\nu \wedge \theta \sqsubseteq \theta' \wedge m' \leqslant m$. Because $(\delta, \theta, m) \in \lceil \Gamma \rceil_\nu$ we already know $\mathtt{dom}(\Gamma) \subseteq \mathtt{dom}(\delta)$. So it suffices to show $\forall x \in \mathtt{dom}(\Gamma).(\delta(x), \theta', m') \in \lceil \Gamma(x) \rceil_\nu$. Let $x \in \mathtt{dom}(\Gamma)$. Then $x \in \mathtt{dom}(\delta)$ and by $(\delta, \theta, \Delta) \in \lceil \Gamma \rceil_\nu$ also $(\delta(x), \theta, m) \in \lceil \Gamma(x) \rceil_\nu$. By monotonicity of the value relation (Lemma 8.4) $(\delta(x), \theta', m') \in \lceil \Gamma(x) \rceil_\nu$ which is what we needed to show. □

Lemma 8.24.

1. If $(\nu, \nu', W, m) \in \llbracket \tau \rrbracket^{\mathcal{A}}_{\mathcal{V}}$, then for all $m' \leqslant m$ also $(\nu, \nu', W, m') \in \llbracket \tau \rrbracket^{\mathcal{A}}_{\mathcal{V}}$.
2. If $(\nu, \nu', W, m) \in \llbracket A \rrbracket^{\mathcal{A}}_{\mathcal{V}}$, then for all $m' \leqslant m$ also $(\nu, \nu', W, m') \in \llbracket A \rrbracket^{\mathcal{A}}_{\mathcal{V}}$.

Proof. By mutual induction on τ and A.

- unit: Let $((), (), W, m) \in \llbracket \mathtt{unit} \rrbracket^{\mathcal{A}}_{\mathcal{V}}$ and $m' \leqslant m$. Then also $((), (), W, m') \in \llbracket \mathtt{unit} \rrbracket^{\mathcal{A}}_{\mathcal{V}}$.
- $\mathbb{N}$: Let $(n, n, W, m) \in \llbracket \mathbb{N} \rrbracket^{\mathcal{A}}_{\mathcal{V}}$ and $m' \leqslant m$. Then $n \in \mathbb{N}$ and hence also $(n, n, W, m') \in \llbracket \mathbb{N} \rrbracket^{\mathcal{A}}_{\mathcal{V}}$.
- $\tau_1 \times \tau_2$: Let $((\nu_1, \nu_2), (\nu_1', \nu_2'), W, m) \in \llbracket \tau_1 \times \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$ and $m' \leqslant m$. Then $(\nu_1, \nu_1', W, m) \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$ and $(\nu_2, \nu_2', W, m) \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$. By induction $(\nu_1, \nu_1', W, m') \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$ and $(\nu_2, \nu_2', W, m') \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$. Hence $((\nu_1, \nu_2), (\nu_1', \nu_2'), W, m') \in \llbracket \tau_1 \times \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$.
- $\tau_1 + \tau_2$: Assume $(\mathtt{inl}\ \nu_0, \mathtt{inl}\ \nu_0', W, m) \in \llbracket \tau_1 + \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$ and $m' \leqslant m$. Then $(\nu_0, \nu_0', W, m) \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$. By induction $(\nu_0, \nu_0', W, m') \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$. Hence $(\mathtt{inl}\ \nu_0, \mathtt{inl}\ \nu_0', W, m') \in \llbracket \tau_1 + \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$. The case for inr works analogously.
- $\tau_1 \xrightarrow{\Sigma,p} \tau_2$. Assume $(\lambda x.e, \lambda x.e', W, m) \in \llbracket \tau_1 \xrightarrow{\Sigma,p} \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$ and $m' \leqslant m$.
  –

Let $W' \sqsupseteq W$, $m'' < m'$, $(v_0, v_0', W', m'') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$ and $\Sigma_1 \supseteq \Sigma \subseteq \Sigma_2$ such that $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$. We need to show $([v_0/x]e, [v_0'/x]e', W', \Sigma_1, \Sigma_2, m'') \in [\![\tau_2]\!]^{\mathcal{A}}_{E}$.

Because $m' \leqslant m$ and $m'' < m'$, also $m'' < m$. Hence we get this from $(\lambda x.e, \lambda x.e', W, m) \in [\![\tau_1 \overset{\Sigma,p}{\to} \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$.

We already know $(\lambda\ x.e, W.\theta_1, m) \in \lceil \tau_1 \overset{\Sigma,p}{\to} \tau_2 \rceil_{\mathcal{V}}$ and $(\lambda\ x.e', W.\theta_2, m) \in \lceil \tau_1 \overset{\Sigma,p}{\to} \tau_2 \rceil_{\mathcal{V}}$. We get $(\lambda\ x.e, W.\theta_1, m') \in \lceil \tau_1 \overset{\Sigma,p}{\to} \tau_2 \rceil_{\mathcal{V}}$ and $(\lambda\ x.e', W.\theta_2, m') \in \lceil \tau_1 \overset{\Sigma,p}{\to} \tau_2 \rceil_{\mathcal{V}}$ by Lemma 8.4.

- $\mathtt{ref}\ \tau$:

  Let $(l, l', W, m) \in [\![\mathtt{ref}\ \tau]\!]^{\mathcal{A}}_{\mathcal{V}}$ and $m' \leqslant m$. Then $W.\theta_1(l) = \tau = W.\theta_2(l)$ and $(l, l') \in W.\beta$. Hence $(l, l', W, m') \in [\![\mathtt{ref}\ \tau]\!]^{\mathcal{A}}_{\mathcal{V}}$.

- Let $(v, v', W, m) \in [\![A^p]\!]^{\mathcal{A}}_{\mathcal{V}}$ and $m' \leqslant m$. There are two cases:

  1. $l \sqsubseteq \mathcal{A}$. In this case $(v, v', W, m) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$. By induction $(v, v', W, m') \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$. Hence $(v, v', W, m') \in [\![A^p]\!]^{\mathcal{A}}_{\mathcal{V}}$.
  2. $l \not\sqsubseteq \mathcal{A}$. Then $(v, W.\theta_1, m) \in \lceil A \rceil_{\mathcal{V}}$ and $(v', W.\theta_2, m) \in \lceil A \rceil_{\mathcal{V}}$. We get $(v, W.\theta_1, m') \in \lceil A \rceil_{\mathcal{V}}$ and $(v', W.\theta_2, m') \in \lceil A \rceil_{\mathcal{V}}$ by Lemma 8.4 which gives us $(v, v', W, m') \in [\![A^p]\!]^{\mathcal{A}}_{\mathcal{V}}$.

□

Lemma 8.25. For all v, v', W, W', m, τ. $(v, v', W, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}} \wedge W \sqsubseteq W' \to (v, v', W', m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$ and for all v, v', W, W', m, A. $(v, v', W, m) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}} \wedge W \sqsubseteq W' \to (v, v', W', m) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$.

Proof. By mutual induction on the structure of τ and A.

- unit: Then $v = () = v'$ and $((), (), W', m) \in [\![\mathtt{unit}]\!]^{\mathcal{A}}_{\mathcal{V}}$ anyway.
- $\mathcal{N}$: Let Then $v = n = v'$ and $n \in \mathcal{N}$ and hence also $(n, n, W', m) \in [\![\mathcal{N}]\!]^{\mathcal{A}}_{\mathcal{V}}$.
- $\tau_1 \times \tau_2$: Then $v = (v_1, v_2)$, $v' = (v_1', v_2')$ and $(v_1, v_1', W, m) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$ and $(v_2, v_2', W, m) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$. By induction also $(v_1, v_1', W', m) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$ and $(v_2, v_2', W', m) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$. This suffices to show the goal.
- $\tau_1 + \tau_2$: W.l.o.g. assume $v = \mathtt{inl}\ v_1$ and $v' = \mathtt{inl}\ v_2$. Then $(v_1, v_2, W, m) \in \lceil \tau_1 \rceil_{\mathcal{V}}$. By induction $(v_1, v_2, W', m) \in \lceil \tau_1 \rceil_{\mathcal{V}}$. This proves the goal.
- $\tau_1 \overset{\Sigma,p}{\to} \tau_2$: In this case $v = \lambda x.e$ and $v' = \lambda x.e'$.
  - Let $W'' \sqsupseteq W'$, $m' < m$, v_1, v_2 s.t. $(v_1, v_2, W'', m') \in \lceil \tau_1 \rceil_{\mathcal{V}}$ and Σ_1, Σ_2 such that $\Sigma_1' \supseteq \Sigma \subseteq \Sigma_2$ and $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$. Also let $m' < m$. We have to show $([v_1/x]e, [v_2/x]e', W'', \Sigma_1, \Sigma_2, m') \in [\![\tau_2]\!]^{\mathcal{A}}_{E}$. By transitivity of $\sqsubseteq$ (Lemma 7.2) we have $W \sqsubseteq W''$. Since we already know $m' < m$, $(v_1, v_2, W'', m') \in \lceil \tau_1 \rceil_{\mathcal{V}}$ and $\Sigma' \supseteq \Sigma_{\mathcal{A}}$ we get $([v_1/x]e, [v_2/x]e', W'', \Sigma_1, \Sigma_2, m') \in [\![\tau_2]\!]^{\mathcal{A}}_{E}$ from $(\lambda x.e, \lambda x.e', W, m) \in [\![\tau_1 \overset{\Sigma,p}{\to} \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$.
  - From $(\lambda x.e, \lambda x.e', W, m) \in [\![\tau_1 \overset{\Sigma,p}{\to} \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$ we know $(\lambda\ x.e, W.\theta_1, m) \in \lceil \tau_1 \overset{\Sigma,p}{\to} \tau_2 \rceil_{\mathcal{V}}$. We get $(\lambda\ x.e, W'.\theta_1, m) \in \lceil \tau_1 \overset{\Sigma,p}{\to} \tau_2 \rceil_{\mathcal{V}}$ by Lemma 8.4.
  - From $(\lambda x.e, \lambda x.e', W, m) \in [\![\tau_1 \overset{\Sigma,p}{\to} \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$ we know $(\lambda\ x.e', W.\theta_2, m) \in \lceil \tau_1 \overset{\Sigma,p}{\to} \tau_2 \rceil_{\mathcal{V}}$. We get $(\lambda\ x.e', W'.\theta_2, m) \in \lceil \tau_1 \overset{\Sigma,p}{\to} \tau_2 \rceil_{\mathcal{V}}$ by Lemma 8.4.
- $\mathtt{ref}\ \tau'$: In this case $v = l$, $v' = l'$ and $W.\theta_1(l) = \tau' = W.\theta_2(l)$ and $(l, l') \in W.\beta$. Because $W' \sqsupseteq W$ we know $W'.\theta_1 \sqsupseteq W.\theta_1$, $W'.\theta_2 \sqsupseteq W.\theta_2$ and $W'.\beta \supseteq W.\beta$. Hence also $W'.\theta_1(l) = \tau' = W'.\theta_2(l)$ and $(l, l') \in W'.\beta$. Consequently $(l, l', W', m) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$.
- A^p: There are two cases:
  - $p \sqsubseteq \mathcal{A}$: In this case $(v, v', W, m) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$ By induction $(v, v', W', m) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$ and hence $(v, v', W', m) \in [\![A^p]\!]^{\mathcal{A}}_{\mathcal{V}}$.
  - $p \not\sqsubseteq \mathcal{A}$: In this case $(v, W.\theta_1, m) \in \lceil \tau \rceil_{\mathcal{V}}$ and $(v', W.\theta_2, m) \in \lceil \tau \rceil_{\mathcal{V}}$. Because $W \sqsubseteq W'$ in particular $W.\theta_1 \sqsubseteq W'.\theta_1$ and $W.\theta_2 \sqsubseteq W'.\theta_2$. Hence by Lemma 8.4 $(v, W'.\theta_1, m) \in \lceil \tau \rceil_{\mathcal{V}}$ and $(v', W'.\theta_2, m) \in \lceil \tau \rceil_{\mathcal{V}}$ and consequently $(v, v', W', m) \in [\![A^p]\!]^{\mathcal{A}}_{\mathcal{V}}$.

□

Lemma 8.26 (Context monotonicity)**.** For all $\Gamma, W, W', \gamma, \mathfrak{m}, \mathfrak{m}'.(\gamma, W, \mathfrak{m}) \in [\![\Gamma]\!]^{\mathcal{A}}_{\mathcal{V}} \wedge W \sqsubseteq W' \wedge \mathfrak{m}' \leqslant \mathfrak{m} \to (\gamma, W', \mathfrak{m}') \in [\![\Gamma]\!]^{\mathcal{A}}_{\mathcal{V}}$.

Proof. Let $\Gamma, W, W', \gamma, \mathfrak{m}, \mathfrak{m}'$ such that $(\gamma, W, \mathfrak{m}) \in [\![\Gamma]\!]^{\mathcal{A}}_{\mathcal{V}} \wedge W \sqsubseteq W' \wedge \mathfrak{m}' \leqslant \mathfrak{m}$. Because $(\gamma, W, \mathfrak{m}) \in [\![\Gamma]\!]^{\mathcal{A}}_{\mathcal{V}}$ we already know $\mathtt{dom}(\Gamma) \subseteq \mathtt{dom}(\gamma)$. So it suffices to show $\forall x \in \mathtt{dom}(\Gamma).(\gamma_1(x), \gamma_2(x), W', \mathfrak{m}') \in [\![\Gamma(x)]\!]^{\mathcal{A}}_{\mathcal{V}}$. Let $x \in \mathtt{dom}(\Gamma)$. Then $x \in \mathtt{dom}(\gamma)$ and by $(\gamma, W, \mathfrak{m}) \in [\![\Gamma]\!]^{\mathcal{A}}_{\mathcal{V}}$ also $(\gamma_1(x), \gamma_2(x), W, \mathfrak{m}) \in [\![\Gamma(x)]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.25 and Lemma 8.24 $(\gamma_1(x), \gamma_2(x), W', \mathfrak{m}') \in [\![\Gamma(x)]\!]^{\mathcal{A}}_{\mathcal{V}}$ which is what we needed to show. □

Lemma 8.27. For all Σ we have $(\Sigma_{\mathcal{A}})_{\mathcal{A}} = \Sigma_{\mathcal{A}}$.

Proof. $\sqsubseteq$: Let $\sigma \in (\Sigma_{\mathcal{A}})_{\mathcal{A}}$. Then in partiuclar $\sigma \in \Sigma_{\mathcal{A}}$.

$\sqsupseteq$: Let $\sigma \in \Sigma_{\mathcal{A}}$. Then $\mathtt{pol}(\Sigma) \sqsubseteq \mathcal{A}$. Because of this and of $\sigma \in \Sigma_{\mathcal{A}}$ we have $\sigma \in (\Sigma_{\mathcal{A}})_{\mathcal{A}}$.

□

Lemma 8.28.

1. If $\Sigma \supseteq \Sigma'$, then $\Sigma_{\mathcal{A}} \supseteq \Sigma'_{\mathcal{A}}$.
2. If $\Sigma \supseteq \Sigma'_{\mathcal{A}}$, then $\Sigma_{\mathcal{A}} \supseteq \Sigma'_{\mathcal{A}}$.

Proof.

1. Let $\Sigma \supseteq \Sigma'$. Let $\sigma \in \Sigma'_{\mathcal{A}}$. Then $\sigma \in \Sigma'$ and $\mathtt{pol}(\sigma) \sqsubseteq \mathcal{A}$. By assumption $\sigma \in \Sigma$ and hence $\sigma \in \Sigma_{\mathcal{A}}$.
2. By 1. $\Sigma_{\mathcal{A}} \supseteq (\Sigma'_{\mathcal{A}})_{\mathcal{A}}$. By Lemma 8.27 $(\Sigma'_{\mathcal{A}})_{\mathcal{A}} = \Sigma'_{\mathcal{A}}$. The goal follows by transitivity.

□

Lemma 8.29. Let $(e, e', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ and $W' \sqsupseteq W$, $\Sigma_1 \supseteq \Sigma, \Sigma_2 \supseteq \Sigma'$, $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$ and $\mathfrak{m}' \leqslant \mathfrak{m}$. Then $(e, e', W', \Sigma_1, \Sigma_2, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.

Proof. By induction on $\mathfrak{m}$. There are two cases:

1. $(e, e', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. In this case it suffices to show $(e, e', W', \Sigma_1, \Sigma_2, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. By assumption $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$. Let Σ'_1, Σ'_2 such that

   - $\Sigma'_1 \supseteq \Sigma_1$,
   - $\Sigma'_2 \supseteq \Sigma_2$,
   - $\Sigma'_1 \approx_{\mathcal{A}} \Sigma'_2$,

   W'' and $\mathfrak{m}''$ such that

   - $\mathfrak{m}'' < \mathfrak{m}'$,
   - $W'' \sqsupseteq W'$ and

   S_1, S_2 such that

   - $(S_1, S_2, \mathfrak{m}'') \overset{\mathcal{A}}{\triangleright} W''$.

   By transitivity also

   - $\Sigma'_1 \supseteq \Sigma$,
   - $\Sigma'_2 \supseteq \Sigma'$,
   - $W'' \sqsupseteq W$ (Lemma 7.2) and
   - $\mathfrak{m}'' < \mathfrak{m}$.

   Hence we are in one of three cases:

(a) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1'', \omega, e_2', \Sigma_2'', S_2', \omega'. \\ \Sigma_1' \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1''} e_1',\, S_1' \;\wedge \\ \Sigma_2' \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2''} e_2',\, S_2' \;\rightarrow \\ (\omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \vee \Sigma_1'' \sqsubseteq \mathcal{A} \vee \Sigma_2'' \sqsubseteq \mathcal{A}) \;\rightarrow \\ \exists W'''. W''' \sqsupseteq W'' \wedge\; (S_1', S_2', \mathfrak{m}'') \overset{\mathcal{A}}{\triangleright} (W''') \;\wedge \\ \omega \approx^{\mathcal{A}}_{W'''.\beta} \omega' \wedge\; (e_1', e_2', W''', \Sigma, \Sigma', \mathfrak{m}'') \in [\![\tau]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

In this case it suffices to show

$(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1'', \omega, e_2', \Sigma_2'', S_2', \omega'. \\ \Sigma_1' \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1''} e_1',\, S_1' \;\wedge \\ \Sigma_2' \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2''} e_2',\, S_2' \;\rightarrow \\ (\omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \vee \Sigma_1'' \sqsubseteq \mathcal{A} \vee \Sigma_2'' \sqsubseteq \mathcal{A}) \;\rightarrow \\ \exists W'''. W''' \sqsupseteq W'' \wedge\; (S_1', S_2', \mathfrak{m}'') \overset{\mathcal{A}}{\triangleright} (W''') \;\wedge \\ \omega \approx^{\mathcal{A}}_{W'''.\beta} \omega' \wedge\; (e_1', e_2', W''', \Sigma_1, \Sigma_2, \mathfrak{m}'') \in [\![\tau]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

By assumption neither e nor e' is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1'', \Sigma_2'', S_1', S_2'$ such that

- $e, \Sigma_1', S_1 \succ e_\beta, S_1', \omega, \Sigma_1''$
- $e', \Sigma_2', S_2 \succ e_\beta', S_2', \omega', \Sigma_2''$

Also assume $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \vee \Sigma_1'' \sqsubseteq \mathcal{A} \vee \Sigma_1'' \sqsubseteq \mathcal{A}$. Then there is a W''' such that

- $W''' \sqsupseteq W''$
- $(S_1', S_2', \mathfrak{m}'') \overset{\mathcal{A}}{\triangleright} W'''$
- $\omega \approx^{\mathcal{A}}_{W'''.\beta} \omega'$
- $(e_\beta, e_\beta', W''', \Sigma, \Sigma', \mathfrak{m}'') \in [\![\tau]\!]^{\mathcal{A}}_{E}$

It suffices to show

- $W''' \sqsupseteq W''$. We already know that.
- $(S_1', S_2', \mathfrak{m}'') \overset{\mathcal{A}}{\triangleright} W'''$ We already know that.
- $\omega \approx^{\mathcal{A}}_{W'''.\beta} \omega'$. We already know that.
- $(e_\beta, e_\beta', W''', \Sigma_1, \Sigma_2, \mathfrak{m}'') \in [\![\tau]\!]^{\mathcal{A}}_{E}$. We get this by induction.

(b) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1'', \omega. \\ \Sigma_1' \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1''} e_1',\, S_1' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \;\wedge \\ (\exists W'''. W''' \sqsupseteq W'' \wedge (S_1', S_2, \mathfrak{m}'') \overset{\mathcal{A}}{\triangleright} (W''') \;\wedge \\ (e_1', e_2, W''', \Sigma, \Sigma', \mathfrak{m}'') \in [\![\tau]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$

In this cases it suffices to show

$(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1'', \omega. \\ \Sigma_1' \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1''} e_1',\, S_1' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \;\wedge \\ (\exists W'''. W''' \sqsupseteq W'' \wedge (S_1', S_2, \mathfrak{m}'') \overset{\mathcal{A}}{\triangleright} (W''') \;\wedge \\ (e_1', e_2, W''', \Sigma_1, \Sigma_2, \mathfrak{m}'') \in [\![\tau]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$

By assumption e is not a value.So let $\omega, e_\beta, \Sigma_1'', S_1'$ such that

- $e, \Sigma_1', S_1 \succ e_\beta, S_1', \omega, \Sigma_1''$.

Then

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is a W''' such that

- $W''' \sqsupseteq W''$
- $(S_1', S_2, \mathfrak{m}'') \overset{\mathcal{A}}{\triangleright} W'''$
- $(e_\beta, e', W''', \Sigma, \Sigma', \mathfrak{m}'') \in [\![\tau]\!]^{\mathcal{A}}_{E})$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this.

- $W''' \sqsupseteq W''$. We already know this.
- $(S_1', S_2, m'') \overset{\mathcal{A}}{\triangleright} W'''$. We already know this.
- $(e_\beta, e', W''', \Sigma_1, \Sigma_2, m'') \in [\![\tau]\!]^{\mathcal{A}}_{E}$. We get this using the induction hypothesis.

(c) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2'', \omega. \\ \Sigma_2' \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2''} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W'''. W''' \sqsupseteq W'' \wedge (S_1, S_2', m'') \overset{\mathcal{A}}{\triangleright} W''' \wedge \\ (e_1, e_2', W''', \Sigma, \Sigma', m'') \in [\![\tau]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$

In this case it suffices to show

$(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2'', \omega. \\ \Sigma_2' \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2''} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W'''. W''' \sqsupseteq W'' \wedge (S_1, S_2', m'') \overset{\mathcal{A}}{\triangleright} W''' \wedge \\ (e_1, e_2', W''', \Sigma_1, \Sigma_2, m'') \in [\![\tau]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$

By assumption e' is not a value. So let $\omega', e_\beta', \Sigma_2'', S_2'$ such that

- $e', \Sigma_2', S_2 \succ e_\beta', S_2', \omega', \Sigma_2''$

Then

- $\neg(\mathrm{pol}(\omega') \sqsubseteq \mathcal{A})$

and there is a W''' such that

- $W''' \sqsupseteq W''$
- $(S_1, S_2', m'') \overset{\mathcal{A}}{\triangleright} W'''$
- $(e, e_\beta', W''', \Sigma, \Sigma', m'') \in [\![\tau]\!]^{\mathcal{A}}_{E})$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega') \sqsubseteq \mathcal{A})$. We already know this.
- $W''' \sqsupseteq W''$. We already know this.
- $(S_1, S_2', m'') \overset{\mathcal{A}}{\triangleright} W'''$. We already know this.
- $(e, e_\beta', W''', \Sigma_1, \Sigma_2, m'') \in [\![\tau]\!]^{\mathcal{A}}_{E}$. We get this using the induction hypothesis.

2. $(e, e', W, \Sigma, \Sigma', m) \in \{(v, v', W, \Sigma_{c_1}, \Sigma_{c_2}, m) \mid (v, v', W, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}\}$. It suffices to show $(e, e', W', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. We already know $(e, e', W, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$ and that e and e' are values. We get the goal by Lemma 8.24 and Lemma 8.25.

□

Lemma 8.30 (Equivalence of high expressions)**.** If $(e, \theta, m) \in \lceil\tau\rceil^{pc}_{E}$ and $(e', \theta', m) \in \lceil\tau\rceil^{pc}_{E}$ and $\tau \not\sqsubseteq \mathcal{A}$ and $pc \not\sqsubseteq \mathcal{A}$, then $\forall \Sigma, \Sigma', \beta.\ \Sigma \approx_{\mathcal{A}} \Sigma' \to (e, e', (\theta, \theta', \beta), \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$.

Proof. By induction on m. There are two cases:

1. $(e, \theta, m) \in \lceil\tau\rceil^{pc}_{E_\beta}$. In this case e is not a value.
   It suffices to show $(e, e', (\theta, \theta', \beta), \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{E_\beta}$. We already know $\Sigma \approx_{\mathcal{A}} \Sigma'$. Let Σ_1, Σ_2. such that

   - $\Sigma_1 \supseteq \Sigma$,
   - $\Sigma_2 \supseteq \Sigma'$,
   - $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

   W', m' such that

   - $m' < m$,
   - $W' \sqsupseteq (\theta, \theta', \beta)$,

   and S_1, S_2 such that

   - $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

It suffices to show $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xrightarrow{\omega;\Sigma_1'} e_1',\, S_1' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$

We already know that e is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $e, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$.

Because $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$, also

- $(S_1, m') \triangleright W'.\theta_1$.

Because $W' \sqsupseteq (\theta, \theta', \beta)$ also

- $W'.\theta_1 \sqsupseteq \theta$

Hence from $(e, \theta, m) \in \lceil\tau\rceil^{pc}_{E_\beta}$

- $\forall p. \mathrm{pol}(\omega) = p \rightarrow pc \sqsubseteq p$

and there is a θ'' such that

- $\theta'' \sqsupseteq W'.\theta_1$
- $(S_1', m') \triangleright \theta''$
- $(e_\beta, \theta'', m') \in \lceil\tau\rceil^{pc}_{E}$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. Assume $\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}$. Then we know $pc \sqsubseteq \mathrm{pol}(\omega)$. By transitivity Lemma 4.1 $pc \sqsubseteq \mathcal{A}$. But by assumption $pc \not\sqsubseteq \mathcal{A}$. ↯
- $(\theta'', W'.\theta_2, W'.\beta) \sqsupseteq W'$. We have to show the following
  - $\theta'' \sqsupseteq W'.\theta_1$ We already know this.
  - $W'.\theta_2 \sqsupseteq W'.\theta_2$ We have this by Lemma 7.2.
  - $W'.\beta \supseteq W'.\beta$ We have this by reflexivity.
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (\theta'', W'.\theta_2, W'.\beta)$. We have to show:
  - $W'.\beta \subseteq \mathrm{dom}(\theta'') \times \mathrm{dom}(W'.\theta_2)$. From $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ we know $W'.\beta \subseteq \mathrm{dom}(W'.\theta_1) \times \mathrm{dom}(W'.\theta_2)$. Because $\theta'' \sqsupseteq W'.\theta_1$, we have $\mathrm{dom}(W'.\theta_1) \subseteq \mathrm{dom}(\theta'')$. Hence $\mathrm{dom}(W'.\theta_1) \times \mathrm{dom}(W'.\theta_2) \subseteq \mathrm{dom}(\theta'') \times \mathrm{dom}(W'.\theta_2)$. We get $W'.\beta \subseteq \mathrm{dom}(\theta'') \times \mathrm{dom}(W'.\theta_2)$ by transitivity.
  - $(\forall (l, l') \in W'.\beta.\ \theta''(l) = W'.\theta_2(l') \wedge (S_1'(l), S_2(l'), (\theta'', W'.\theta_2, W'.\beta), m') \in [\![\theta''(l)]\!]^{\mathcal{A}}_{\mathcal{V}})$.
    Let $(l, l') \in W'.\beta$.. Because $W'.\beta \subseteq \mathrm{dom}(W'.\theta_1) \times \mathrm{dom}(W'.\theta_2)$, we must have $l \in \mathrm{dom}(W'.\theta_1)$. Because $\theta'' \sqsupseteq W'.\theta_1$, of course also $l \in \mathrm{dom}(\theta'')$ and $\theta''(l) = W'.\theta_1(l)$. From $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ we know $W'.\theta_1(l) = W'.\theta_2(l') \wedge (S_1(l), S_2(l'), W', m') \in [\![W'.\theta_1(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$.
    Because $\theta'' \sqsupseteq W'.\theta_1$ we know that $W'.\theta_1(l) = \theta''(l)$. Hence $\theta''(l) = W'.\theta_2(l')$.
    By Lemma 8.3 either $S_1'(l) = S_1(l)$ or $\mathrm{pol}(\mathrm{type}(S_1', l)) = \mathrm{pol}(\omega)$.
    In the first case this gives us $(S_1'(l), S_2(l'), W', m') \in [\![W'.\theta_1(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$ which is equivalent to $(S_1'(l), S_2(l'), W', m') \in [\![\theta''(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$. We have already shown that $(\theta'', W'.\theta_2, W'.\beta) \sqsupseteq W'$, so we get the goal by Lemma 8.25.
    In the second case $\neg(\mathrm{pol}(\mathrm{type}(S_1', l)) \sqsubseteq \mathcal{A})$. We also know $(S_1', m') \triangleright \theta''$. Hence $\theta''(l) = \mathrm{type}(S_1', l)$. Hence we have to show $(S_1'(l), S_2(l'), (\theta'', W'.\theta_2, W'.\beta), m') \in [\![\mathrm{type}(S_1', l)]\!]^{\mathcal{A}}_{\mathcal{V}}$.
    $\mathrm{type}(S_1', l)$ must have the form A^p. We already know $p = \mathrm{pol}(\mathrm{type}(S_1', l)) \not\sqsubseteq \mathcal{A}$. Hence it suffices to show
    - $(S_1'(l), \theta'', m') \in \lceil A\rceil_{\mathcal{V}}$ From $(S_1', m') \triangleright \theta''$ and $l \in \mathrm{dom}(\theta'')$ we get $(S_1'(l), \theta'', m') \in \lceil\mathrm{type}(S_1', l)\rceil_{\mathcal{V}}$ which implies the goal.
    - $(S_2(l'), W'.\theta_2, m') \in \lceil A\rceil_{\mathcal{V}}$ From $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ we get $(S_2, m') \triangleright W'.\theta_2$. Because also $l' \in \mathrm{dom}(W'.\theta_2)$ this gives us $(S_2(l'), W'.\theta_2, m') \in \lceil W'.\theta_2(l')\rceil_{\mathcal{V}}$. We have already shown that $W'.\theta_2(l') = \theta''(l) = \mathrm{type}(S_1', l)$ So we have $(S_2(l'), W'.\theta_2, m') \in \lceil\mathrm{type}(S_1', l)\rceil_{\mathcal{V}}$ which implies the goal.

- $(S_1', m') \triangleright \theta''$. We already know this.
- $(S_2, m') \triangleright W'.\theta_2$. We know $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ which implies the claim.

- $(e_\beta, e', (\theta'', W'.\theta_2, W'.\beta), \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E$. We already know $(e_\beta, \theta'', m') \in \lceil\tau\rceil^{pc}_E$, $pc \not\sqsubseteq \mathcal{A}$ and $\tau \not\sqsubseteq \mathcal{A}$. We can also get $(e', W'.\theta_2, m') \in \lceil\tau\rceil^{pc}_E$ by Lemma 8.5. We get the goal using the induction hypothesis.

2. $(e, \theta, m) \in \lceil\tau\rceil^{pc}_{E_v}$. In this case e is a value v and
   - $(v, \theta, m) \in \lceil\tau\rceil_{\mathcal{V}}$.

   There are two further cases:

   (a) $(e', \theta', m) \in \lceil\tau\rceil^{pc}_{E_\beta}$. In this case e' is not a value.
   It suffices to show $(v, e', (\theta, \theta', \beta), \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{E_\beta}$. We already know $\Sigma \approx_{\mathcal{A}} \Sigma'$. Let Σ_1, Σ_2. such that
   - $\Sigma_1 \supseteq \Sigma$,
   - $\Sigma_2 \supseteq \Sigma'$,
   - $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

   W', m' such that
   - $m' < m$,
   - $W' \sqsupseteq (\theta, \theta', \beta)$,

   and S_1, S_2 such that
   - $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

   It suffices to show $(v, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega;\Sigma_2'} e_2', S_2' \rightarrow \neg(pol(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E) \end{array} \right\}$
   We already know that e' is not a value. So let $\omega, e_\beta', \Sigma_2', S_2'$ such that
   - $e', \Sigma_2, S_2 \succ e_\beta', S_2', \omega, \Sigma_2'$.

   Because $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$, also
   - $(S_2, m') \triangleright W'.\theta_2$.

   Because $W' \sqsupseteq (\theta, \theta', \beta)$ also
   - $W'.\theta_2 \sqsupseteq \theta'$

   Hence from $(e', \theta', m) \in \lceil\tau\rceil^{pc}_{E_\beta}$
   - $\forall p. pol(\omega) = p \rightarrow pc \sqsubseteq p$

   and there is a θ'' such that
   - $\theta'' \sqsupseteq W'.\theta_2$
   - $(S_2', m') \triangleright \theta''$
   - $(e_\beta', \theta'', m') \in \lceil\tau\rceil^{pc}_E$

   It suffices to show the following:
   - $\neg(pol(\omega) \sqsubseteq \mathcal{A})$. Assume $pol(\omega) \sqsubseteq \mathcal{A}$. Then we know $pc \sqsubseteq pol(\omega)$. By transitivity Lemma 4.1 $pc \sqsubseteq \mathcal{A}$. But by assumption $pc \not\sqsubseteq \mathcal{A}$. ↯
   - $(W'.\theta_1, \theta'', W'.\beta) \sqsupseteq W'$. We have to show the following
     - $W'.\theta_1 \sqsupseteq W'.\theta_1$ We have this by Lemma 7.2.
     - $\theta'' \sqsupseteq W'.\theta_2$ We already know this.
     - $W'.\beta \supseteq W'.\beta$ We have this by reflexivity.
   - $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} (W'.\theta_1, \theta'', W'.\beta)$. We have to show:
     - $W'.\beta \subseteq dom(W'.\theta_1) \times dom(\theta'')$. From $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ we know $W'.\beta \subseteq dom(W'.\theta_1) \times dom(W'.\theta_2)$. Because $\theta'' \sqsupseteq W'.\theta_2$, we have $dom(W'.\theta_2) \subseteq dom(\theta'')$. Hence $dom(W'.\theta_1) \times dom(W'.\theta_2) \subseteq dom(W'.\theta_1) \times dom(\theta'')$. We get $W'.\beta \subseteq dom(W'.\theta_1) \times dom(\theta'')$ by transitivity.

– $(\forall(l,l') \in W'.\beta.\, W'.\theta_1(l) = \theta''(l') \wedge (S_1(l), S_2'(l'), (W'.\theta_1, \theta'', W'.\beta), m') \in [\![W'.\theta_1(l)]\!]^{\mathcal{A}}_{\mathcal{V}})$.
Let $(l,l') \in W'.\beta$.. Because $W'.\beta \subseteq \mathtt{dom}(W'.\theta_1) \times \mathtt{dom}(W'.\theta_2)$, we must have $l' \in \mathtt{dom}(W'.\theta_1)$. Because $\theta'' \sqsupseteq W'.\theta_2$, of course also $l' \in \mathtt{dom}(\theta'')$ and $\theta''(l') = W'.\theta_2(l')$.
From $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ we know $W'.\theta_1(l) = W'.\theta_2(l') \wedge (S_1(l), S_2(l'), W', m') \in [\![W'.\theta_1(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$.
Because $\theta'' \sqsupseteq W'.\theta_2$ we know that $W'.\theta_2(l') = \theta''(l')$. Hence $W'.\theta_1(l) = \theta''(l')$.
By Lemma 8.3 either $S_2'(l') = S_2(l')$ or $\mathtt{pol}(\mathtt{type}(S_2', l')) = \mathtt{pol}(\omega)$.
In the first case this gives us $(S_1(l), S_2'(l'), W', m') \in [\![W'.\theta_1(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$ We have already shown that $(W'.\theta_1, \theta'', W'.\beta) \sqsupseteq W'$, so we get the goal by Lemma 8.25.
In the second case $\neg(\mathtt{pol}(\mathtt{type}(S_2', l')) \sqsubseteq \mathcal{A})$. We also know $(S_2', m') \triangleright \theta''$. Hence $\theta''(l') = \mathtt{type}(S_2', l')$. We have already shown that $W'.\theta_1(l) = \theta''(l')$. Hence it suffices to show $(S_1(l), S_2'(l'), (W'.\theta_1, \theta'', W'.\beta), m') \in [\![\mathtt{type}(S_2', l')]\!]^{\mathcal{A}}_{\mathcal{V}}$.
$\mathtt{type}(S_2', l')$ must have the form A^p. We already know $p = \mathtt{pol}(\mathtt{type}(S_2', l')) \not\sqsubseteq \mathcal{A}$. Hence it suffices to show
* $(S_1(l), W'.\theta_1, m') \in \lceil A \rceil_{\mathcal{V}}$ From $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ we get $(S_1, m') \triangleright W'.\theta_1$. Because also $l \in \mathtt{dom}(W'.\theta_1)$ this gives us $(S_1(l), W'.\theta_1, m') \in \lceil W'.\theta_1(l) \rceil_{\mathcal{V}}$. We have already shown that $W'.\theta_1(l) = \theta''(l') = \mathtt{type}(S_2', l')$ So we have $(S_1(l), W'.\theta_1, m') \in \lceil \mathtt{type}(S_2', l') \rceil_{\mathcal{V}}$ which implies the goal.
* $(S_2'(l'), \theta'', m') \in \lceil A \rceil_{\mathcal{V}}$ From $(S_1', m') \triangleright \theta''$ and $l' \in \mathtt{dom}(\theta'')$ we get $(S_2'(l'), \theta'', m') \in \lceil \mathtt{type}(S_2', l') \rceil_{\mathcal{V}}$ which implies the goal.

– $(S_1, m') \triangleright W'.\theta_2$. We know $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ which implies the claim.
– $(S_2', m') \triangleright \theta''$. We already know this.

- $(v, e'_\beta, (W'.\theta_1, \theta'', W'.\beta), \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We already know $(e'_\beta, \theta'', m') \in \lceil \tau \rceil^{pc}_{\mathsf{E}}$, $pc \not\sqsubseteq \mathcal{A}$ and $\tau \not\sqsubseteq \mathcal{A}$. We can also get $(v, W'.\theta_1, m') \in \lceil \tau \rceil^{pc}_{\mathsf{E}}$ by Lemma 8.5. We get the goal using the induction hypothesis.

(b) $(e', \theta', m) \in \lceil \tau \rceil^{pc}_{\mathsf{E}_v}$. In this case e' is a value v' and

- $(v', \theta', m) \in \lceil \tau \rceil_{\mathcal{V}}$. It suffices to show $(v, v', (\theta, \theta', \beta), m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. τ has the form A^p for some p. Since $\tau \not\sqsubseteq \mathcal{A}$ also $p \not\sqsubseteq \mathcal{A}$. Hence it suffices to show $(v, \theta, m) \in \lceil A \rceil_{\mathcal{V}}$ and $(v', \theta', m) \in \lceil A \rceil_{\mathcal{V}}$. These follow directly from $(v, \theta, m) \in \lceil \tau \rceil_{\mathcal{V}}$ and $(v', \theta', m) \in \lceil \tau \rceil_{\mathcal{V}}$.

□

Lemma 8.31 (Binary Semantic subtyping)**.**

1. $\forall A, A'.\ A <: A' \to [\![A]\!]^{\mathcal{A}}_{\mathcal{V}} \subseteq [\![A']\!]^{\mathcal{A}}_{\mathcal{V}}$
2. $\forall \tau, \tau'.$
   (a) $\tau <: \tau' \to [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}} \subseteq [\![\tau']\!]^{\mathcal{A}}_{\mathcal{V}}$
   (b) $\tau <: \tau' \to [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}} \subseteq [\![\tau']\!]^{\mathcal{A}}_{\mathsf{E}}$

Proof. By mutual induction on $A <: A'$ and $\tau <: \tau'$.

1. - **sub-ref** In this case $A = \mathtt{ref}\ \tau_A = A'$. Hence $[\![A]\!]^{\mathcal{A}}_{\mathcal{V}} = [\![A']\!]^{\mathcal{A}}_{\mathcal{V}}$ and we get the claim by reflexivity.
   - **sub-prod** In this case
     – $A = \tau_0 \times \tau_0'$
     – $A' = \tau_1 \times \tau_1'$
     – $\tau_0 <: \tau_1$
     – $\tau_0' <: \tau_1'$

     Let $((v_1, v_2), (v_1', v_2'), W, m) \in [\![\tau_0 \times \tau_0']\!]^{\mathcal{A}}_{\mathcal{V}}$. Then
     – $(v_1, v_1', W, m) \in [\![\tau_0]\!]^{\mathcal{A}}_{\mathcal{V}}$
     – $(v_2, v_2', W, m) \in [\![\tau_0']\!]^{\mathcal{A}}_{\mathcal{V}}$

     Hence by induction
     – $(v_1, v_1', W, m) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$
     – $(v_2, v_2', W, m) \in [\![\tau_1']\!]^{\mathcal{A}}_{\mathcal{V}}$

     This directly gives us $((v_1, v_2), (v_1', v_2'), W, m) \in [\![\tau_1 \times \tau_1']\!]^{\mathcal{A}}_{\mathcal{V}}$.

- **sub-sum** In this case
  - $A = \tau_0 + \tau_0'$
  - $A' = \tau_1 + \tau_1'$
  - $\tau_0 <: \tau_1$
  - $\tau_0' <: \tau_1'$

  Let $(v, v', W, \mathfrak{m}) \in \llbracket \tau_0 + \tau_0' \rrbracket_{\mathcal{V}}^{\mathcal{A}}$. W.l.o.g. assume $v = \mathtt{inl}\ v_0$ and $v' = \mathtt{inl}\ v_0'$. Then
  - $(v_0, v_0', W, \mathfrak{m}) \in \llbracket \tau_0 \rrbracket_{\mathcal{V}}^{\mathcal{A}}$

  Hence by induction
  - $(v_0, v_0', W, \mathfrak{m}) \in \llbracket \tau_1 \rrbracket_{\mathcal{V}}^{\mathcal{A}}$

  This directly gives us $(\mathtt{inl}\ v_0, \mathtt{inl}\ v_0', W, \mathfrak{m}) \in \llbracket \tau_1 + \tau_1' \rrbracket_{\mathcal{V}}^{\mathcal{A}}$.
- **sub-arrow** In this case
  - $A = \tau_0 \xrightarrow{\Sigma, p} \tau_1$
  - $A' = \tau_0' \xrightarrow{\Sigma', p'} \tau_1'$
  - $\tau_0' <: \tau_0$
  - $\tau_1 <: \tau_1'$
  - $p' \sqsubseteq p$
  - $\Sigma \subseteq \Sigma'$

  Let $(\lambda x.\ e, \lambda x.\ e', W, \mathfrak{m}) \in \llbracket \tau_0 \xrightarrow{\Sigma, p} \tau_1 \rrbracket_{\mathcal{V}}^{\mathcal{A}}$ We need to show $(\lambda x.\ e, \lambda x.\ e', W, \mathfrak{m}) \in \llbracket \tau_0' \xrightarrow{\Sigma', p'} \tau_1' \rrbracket_{\mathcal{V}}^{\mathcal{A}}$. Let W' such that
  - $W' \sqsupseteq W$,

  $\mathfrak{m}'$ such that
  - $\mathfrak{m}' < \mathfrak{m}$,

  v, v' such that
  - $(v, v', W', \mathfrak{m}') \in \llbracket \tau_0' \rrbracket_{\mathcal{V}}^{\mathcal{A}}$

  and Σ_1, Σ_2 such that
  - $\Sigma_1 \supseteq \Sigma' \subseteq \Sigma_2$ and
  - $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$.

  Then by induction
  - $(v, v', W', \mathfrak{m}') \in \llbracket \tau_0 \rrbracket_{\mathcal{V}}^{\mathcal{A}}$

  and by transitivity
  - $\Sigma_1 \supseteq \Sigma \subseteq \Sigma_2$.

  Hence
  - $([v/x]e, [v'/x]e', W', \Sigma_1, \Sigma_2, \mathfrak{m}') \in \lceil \tau_1 \rceil_{\mathcal{V}}$.

  We need to show $([v/x]e, [v'/x]e', W', \Sigma_1, \Sigma_2, \mathfrak{m}') \in \lceil \tau_1' \rceil_{\mathcal{V}}$ which we get by induction. We still need to show
  - $(\lambda x.\ e, W.\theta_1, \mathfrak{m}) \in \lceil \tau_0' \xrightarrow{\Sigma', p'} \tau_1' \rceil_{\mathcal{V}}$
  - $(\lambda x.\ e', W.\theta_2, \mathfrak{m}) \in \lceil \tau_0' \xrightarrow{\Sigma', p'} \tau_1' \rceil_{\mathcal{V}}$.

  We already know
  - $(\lambda x.\ e, W.\theta_1, \mathfrak{m}) \in \lceil \tau_0 \xrightarrow{\Sigma, p} \tau_1 \rceil_{\mathcal{V}}$
  - $(\lambda x.\ e', W.\theta_2, \mathfrak{m}) \in \lceil \tau_0 \xrightarrow{\Sigma, p} \tau_1 \rceil_{\mathcal{V}}$.

  From this we can get the goals by Lemma 8.6.
- **sub-unit** In this case $A = \mathtt{unit} = A'$. Hence $\llbracket A \rrbracket_{\mathcal{V}}^{\mathcal{A}} = \llbracket A' \rrbracket_{\mathcal{V}}^{\mathcal{A}}$ and we get the claim by reflexivity.
- **sub-nat** In this case $A = \mathcal{N} = A'$. Hence $\llbracket A \rrbracket_{\mathcal{V}}^{\mathcal{A}} = \llbracket A' \rrbracket_{\mathcal{V}}^{\mathcal{A}}$ and we get the claim by reflexivity.

2. (a) The only applicable rule is **sub-policy**. In this case
   - $\tau = A^p$
   - $\tau' = B^{p'}$

- $p \sqsubseteq p'$
- $A <: B$

Let $(v, v', W, m) \in \lceil A^p \rceil^{\mathcal{A}}_{\mathcal{V}}$. There are two case

i. $p \sqsubseteq \mathcal{A}$ In this case
   - $(v, v', W, m) \in \lceil A \rceil^{\mathcal{A}}_{\mathcal{V}}$.

   Then by induction also
   - $(v, v', W, m) \in \lceil B \rceil^{\mathcal{A}}_{\mathcal{V}}$.

   Because $p \sqsubseteq \mathcal{A}$ (and in particular therefore not $p \not\sqsubseteq \mathcal{A}$) this suffice to show $(v, v', W, m) \in \lceil B^{p'} \rceil^{\mathcal{A}}_{\mathcal{V}}$.

ii. $p \not\sqsubseteq \mathcal{A}$. Hence we have
   - $(v, W.\theta_1, m) \in \lceil A \rceil_{\mathcal{V}}$
   - $(v', W.\theta_2, m) \in \lceil A \rceil_{\mathcal{V}}$

   By Lemma 8.6 we get
   - $(v, W.\theta_1, m) \in \lceil B \rceil_{\mathcal{V}}$
   - $(v', W.\theta_2, m) \in \lceil B \rceil_{\mathcal{V}}$

   which suffices to show $(v, v', W, m) \in \lceil B^{p'} \rceil^{\mathcal{A}}_{\mathcal{V}}$ because $p \not\sqsubseteq \mathcal{A}$ (and hence in particular not $p \sqsubseteq \mathcal{A}$).

(b) The only applicable rule is **sub-policy**. In this case
- $\tau = A^p$
- $\tau' = B^{p'}$
- $p \sqsubseteq p'$
- $A <: B$

To show $\lceil A^p \rceil^{\mathcal{A}}_{E} \subseteq \lceil B^{p'} \rceil^{\mathcal{A}}_{E}$ we have to show $\forall m, e, e', \Sigma, \Sigma', W.(e, e', W, \Sigma, \Sigma', m) \in \lceil A^p \rceil^{\mathcal{A}}_{E} \to (e, e', W, \Sigma, \Sigma', m) \in \lceil B^{p'} \rceil^{\mathcal{A}}_{E}$. We do this by induction on m. So let $(e, e', W, \Sigma, \Sigma', m) \in \lceil A^p \rceil^{\mathcal{A}}_{E}$. There are two cases:

i. $(e, e', W, \Sigma, \Sigma', m) \in \lceil A^p \rceil^{\mathcal{A}}_{E_\beta}$. In this case it suffices to show $(e, e', W, \Sigma, \Sigma', m) \in \lceil B^{p'} \rceil^{\mathcal{A}}_{E_\beta}$. We get $\Sigma \approx_{\mathcal{A}} \Sigma'$. from the assumption. Let Σ_1, Σ_2 such that
   - $\Sigma_1 \supseteq \Sigma$,
   - $\Sigma_2 \supseteq \Sigma'$,
   - $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

   W', m' such that
   - $m' < m$,
   - $W' \sqsupseteq W$,

   and S_1, S_2 such that
   - $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

   Then there are 3 cases:

A. $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma_1'} e_1', S_1' \wedge \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega';\Sigma_2'} e_2', S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge\; (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', m') \in \lceil A^p \rceil^{\mathcal{A}}_{E} \end{array} \right\}$

   It suffices to show

$(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma_1'} e_1', S_1' \wedge \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega';\Sigma_2'} e_2', S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge\; (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', m') \in \lceil B^{p'} \rceil^{\mathcal{A}}_{E} \end{array} \right\}$

   We know that neither e nor e' is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1'.S_2'$ such that

- $e, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $e', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Also assume $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \ \vee \ \Sigma_2' \sqsubseteq \mathcal{A}$.
This directly gives us a W'' such that

- $W'' \sqsupseteq W'$,
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
- $(e_\beta, e_\beta', W'', \Sigma, \Sigma', m') \in [\![A^p]\!]^{\mathcal{A}}_E$

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
- $(e_\beta, e_\beta', W'', \Sigma, \Sigma', m') \in [\![B^{p'}]\!]^{\mathcal{A}}_E$ We get this from the second induction hypothesis.

B. $(e, e') \in$
$$\left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma_1'} e_1', S_1' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![A^p]\!]^{\mathcal{A}}_E) \end{array} \right\}$$
In this case it suffices to show $(e, e') \in$
$$\left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma_1'} e_1', S_1' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![B^{p'}]\!]^{\mathcal{A}}_E) \end{array} \right\}$$
By assumption e is not a value. So let $\omega, e_\beta, S_1', \Sigma_1'$ such that

- $e, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

From our assumption we get

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_\beta, e', W'', \Sigma, \Sigma', m') \in [\![A^p]\!]^{\mathcal{A}}_E$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(e_\beta, e', \Sigma, \Sigma', m') \in [\![B^{p'}]\!]^{\mathcal{A}}_E$. We get this from the second induction hypothesis.

C. $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega;\Sigma_2'} e_2', S_2' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![A^p]\!]^{\mathcal{A}}_E) \end{array} \right\}$ In this case it suffices to show
$(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega;\Sigma_2'} e_2', S_2' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![B^{p'}]\!]^{\mathcal{A}}_E) \end{array} \right\}$
By assumption e' is not a value. So let $\omega, e_\beta', S_2', \Sigma_2'$ such that

- $e', \Sigma_2, S_2 \succ e_\beta', S_2', \omega, \Sigma_2'$

From our assumption we get

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e, e'_\beta, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![A^p]\!]^{\mathcal{A}}_E$

It suffices to show the following:

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(e, e'_\beta, \Sigma, \Sigma', \mathfrak{m}') \in [\![B^{p'}]\!]^{\mathcal{A}}_E$. We get this from the second induction hypothesis.

ii. $(e, e', W, \Sigma, \Sigma', \mathfrak{m}) \in \left\{(v, v', W, \Sigma_{c_1}, \Sigma_{c_2}, \mathfrak{m}) \,\middle|\, (v, v', W, \mathfrak{m}) \in [\![A^p]\!]^{\mathcal{A}}_{\mathcal{V}}\right\}$. In this case e and e' are values v and v' respectively and

- $(v, v', W, \mathfrak{m}) \in [\![A^p]\!]^{\mathcal{A}}_{\mathcal{V}}$

There are two cases:

A. $p' \sqsubseteq \mathcal{A}$. In this case it suffices to show

- $(v, v', W, \mathfrak{m}) \in [\![B]\!]^{\mathcal{A}}_{\mathcal{V}}$

. Because $p \sqsubseteq p'$, we have $p \sqsubseteq \mathcal{A}$ by transitivity (Lemma 4.1). Hence

- $(v, v', W, \mathfrak{m}) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$

We get $(v, v', W, \mathfrak{m}) \in [\![B]\!]^{\mathcal{A}}_{\mathcal{V}}$ by the first induction.

B. $p' \not\sqsubseteq \mathcal{A}$. We have

- $(v, W.\theta_1, \mathfrak{m}) \in \lceil A \rceil_{\mathcal{V}}$ and
- $(v', W.\theta_2, \mathfrak{m}) \in \lceil A \rceil_{\mathcal{V}}$

by Lemma 8.22 and the definition of $[\![A^p]\!]^{\mathcal{A}}_{\mathcal{V}}$. In this case by Lemma 8.6 also

- $(v, W.\theta_1, \mathfrak{m}) \in \lceil B \rceil_{\mathcal{V}}$
- $(v', W.\theta_2, \mathfrak{m}) \in \lceil B \rceil_{\mathcal{V}}$

Because $p' \not\sqsubseteq \mathcal{A}$ this suffices to show the goal.

□

Lemma 8.32. If $(\gamma, W, \mathfrak{m}) \in [\![\Gamma]\!]^{\mathcal{A}}_{\mathcal{V}}$, then $(\gamma_1, W.\theta_1, \mathfrak{m}) \in \lceil \Gamma \rceil_{\mathcal{V}}$ and $(\gamma_2, W.\theta_2, \mathfrak{m}) \in \lceil \Gamma \rceil_{\mathcal{V}}$.

Proof. Let $(\gamma, W, \mathfrak{m}) \in [\![\Gamma]\!]^{\mathcal{A}}_{\mathcal{V}}$. We have to show

- $(\gamma_1, W.\theta_1, \mathfrak{m}) \in \lceil \Gamma \rceil_{\mathcal{V}}$. We have to show
  - $\mathtt{dom}(\Gamma) \subseteq \mathtt{dom}(\gamma_1)$. Because $(\gamma, W, \mathfrak{m}) \in [\![\Gamma]\!]^{\mathcal{A}}_{E}$ we know $\mathtt{dom}(\Gamma) \subseteq \mathtt{dom}(\gamma) = \mathtt{dom}(\gamma_1) \cap \mathtt{dom}(\gamma_2) \subseteq \mathtt{dom}(\gamma_1)$.
  - $\forall x \in \mathtt{dom}(\Gamma).(\gamma_1(x), W.\theta_1, \mathfrak{m}) \in \lceil \Gamma(x) \rceil_{\mathcal{V}}$. Let $x \in \mathtt{dom}(\Gamma)$. Then, because $(\gamma, W, \mathfrak{m}) \in [\![\Gamma]\!]^{\mathcal{A}}_{E}$, we have $(\gamma_1(x), \gamma_2(x), W, \mathfrak{m}) \in [\![\Gamma(x)]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.22 $(\gamma_1(x), W.\theta_1, \mathfrak{m}) \in \lceil \Gamma(x) \rceil_{\mathcal{V}}$.
- $(\gamma_2, W.\theta_2, \mathfrak{m}) \in \lceil \Gamma \rceil_{\mathcal{V}}$. Analogous to the previous case.

□

Lemma 8.33. $((\Sigma_1 \cup \Sigma_2))_{\mathcal{A}} = ((\Sigma_1))_{\mathcal{A}} \cup (\Sigma_2)_{\mathcal{A}}$.

Proof. $\sqsubseteq$: Let $\sigma \in (\Sigma_1 \cup \Sigma_2)_{\mathcal{A}}$. Then

- $\mathtt{pol}(\sigma) \sqsubseteq \mathcal{A}$ and
- $\sigma \in \Sigma_1 \cup \Sigma_2$.

If $\sigma \in \Sigma_1$, then $\sigma \in (\Sigma_1)_{\mathcal{A}}$ and hence $\sigma \in (\Sigma_1)_{\mathcal{A}} \cup (\Sigma_2)_{\mathcal{A}}$. Alternatively if $\sigma \in \Sigma_2$, then $\sigma \in (\Sigma_2)_{\mathcal{A}}$ and hence $\sigma \in (\Sigma_1)_{\mathcal{A}} \cup (\Sigma_2)_{\mathcal{A}}$.

$\sqsupseteq$: Let $\sigma \in (\Sigma_1)_{\mathcal{A}} \cup (\Sigma_2)_{\mathcal{A}}$. There are two cases:

1. $\sigma \in (\Sigma_1)_{\mathcal{A}}$: Then
   - $\sigma \in \Sigma_1$
   - $\mathtt{pol}(\sigma) \sqsubseteq \mathcal{A}$.

Then also $\sigma \in \Sigma_1 \cup \Sigma_2$ and hence $\sigma \in (\Sigma_1 \cup \Sigma_2)_{\mathcal{A}}$.

2. $\sigma \in (\Sigma_1)_{\mathcal{A}}$: Then
   - $\sigma \in \Sigma_2$
   - $\mathtt{pol}(\sigma) \sqsubseteq \mathcal{A}$.

   Then also $\sigma \in \Sigma_1 \cup \Sigma_2$ and hence $\sigma \in (\Sigma_1 \cup \Sigma_2)_{\mathcal{A}}$.

□

8.4 Fundamental lemma for the binary relation

Lemma 8.34. If $(e, e', W, \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ and $\Sigma \approx_{\mathcal{A}} \Sigma'$, then $(e \text{ then unopen } \sigma, e' \text{ then unopen } \sigma, W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.

Proof. By induction on m. It suffices to show $(\mathtt{opened}\ \sigma\ \mathtt{in}\ e, \mathtt{opened}\ \sigma\ \mathtt{in}\ e', W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We already know $\Sigma \approx_{\mathcal{A}} \Sigma'$. Let Σ_1, Σ_2 such that

- $\Sigma_1 \supseteq \Sigma$,
- $\Sigma_2 \supseteq \Sigma'$,
- $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

W', m' such that

- $m' < m$,
- $W' \sqsupseteq W$,

and S_1, S_2 such that

- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

There are two cases:

1. $(e, e', W, \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. Clearly the following is true:
   - $\Sigma_1 \cup \{\sigma\} \supseteq \Sigma \cup \{\sigma\}$,
   - $\Sigma_2 \cup \{\sigma\} \supseteq \Sigma' \cup \{\sigma\}$ and
   - $\Sigma_1 \cup \{\sigma\} \approx_{\mathcal{A}} \Sigma_2 \cup \{\sigma\}$.

   Hence there are three further options:

   (a) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \cup \{\sigma\} \vdash e_1,\ S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\ S_1' \wedge \\ \Sigma_2 \cup \{\sigma\} \vdash e_2,\ S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\ S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''. W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$

   In this case it is suffices to show

   $(\mathtt{opened}\ \sigma\ \mathtt{in}\ e, \mathtt{opened}\ \sigma\ \mathtt{in}\ e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\ S_1' \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\ S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''. W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$

   It is clear that neither $\mathtt{opened}\ \sigma\ \mathtt{in}\ e$ nor $\mathtt{opened}\ \sigma\ \mathtt{in}\ e'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that
   - $\mathtt{opened}\ \sigma\ \mathtt{in}\ e, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

- $\mathtt{opened}\ \sigma\ \mathtt{in}\ e', \Sigma_2, S_2 \succ e'_\beta, S'_2, \omega', \Sigma'_2$

By assumption neither e nor e' is a value. Hence the reductions must have happened with **Eopened**. Hence by inversion

- $e, \Sigma_1 \cup \{\sigma\}, S_1 \succ e_0, S'_1, \omega, \Sigma'_1$
- $e', \Sigma_2 \cup \{\sigma\}, S_2 \succ e'_0, S'_2, \omega', \Sigma'_2$
- $e_\beta = \mathtt{opened}\ \sigma\ \mathtt{in}\ e_0$
- $e'_\beta = \mathtt{opened}\ \sigma\ \mathtt{in}\ e'_0$

Hence we know

- $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma'_1 \sqsubseteq \mathcal{A} \ \vee\ \Sigma'_2 \sqsubseteq \mathcal{A} \to \exists W''.W'' \sqsupseteq W' \wedge (S'_1, S'_2, m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \ \wedge\ (e_0, e'_0, W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, m') \in [\![\tau]\!]^{\mathcal{A}}_E$

It suffices to show the following:

- $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma'_1 \sqsubseteq \mathcal{A} \ \vee\ \Sigma'_2 \sqsubseteq \mathcal{A} \to \exists W''.W'' \sqsupseteq W' \wedge (S'_1, S'_2, m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \ \wedge\ (\mathtt{opened}\ \sigma\ \mathtt{in}\ e_0, \mathtt{opened}\ \sigma\ \mathtt{in}\ e'_0, W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E$.
  Let $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega'$ or $\Sigma'_1 \sqsubseteq \mathcal{A}$ or $\Sigma'_2 \sqsubseteq \mathcal{A}$. This directly gives us a W'' such that
  - $W'' \sqsupseteq W'$,
  - $(S'_1, S'_2, m') \overset{\mathcal{A}}{\triangleright} W''$,
  - $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
  - $(e_0, e'_0, W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, m') \in [\![\tau]\!]^{\mathcal{A}}_E$

  It suffices to show
  - $W'' \sqsupseteq W'$. We already know that.
  - $(S'_1, S'_2, m') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
  - $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
  - $(\mathtt{opened}\ \sigma\ \mathtt{in}\ e_0, \mathtt{opened}\ \sigma\ \mathtt{in}\ e'_0, W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E$ We get this by induction.

(b) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e'_1, S'_1, \Sigma'_1, \omega. \\ \Sigma_1 \cup \{\sigma\} \vdash e_1, S_1 \overset{\omega;\Sigma'_1}{\Longrightarrow} e'_1, S'_1 \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S'_1, S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e'_1, e_2, W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, m') \in [\![\tau]\!]^{\mathcal{A}}_E) \end{array} \right\}$

In this case it suffices to show

$(\mathtt{opened}\ \sigma\ \mathtt{in}\ e, \mathtt{opened}\ \sigma\ \mathtt{in}\ e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e'_1, S'_1, \Sigma'_1, \omega. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma'_1}{\Longrightarrow} e'_1, S'_1 \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S'_1, S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e'_1, e_2, W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E) \end{array} \right\}$

It is clear that $\mathtt{opened}\ \sigma\ \mathtt{in}\ e$ is not a value. So let $\omega, e_\beta, \Sigma'_1, S'_1$ such that

- $\mathtt{opened}\ \sigma\ \mathtt{in}\ e, \Sigma_1, S_1 \succ e_\beta, S'_1, \omega, \Sigma'_1$

By assumption e is not a value. Hence the reduction must have happened with **Eopened**. By inversion

- $e, \Sigma_1 \cup \{\sigma\}, S_1 \succ e_0, S'_1, \omega, \Sigma'_1$
- $e_\beta = \mathtt{opened}\ \sigma\ \mathtt{in}\ e_0$

Hence

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S'_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_0, e', W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, m') \in [\![\tau]\!]^{\mathcal{A}}_E)$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S'_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.

- $(\texttt{opened}\ \sigma\ \texttt{in}\ e_0, \texttt{opened}\ \sigma\ \texttt{in}\ e', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this using the induction hypothesis.

(c) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \cup \{\sigma\} \vdash e_2,\ S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\ S_2' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

In this case it suffices to show

$(\texttt{opened}\ \sigma\ \texttt{in}\ e, \texttt{opened}\ \sigma\ \texttt{in}\ e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\ S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\ S_2' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

It is clear that $\texttt{opened}\ \sigma\ \texttt{in}\ e'$ is not a value. So let $\omega', e_\beta', \Sigma_2', S_2'$ such that

- $\texttt{opened}\ \sigma\ \texttt{in}\ e', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

By assumption e' is not a value. Hence the reduction must have happened with **Eopened**. By inversion

- $e', \Sigma_2 \cup \{\sigma\}, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
- $e_\beta' = \texttt{opened}\ \sigma\ \texttt{in}\ e_0'$

Clearly $\Sigma_2 \cup \{\sigma\} \supseteq \Sigma' \cup \{\sigma\}$. Hence

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e, e_0', W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}})$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\texttt{opened}\ \sigma\ \texttt{in}\ e, \texttt{opened}\ \sigma\ \texttt{in}\ e_0', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this using the induction hypothesis.

2. $(e, e', W, \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}) \in \left\{ (\nu, \nu', W, \Sigma_{c_1}, \Sigma_{c_2}, \mathfrak{m}) \;\middle|\; (\nu, \nu', W, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}} \right\}$
In particular this means that there are ν, ν' such that $e = \nu$ and $e' = \nu'$. In this case it suffices to show

$(\texttt{opened}\ \sigma\ \texttt{in}\ \nu, \texttt{opened}\ \sigma\ \texttt{in}\ \nu') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\ S_1' \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\ S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''. W'' \sqsupseteq W' \wedge\ (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W'',\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$

It is clear that neither $\texttt{opened}\ \sigma\ \texttt{in}\ \nu$ nor $\texttt{opened}\ \sigma\ \texttt{in}\ \nu'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $\texttt{opened}\ \sigma\ \texttt{in}\ \nu, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $\texttt{opened}\ \sigma\ \texttt{in}\ \nu', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

By assumption both e nor e' are values ν and ν', respectively. Hence the reductions must have happened with **EopenedBeta**. Consequently

- $e_\beta = \nu$
- $e_\beta' = \nu'$
- $S_1' = S_1$

- $S_2' = S_2$
- $\omega = \mathfrak{unopen}(\sigma) = \omega'$
- $\Sigma_1' = \Sigma_1$
- $\Sigma_2' = \Sigma_2$

Hence the reductions are really

- $\mathsf{opened}\ \sigma\ \mathsf{in}\ \nu, \Sigma_1, S_1 \succ \nu, S_1, \mathfrak{unopen}(\sigma), \Sigma_1$
- $\mathsf{opened}\ \sigma\ \mathsf{in}\ \nu', \Sigma_2, S_2 \succ \nu', S_2, \mathfrak{unopen}(\sigma), \Sigma_2$

It suffices to show

- $\mathfrak{unopen}(\sigma) \approx^{\mathcal{A}}_{W'.\beta} \mathfrak{unopen}(\sigma) \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A} \to \exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \mathfrak{unopen}(\sigma) \approx^{\mathcal{A}}_{W''.\beta} \mathfrak{unopen}(\sigma) \wedge (\nu, \nu', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E}$. It suffices to show the conclusion. In particular it suffices to show
  - $W' \sqsupseteq W'$. We get this by Lemma 7.2.
  - $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. We already know this.
  - $\mathfrak{unopen}(\sigma) \approx^{\mathcal{A}}_{W'.\beta} \mathfrak{unopen}(\sigma)$. We get this with **refl**.
  - $(\nu, \nu', W', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E}$. We already know $(\nu, \nu', W, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.24 and Lemma 8.25 we get $(\nu, \nu', W', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$ which implies the subgoal.

□

Lemma 8.35. If $(e, e', W, \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$ and $\Sigma \approx_{\mathcal{A}} \Sigma'$, then $(\mathsf{open}\ \sigma\ \mathsf{in}\ e, \mathsf{open}\ \sigma\ \mathsf{in}\ e', W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$.

Proof. To show this it is sufficient to show $(\mathsf{open}\ \sigma\ \mathsf{in}\ e, \mathsf{open}\ \sigma\ \mathsf{in}\ e', W, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{E_\beta}$. We already know $\Sigma \approx_{\mathcal{A}} \Sigma'$. Let Σ_1, Σ_2 such that

- $\Sigma_1 \supseteq \Sigma$,
- $\Sigma_2 \supseteq \Sigma'$,
- $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

W', m' such that

- $m' < m$,
- $W' \sqsupseteq W$,

and S_1, S_2 such that

- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

. It suffices to show

$$(\mathsf{open}\ \sigma\ \mathsf{in}\ e, \mathsf{open}\ \sigma\ \mathsf{in}\ e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma_1'} e_1', S_1' \wedge \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega';\Sigma_2'} e_2', S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E} \end{array} \right\}$$

It is clear that neither $\mathsf{open}\ \sigma\ \mathsf{in}\ e$ nor $\mathsf{open}\ \sigma\ \mathsf{in}\ e'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $\mathsf{open}\ \sigma\ \mathsf{in}\ e, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $\mathsf{open}\ \sigma\ \mathsf{in}\ e', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

The reduction must have happened with **Eopen**. Consequently

- $e_\beta = \mathsf{opened}\ \sigma\ \mathsf{in}\ e$

- $e'_\beta = \mathsf{opened}\ \sigma\ \mathsf{in}\ e'$
- $S'_1 = S_1$
- $S'_2 = S_2$
- $\omega = \mathsf{open}(\sigma) = \omega'$
- $\Sigma'_1 = \Sigma_1$
- $\Sigma'_2 = \Sigma_2$

Hence the reductions are really

- $\mathsf{open}\ \sigma\ \mathsf{in}\ e, \Sigma_1, S_1 \succ \mathsf{opened}\ \sigma\ \mathsf{in}\ e, S_1, \mathsf{open}(\sigma), \Sigma_1$
- $\mathsf{open}\ \sigma\ \mathsf{in}\ v', \Sigma_2, S_2 \succ \mathsf{opened}\ \sigma\ \mathsf{in}\ e', S_2, \mathsf{open}(\sigma), \Sigma_2$

It suffices to show

- $\mathsf{open}(\sigma) \approx^{\mathcal{A}}_{W'.\beta} \mathsf{open}(\sigma) \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A} \to \exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \mathsf{open}(\sigma) \approx^{\mathcal{A}}_{W''.\beta} \mathsf{open}(\sigma) \wedge$
  $(\mathsf{opened}\ \sigma\ \mathsf{in}\ e, \mathsf{opened}\ \sigma\ \mathsf{in}\ e', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. It suffices to show the conclusion. In particular it suffices to show
  - $W' \sqsupseteq W'$. We get this by Lemma 7.2.
  - $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. We already know this.
  - $\mathsf{open}(\sigma) \approx^{\mathcal{A}}_{W'.\beta} \mathsf{open}(\sigma)$. We get this with **refl**.
  - $(\mathsf{opened}\ \sigma\ \mathsf{in}\ e, \mathsf{opened}\ \sigma\ \mathsf{in}\ e', W', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. By assumption we have $(e, e', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, W, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. By Lemma 8.24 and Lemma 8.25 this gives us $(e, e', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, W', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get the remaining subgoal with Lemma 8.34.

□

Lemma 8.36. If $(e_1, e'_1, W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}$ and $(e_2, e'_2, W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}}$, then $((e_1, e_2), (e'_1, e'_2), W, \Sigma, \Sigma', \mathfrak{m}) \in [\![(\tau_1 \times \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$.

Proof. By induction on $\mathfrak{m}$. There are two cases:

1. $(e_1, e'_1, W, \Sigma, \Sigma' \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. In this case it suffices to show $((e_1, e_2), (e'_1, e'_2), W, \Sigma, \Sigma' \mathfrak{m}) \in [\![(\tau_1 \times \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. We get $\Sigma \approx_{\mathcal{A}} \Sigma'$ from $(e_1, e'_1, W, \Sigma, \Sigma' \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. Let Σ_1, Σ_2 such that
   - $\Sigma_1 \supseteq \Sigma$,
   - $\Sigma_2 \supseteq \Sigma'$,
   - $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

   $W', \mathfrak{m}'$ such that
   - $\mathfrak{m}' < \mathfrak{m}$,
   - $W' \sqsupseteq W$,

   and S_1, S_2 such that
   - $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$.

   . There are three further cases

$$\text{(a)}\ (e_1, e'_1) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V}\ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e'_1, S'_1, \Sigma'_1, \omega, e'_2, \Sigma'_2, S'_2, \omega'. \\ \Sigma_1 \vdash e_1, S_1 \xrightarrow{\omega; \Sigma'_1} e'_1, S'_1 \wedge \\ \Sigma_2 \vdash e_2, S_2 \xrightarrow{\omega'; \Sigma'_2} e'_2, S'_2 \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma'_1 \sqsubseteq \mathcal{A} \vee \Sigma'_2 \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S'_1, S'_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e'_1, e'_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$$

In that case it suffices to show

$$((e_1,e_2),(e_1',e_2')) \in \left\{ (e_1,e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\, S_1' \wedge \\ \Sigma_2 \vdash e_2,\, S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2',\, S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge\; (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$$

By assumption neither e_1, nor e_1' is a value. Hence (e_1,e_2) and (e_1',e_2') also are not values. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $(e_1,e_2), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $(e_1',e_2'), \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Since neither e_1 nor e_1' is a value, the reductions must have happened with **EPairl**. Hence by inversion

- $e_1, \Sigma_1, S_1 \succ e_l, S_1', \omega, \Sigma_1'$
- $e', \Sigma_2, S_2 \succ e_l', S_2', \omega', \Sigma_2'$
- $e_\beta = (e_l, e_2)$
- $e_\beta' = (e_l', e_2')$

Also let $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \;\vee\; \Sigma_2' \sqsubseteq \mathcal{A}$. We know there is a W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$
- $(e_l, e_l', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}$

It suffice to show the following:

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
- $((e_l,e_2),(e_l',e_2'), W'', \Sigma, \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$ We have $W'' \sqsupseteq W$ by transitivity (Lemma 7.2). Hence we also have $(e_2, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}}$ by Lemma 8.29. We get the claim by induction.

(b) $$(e_1,e_1') \in \left\{ (e_1,e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\, S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$$

In this case it suffices to show $((e_1,e_2),(e_1',e_2')) \in$

$$\left\{ (e_1,e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\, S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}.$$

By assumption e_1 is not a value. Hence (e_1,e_2) also is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $(e_1,e_2), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

By assumption e_1 is not a value. Hence the reduction must have happened with **EPairl**. By inversion

- $e_1, \Sigma_1, S_1 \succ e_l, S_1', \omega, \Sigma_1'$
- $e_\beta = (e_l, e_2)$

From our assumption we get

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_\iota, e_1', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}})$

It suffices to show the following:

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $((e_\iota, e_2), (e_1', e_2'), \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^\perp]\!]^{\mathcal{A}}_{\mathsf{E}}$. We know $(e_\iota, e_1', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}})$. We get $(e_2, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}}$ by Lemma 8.29. The goal follows using the induction hypothesis.

(c) $(e_1, e_1') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

In this case it suffices to show $((e_1, e_2), (e_1', e_2')) \in$
$\left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^\perp]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

By assumption e_1' is not a value. Hence (e_1', e_2') also is not a value. So let $\omega, e_\beta', \Sigma_2', S_2'$ such that

- $(e_1', e_2'), \Sigma_2, S_2 \succ e_\beta', S_2', \omega, \Sigma_2'$

By assumption e_1' is not a value. Hence the reduction must have happened with **EPairl**. By inversion

- $e_1', \Sigma_2, S_2 \succ e_1', S_2', \omega, \Sigma_2'$
- $e_\beta' = (e_\iota', e_2')$

From our assumption we get

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_1, e_\iota', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}})$

It suffices to show the following:

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $((e_1, e_2), (e_\iota', e_2'), \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^\perp]\!]^{\mathcal{A}}_{\mathsf{E}}$. We know $(e_1, e_\iota', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}})$. We get $(e_2, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}}$ by Lemma 8.29. The goal follows using the induction hypothesis.

2. $(e_1, e_1', W, \Sigma, \Sigma', \mathfrak{m}) \in \left\{ (v, v', W, \Sigma_1, \Sigma_2, \mathfrak{m}) \;\middle|\; (v, v', W, \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}} \right\}$

Hence e_1 and e_1' are values v_1 and v_1', respectively, and $(v_1, v_1', W, \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$. There are two further cases:

(a) $(e_2, e_2', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. In this case it suffices to show $((v_1, e_2), (v_1', e_2'), W, \Sigma, \Sigma' \mathfrak{m}) \in [\![(\tau_1 \times \tau_2)^\perp]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. We get $\Sigma \approx_{\mathcal{A}} \Sigma'$ from $(e_2, e_2', W, \Sigma, \Sigma' \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. Let Σ_1, Σ_2 such that

- $\Sigma_1 \supseteq \Sigma$,
- $\Sigma_2 \supseteq \Sigma'$,
- $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

$W', \mathfrak{m}'$ such that

- $\mathfrak{m}' < \mathfrak{m}$,
- $W' \sqsupseteq W$,

and S_1, S_2 such that

- $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$.

There are three further cases:

i. $(e_2, e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\, S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge\; (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$

In that case it suffices to show

$((v_1, e_2), (v_1', e_2')) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\, S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge\; (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$

By assumption neither e_2, nor e_2' is a value. Hence (v_1, e_2) and (v_1', e_2') also are not values. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $(v_1, e_2), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $(v_1', e_2'), \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Since v_1 and v_1' is are values but e_2 and e_2' are not, the reductions must have happened with **EPairr**. Hence by inversion

- $e_2, \Sigma_1, S_1 \succ e_r, S_1', \omega, \Sigma_1'$
- $e', \Sigma_2, S_2 \succ e_r', S_2', \omega', \Sigma_2'$
- $e_\beta = (v_1, e_r)$
- $e_\beta' = (v_1', e_r')$

Also let $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \;\vee\; \Sigma_2' \sqsubseteq \mathcal{A}$. Then there is a W'' such that

- $W'' \sqsupseteq W'$,
- $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
- $(e_r, e_r', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}}$

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
- $((v_1, e_r), (v_2', e_r'), W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$ We have $W'' \sqsupseteq W$ by transitivity (Lemma 7.2). Hence we also have $(v_1, v_1', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}$ by Lemma 8.29. We get the claim by induction.

ii. $(e_2, e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

In this case it suffices to show

$$((v_1, e_2), (v_1', e_2')) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^{\perp}]\!]_{\mathsf{E}}^{\mathcal{A}}) \end{array} \right\}$$

By assumption e_2 is not a value. Hence (v_1, e_2) is not a value, either. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $(v_1, e_2), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

By assumption v_1 is a value but e_2 is not Hence the reduction must have happened with **EPairr**. By inversion

- $e_2, \Sigma_1, S_1 \succ e_r, S_1', \omega, \Sigma_1'$
- $e_\beta = (v_1, e_r)$

From our assumption we get

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_r, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]_{\mathsf{E}}^{\mathcal{A}})$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $((v_1, e_r), (v_1', e_2'), \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^{\perp}]\!]_{\mathsf{E}}^{\mathcal{A}}$. We know $(e_r, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]_{\mathsf{E}}^{\mathcal{A}})$. We get $(v_1, v_1', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]_{\mathsf{E}}^{\mathcal{A}}$ by Lemma 8.29. The goal follows using the induction hypothesis.

iii. $$(e_2, e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]_{\mathsf{E}}^{\mathcal{A}}) \end{array} \right\}$$

In this case it suffices to show $((v_1, e_2), (v_1', e_2')) \in$

$$\left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^{\perp}]\!]_{\mathsf{E}}^{\mathcal{A}}) \end{array} \right\}$$

By assumption e_2' is not a value. Hence (v_1', e_2') also is not a value. So let $\omega, e_r', \Sigma_2', S_2'$ such that

- $(v_1', e_2'), \Sigma_2, S_2 \succ e_\beta', S_2', \omega, \Sigma_2'$

By assumption v_1' is a value but e_2' is not. Hence the reduction must have happened with **EPairr**. By inversion

- $e_2', \Sigma_2, S_2 \succ e_r', S_2', \omega, \Sigma_2'$
- $e_\beta' = (v_1', e_r')$

From our assumption we get

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_2, e_r', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]_{\mathsf{E}}^{\mathcal{A}})$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.

- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $((v_1, e_2), (v_1', e_r'), \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^{\perp}]\!]^{\mathcal{A}}_{E}$. We know $(e_2, e_r', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_{E}$. We get $(v_1, v_1', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{E}$ by Lemma 8.29. The goal follows using the induction hypothesis.

(b) $(e_2, e_2', W, \Sigma, \Sigma', \mathfrak{m}) \in \{(v, v', W, \Sigma_{c_1}, \Sigma_{c_2}, , \mathfrak{m}) \mid (v, v', W, \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}\}$

In this case e_2 and e_2' are values v_2 and v_2', respectively, and $(v_2, v_2', W, \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$. It suffices to show $((v_1, v_2), (v_1', v_2'), W, \mathfrak{m}) \in [\![(\tau_1 \times \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\perp \sqsubseteq \mathcal{A}$ (Lemma 4.19), it suffices to show $((v_1, v_2), (v_1', v_2'), W, \mathfrak{m}) \in [\![\tau_1 \times \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$. To show this we need to show $(v_1, v_1', W, \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$ and $(v_2, v_2', W, \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$ both of which we have already.

□

Lemma 8.37. If $(e_1, e_1', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![(\tau_1 \xrightarrow{\Sigma_m, p} \tau_2)^q]\!]^{\mathcal{A}}_{E}$ and $(e_2, e_2', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{E}$ and $\Sigma \supseteq \Sigma_m \subseteq \Sigma'$ and $q \sqsubseteq p$, $q \sqsubseteq \tau_2$ and $\Sigma \approx_{\mathcal{A}} \Sigma'$, then $(e_1\ e_2, e_1'\ e_2', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{E}$.

Proof. By induction on $\mathfrak{m}$. It suffices to show $(e_1\ e_2, e_1'\ e_2', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{E_\beta}$. We already have $\Sigma \approx_{\mathcal{A}} \Sigma'$ by assumption. Let Σ_1, Σ_2 such that

- $\Sigma_1 \supseteq \Sigma$,
- $\Sigma_2 \supseteq \Sigma'$,
- $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

$W', \mathfrak{m}'$ such that

- $\mathfrak{m}' < \mathfrak{m}$,
- $W' \sqsupseteq W$,

and S_1, S_2 such that

- $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$.

There are two cases

1. $(e_1, e_1', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![(\tau_1 \overset{\Sigma_m; p}{\to} \tau_2)^q]\!]^{\mathcal{A}}_{E_\beta}$. There are three further cases:

(a) $(e_1, e_1') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \overset{\omega; \Sigma_1'}{\Longrightarrow} e_1',\ S_1' \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \overset{\omega'; \Sigma_2'}{\Longrightarrow} e_2',\ S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \overset{\Sigma_m; p}{\to} \tau_2)^q]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

In that case it suffices to show

$(e_1\ e_2, e_1'\ e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \overset{\omega; \Sigma_1'}{\Longrightarrow} e_1',\ S_1' \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \overset{\omega'; \Sigma_2'}{\Longrightarrow} e_2',\ S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

Neither $e_1\ e_2$ nor $e_1'\ e_2'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $e_1\ e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $e_1'\ e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Since neither e_1 nor e_1' is a value and therefore also not a function, the reductions must have happened with **EAppl**. Hence by inversion

- $e_1, \Sigma_1, S_1 \succ e_\iota, S_1', \omega, \Sigma_1'$
- $e_1', \Sigma_2, S_2 \succ e_\iota', S_2', \omega', \Sigma_2'$
- $e_\beta = e_\iota\ e_2$
- $e_\beta' = e_\iota'\ e_2'$

Also let $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \ \vee \ \Sigma_2' \sqsubseteq \mathcal{A}$. This directly gives us a W'' such that

- $W'' \sqsupseteq W'$,
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
- $(e_\iota, e_\iota', W'', \Sigma, \Sigma', m') \in [\![(\tau_1 \overset{\Sigma_m;p}{\to} \tau_2)^q]\!]^{\mathcal{A}}_E$

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
- $(e_\iota\ e_2, e_\iota'\ e_2', W'', \Sigma, \Sigma', m') \in [\![\tau_2]\!]^{\mathcal{A}}_E$ We have $W'' \sqsupseteq W$ by transitivity (Lemma 7.2). Hence we also have $(e_2, e_2', W'', \Sigma, \Sigma', m') \in [\![\tau_1]\!]^{\mathcal{A}}_E$ by Lemma 8.29. We get the claim by induction.

(b) $$(e_1, e_1') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\ S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\ S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![(\tau_1 \overset{\Sigma_m;p}{\to} \tau_2)^q]\!]^{\mathcal{A}}_E) \end{array} \right\}$$

In this case it suffices to show

$$(e_1\ e_2, e_1'\ e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\ S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\ S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![\tau_2]\!]^{\mathcal{A}}_E) \end{array} \right\}$$

It is clear that $e_1\ e_2$ is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $e_1\ e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

By assumption e_1 is not a value and therefore also not a λ-expression. Hence the reduction must have happened with **EAppl**. By inversion

- $e_1, \Sigma_1, S_1 \succ e_\iota, S_1', \omega, \Sigma_1'$
- $e_\beta = e_\iota\ e_2$

From our assumption we get

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_\iota, e_1', W'', \Sigma, \Sigma', m') \in [\![(\tau_1 \overset{\Sigma_m;p}{\to} \tau_2)^q]\!]^{\mathcal{A}}_E$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(e_\iota\ e_2, e_1'\ e_2', \Sigma, \Sigma', m') \in [\![\tau_2]\!]^{\mathcal{A}}_E$. We know $(e_\iota, e_1', W'', \Sigma, \Sigma', m') \in [\![(\tau_1 \overset{\Sigma_m;p}{\to} \tau_2)^q]\!]^{\mathcal{A}}_E$. We get $(e_2, e_2', W'', \Sigma, \Sigma', m') \in [\![\tau_1]\!]^{\mathcal{A}}_E$ by Lemma 8.29. The goal follows using the induction hypothesis.

(c) $$(e_1, e_1') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\ S_2 \overset{\omega;\Sigma_2'}{\Longrightarrow} e_2',\ S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![(\tau_1 \overset{\Sigma_m;p}{\to} \tau_2)^q]\!]^{\mathcal{A}}_E) \end{array} \right\}$$

In this case it suffices to show $(e_1\ e_2, e_1'\ e_2') \in$

$$\left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\ S_2 \xrightarrow{\omega;\Sigma_2'} e_2',\ S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathrm{E}}) \end{array} \right\}$$

Clearly $e_1'\ e_2'$ is not a value. So let $\omega, e_\beta', \Sigma_2', S_2'$ such that

- $e_1'\ e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega, \Sigma_2'$

By assumption e_1' is not a value and therefore also not a λ-expression. Hence the reduction must have happened with **EAppl**. By inversion

- $e_1', \Sigma_2, S_2 \succ e_l', S_2', \omega, \Sigma_2'$
- $e_\beta' = e_l'\ e_2'$

From our assumption we get

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_1, e_l', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \overset{\Sigma_{\mathfrak{m}};p}{\to} \tau_2)^q]\!]^{\mathcal{A}}_{\mathrm{E}}$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(e_1\ e_2, e_l'\ e_2', \Sigma, \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathrm{E}}$. We know $(e_1, e_l', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \overset{\Sigma_{\mathfrak{m}};p}{\to} \tau_2)^q]\!]^{\mathcal{A}}_{\mathrm{E}}$. We get $(e_2, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathrm{E}}$ by Lemma 8.29. The goal follows using the induction hypothesis.

2. $(e_1, e_1', W, \Sigma, \Sigma', \mathfrak{m}) \in \left\{ (v, v', W, \Sigma_{c_1}, \Sigma_{c_2}, \mathfrak{m}) \;\middle|\; (v, v', W, \mathfrak{m}) \in [\![(\tau_1 \overset{\Sigma_{\mathfrak{m}};p}{\to} \tau_2)^q]\!]^{\mathcal{A}}_{\mathcal{V}} \right\}$

Hence e_1 and e_1' are values v_1 and v_1' respectively such that $(v_1, v_1', W, \mathfrak{m}) \in [\![(\tau_1 \overset{\Sigma_{\mathfrak{m}};p}{\to} \tau_2)^q]\!]^{\mathcal{A}}_{\mathcal{V}}$. Either $q \sqsubseteq \mathcal{A}$ or $q \not\sqsubseteq \mathcal{A}$. In the first case $(v_1, v_1', W, \mathfrak{m}) \in [\![\tau_1 \overset{\Sigma_{\mathfrak{m}};p}{\to} \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$ and in the second case both $(v_1, W.\theta_1, \mathfrak{m}) \in \lceil \tau_1 \overset{\Sigma_{\mathfrak{m}};p}{\to} \tau_2 \rceil_{\mathcal{V}}$ and $(v_1', W.\theta_2, \mathfrak{m}) \in \lceil \tau_1 \overset{\Sigma_{\mathfrak{m}};p}{\to} \tau_2 \rceil_{\mathcal{V}}$. In both cases this means that there are e_b and e_b' such that

- $e_1 = \lambda x.\ e_b$ and
- $e_1' = \lambda x.\ e_b'$.

There are again two cases

(a) $(e_2, e_2', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathrm{E}_\beta}$. There are three further cases:

i. $(e_2, e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \xrightarrow{\omega;\Sigma_1'} e_1',\ S_1' \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \xrightarrow{\omega';\Sigma_2'} e_2',\ S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge \ (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge \ (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathrm{E}} \end{array} \right\}$

In that case it suffices to show

$$((\lambda x.\ e_b)\ e_2, (\lambda x.\ e_b')\ e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\ S_1' \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\ S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau_2]\!]^{\mathcal{A}}_E \end{array} \right\}$$

Clearly $(\lambda x.\ e_b)\ e_2$ and $(\lambda x.\ e_b')\ e_2'$ are not values. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $(\lambda x.\ e_b)\ e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $(\lambda x.\ e_b')\ e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Since e_2 and e_2' are not values by assumption, the reductions must have happened with **EAppr**. Hence by inversion

- $e_2, \Sigma_1, S_1 \succ e_r, S_1', \omega, \Sigma_1'$
- $e_2', \Sigma_2, S_2 \succ e_r', S_2', \omega', \Sigma_2'$
- $e_\beta = (\lambda x.\ e_b)\ e_r$
- $e_\beta' = (\lambda x.\ e_b')\ e_r'$

Also let $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \ \vee\ \Sigma_2' \sqsubseteq \mathcal{A}$. This directly gives us a W'' such that

- $W'' \sqsupseteq W'$,
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
- $(e_r, e_r', W'', \Sigma, \Sigma', m') \in [\![\tau_1]\!]^{\mathcal{A}}_E$

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
- $((\lambda x.\ e_b)\ e_r, (\lambda x.\ e_b')\ e_r', W'', \Sigma, \Sigma', m') \in [\![\tau_2]\!]^{\mathcal{A}}_E$ We have $W'' \sqsupseteq W$ by transitivity (Lemma 7.2). Hence we also have $(\lambda x.\ e_b, \lambda x.\ e_b', W'', \Sigma, \Sigma', m') \in [\![(\tau_1 \overset{\Sigma_m;p}{\Rightarrow} \tau_2)^q]\!]^{\mathcal{A}}_E$ by Lemma 8.29. We get the claim by induction.

ii. $$(e_2, e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\ S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\ S_1' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![\tau_1]\!]^{\mathcal{A}}_E) \end{array} \right\}$$

In this case it suffices to show

$$((\lambda x.\ e_b)\ e_2, (\lambda x.\ e_b')\ e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\ S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\ S_1' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![\tau_2]\!]^{\mathcal{A}}_E) \end{array} \right\}$$

It is clear that $(\lambda x.\ e_b)\ e_2$ is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $(\lambda x.\ e_b)\ e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

Because e_2 is not a value the reduction must have happened with **EAppr**. By inversion

- $e_2, \Sigma_1, S_1 \succ e_r, S_1', \omega, \Sigma_1'$
- $e_\beta = (\lambda x.\ e_b)\ e_r$

From our assumption we get

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_r, e_2', W'', \Sigma, \Sigma', m') \in [\![\tau_1]\!]^{\mathcal{A}}_E)$

It suffices to show the following:

- $\neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $((\lambda x.\ e_b)\ e_r, (\lambda x.\ e_b')\ e_2', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_E$. We know $(e_r, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_E$. We get $(\lambda x.\ e_b, \lambda x.\ e_b', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \overset{\Sigma_m;p}{\to} \tau_2)^q]\!]^{\mathcal{A}}_E$ by Lemma 8.29. The goal follows using the induction hypothesis.

iii. $(e_2, e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\ S_2 \overset{\omega;\Sigma_2'}{\Longrightarrow} e_2',\ S_2' \to \neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_E) \end{array} \right\}$

In this case it suffices to show

$((\lambda x.\ e_b)\ e_2, (\lambda x.\ e_b')\ e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\ S_2 \overset{\omega;\Sigma_2'}{\Longrightarrow} e_2',\ S_2' \to \neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_E) \end{array} \right\}$

It is clear that $(\lambda x.\ e_b')\ e_2'$ is not a value. So let $\omega, e_\beta', \Sigma_2', S_2'$ such that

- $(\lambda x.\ e_b')\ e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega, \Sigma_2'$

Because e_2' is not a value, the reduction must have happened with **EAppr**. By inversion

- $e_2', \Sigma_2, S_2 \succ e_r', S_2', \omega, \Sigma_2'$
- $e_\beta' = (\lambda x.\ e_b')\ e_r'$

From our assumption we get

- $\neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_2, e_r', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_E)$

It suffices to show the following:

- $\neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $((\lambda x.\ e_b)\ e_2, (\lambda x.\ e_b')\ e_r', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_E$. We know $(e_2, e_r', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_E$. We get $(\lambda x.\ e_b, \lambda x.\ e_b', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \overset{\Sigma_m;p}{\to} \tau_2)^q]\!]^{\mathcal{A}}_E$ by Lemma 8.29. The goal follows using the induction hypothesis.

(b) $(e_2, e_2', W, \Sigma, \Sigma', \mathfrak{m}) \in \left\{ (v, v', W, \Sigma_c, \mathfrak{m}) \;\middle|\; (v, v', W, \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}} \right\}$

In this case e_2 and e_2' are values v_2 and v_2', respectively, such that $(v_2, v_2', W, \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$.

It suffices to show $((\lambda x.\ e_b)\ v_2, (\lambda x.\ e_b')\ v_2') \in$

$$\left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\ S_1' \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2',\ S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_E \end{array} \right\}$$

.

It is clear that both $(\lambda x.\ e_b)\ v_2$ and $(\lambda x.\ e_b')\ v_2'$ are not values. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $(\lambda x.\ e_b)\ v_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $(\lambda x.\ e_b')\ v_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Since v_2 and v_2' are values, the reductions must have happened with **EAppBeta**. Hence

- $e_\beta = [v_2/x]e_b$
- $e_\beta' = [v_2'/x]e_b'$
- $\omega = \epsilon = \omega'$
- $S_1' = S_1$
- $S_2' = S_2$
- $\Sigma_1' = \Sigma_1$
- $\Sigma_2' = \Sigma_2$

So the reductions are really

- $(\lambda x.\ e_b)\ v_2, \Sigma_1, S_1 \succ [v_2/x]e_b, S_1, \epsilon, \Sigma_1$
- $(\lambda x.\ e_b')\ v_2', \Sigma_2, S_2 \succ [v_2'/x]e_b', S_2, \epsilon, \Sigma_2$

Also let $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.
It suffices to show

- $W' \sqsupseteq W'$. We get this by Lemma 7.2.
- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. We already know this.
- $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon$. We get this with **refl**.
- $([v_2/x]e_b, [v_2'/x]e_b', W', \Sigma, \Sigma', m') \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_E$.
  By assumption $(v_2, v_2', W, m) \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_V$ and $W' \sqsupseteq W$. Hence by Lemma 8.24 and Lemma 8.25 also
  - $(v_2, v_2', W', m') \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_V$.

  There are two cases:
  i. $q \sqsubseteq \mathcal{A}$: In this case $(\lambda x.\ e_b, \lambda x.\ e_b', W, m) \in \llbracket \tau_1 \overset{\Sigma_m;p}{\to} \tau_2 \rrbracket^{\mathcal{A}}_V$. Because $W' \sqsupseteq W$, $m' < m$, $(v_2, v_2', W', m') \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_V$, $\Sigma \supseteq \Sigma_m \subseteq \Sigma'$ and $\Sigma \approx_{\mathcal{A}} \Sigma'$, this gives us
  - $([v_2/x]e_b, [v_2'/x]e_b', W', \Sigma, \Sigma', m') \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_E$.

  ii. $q \not\sqsubseteq \mathcal{A}$: In this case
  - $(\lambda x.\ e_b, W.\theta_1, m) \in \lceil \tau_1 \overset{\Sigma_m;p}{\to} \tau_2 \rceil_V$
  - $(\lambda x.\ e_b', W.\theta_2, m) \in \lceil \tau_1 \overset{\Sigma_m;p}{\to} \tau_2 \rceil_V$

  By Lemma 8.30 it suffices to show
  - $([v_2/x]e_b, W'.\theta_1, m') \in \lceil \tau_2 \rceil^p_E$.
    From $(v_2, v_2', W', m') \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_V$ we get
    ☞ $(v_2, W'.\theta_1, m') \in \lceil \tau_1 \rceil_V$
    by Lemma 8.22. Because $W' \sqsupseteq W$ we have
    ☞ $W'.\theta_1 \sqsupseteq W.\theta_1$
    in addition to
    ☞ $m' < m$
    which we know anyway. The goal follows directly from $(\lambda x.\ e_b, W.\theta_1, m) \in \lceil \tau_1 \overset{\Sigma_m;p}{\to} \tau_2 \rceil_V$.
  - $([v_2'/x]e_b', W''.\theta_2, m') \in \lceil \tau_2 \rceil^p_E$
    From $(v_2, v_2', W', m') \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_V$ we get
    ☞ $(v_2', W'.\theta_2, m') \in \lceil \tau_1 \rceil_V$
    by Lemma 8.22. Because $W' \sqsupseteq W$ we have
    ☞ $W'.\theta_2 \sqsupseteq W.\theta_2$
    in addition to
    ☞ $m' < m$
    which we know anyway. The goal follows directly from $(\lambda x.\ e_b', W.\theta_2, m) \in \lceil \tau_1 \overset{\Sigma_m;p}{\to} \tau_2 \rceil_V$.
  - $\tau_2 \not\sqsubseteq \mathcal{A}$. Assume $\tau_2 \sqsubseteq \mathcal{A}$. Because $q \sqsubseteq \tau_2$ we get $q \sqsubseteq \mathcal{A}$ by transitivity (Lemma 4.1). But $q \not\sqsubseteq \mathcal{A}$. ↯
  - $p \not\sqsubseteq \mathcal{A}$. Assume $p \sqsubseteq \mathcal{A}$. Because $q \sqsubseteq p$ we get $q \sqsubseteq \mathcal{A}$ by transitivity (Lemma 4.1). But $q \not\sqsubseteq \mathcal{A}$. ↯

□

Lemma 8.38. If $(e, e', W, \Sigma, \Sigma', m) \in \llbracket (\tau_1 \times \tau_2)^p \rrbracket^{\mathcal{A}}_E$, $\Sigma \approx_{\mathcal{A}} \Sigma'$ and $p \sqsubseteq \tau_1$, then $(\mathsf{fst}\,(e)\,, \mathsf{fst}\,(e')\,, W, \Sigma, \Sigma', m) \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_E$.

Proof. By induction on $\mathfrak{m}$. It suffices to show $(\mathsf{fst}(e), \mathsf{fst}(e'), W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{E_\beta}$. We already have $\Sigma \approx_{\mathcal{A}} \Sigma'$ by assumption. Let Σ_1, Σ_2 such that

- $\Sigma_1 \supseteq \Sigma$,
- $\Sigma_2 \supseteq \Sigma'$,
- $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

$W', \mathfrak{m}'$ such that

- $\mathfrak{m}' < \mathfrak{m}$,
- $W' \sqsupseteq W$,

and S_1, S_2 such that

- $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$.

There are two cases

1. $(e, e', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![(\tau_1 \times \tau_2)^p]\!]^{\mathcal{A}}_{E_\beta}$. In this case there are three further cases:

   (a) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma_1'} e_1', S_1' \;\wedge \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega';\Sigma_2'} e_2', S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''. W'' \sqsupseteq W' \wedge\; (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \;\wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^p]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

   In this case it is suffices to show

   $(\mathsf{fst}(e), \mathsf{fst}(e')) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma_1'} e_1', S_1' \;\wedge \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega';\Sigma_2'} e_2', S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''. W'' \sqsupseteq W' \wedge\; (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \;\wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

   It is clear that neither $\mathsf{fst}(e)$ nor $\mathsf{fst}(e')$ are values. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

   - $\mathsf{fst}(e), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
   - $\mathsf{fst}(e'), \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

   By assumption neither e nor e' are values. Hence the reductions must have happened with **EFst**. Hence by inversion

   - $e, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
   - $e', \Sigma_2, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
   - $e_\beta = \mathsf{fst}(e_0)$
   - $e_\beta' = \mathsf{fst}(e_0')$

   Also assume $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \;\vee\; \Sigma_2' \sqsubseteq \mathcal{A}$. This directly gives us a W'' such that

   - $W'' \sqsupseteq W'$,
   - $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$,
   - $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
   - $(e_0, e_0', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^p]\!]^{\mathcal{A}}_{E}$

   It suffices to show

   - $W'' \sqsupseteq W'$. We already know that.
   - $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.

- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
- $(\mathtt{fst}(e_0), \mathtt{fst}(e_0'), W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}$ We get this by induction.

(b) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

In this case it suffices to show

$(\mathtt{fst}(e), \mathtt{fst}(e')) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

It is clear that $\mathtt{fst}(e)$ is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $\mathtt{fst}(e), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

By assumption e is not a value. Hence the reduction must have happened with **EFst**. By inversion

- $e, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e_\beta = \mathtt{fst}(e_0)$

Hence

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_0, e', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathsf{E}})$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\mathtt{fst}(e_0), \mathtt{fst}(e'), W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this using the induction hypothesis.

(c) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 \times \tau_2)^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

In this case it suffices to show

$(\mathtt{fst}(e), \mathtt{fst}(e')) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

It is clear that $\mathtt{fst}(e')$ is not a value. So let $\omega', e_\beta', \Sigma_2', S_2'$ such that

- $\mathtt{fst}(e'), \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

By assumption e' is not a value. Hence the reduction must have happened with **EFst**. By inversion

- $e', \Sigma_2, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
- $e_\beta' = \mathtt{fst}(e_0')$

Hence

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$

- $(e, e_0', W'', \Sigma, \Sigma', m') \in [\![(\tau_1 \times \tau_2)^p]\!]^{\mathcal{A}}_E)$

It suffices to show the following:

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\mathtt{fst}(e), \mathtt{fst}(e_0'), W'', \Sigma, \Sigma', m') \in [\![\tau_1]\!]^{\mathcal{A}}_E$. We get this using the induction hypothesis.

2. $(e, e', W, \Sigma, \Sigma', m) \in \left\{(v, v', W, \Sigma_{c_1}, \Sigma_{c_2}, m) \;\middle|\; (v, v', W, m) \in [\![(\tau_1 \times \tau_2)^p]\!]^{\mathcal{A}}_V\right\}$

Consequently e and e' are values v and v', respectively and $(v, v', W, m) \in [\![(\tau_1 \times \tau_2)^p]\!]^{\mathcal{A}}_V$. There are two options. Either $p \sqsubseteq \mathcal{A}$ or $p \not\sqsubseteq \mathcal{A}$. In the first case $(v, v', W, m) \in [\![\tau_1 \times \tau_2]\!]^{\mathcal{A}}_V$ and in the second case $(v, W.\theta_1, m) \in \lceil \tau_1 \times \tau_2 \rceil v$ and $(v', W.\theta_2, m) \in \lceil \tau_1 \times \tau_2 \rceil v$. In either case v has the form (v_1, v_2) and v' has the form (v_1', v_2').

It suffices to show

$$(\mathtt{fst}((v_1, v_2)), \mathtt{fst}((v_1', v_2'))) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\; (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau_1]\!]^{\mathcal{A}}_E \end{array} \right\}$$

It is clear that neither $\mathtt{fst}\ (v_1, v_2)$ nor $\mathtt{fst}\ (v_1', v_2')$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $\mathtt{fst}\ (v_1, v_2), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $\mathtt{fst}\ (v_1', v_2'), \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

The reduction must have happened with **EFstBeta**. Consequently

- $e_\beta = v_1$
- $e_\beta' = v_1'$
- $S_1' = S_1$
- $S_2' = S_2$
- $\omega = \epsilon = \omega'$
- $\Sigma_1' = \Sigma_1$
- $\Sigma_2' = \Sigma_2$

Hence the reductions are really

- $\mathtt{fst}\ (v_1, v_2), \Sigma_1, S_1 \succ v_1, S_1, \epsilon, \Sigma_1$
- $\mathtt{fst}\ (v_1', v_2'), \Sigma_2, S_2 \succ v_1', S_2, \epsilon, \Sigma_2$

It suffices to show

- $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A} \rightarrow \exists W''.W'' \sqsupseteq W' \wedge$
  $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'' \wedge\; \epsilon \approx^{\mathcal{A}}_{W''.\beta} \epsilon \wedge (v_1, v_1', W'', \Sigma, \Sigma', m') \in [\![\tau_1]\!]^{\mathcal{A}}_E$.
  It suffices to show the conclusion. In particular it suffices to show
  - $W' \sqsupseteq W'$. We get this by Lemma 7.2.
  - $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. We already know this.
  - $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon$. We get this with **refl**.
  - $(v_1, v_1', W', \Sigma, \Sigma', m') \in [\![\tau_1]\!]^{\mathcal{A}}_E$. There are two cases:
    (a) $p \sqsubseteq \mathcal{A}$ In this case
    * $((v_1, v_2), (v_2', v_2'), W, m) \in [\![\tau_1 \times \tau_2]\!]^{\mathcal{A}}_V$.
    Hence

$*$ $(v_1, v_1', W, m) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$ and
$*$ $(v_2, v_2', W, m) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$.
By Lemma 8.24 and Lemma 8.25 we get $(v_1, v_1', W', m') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$. The goal follows directly.

(b) $p \not\sqsubseteq \mathcal{A}$ In this case
$*$ $((v_1, v_2), W.\theta_1, m) \in \lceil \tau_1 \times \tau_2 \rceil_{\mathcal{V}}$ and
$*$ $((v_1', v_2'), W.\theta_2, m) \in \lceil \tau_1 \times \tau_2 \rceil_{\mathcal{V}}$.
Hence
$*$ $(v_1, W.\theta_1, m) \in \lceil \tau_1 \rceil_{\mathcal{V}}$ and
$*$ $(v_1', W.\theta_2, m) \in \lceil \tau_1 \rceil_{\mathcal{V}}$
which suffices to show $(v_1, v_1', W, \Sigma, m) \in [\![\tau_1]\!]^{\mathcal{A}}_{E})$ if $\tau_1 \not\sqsubseteq \mathcal{A}$. This is the case because $p \sqsubseteq \tau_1$ and $p \not\sqsubseteq \mathcal{A}$. We get the goal by Lemma 8.29.

□

Lemma 8.39. If $(e, e', W, \Sigma, \Sigma', m) \in [\![(\tau_1 \times \tau_2)^p]\!]^{\mathcal{A}}_{E}$, $\Sigma \approx_{\mathcal{A}} \Sigma'$ and $p \sqsubseteq \tau_2$, then $(\mathsf{snd}\,(e), \mathsf{snd}\,(e'), W, \Sigma, \Sigma', m) \in [\![\tau_2]\!]^{\mathcal{A}}_{E}$.

Proof. Analogous to the proof of Lemma 8.38. □

Lemma 8.40. If $(e, e', W, \Sigma, \Sigma', m) \in [\![\tau_1]\!]^{\mathcal{A}}_{E}$, then $\forall \tau_2.\ (\mathsf{inl}\,(e), \mathsf{inl}\,(e'), W, \Sigma, \Sigma', m) \in [\![(\tau_1 + \tau_2)^{\perp}]\!]^{\mathcal{A}}_{E}$.

Proof. By induction on m. There are two cases:

1. $(e, e', W, \Sigma, \Sigma', m) \in [\![\tau_1]\!]^{\mathcal{A}}_{E_\beta}$. In this case it suffices to show $\forall \tau_2.(\mathtt{inl}\ e, \mathtt{inl}\ e', W, \Sigma, \Sigma', m) \in [\![(\tau_1 + \tau_2)^{\perp}]\!]^{\mathcal{A}}_{E_\beta}$. Let τ_2 be a type. We get $\Sigma \approx_{\mathcal{A}} \Sigma'$ from $(e, e', W, \Sigma, \Sigma', m) \in [\![\tau_1]\!]^{\mathcal{A}}_{E_\beta}$. Let Σ_1, Σ_2 such that
   - $\Sigma_1 \supseteq \Sigma$,
   - $\Sigma_2 \supseteq \Sigma'$,
   - $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

   W', m' such that
   - $m' < m$,
   - $W' \sqsupseteq W$,

   and S_1, S_2 such that
   - $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

   There three further cases:

   (a) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\, S_1' \wedge \\ \Sigma_2 \vdash e_2,\, S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau_1]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

   In this case it is suffices to show

   $(\mathtt{inl}\ e, \mathtt{inl}\ e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\, S_1' \wedge \\ \Sigma_2 \vdash e_2,\, S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![(\tau_1 + \tau_2)^{\perp}]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

   By assumption neither e nor e' is a value. Consequently $\mathtt{inl}\ e$ and $\mathtt{inl}\ e'$ are not values, either. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $\mathtt{inl}\ e, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $\mathtt{inl}\ e', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

The reductions must have happened with **EInl**. Hence by inversion

- $e, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e', \Sigma_2, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
- $e_\beta = \mathtt{inl}\ e_0$
- $e_\beta' = \mathtt{inl}\ e_0'$

Also assume $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \ \vee \ \Sigma_2' \sqsubseteq \mathcal{A}$. This directly gives us a W'' such that

- $W'' \sqsupseteq W'$,
- $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
- $(e_0, e_0', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}$.

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
- $(\mathtt{inl}(e_0), \mathtt{inl}(e_0'), W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 + \tau_2)^\perp]\!]^{\mathcal{A}}_{\mathsf{E}}$ We get this by induction.

(b) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\ S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\ S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

In this case it suffices to show

$(\mathtt{inl}\ e, \mathtt{inl}\ e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\ S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\ S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 + \tau_2)^\perp]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

By assumption e is not a value. Hence $\mathtt{inl}\ e$ is not a value, either. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $\mathtt{inl}\ e, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

The reduction must have happened with **EInl**. By inversion

- $e, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e_\beta = \mathtt{inl}\ e_0$

Hence

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_0, e', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}})$

It suffices to show the following:

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\mathtt{inl}\ e_0, \mathtt{inl}\ e', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 + \tau_2)^\perp]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this using the induction hypothesis.

(c) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\ S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\ S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

In this case it suffices to show

$$(\mathtt{inl}\ e, \mathtt{inl}\ e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\ S_2 \xrightarrow{\omega;\Sigma_2'} e_2',\ S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 + \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$$

By assumption e' is not a value. Hence $\mathtt{inl}(e')$ is not a value, either. So let $\omega', e_\beta', \Sigma_2', S_2'$ such that

- $\mathtt{inl}\ e', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

The reduction must have happened with **EInl**. By inversion

- $e', \Sigma_2, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
- $e_\beta' = \mathtt{inl}\ e_0'$

Hence

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e, e_0', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}})$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\mathtt{inl}\ e, \mathtt{inl}\ e_0', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\tau_1 + \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this using the induction hypothesis.

2. $(e, e', W, \Sigma, \Sigma', \mathfrak{m}) \in \left\{ (v, v', W, \Sigma_{c_1}, \Sigma_{c_2}, \mathfrak{m}) \;\middle|\; (v, v', W, \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}} \right\}$

   Consequently e and e' are values v and v', respectively and $(v, v', W, \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$. Consequently $\mathtt{inl}\ v$ and $\mathtt{inl}\ v'$ are also values. Because $\perp \sqsubseteq \mathcal{A}$ (Lemma 4.19), it suffices to show $(\mathtt{inl}\ v, \mathtt{inl}\ v', W, \mathfrak{m}) \in \lceil \tau_1 + \tau_2 \rceil_v$. This follows directly from $(v, v', W, \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$.

□

Lemma 8.41. If $(e, e', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}}$, then $\forall \tau_1.\ (\mathsf{inr}\,(e)\,, \mathsf{inr}\,(e')\,, W, \Sigma, \Sigma', \mathfrak{m}) \in [\![(\tau_1 + \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$.

Proof. Analogous to the proof of Lemma 8.40. □

Lemma 8.42. If

- $(e, e', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![(\tau_1 + \tau_2)^{p}]\!]^{\mathcal{A}}_{\mathsf{E}}$,
- $p \sqsubseteq \tau$,
- $\Sigma \approx_{\mathcal{A}} \Sigma'$,
- $\forall W', \mathfrak{m}'. W' \sqsupseteq W \wedge \mathfrak{m}' \leqslant \mathfrak{m} \to \forall v, v'. (v, v', W', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}} \to ([v/x]e_1, [v'/x]e_1', W', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$,
- $\forall W', \mathfrak{m}'. W' \sqsupseteq W \wedge \mathfrak{m}' \leqslant \mathfrak{m} \to \forall w, w'. (w, w', W', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}} \to ([w/x]e_2, [w'/x]e_2', W', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$,
- $\forall W', \mathfrak{m}'. W' \sqsupseteq W \wedge \mathfrak{m}' \leqslant \mathfrak{m} \to \forall v. (v, W'.\theta_1, \mathfrak{m}') \in \lceil \tau_1 \rceil_v \to ([v/x]e_1, W'.\theta_1, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$,
- $\forall W', \mathfrak{m}'. W' \sqsupseteq W \wedge \mathfrak{m}' \leqslant \mathfrak{m} \to \forall v. (v, W'.\theta_2, \mathfrak{m}') \in \lceil \tau_1 \rceil_v \to ([v/x]e_1', W'.\theta_2, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$,
- $\forall W', \mathfrak{m}'. W' \sqsupseteq W \wedge \mathfrak{m}' \leqslant \mathfrak{m} \to \forall v. (v, W'.\theta_1, \mathfrak{m}') \in \lceil \tau_2 \rceil_v \to ([v/y]e_2, W'.\theta_1, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$, and
- $\forall W', \mathfrak{m}'. W' \sqsupseteq W \wedge \mathfrak{m}' \leqslant \mathfrak{m} \to \forall v. (v, W'.\theta_2, \mathfrak{m}') \in \lceil \tau_2 \rceil_v \to ([v/y]e_2', W'.\theta_2, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$,

then $\left(\begin{array}{ll} \mathsf{case}\ e\ \mathsf{of} & \mathsf{case}\ e'\ \mathsf{of} \\ |\,\mathsf{inl}\,(x) \Rightarrow e_1 & |\,\mathsf{inl}\,(x) \Rightarrow e_1' \\ |\,\mathsf{inr}\,(y) \Rightarrow e_2 & |\,\mathsf{inr}\,(y) \Rightarrow e_2' \end{array} , W, \Sigma, \Sigma', \mathfrak{m} \right) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.

Proof. By induction on m. It suffices to show $(\mathsf{case}(e, x.e_1, y.e_2), \mathsf{case}(e', x.e_1', y.e_2'), W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{E_\beta}$. We already have $\Sigma \approx_{\mathcal{A}} \Sigma'$ by assumption. Let Σ_1, Σ_2 such that

- $\Sigma_1 \supseteq \Sigma$,
- $\Sigma_2 \supseteq \Sigma'$,
- $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

W', m' such that

- $m' < m$,
- $W' \sqsupseteq W$,

and S_1, S_2 such that

- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

There are two cases:

1. $(e, e', W, \Sigma, \Sigma', m) \in [\![(\tau_1 + \tau_2)^p]\!]^{\mathcal{A}}_{E_\beta}$. There are several further cases:

   (a) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \;\wedge \\ \Sigma_2 \vdash e_2, S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2', S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''. W'' \sqsupseteq W' \wedge\; (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \;\wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![(\tau_1 + \tau_2)^p]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

   In this case it is suffices to show

   $(\mathsf{case}(e, x.e_1, y.e_2), \mathsf{case}(e', x.e_1', y.e_2')) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \;\wedge \\ \Sigma_2 \vdash e_2, S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2', S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''. W'' \sqsupseteq W' \wedge\; (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \;\wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

   Clearly neither $\mathsf{case}(e, x.e_1, y.e_2)$ nor $\mathsf{case}(e', x.e_1', y.e_2')$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

   - $\mathsf{case}(e, x.e_1, y.e_2), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
   - $\mathsf{case}(e', x.e_1', y.e_2'), \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

   Because neither e nor e' is a value reductions must have happened with **ECase**. Hence by inversion

   - $e, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
   - $e', \Sigma_2, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
   - $e_\beta = \mathsf{case}(e_0, x.e_1, y.e_2)$
   - $e_\beta' = \mathsf{case}(e_0', x.e_1', y.e_2')$

   Also assume $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \;\vee\; \Sigma_2' \sqsubseteq \mathcal{A}$. This directly gives us a W'' such that

   - $W'' \sqsupseteq W'$,
   - $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$,
   - $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
   - $(e_0, e_0', W'', \Sigma, \Sigma', m') \in [\![(\tau_1 + \tau_2)^p]\!]^{\mathcal{A}}_{E}$

   It suffices to show

   - $W'' \sqsupseteq W'$. We already know that.

- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
- $(case(e_0, x.e_1, y.e_2), case(e_0', x.e_1', y.e_2'), W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E$ We get this by induction if we can also show
  - $\forall W''', m''.W''' \sqsupseteq W'' \wedge m'' \leqslant m \to \forall (v, v', W''', m'') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}.([v/x]e_1, [v'/x]e_1', W''', \Sigma, \Sigma', m'') \in [\![\tau]\!]^{\mathcal{A}}_E$.
    Let $W''' \sqsupseteq W''$ and $m'' \leqslant m'$. Then in particular by transitivity $m'' < m'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', m''.W''' \sqsupseteq W'' \wedge m'' \leqslant m \to \forall (w, w', W''', m'') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}.([w/x]e_2, [w'/x]e_2', W''', \Sigma, \Sigma', m'') \in [\![\tau]\!]^{\mathcal{A}}_E$.
    Let $W''' \sqsupseteq W''$ and $m'' \leqslant m'$. Then in particular by transitivity $m'' < m'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', m''.W''' \sqsupseteq W'' \wedge m'' \leqslant m \to \forall v.(v, W'''.\theta_1, m'') \in \lceil \tau_1 \rceil_{\mathcal{V}} \to ([v/x]e_1, W'''.\theta_1, m'') \in \lceil \tau \rceil^{pc \sqcup p}_E$.
    Let $W''' \sqsupseteq W''$ and $m'' \leqslant m'$. Then in particular by transitivity $m'' < m'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', m''.W''' \sqsupseteq W'' \wedge m'' \leqslant m \to \forall v.(v, W'''.\theta_2, m'') \in \lceil \tau_1 \rceil_{\mathcal{V}} \to ([v/x]e_1', W'''.\theta_2, m'') \in \lceil \tau \rceil^{pc \sqcup p}_E$.
    Let $W''' \sqsupseteq W''$ and $m'' \leqslant m'$. Then in particular by transitivity $m'' < m'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', m''.W''' \sqsupseteq W'' \wedge m'' \leqslant m \to \forall v.(v, W'''.\theta_1, m'') \in \lceil \tau_2 \rceil_{\mathcal{V}} \to ([v/y]e_2, W'''.\theta_1, m'') \in \lceil \tau \rceil^{pc \sqcup p}_E$.
    Let $W''' \sqsupseteq W''$ and $m'' \leqslant m'$. Then in particular by transitivity $m'' < m'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', m''.W''' \sqsupseteq W'' \wedge m'' \leqslant m \to \forall v.(v, W'''.\theta_2, m'') \in \lceil \tau_2 \rceil_{\mathcal{V}} \to ([v/y]e_2', W'''.\theta_2, m'') \in \lceil \tau \rceil^{pc \sqcup p}_E$.
    Let $W''' \sqsupseteq W''$ and $m'' \leqslant m'$. Then in particular by transitivity $m'' < m'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.

.

(b) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \to \neg(pol(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![(\tau_1 + \tau_2)^p]\!]^{\mathcal{A}}_E) \end{array} \right\}$

In this case it suffices to show

$(case(e, x.e_1, y.e_2), case(e, x.e_1', y.e_2')) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \to \neg(pol(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E) \end{array} \right\}$

It is clear that $case(e, x.e_1, y.e_2)$ is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $case(e, x.e_1, y.e_2), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

By assumption e is not a value. Therefore the reduction must have happened with **ECase**. By inversion

- $e, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e_\beta = case(e_0, x.e_1, y.e_2)$

Hence

- $\neg(pol(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_0, e', W'', \Sigma, \Sigma', m') \in [\![(\tau_1 + \tau_2)^p]\!]^{\mathcal{A}}_E)$

It suffices to show the following:

- $\neg(pol(\omega) \sqsubseteq \mathcal{A})$. We already know this

- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(case(e_0, x.e_1, y.e_2), case(e', x.e_1', y.e_2'), W'', \Sigma, \Sigma', m') \in [\![\tau]\!]_E^{\mathcal{A}}$. We get this using the induction hypothesis if we can also show
  - $\forall W''', m''.W''' \sqsupseteq W'' \wedge m'' \leqslant m \to \forall (v, v', W''', m'') \in [\![\tau_1]\!]_V^{\mathcal{A}}.([v/x]e_1, [v'/x]e_1', W''', \Sigma, \Sigma', m'') \in [\![\tau]\!]_E^{\mathcal{A}}$.
    Let $W''' \sqsupseteq W''$ and $m'' \leqslant m'$. Then in particular by transitivity $m'' < m'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', m''.W''' \sqsupseteq W'' \wedge m'' \leqslant m \to \forall (w, w', W''', m'') \in [\![\tau_2]\!]_V^{\mathcal{A}}.([w/x]e_2, [w'/x]e_2', W''', \Sigma, \Sigma', m'') \in [\![\tau]\!]_E^{\mathcal{A}}$.
    Let $W''' \sqsupseteq W''$ and $m'' \leqslant m'$. Then in particular by transitivity $m'' < m'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', m''.W''' \sqsupseteq W'' \wedge m'' \leqslant m \to \forall v.(v, W'''.\theta_1, m'') \in \lceil \tau_1 \rceil_V \to ([v/x]e_1, W'''.\theta_1, m'') \in \lceil \tau \rceil_E^{pc \sqcup p}$.
    Let $W''' \sqsupseteq W''$ and $m'' \leqslant m'$. Then in particular by transitivity $m'' < m'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', m''.W''' \sqsupseteq W'' \wedge m'' \leqslant m \to \forall v.(v, W'''.\theta_2, m'') \in \lceil \tau_1 \rceil_V \to ([v/x]e_1', W'''.\theta_2, m'') \in \lceil \tau \rceil_E^{pc \sqcup p}$.
    Let $W''' \sqsupseteq W''$ and $m'' \leqslant m'$. Then in particular by transitivity $m'' < m'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', m''.W''' \sqsupseteq W'' \wedge m'' \leqslant m \to \forall v.(v, W'''.\theta_1, m'') \in \lceil \tau_2 \rceil_V \to ([v/y]e_2, W'''.\theta_1, m'') \in \lceil \tau \rceil_E^{pc \sqcup p}$.
    Let $W''' \sqsupseteq W''$ and $m'' \leqslant m'$. Then in particular by transitivity $m'' < m'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', m''.W''' \sqsupseteq W'' \wedge m'' \leqslant m \to \forall v.(v, W'''.\theta_2, m'') \in \lceil \tau_2 \rceil_V \to ([v/y]e_2', W'''.\theta_2, m'') \in \lceil \tau \rceil_E^{pc \sqcup p}$.
    Let $W''' \sqsupseteq W''$ and $m'' \leqslant m'$. Then in particular by transitivity $m'' < m'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.

.

(c) $$(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2, S_2 \overset{\omega;\Sigma_2'}{\Longrightarrow} e_2', S_2' \to \neg(pol(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![(\tau_1 + \tau_2)^p]\!]_E^{\mathcal{A}}) \end{array} \right\}$$

In this case it suffices to show

$$(case(e, x.e_1, y.e_2), case(e, x.e_1', y.e_2')) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2, S_2 \overset{\omega;\Sigma_2'}{\Longrightarrow} e_2', S_2' \to \neg(pol(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]_E^{\mathcal{A}}) \end{array} \right\}$$

It is clear that $case(e', x.e_1', y.e_2')$ is not a value. So let $\omega, e_\beta', \Sigma_2', S_2'$ such that

- $case(e', x.e_1', y.e_2'), \Sigma_2, S_2 \succ e_\beta', S_2', \omega, \Sigma_2'$

By assumption e' is not a value. Therefore the reduction must have happened with **ECase**. By inversion

- $e', \Sigma_2, S_2 \succ e_0', S_2', \omega, \Sigma_2'$
- $e_\beta' = case(e_0', x.e_1', y.e_2')$

Hence

- $\neg(pol(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e, e_0', W'', \Sigma, \Sigma', m') \in [\![(\tau_1 + \tau_2)^p]\!]_E^{\mathcal{A}})$

It suffices to show the following:

- $\neg(pol(\omega) \sqsubseteq \mathcal{A})$. We already know this

- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\mathsf{case}(e, x.e_1, y.e_2), \mathsf{case}(e_0', x.e_1', y.e_2'), W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this using the induction hypothesis if we can also show
  - $\forall W''', \mathfrak{m}''. W''' \sqsupseteq W'' \wedge \mathfrak{m}'' \leqslant \mathfrak{m} \to \forall (v, v', W''', \mathfrak{m}'') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}. ([v/x]e_1, [v'/x]e_1', W''', \Sigma, \Sigma', \mathfrak{m}'') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.
    Let $W''' \sqsupseteq W''$ and $\mathfrak{m}'' \leqslant \mathfrak{m}'$. Then in particular by transitivity $\mathfrak{m}'' < \mathfrak{m}'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', \mathfrak{m}''. W''' \sqsupseteq W'' \wedge \mathfrak{m}'' \leqslant \mathfrak{m} \to \forall (w, w', W''', \mathfrak{m}'') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}. ([w/x]e_2, [w'/x]e_2', W''', \Sigma, \Sigma', \mathfrak{m}'') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.
    Let $W''' \sqsupseteq W''$ and $\mathfrak{m}'' \leqslant \mathfrak{m}'$. Then in particular by transitivity $\mathfrak{m}'' < \mathfrak{m}'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', \mathfrak{m}''. W''' \sqsupseteq W'' \wedge \mathfrak{m}'' \leqslant \mathfrak{m} \to \forall v. (v, W'''.\theta_1, \mathfrak{m}'') \in \lceil \tau_1 \rceil_{\mathcal{V}} \to ([v/x]e_1, W'''.\theta_1, \mathfrak{m}'') \in \lceil \tau \rceil^{\mathsf{pc} \sqcup \mathsf{p}}_{\mathsf{E}}$.
    Let $W''' \sqsupseteq W''$ and $\mathfrak{m}'' \leqslant \mathfrak{m}'$. Then in particular by transitivity $\mathfrak{m}'' < \mathfrak{m}'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', \mathfrak{m}''. W''' \sqsupseteq W'' \wedge \mathfrak{m}'' \leqslant \mathfrak{m} \to \forall v. (v, W'''.\theta_2, \mathfrak{m}'') \in \lceil \tau_1 \rceil_{\mathcal{V}} \to ([v/x]e_1', W'''.\theta_2, \mathfrak{m}'') \in \lceil \tau \rceil^{\mathsf{pc} \sqcup \mathsf{p}}_{\mathsf{E}}$.
    Let $W''' \sqsupseteq W''$ and $\mathfrak{m}'' \leqslant \mathfrak{m}'$. Then in particular by transitivity $\mathfrak{m}'' < \mathfrak{m}'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', \mathfrak{m}''. W''' \sqsupseteq W'' \wedge \mathfrak{m}'' \leqslant \mathfrak{m} \to \forall v. (v, W'''.\theta_1, \mathfrak{m}'') \in \lceil \tau_2 \rceil_{\mathcal{V}} \to ([v/y]e_2, W'''.\theta_1, \mathfrak{m}'') \in \lceil \tau \rceil^{\mathsf{pc} \sqcup \mathsf{p}}_{\mathsf{E}}$.
    Let $W''' \sqsupseteq W''$ and $\mathfrak{m}'' \leqslant \mathfrak{m}'$. Then in particular by transitivity $\mathfrak{m}'' < \mathfrak{m}'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.
  - $\forall W''', \mathfrak{m}''. W''' \sqsupseteq W'' \wedge \mathfrak{m}'' \leqslant \mathfrak{m} \to \forall v. (v, W'''.\theta_2, \mathfrak{m}'') \in \lceil \tau_2 \rceil_{\mathcal{V}} \to ([v/y]e_2', W'''.\theta_2, \mathfrak{m}'') \in \lceil \tau \rceil^{\mathsf{pc} \sqcup \mathsf{p}}_{\mathsf{E}}$.
    Let $W''' \sqsupseteq W''$ and $\mathfrak{m}'' \leqslant \mathfrak{m}'$. Then in particular by transitivity $\mathfrak{m}'' < \mathfrak{m}'$ and (Lemma 7.2) also $W''' \sqsupseteq W$. The claim follows directly from the assumptions.

  .

2. $(e, e', W, \Sigma, \Sigma', \mathfrak{m}) \in \left\{ (v, v', W, \Sigma_{c_1}, \Sigma_{c_2}, \mathfrak{m}) \;\middle|\; (v, v', W, \mathfrak{m}) \in [\![(\tau_1 + \tau_2)^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathcal{V}} \right\}$

   Consequently e and e' are values v and v', respectively and $(v, v', W, \mathfrak{m}) \in [\![(\tau_1 + \tau_2)^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. There are two cases

   (a) $\mathsf{p} \sqsubseteq \mathcal{A}$. In this case $(v, v', W, \mathfrak{m}) \in [\![\tau_1 + \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$. It is suffices to show

   $$(\mathsf{case}(v, x.e_1, y.e_2), \mathsf{case}(v', x.e_1', y.e_2')) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega; \Sigma_1'}{\Longrightarrow} e_1', S_1' \;\wedge \\ \Sigma_2 \vdash e_2, S_2 \overset{\omega'; \Sigma_2'}{\Longrightarrow} e_2', S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''. W'' \sqsupseteq W' \wedge\; (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$$

   Clearly neither $\mathsf{case}(v, x.e_1, y.e_2)$ nor $\mathsf{case}(v', x.e_1', y.e_2')$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

   - $\mathsf{case}(v, x.e_1, y.e_2), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
   - $\mathsf{case}(v', x.e_1', y.e_2'), \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

   There are two cases:

   i. $v = \mathtt{inl}\ v_0$, $v' = \mathtt{inl}\ v_0'$ and $(v_0, v_0', W, \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$ In this case the reductions must have happened with **ECasel**. Hence by inversion
      - $e_\beta = [v_0/x]e_1$
      - $e_\beta' = [v_0'/x]e_1'$
      - $\omega = \epsilon = \omega'$
      - $S_1' = S_1$
      - $S_2' = S_2$

- $\Sigma_1' = \Sigma_1$
- $\Sigma_2' = \Sigma_2$

So the reductions are really

- $\mathtt{case}(\mathtt{inl}\ v_0, x.e_1, y.e_2), \Sigma_1, S_1 \succ [v_0/x]e_1, S_1, \epsilon, \Sigma_1$
- $\mathtt{case}(\mathtt{inl}\ v_0', x.e_1', y.e_2'), \Sigma_2, S_2 \succ [v_0'/x]e_1', S_2, \epsilon, \Sigma_2$

It suffices to show

- $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon \vee \Sigma_1 \sqsubseteq \mathcal{A} \wedge \Sigma_2 \sqsubseteq \mathcal{A} \to \exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \epsilon \approx^{\mathcal{A}}_{W''.\beta} \epsilon \wedge ([v_0/x]e_1, [v_0'/x]e_1', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.
  It suffices to show the conclusion. In particular it suffices to show
  - $W' \sqsupseteq W'$. We get this by Lemma 7.2.
  - $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
  - $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon$. We get this by **refl**.
  - $([v_0/x]e_1, [v_0'/x]e_1', W', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. By Lemma 8.24 and Lemma 8.25 we have $(v_0, v_0', W', m') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get the claim from our assumption.

ii. $v = \mathtt{inr}\ v_0$, $v' = \mathtt{inr}\ v_0'$ and $(v_0, v_0', W, m) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$ In this case the reductions must have happened with **ECaser**. Hence by inversion

- $e_\beta = [v_0/x]e_2$
- $e_\beta' = [v_0'/x]e_2'$
- $\omega = \epsilon = \omega'$
- $S_1' = S_1$
- $S_2' = S_2$
- $\Sigma_1' = \Sigma_1$
- $\Sigma_2' = \Sigma_2$

So the reductions are really

- $\mathtt{case}(\mathtt{inr}\ v_0, x.e_1, y.e_2), \Sigma_1, S_1 \succ [v_0/x]e_2, S_1, \epsilon, \Sigma_1$
- $\mathtt{case}(\mathtt{inr}\ v_0', x.e_1', y.e_2'), \Sigma_2, S_2 \succ [v_0'/x]e_2', S_2, \epsilon, \Sigma_2$

It suffices to show

- $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon \vee \Sigma_1 \sqsubseteq \mathcal{A} \wedge \Sigma_2 \sqsubseteq \mathcal{A} \to \exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \epsilon \approx^{\mathcal{A}}_{W''.\beta} \epsilon \wedge ([v_0/x]e_1, [v_0'/x]e_1', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.
  It suffices to show the conclusion. In particular it suffices to show
  - $W' \sqsupseteq W'$. We get this by Lemma 7.2.
  - $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
  - $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon$. We get this by **refl**.
  - $([v_0/x]e_1, [v_0'/x]e_1', W', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. By Lemma 8.24 and Lemma 8.25 we have $(v_0, v_0', W', m') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get the claim from our assumption.

(b) $p \not\sqsubseteq \mathcal{A}$. In this case

- $(v, W.\theta_1, m) \in \lceil \tau_1 + \tau_2 \rceil_{\mathcal{V}}$ and
- $(v', W.\theta_2, m) \in \lceil \tau_1 + \tau_2 \rceil_{\mathcal{V}}$.

Because $p \sqsubseteq \tau$ also.

- $\tau \not\sqsubseteq \mathcal{A}$. If this was not the case we would have $p \sqsubseteq \mathcal{A}$ by transitivity (Lemma 4.1) which would contradict the assumption.

By Lemma 4.6 $p \sqsubseteq pc \sqcup p$. Hence also

- $pc \sqcup p \not\sqsubseteq \mathcal{A}$. If this was not the case we would have $p \sqsubseteq \mathcal{A}$ by transitivity (Lemma 4.1) which would contradict the assumption.

Hence by Lemma 8.30 it suffices to show

- $(\mathtt{case}(v, e_1, e_2), W.\theta_1, m) \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$. It suffices to show $(\mathtt{case}(v, e_1, e_2), W.\theta_1, m) \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}_\beta}$.
  It is clear that $\mathtt{case}(v, e_1, e_2)$ is not a value. So let S, θ', m' such that
  - $\theta' \sqsupseteq W.\theta_1$,
  - $(S, m') \triangleright \theta'$,
  - $m' < m$,

and $e_\beta, S', \omega, \Sigma_1, \Sigma_1'$ such that
- $\mathtt{case}(v, e_1, e_2), \Sigma_1, S \succ e_\beta, S', \omega, \Sigma_1'$.

Because $(v, W.\theta_1, m) \in \lceil \tau_1 + \tau_2 \rceil_\mathcal{V}$, there are two cases

i. $v = \mathtt{inl}\ v_0$ and $(v_0, W.\theta_1, m) \in \lceil \tau_1 \rceil_\mathcal{V}$. In this case the reduction must have happened with **ECasel**. Hence
   - $e_\beta = [v_0/x]e_1$
   - $S' = S$
   - $\omega = \epsilon$
   - $\Sigma_1' = \Sigma_1$.

   So the reduction is really
   - $\mathtt{case}(\mathtt{inl}\ v_0, e_1, e_2), \Sigma_1, S \succ [v_0/x]e_1, S, \epsilon, \Sigma_1$.

   It suffices to show
   - $\forall q.\mathtt{pol}(\epsilon) = q \to pc \sqcup p \sqsubseteq p$. Because $\mathtt{pol}(\epsilon)$ is undefined there is nothing to show.
   - $\theta' \sqsupseteq \theta'$. We get this by Lemma 6.2.
   - $(S, m') \triangleright \theta'$. We already know that.
   - $([v_0/x]e_1, \theta', m') \in \lceil \tau \rceil_E^{pc \sqcup p}$. By Lemma 8.4 $(v_0, \theta', m') \in \lceil \tau_1 \rceil_\mathcal{V}$. We get $([v_0/x]e_1, \theta', m') \in \lceil \tau \rceil_E^{pc \sqcup p}$ by assumption.

ii. $v = \mathtt{inr}\ v_0$ and $(v_0, W.\theta_1, m) \in \lceil \tau_2 \rceil_\mathcal{V}$. In this case the reduction must have happened with **ECaser**. Hence
   - $e_\beta = [v_0/x]e_2$
   - $S' = S$
   - $\omega = \epsilon$
   - $\Sigma_1' = \Sigma_1$.

   So the reduction is really
   - $\mathtt{case}(\mathtt{inr}\ v_0, e_1, e_2), \Sigma_1, S \succ [v_0/x]e_2, S, \epsilon, \Sigma_1$.

   It suffices to show
   - $\forall q.\mathtt{pol}(\epsilon) = q \to pc \sqcup p \sqsubseteq p$. Because $\mathtt{pol}(\epsilon)$ is undefined there is nothing to show.
   - $\theta' \sqsupseteq \theta'$. We get this by Lemma 6.2.
   - $(S, m') \triangleright \theta'$. We already know that.
   - $([v_0/x]e_2, \theta', m') \in \lceil \tau \rceil_E^{pc \sqcup p}$. By Lemma 8.4 $(v_0, \theta', m') \in \lceil \tau_2 \rceil_\mathcal{V}$. We get $([v_0/x]e_2, \theta', m') \in \lceil \tau \rceil_E^{pc \sqcup p}$ by assumption.

- $(\mathtt{case}(v', e_1', e_2'), W.\theta_2, m) \in \lceil \tau \rceil_E^{pc \sqcup p}$. It suffices to show $(\mathtt{case}(v', e_1', e_2'), W.\theta_2, m) \in \lceil \tau \rceil_{E_\beta}^{pc \sqcup p}$.

  It is clear that $\mathtt{case}(v', e_1', e_2')$ is not a value. So let S, θ', m' such that
  - $\theta' \sqsupseteq W.\theta_2$,
  - $(S, m') \triangleright \theta'$,
  - $m' < m$,

  and $e_\beta', S', \omega, \Sigma_2, \Sigma_2'$ such that
  - $\mathtt{case}(v', e_1', e_2'), \Sigma_2, S \succ e_\beta', S', \omega, \Sigma_2'$.

  Because $(v', W.\theta_2, m) \in \lceil \tau_1 + \tau_2 \rceil_\mathcal{V}$, there are two cases

  i. $v' = \mathtt{inl}\ v_0$ and $(v_0, W.\theta_2, m) \in \lceil \tau_1 \rceil_\mathcal{V}$. In this case the reduction must have happened with **ECasel**. Hence
     - $e_\beta' = [v_0/x]e_1'$
     - $S' = S$
     - $\omega = \epsilon$
     - $\Sigma_2' = \Sigma_2$.

     So the reduction is really
     - $\mathtt{case}(\mathtt{inl}\ v_0, e_1', e_2'), \Sigma_2, S \succ [v_0/x]e_2', S, \epsilon, \Sigma_2$.

     It suffices to show
     - $\forall q.\mathtt{pol}(\epsilon) = q \to pc \sqcup p \sqsubseteq p$. Because $\mathtt{pol}(\epsilon)$ is undefined there is nothing to show.
     - $\theta' \sqsupseteq \theta'$. We get this by Lemma 6.2.
     - $(S, m') \triangleright \theta'$. We already know that.

- $([\nu_0/x]e_2', \theta', m') \in \lceil\tau\rceil_E^{pc\sqcup p}$.
  By Lemma 8.4 $(\nu_0, \theta', m') \in \lceil\tau_1\rceil_\nu$. We get $([\nu_0/x]e_2', \theta', m') \in \lceil\tau\rceil_E^{pc\sqcup p}$ by assumption.

ii. $\nu = \mathtt{inr}\ \nu_0$ and $(\nu_0, W.\theta_2, m) \in \lceil\tau_2\rceil_\nu$. In this case the reduction must have happened with **ECaser**. Hence
- $e_\beta' = [\nu_0/x]e_2'$
- $S' = S$
- $\omega = \epsilon$
- $\Sigma_2' = \Sigma_2$.

So the reduction is really
- $\mathtt{case}(\mathtt{inr}\ \nu_0, e_1', e_2'), \Sigma_2, S \succ [\nu_0/x]e_2', S, \epsilon, \Sigma_2$.

It suffices to show
- $\forall q.\mathtt{pol}(\epsilon) = q \to pc \sqcup p \sqsubseteq p$. Because $\mathtt{pol}(\epsilon)$ is undefined there is nothing to show.
- $\theta' \sqsupseteq \theta'$. We get this by Lemma 6.2.
- $(S, m') \triangleright \theta'$. We already know that.
- $([\nu_0/x]e_2', \theta', m') \in \lceil\tau\rceil_E^{pc\sqcup p}$.
  By Lemma 8.4 $(\nu_0, \theta', m') \in \lceil\tau_2\rceil_\nu$. We get $([\nu_0/x]e_2', \theta', m') \in \lceil\tau\rceil_E^{pc\sqcup p}$ by assumption.

□

Lemma 8.43.

1. If $\nu \overset{\beta}{\simeq}{}_\tau^{\mathcal{A}} \nu'$, $(\nu, \theta_1, m) \in \lceil\tau\rceil_\nu$,$(\nu', \theta_2, m) \in \lceil\tau\rceil_\nu$ and $\mathtt{firstorder}(\tau)$, then $(\nu, \nu', (\theta_1, \theta_2, \beta), m) \in [\![\tau]\!]_\nu^{\mathcal{A}}$.
2. If $\nu \overset{\beta}{\simeq}{}_A^{\mathcal{A}} \nu'$,$(\nu, \theta_1, m) \in \lceil A\rceil_\nu$,$(\nu', \theta_2, m) \in \lceil A\rceil_\nu$ and $\mathtt{firstorder}(A)$, then $(\nu, \nu', (\theta_1, \theta_2, \beta), m) \in [\![A]\!]_\nu^{\mathcal{A}}$.

Proof. By mutual induction on $\mathtt{firstorder}(A)$ and $\mathtt{firstorder}(\tau)$.

- **FPol**: In this case $\tau = (A')^p$ for some policy p and type A' such that $\mathtt{firstorder}(A')$. There are two cases

  1. $p \sqsubseteq \mathcal{A}$: In this case we need to show $(\nu, \nu', (\theta_1, \theta_2, \beta), m) \in [\![A']\!]_\nu^{\mathcal{A}}$. By induction it suffices to show
     - $\nu \overset{\beta}{\simeq}{}_{A'}^{\mathcal{A}} \nu'$. The only rule by which $\nu \overset{\beta}{\simeq}{}_\tau^{\mathcal{A}} \nu'$ could have been derived is **eqLow** which has this as a premiss.
     - $(\nu, \theta_1, m) \in \lceil A'\rceil_\nu$. This follows directly from $(\nu, \theta_1, m) \in \lceil (A')^p\rceil_\nu$.
     - $(\nu, \theta_2, m) \in \lceil A'\rceil_\nu$. This follows directly from $(\nu, \theta_2, m) \in \lceil (A')^p\rceil_\nu$.
     - $\mathtt{firstorder}(A')$. This is an assumption of the rule.
  2. $p \not\sqsubseteq \mathcal{A}$. In this case it suffices to show
     - $(\nu, \theta_1, m) \in \lceil A'\rceil_\nu$. This follows directly from $(\nu, \theta_1, m) \in \lceil (A')^p\rceil_\nu$.
     - $(\nu, \theta_2, m) \in \lceil A'\rceil_\nu$. This follows directly from $(\nu, \theta_2, m) \in \lceil (A')^p\rceil_\nu$.

- **FUnit:** In this case $A = \mathtt{unit}$. From $(\nu, \theta_1, m) \in \lceil A\rceil_\nu$ and $(\nu', \theta_2, m) \in \lceil A\rceil_\nu$ it follows directly that
  - $\nu = ()$ and
  - $\nu' = ()$.

  The claim follows directly from the definition of $[\![\mathtt{unit}]\!]_\nu^{\mathcal{A}}$.

- **Fnat:** In this case $A = \mathcal{N}$. From $(\nu, \theta_1, m) \in \lceil A\rceil_\nu$ and $(\nu', \theta_2, m) \in \lceil A\rceil_\nu$ it follows directly that
  - $\nu = n$ and
  - $\nu' = m$.
  - $n, m \in \mathbb{N}$

  Because $n \overset{\beta}{\simeq}{}_{\mathcal{N}}^{\mathcal{A}} m$ we know that $n = m$. The claim follows directly from the definition of $[\![\mathcal{N}]\!]_\nu^{\mathcal{A}}$.

- **FProd**. In this case $A = \tau_1 \times \tau_2$ for some types τ_1 and τ_2 such that $\mathtt{firstorder}(\tau_1)$ and $\mathtt{firstorder}(\tau_2)$. From $(v, \theta_1, m) \in \lceil \tau_1 \times \tau_2 \rceil_\mathcal{V}$ and $(v', \theta_2, m) \in \lceil \tau_1 \times \tau_2 \rceil_\mathcal{V}$, it follows directly that there are v_1, v_2, v_1', v_2' such that
  - $v = (v_1, v_2)$,
  - $v' = (v_1', v_2')$,
  - $(v_1, \theta_1, m) \in \lceil \tau_1 \rceil_\mathcal{V}$,
  - $(v_2, \theta_1, m) \in \lceil \tau_2 \rceil_\mathcal{V}$,
  - $(v_1', \theta_2, m) \in \lceil \tau_1 \rceil_\mathcal{V}$, and
  - $(v_2', \theta_2, m) \in \lceil \tau_2 \rceil_\mathcal{V}$.

  Furthermore $(v_1, v_2) \overset{\beta}{\simeq}^\mathcal{A}_{\tau_1 \times \tau_2} (v_1', v_2')$ must have been derived using **eqPair**. This gives us by inversion
  - $v_1 \overset{\beta}{\simeq}^\mathcal{A}_{\tau_1} v_1'$
  - $v_1 \overset{\beta}{\simeq}^\mathcal{A}_{\tau_2} v_2'$

  Hence by induction.
  - $(v_1, v_1', (\theta_1, \theta_2, \beta), m) \in [\![\tau_1]\!]^\mathcal{A}_\mathcal{V}$ and
  - $(v_2, v_2', (\theta_1, \theta_2, \beta), m) \in [\![\tau_2]\!]^\mathcal{A}_\mathcal{V}$.

  Consequently $((v_1, v_2), (v_1', v_2'), (\theta_1, \theta_2, \beta), m) \in [\![\tau_1 \times \tau_2]\!]^\mathcal{A}_\mathcal{V}$ which is what we needed to show.

- **FSum:** In this case $A = \tau_1 + \tau_2$ for some types τ_1 and τ_2 such that $\mathtt{firstorder}(\tau_1)$ and $\mathtt{firstorder}(\tau_2)$. The equivalence could only have been derived with **eqInl** or **eqInr**.

  1. **eqInl**: In this case
     - $v = \mathtt{inl}\ v_0$,
     - $v' = \mathtt{inl}\ v_0'$, and
     - $v_0 \overset{\beta}{\simeq}^\mathcal{A}_{\tau_1} v_0'$

     From $(\mathtt{inl}\ v_0, \theta_1, m) \in \lceil \tau_1 + \tau_2 \rceil_\mathcal{V}$ and $(\mathtt{inl}\ v_0', \theta_2, m) \in \lceil \tau_1 + \tau_2 \rceil_\mathcal{V}$ we get
     - $(v_0, \theta_1, m) \in \lceil \tau_1 \rceil_\mathcal{V}$
     - $(v_0', \theta_2, m) \in \lceil \tau_1 \rceil_\mathcal{V}$.

     Hence by induction
     - $(v_0, v_0', (\theta_1, \theta_2, \beta), m) \in [\![\tau_1]\!]^\mathcal{A}_\mathcal{V}$.

     Consequently $(\mathtt{inl}\ v_0, \mathtt{inl}\ v_0', (\theta_1, \theta_2, \beta), m) \in [\![\tau_1 + \tau_2]\!]^\mathcal{A}_\mathcal{V}$ which is what we needed to show.
  2. **eqInr**: In this case
     - $v = \mathtt{inr}\ v_0$,
     - $v' = \mathtt{inr}\ v_0'$, and
     - $v_0 \overset{\beta}{\simeq}^\mathcal{A}_{\tau_2} v_0'$

     From $(\mathtt{inr}\ v_0, \theta_1, m) \in \lceil \tau_1 + \tau_2 \rceil_\mathcal{V}$ and $(\mathtt{inr}\ v_0', \theta_2, m) \in \lceil \tau_1 + \tau_2 \rceil_\mathcal{V}$ we get
     - $(v_0, \theta_1, m) \in \lceil \tau_2 \rceil_\mathcal{V}$
     - $(v_0', \theta_2, m) \in \lceil \tau_2 \rceil_\mathcal{V}$.

     Hence by induction
     - $(v_0, v_0', (\theta_1, \theta_2, \beta), m) \in [\![\tau_2]\!]^\mathcal{A}_\mathcal{V}$.

     Consequently $(\mathtt{inr}\ v_0, \mathtt{inr}\ v_0', (\theta_1, \theta_2, \beta), m) \in [\![\tau_1 + \tau_2]\!]^\mathcal{A}_\mathcal{V}$ which is what we needed to show.

- **FRef**: In this case $A = \mathtt{ref}\ \tau_0$ for some τ_0 such that $\mathtt{firstorder}(\tau_0)$. Because $(v, \theta_1, m) \in \lceil \mathtt{ref}\ \tau_0 \rceil_\mathcal{V}$ and $(v', \theta_2, m) \in \lceil \mathtt{ref}\ \tau_0 \rceil_\mathcal{V}$, we know there are locations l, l' such that
  - $v = l$,
  - $v' = l'$,
  - $\theta_1(l) = \tau_0$, and
  - $\theta_2(l') = \tau_0$

$l \,{}^{\beta}\!\simeq^{\mathcal{A}}_{\mathtt{ref}\ \tau_0}\, l'$ must have been derived by **eqRef**. Hence by inversion

- $(l, l') \in \beta$.

$(l, l', (\theta_1, \theta_2, \beta), m) \in [\![\mathtt{ref}\ \tau_0]\!]^{\mathcal{A}}_{\mathcal{V}}$ follows directly.

□

Lemma 8.44. If $\mathtt{firstorder}(\tau)$ and $(v, v', W, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$, then also $v \,{}^{W.\beta}\!\simeq^{\mathcal{A}}_{\tau}\, v'$ and if $\mathtt{firstorder}(A)$ and $(v, v', W, m) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$, then also $v \,{}^{W.\beta}\!\simeq^{\mathcal{A}}_{A}\, v'$.

Proof. By mutual induction on $\mathtt{firstorder}(\tau)$ and $\mathtt{firstorder}(A)$.

- **FPol**: In this case $\tau = (A')^p$ for some policy p and type A' such that $\mathtt{firstorder}(A')$. There are two cases
  1. $p \sqsubseteq \mathcal{A}$: In this case $(v, v', W, m) \in [\![A']\!]^{\mathcal{A}}_{\mathcal{V}}$. By induction $v \,{}^{W.\beta}\!\simeq^{\mathcal{A}}_{A'}\, v'$. By **eqLow** this suffices to show the goal.
  2. $p \not\sqsubseteq \mathcal{A}$. We get the goal by **eqHigh**.
- **FUnit:** In this case $A = \mathtt{unit}$. From $(v, v', W, m) \in [\![\mathtt{unit}]\!]^{\mathcal{A}}_{\mathcal{V}}$ we get
  - $v = ()$ and
  - $v' = ()$.

  The claim follows by **eqUnit**.
- **Fnat:** In this case $A = \mathcal{N}$. From $(v, v', W, m) \in [\![\mathcal{N}]\!]^{\mathcal{A}}_{\mathcal{V}}$ we get
  - $v = n$ and
  - $v' = n$.

  The claim follows by **eqNat**.
- **FProd**. In this case $A = \tau_1 \times \tau_2$ for some types τ_1 and τ_2 such that $\mathtt{firstorder}(\tau_1)$ and $\mathtt{firstorder}(\tau_2)$. From $(v, v', W, m) \in [\![\tau_1 \times \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$, it follows directly that there are v_1, v_2, v_1', v_2' such that
  - $v = (v_1, v_2)$,
  - $v' = (v_1', v_2')$,
  - $(v_1, v_1', W, m) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$,
  - $(v_2, v_2', W, m) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$,

  Hence by induction
  - $v_1 \,{}^{W.\beta}\!\simeq^{\mathcal{A}}_{\tau_1}\, v_1'$ and
  - $v_2 \,{}^{W.\beta}\!\simeq^{\mathcal{A}}_{\tau_2}\, v_2'$.

  The claim follows by **eqPair**.
- **FSum:** In this case $A = \tau_1 + \tau_2$ for some types τ_1 and τ_2 such that $\mathtt{firstorder}(\tau_1)$ and $\mathtt{firstorder}(\tau_2)$. From $(v, v', W, m) \in [\![\tau_1 + \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$ it follows directly that there are several cases:
  1. $v = \mathtt{inl}\ v_0$, $v' = \mathtt{inl}\ v_0'$ and
     - $(v_0, v_0', W, m) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$.

     Hence by induction
     - $v_0 \,{}^{W.\beta}\!\simeq^{\mathcal{A}}_{\tau_1}\, v_0'$.

     The goal follows by **eqInl**.
  2. $v = \mathtt{inr}\ v_0$, $v' = \mathtt{inr}\ v_0'$ and
     - $(v_0, v_0', W, m) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$.

     Hence by induction
     - $v_0 \,{}^{W.\beta}\!\simeq^{\mathcal{A}}_{\tau_2}\, v_0'$.

     The goal follows by **eqInr**.

- **FRef**: In this case $A = \mathtt{ref}\ \tau_0$ for some τ_0 such that $\mathtt{firstorder}(\tau_0)$. Because $(v, v', W, m) \in [\![\mathtt{ref}\ \tau_0]\!]^{\mathcal{A}}_{\mathcal{V}}$ we know there are locations l, l' such that
  - $v = l$,
  - $v' = l'$ and
  - $(l, l') \in W.\beta$.

  By **eqRef** this suffices to show the goal.

□

Lemma 8.45. If $v \overset{\beta}{\simeq}{}^{\mathcal{A}}_{\tau} v'$ and $\beta' \supseteq \beta$, then $v \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{\tau} v'$.

Proof. By induction on the derivation of $v \overset{\beta}{\simeq}{}^{\mathcal{A}}_{\tau} v'$. The only intersting case is the case for **eqRef**. In all other cases we just replace the premisses with either the same premisses or the premisses we get from the induction hypothesis.

In the case of **eqRef** we have $l \overset{\beta}{\simeq}{}^{\mathcal{A}}_{\tau} l'$ and $(l, l') \in \beta$. Because $\beta' \supseteq \beta$, also $(l, l') \in \beta'$. We get $l \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{\tau} l'$ by **eqRef**. □

Lemma 8.46. If $\Sigma \sqsubseteq \mathcal{A}$, $p'(\Sigma) \sqsubseteq p$ and $p \sqsubseteq \mathcal{A}$, then $p' \sqsubseteq \mathcal{A}$.

Proof. If $p' = \bot$, this is true by Lemma 4.19. Otherwise we can assume that p' is a flow lock policy. By assumption

- $p'(\Sigma) \sqsubseteq p$,
- $p \sqsubseteq \mathcal{A}$.

Consequently by transitivity (Lemma 4.1) we have

- $p'(\Sigma) \sqsubseteq \mathcal{A}$.

By Lemma 4.15

- $p'(\Sigma)(\Sigma) \sqsubseteq \mathcal{A}(\Sigma)$.

By Lemma 4.16 and Lemma 4.1 this gives us

- $p'(\Sigma) \sqsubseteq \mathcal{A}(\Sigma)$.

Remember that an attacker $\mathcal{A}$ is a pair $(a, \Sigma^{\mathcal{A}})$ and its policy is the single clause $\Sigma^{\mathcal{A}} \Rightarrow a$.

So $\mathcal{A}(\Sigma) = \Sigma^{\mathcal{A}} \backslash \Sigma \Rightarrow a$. From $p'(\Sigma) \sqsubseteq \mathcal{A}(\Sigma)$ we can therefore gather that there is a clause c in p' of the form $\Sigma_c \Rightarrow a$ such that

- $\Sigma_c \backslash \Sigma \subseteq \Sigma^{\mathcal{A}} \backslash \Sigma$.

Consequently

- $(\Sigma_c \backslash \Sigma) \cup \Sigma \subseteq (\Sigma^{\mathcal{A}} \backslash \Sigma) \cup \Sigma$.

This simplifies to

- $\Sigma_c \cup \Sigma \subseteq \Sigma^{\mathcal{A}} \cup \Sigma$.

Because $\Sigma_1 \sqsubseteq \mathcal{A}$ we have

- $\Sigma \subseteq \Sigma^{\mathcal{A}}$.

In this case $\Sigma^{\mathcal{A}} \cup \Sigma = \Sigma^{\mathcal{A}}$. Hence

- $\Sigma_c \cup \Sigma \subseteq \Sigma^{\mathcal{A}}$.

Consequently also

- $\Sigma_c \subseteq \Sigma^{\mathcal{A}}$.

This gives us

- $\Sigma_c \Rightarrow a \sqsubseteq \Sigma^{\mathcal{A}} \Rightarrow a$.

Because $\Sigma_c \Rightarrow a \in p'$ this gives us

- $p' \sqsubseteq \Sigma^{\mathcal{A}} \Rightarrow a$

which is exactly what we needed to show. □

Lemma 8.47. If $(e, e', W, \Sigma, \Sigma', m) \in [\![\tau']\!]^{\mathcal{A}}_{E}$, $\Sigma \approx_{\mathcal{A}} \Sigma'$ and $\tau'(\Sigma) <: \tau$ and $\tau'(\Sigma') <: \tau$, then $(\mathsf{new}\,(e, \tau)\,, \mathsf{new}\,(e', \tau)\,, W, \Sigma, \Sigma', [\![(\mathsf{ref}\,\tau)^{\perp}]\!]^{\mathcal{A}}_{E}$.

Proof. By induction on m. It suffices to show $(new(e, \tau), new(e', \tau), W, \Sigma, \Sigma', m) \in [\![(ref(\tau))^{\perp}]\!]^{\mathcal{A}}_{E_\beta}$. We already have $\Sigma \approx_{\mathcal{A}} \Sigma'$ by assumption. Let Σ_1, Σ_2 such that

- $\Sigma_1 \supseteq \Sigma$,
- $\Sigma_2 \supseteq \Sigma'$,
- $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

W', m' such that

- $m' < m$,
- $W' \sqsupseteq W$,

and S_1, S_2 such that

- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

There are two cases:

1. $(e, e', W, \Sigma, \Sigma', m) \in [\![\tau']\!]^{\mathcal{A}}_{E_\beta}$. In this case there are three further cases:

   (a) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \;\wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\; (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \;\wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau']\!]^{\mathcal{A}}_{E} \end{array} \right\}$

   In this case it is suffices to show

   $(new(e, \tau), new(e', \tau)) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \;\wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\; (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \;\wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![(ref(\tau))^{\perp}]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

   It is clear that neither $new(e, \tau)$ nor $new(e', \tau)$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

   - $new(e, \tau), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
   - $new(e', \tau), \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

   By assumption neither e nor e' are values. Hence the reductions must have happened with **ENew**. Hence by inversion

   - $e, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
   - $e', \Sigma_2, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
   - $e_\beta = new(e_0, \tau)$
   - $e_\beta' = new(e_0', \tau)$

   Also assume $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \;\vee\; \Sigma_2' \sqsubseteq \mathcal{A}$. This directly gives us a W'' such that

   - $W'' \sqsupseteq W'$,

- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
- $(e_0, e_0', W'', \Sigma, \Sigma', m') \in [\![\tau']\!]^{\mathcal{A}}_{E}$

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
- $(new(e_0, p), new(e_0', p), W'', \Sigma, \Sigma', m') \in [\![(\text{ref } \tau)^{\perp}]\!]^{\mathcal{A}}_{E}$. We get this by induction.

(b) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \to \neg(\text{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![\tau']\!]^{\mathcal{A}}_{E}) \end{array} \right\}$

In this case it suffices to show

$(new(e, \tau), new(e', \tau)) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \to \neg(\text{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![(\text{ref } \tau)^{\perp}]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$.

It is clear that $new(e, \tau)$ is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $new(e, \tau), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

By assumption e is not a value. Hence the reduction must have happened with **ENew**. By inversion

- $e, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e_\beta = new(e_0, \tau)$

Hence

- $\neg(\text{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_0, e', W'', \Sigma, \Sigma', m') \in [\![\tau']\!]^{\mathcal{A}}_{E}$

It suffices to show the following:

- $\neg(\text{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(new(e_0, \tau), new(e', \tau), W'', \Sigma, \Sigma', m') \in [\![(\text{ref } \tau)^{\perp}]\!]^{\mathcal{A}}_{E}$. We get this using the induction hypothesis.

(c) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \to \neg(\text{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![\tau']\!]^{\mathcal{A}}_{E}) \end{array} \right\}$

In this case it suffices to show

$(new(e, \tau), new(e', \tau)) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \to \neg(\text{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![(\text{ref } \tau)^{\perp}]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$

It is clear that $new(e', \tau)$ is not a value. So let $\omega', e_\beta', \Sigma_2', S_2'$ such that

- $new(e', \tau), \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

By assumption e' is not a value. Hence the reduction must have happened with **ENew**. By inversion

- $e', \Sigma_2, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
- $e_\beta' = new(e_0', \tau)$

Hence

- $\neg(pol(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e, e_0', W'', \Sigma, \Sigma', m') \in [\![\tau']\!]^{\mathcal{A}}_E$

It suffices to show the following:

- $\neg(pol(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(new(e, \tau), new(e_0', \tau), W'', \Sigma, \Sigma', m') \in [\![(\text{ref } \tau)^\perp]\!]^{\mathcal{A}}_E$. We get this using the induction hypothesis.

2. $(e, e', W, \Sigma, \Sigma', m) \in \left\{(v, v', W, \Sigma_{c_1}, \Sigma_{c_2}, m) \;\middle|\; (v, v', W, m) \in [\![\tau']\!]^{\mathcal{A}}_{\mathcal{V}}\right\}$

So there are v and v' such that $e = v$ and $e' = v'$ and $(v, v', W, m) \in [\![\tau']\!]^{\mathcal{A}}_{\mathcal{V}}$.

It suffices to show

$$(new(v, \tau), new(v', \tau)) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\, S_1' \;\wedge \\ \Sigma_2 \vdash e_2,\, S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\; (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![(\text{ref } \tau)^\perp]\!]^{\mathcal{A}}_E \end{array} \right\}$$

It is clear that neither $new(v, \tau)$ nor $new(v', \tau)$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $new(v, \tau), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $new(v', \tau), \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

The reductions must have happened with **ENewBeta**. Hence there are A, p, l, l' such that

- $\tau = A^p$
- $e_\beta = l$
- $e_\beta' = l'$
- $l \notin dom(S_1)$
- $l' \notin dom(S_2)$
- $\Sigma_1' = \Sigma_1$
- $\Sigma_2' = \Sigma_2$
- $S_1' = S_1 \cup \{l \rightarrowtail (v, \tau)\}$
- $S_2' = S_2 \cup \{l' \rightarrowtail (v', \tau)\}$
- $\omega = l_\tau(v)$
- $\omega' = l'_\tau(v')$

Hence the reductions are really

- $new(v, \tau), \Sigma_1, S_1 \succ l, S_1 \cup \{l \rightarrowtail (v, p)\}, l_\tau(v), \Sigma_1$
- $new(v', \tau), \Sigma_2, S_2 \succ l', S_2 \cup \{l' \rightarrowtail (v', p)\}, l'_\tau(v'), \Sigma_2$

Also assume $l_\tau(v) \approx^{\mathcal{A}}_{W'.\beta} l'_\tau(v') \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$. We know $\tau'(\Sigma) <: \tau$ and $\tau'(\Sigma') <: \tau$ or more specifically $\tau'(\Sigma) <: A^p$ and $\tau'(\Sigma') <: A^p$. Hence there must be a type B and policy p' such that

- $\tau' = \mathsf{B}^{\mathfrak{p}'}$,
- $\mathfrak{p}'(\Sigma) \sqsubseteq \mathfrak{p}$,
- $\mathfrak{p}'(\Sigma') \sqsubseteq \mathfrak{p}$ and
- $\mathsf{B} <: \mathsf{A}$.

It is clear that $W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}$ is an injective partial function because $\mathfrak{l} \notin \mathsf{dom}(S_1)$ and $\mathfrak{l}' \notin \mathsf{dom}(S_2)$. Hence it suffices to show

- $(W'.\theta_1 \cup \{\mathfrak{l}, \tau\}, W'.\theta_2 \cup \{\mathfrak{l}', \tau\}, W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}) \sqsupseteq W'$ We have to show
  - $W'.\theta_1 \cup \{\mathfrak{l}, \tau\} \sqsupseteq W'.\theta_1$. Let $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_1)$. Then clearly also $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_1 \cup \{\mathfrak{l}, \tau\})$. We still have to show $W'.\theta_1(\mathfrak{l}'') = W'.\theta_1 \cup \{\mathfrak{l}, \tau\}(\mathfrak{l}'')$ This is the case if $\mathfrak{l}'' \neq \mathfrak{l}$.

    We show $\mathfrak{l}'' \neq \mathfrak{l}$: By assumption $\mathfrak{l} \notin \mathsf{dom}(S_1)$ and $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence in particular $\mathsf{dom}(W'.\theta_1) \subseteq \mathsf{dom}(S_1)$. Because $\mathfrak{l} \notin \mathsf{dom}(S_1)$ therefore also $\mathfrak{l} \notin \mathsf{dom}(W'.\theta_1)$. But $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_1)$. Hence we must have $\mathfrak{l}'' \neq \mathfrak{l}$.
  - $W'.\theta_2 \cup \{\mathfrak{l}', \tau\} \sqsupseteq W'.\theta_2$. Let $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_2)$. Then clearly also $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_2 \cup \{\mathfrak{l}', \tau\})$. We still have to show $W'.\theta_2(\mathfrak{l}'') = W'.\theta_2 \cup \{\mathfrak{l}', \tau\}(\mathfrak{l}'')$ This is the case if $\mathfrak{l}'' \neq \mathfrak{l}'$.

    We show $\mathfrak{l}'' \neq \mathfrak{l}'$: By assumption $\mathfrak{l}' \notin \mathsf{dom}(S_2)$ and $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence in particular $\mathsf{dom}(W'.\theta_2) \subseteq \mathsf{dom}(S_2)$. Because $\mathfrak{l}' \notin \mathsf{dom}(S_2)$ therefore also $\mathfrak{l}' \notin \mathsf{dom}(W'.\theta_2)$. But $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_2)$. Hence we must have $\mathfrak{l}'' \neq \mathfrak{l}'$.
  - $W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\} \supseteq W'.\beta$. This is obvious.
- $(S_1 \cup \{\mathfrak{l} \rightarrowtail (\nu, \tau)\}, S_2 \cup \{\mathfrak{l}' \rightarrowtail (\nu', \tau)\}, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'.\theta_1 \cup \{\mathfrak{l}, \tau\}, W'.\theta_2 \cup \{\mathfrak{l}', \tau\}, W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\})$.
  We have to show
  - $W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\} \subseteq \mathsf{dom}(W'.\theta_1 \cup \{\mathfrak{l}, \tau\}) \times \mathsf{dom}(W'.\theta_2 \cup \{\mathfrak{l}', \tau\})$.
    Let $(\mathfrak{l}_1, \mathfrak{l}_2) \in W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}$. There are two options:
    (a) $(\mathfrak{l}_1, \mathfrak{l}_2) \neq (\mathfrak{l}, \mathfrak{l}')$. In this case $(\mathfrak{l}_1, \mathfrak{l}_2) \in W'.\beta$. By assumption $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence $W'.\beta \subseteq \mathsf{dom}(W'.\theta_1) \times \mathsf{dom}(W'.\theta_2)$. Therefore $(\mathfrak{l}_1, \mathfrak{l}_2) \in \mathsf{dom}(W'.\theta_1) \times \mathsf{dom}(W'.\theta_2)$. Then also $(\mathfrak{l}_1, \mathfrak{l}_2) \in \mathsf{dom}(W'.\theta_1 \cup \{\mathfrak{l}, \tau\}) \times \mathsf{dom}(W'.\theta_2 \cup \{\mathfrak{l}', \tau\})$.
    (b) $(\mathfrak{l}_1, \mathfrak{l}_2) = (\mathfrak{l}, \mathfrak{l}')$. It suffices to show $(\mathfrak{l}, \mathfrak{l}') \in \mathsf{dom}(W'.\theta_1 \cup \{\mathfrak{l}, \tau\}) \times \mathsf{dom}(W'.\theta_2 \cup \{\mathfrak{l}', \tau\})$ which is clearly the case.
  - $\forall (\mathfrak{l}_1, \mathfrak{l}_2) \in W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}.W'.\theta_1 \cup \{\mathfrak{l}, \tau\}(\mathfrak{l}_1) = W'.\theta_2 \cup \{\mathfrak{l}', \tau\}(\mathfrak{l}_2) \wedge$
    $(S_1 \cup \{\mathfrak{l} \rightarrowtail (\nu, \tau)\}(\mathfrak{l}_1), S_2 \cup \{\mathfrak{l}' \rightarrowtail (\nu', \tau)\}(\mathfrak{l}_2), (W'.\theta_1 \cup \{\mathfrak{l}, \tau\}, W'.\theta_2 \cup \{\mathfrak{l}', \tau\}, W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}), \mathfrak{m}') \in [\![W'.\theta_1 \cup \{\mathfrak{l}, \tau\}(\mathfrak{l}_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$.
    Let $(\mathfrak{l}_1, \mathfrak{l}_2) \in W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}$. There are two cases:
    (a) $(\mathfrak{l}_1, \mathfrak{l}_2) \neq (\mathfrak{l}, \mathfrak{l}')$. Then $(\mathfrak{l}_1, \mathfrak{l}_2) \in W'.\beta$. Because $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$ we know $W'.\beta \subseteq \mathsf{dom}(W.\theta_1) \times \mathsf{dom}(W.\theta_2)$. Hence
    * $\mathfrak{l}_1 \in \mathsf{dom}(W.\theta_1)$ and
    * $\mathfrak{l}_2 \in \mathsf{dom}(W.\theta_2)$.

    By the same argument as in the previous case this means that
    * $\mathfrak{l}_1 \neq \mathfrak{l}$
    * $\mathfrak{l}_2 \neq \mathfrak{l}'$.

    Therefore

    $$W'.\theta_1 \cup (\mathfrak{l}, \tau)(\mathfrak{l}_1) = W'.\theta_1(\mathfrak{l}_1) \overset{(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'}{=} W'.\theta_2(\mathfrak{l}_2) = W'.\theta_2 \cup \{\mathfrak{l}', \tau\}(\mathfrak{l}_2)$$

    .
    We also get
    * $(S_1(\mathfrak{l}_1), S_2(\mathfrak{l}_2), W', \mathfrak{m}') \in [\![W'.\theta_1(\mathfrak{l}_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$

    from $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. We have already shown in a previous case that $(W'.\theta_1 \cup \{\mathfrak{l}, \tau\}, W'.\theta_2 \cup \{\mathfrak{l}', \tau\}, W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}) \sqsupseteq W'$. Hence we get
    * $(S_1(\mathfrak{l}_1), S_2(\mathfrak{l}_2), (W'.\theta_1 \cup \{\mathfrak{l}, \tau\}, W'.\theta_2 \cup \{\mathfrak{l}', \tau\}, W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}), \mathfrak{m}') \in [\![W'.\theta_1(\mathfrak{l}_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$

    by Lemma 8.25. Because $\mathfrak{l}_1 \neq \mathfrak{l}$ and $\mathfrak{l}_2 \neq \mathfrak{l}'$ this is equivalent to the remaining subgoal.

(b) $(\mathfrak{l}_1, \mathfrak{l}_2) = (\mathfrak{l}, \mathfrak{l}')$. In this case

$$W'.\theta_1 \cup (\mathfrak{l}, \tau)(\mathfrak{l}_1) = W'.\theta_1 \cup (\mathfrak{l}, \tau)(\mathfrak{l}) = \tau = W'.\theta_2 \cup (\mathfrak{l}', \tau)(\mathfrak{l}') = W'.\theta_2 \cup (\mathfrak{l}', \tau)(\mathfrak{l}_2)$$

.

The second subgoal simplifies to $(\nu, \nu', (W'.\theta_1 \cup \{\mathfrak{l}, \tau\}, W'.\theta_2 \cup \{\mathfrak{l}', \tau\}, W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}), \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$.

τ has the form $A^{\mathfrak{p}}$. We do case analysis on whether $\mathfrak{p} \sqsubseteq \mathcal{A}$ or not:

i. $\mathfrak{p} \sqsubseteq \mathcal{A}$.

We do case analysis on $\mathfrak{l}_\tau(\nu) \approx^{\mathcal{A}}_{W'.\beta} \mathfrak{l}'_\tau(\nu') \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.

A. $\mathfrak{l}_\tau(\nu) \approx^{\mathcal{A}}_{W'.\beta} \mathfrak{l}'_\tau(\nu')$.

From $(\nu, \nu', W, \mathfrak{m}) \in [\![\tau']\!]^{\mathcal{A}}_{\mathcal{V}}$ or rather $(\nu, \nu', W, \mathfrak{m}) \in [\![B^{\mathfrak{p}'}]\!]^{\mathcal{A}}_{\mathcal{V}}$ we get

- $(\nu, W'.\theta_1, \mathfrak{m}') \in \lceil B \rceil_{\mathcal{V}}$ and
- $(\nu', W'.\theta_2, \mathfrak{m}') \in \lceil B \rceil_{\mathcal{V}}$

by Lemma 8.22,the definition of $\lceil B^{\mathfrak{p}'} \rceil_{\mathcal{V}}$ and Lemma 8.4. From this we get

- $(\nu, W'.\theta_1, \mathfrak{m}') \in \lceil A \rceil_{\mathcal{V}}$ and
- $(\nu', W'.\theta_2, \mathfrak{m}') \in \lceil A \rceil_{\mathcal{V}}$

by Lemma 8.31.

- $(\nu, W'.\theta_1, \mathfrak{m}') \in \lceil A^{\mathfrak{p}} \rceil_{\mathcal{V}}$ and
- $(\nu', W'.\theta_2, \mathfrak{m}') \in \lceil A^{\mathfrak{p}} \rceil_{\mathcal{V}}$

follows directly from the definition of $\lceil A^{\mathfrak{p}} \rceil_{\mathcal{V}}$. The only rule with which $\mathfrak{l}_\tau(\nu) \approx^{\mathcal{A}}_{W'.\beta} \mathfrak{l}'_\tau(\nu')$ can be derived is **extend-τ** as it is clear from the structure of the observations that neither **refl** nor **extend** is applicable. **high** is also not applicable because $\mathfrak{p} \sqsubseteq \mathcal{A}$ by assumption.

By inversion

- $\nu \, {}^{W'.\beta}\!\simeq^{\mathcal{A}}_{A^{\mathfrak{p}}} \nu'$.

Also remember that we have restricted ourselves to first order state. Therefore we also have $\mathtt{firstorder}(A^{\mathfrak{p}})$. Therefore Lemma 8.43 gives us $(\nu, \nu', W', \mathfrak{m}') \in [\![A^{\mathfrak{p}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. The goal follows by Lemma 8.25.

B. $\Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.

First we show that $\mathfrak{p}' \sqsubseteq \mathcal{A}$: By assumption $\Sigma_1 \supseteq \Sigma$, $\Sigma_2 \supseteq \Sigma'$, $\mathfrak{p}'(\Sigma) \sqsubseteq \mathfrak{p}$ and $\mathfrak{p}'(\Sigma') \sqsubseteq \mathfrak{p}$. Hence by Lemma 4.3 and transitivity (Lemma 4.1)

- $\mathfrak{p}'(\Sigma_1) \sqsubseteq \mathfrak{p}$ and
- $\mathfrak{p}'(\Sigma_2) \sqsubseteq \mathfrak{p}$.

In both cases ($\Sigma_1 \sqsubseteq \mathcal{A}$ and $\Sigma_2 \sqsubseteq \mathcal{A}$) we get $\mathfrak{p}' \sqsubseteq \mathcal{A}$ by Lemma 8.46.

Now we can continue with the main proof. We already know $(\nu, \nu', W, \mathfrak{m}) \in [\![B^{\mathfrak{p}'}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\mathfrak{p}' \sqsubseteq \mathcal{A}$, this means that $(\nu, \nu', W, \mathfrak{m}) \in [\![B]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.31 $(\nu, \nu', W, \mathfrak{m}) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$. From this we can directly follow $(\nu, \nu', W, \mathfrak{m}) \in [\![A^{\mathfrak{p}}]\!]^{\mathcal{A}}_{\mathcal{V}}$ because $\mathfrak{p} \sqsubseteq \mathcal{A}$ by assumption. The goal follows by Lemma 8.25 and Lemma 8.24.

ii. $\mathfrak{p} \not\sqsubseteq \mathcal{A}$.

Because $\mathfrak{p} \not\sqsubseteq \mathcal{A}$, it suffices to show

* $(\nu, W'.\theta_1 \cup \{\mathfrak{l}, \tau\}, \mathfrak{m}') \in \lceil A \rceil_{\mathcal{V}}$ and

* $(\nu', W'.\theta_2 \cup \{\mathfrak{l}', \tau\} \mathfrak{m}') \in \lceil A \rceil_{\mathcal{V}}$.

By Lemma 8.4 it suffices to show

* $(\nu, W'.\theta_1, \mathfrak{m}') \in \lceil A \rceil_{\mathcal{V}}$ and

* $(\nu', W'.\theta_2, \mathfrak{m}') \in \lceil A \rceil_{\mathcal{V}}$.

From $(\nu, \nu', W, \mathfrak{m}) \in [\![B^{\mathfrak{p}'}]\!]^{\mathcal{A}}_{\mathcal{V}}$ we get

* $(\nu, W'.\theta_1, \mathfrak{m}') \in \lceil B \rceil_{\mathcal{V}}$ and

* $(\nu', W'.\theta_2, \mathfrak{m}') \in \lceil B \rceil_{\mathcal{V}}$

by Lemma 8.22, the definition of $\lceil B^{\mathfrak{p}'} \rceil_{\mathcal{V}}$ and Lemma 8.4. We get the remaining subgoals by Lemma 8.6.

– $(S_1 \cup \{l \rightarrowtail (v,\tau)\}, m') \triangleright W'.\theta_1 \cup \{l,\tau\}$. For this we have to show
  * $\mathrm{dom}(W'.\theta_1 \cup \{l,\tau\}) \subseteq \mathrm{dom}(S_1 \cup \{l \rightarrowtail (v,\tau)\})$.

    $\mathrm{dom}(W'.\theta_1 \cup \{l,\tau\}) = \mathrm{dom}(W'.\theta_1) \cup \{l\} \overset{(S_1,S_2,m') \overset{\mathcal{A}}{\triangleright} W'}{\subseteq} \mathrm{dom}(S_1) \cup \{l\} = \mathrm{dom}(S_1 \cup \{l \rightarrowtail (v,\tau)\})$.
  * $\forall l'' \in \mathrm{dom}(W'.\theta_1 \cup \{l,\tau\}).(S_1 \cup \{l \rightarrowtail (v,\tau)\}(l''), W'.\theta_1 \cup \{l,\tau\}, m') \in \lceil W'.\theta_1 \cup \{l,\tau\}(l'')\rceil_{\mathcal{V}}$.
    Let $l'' \in \mathrm{dom}(W'.\theta_1 \cup \{l,\tau\})$. There are two cases:

    (a) $l'' \neq l$. In this case $l'' \in \mathrm{dom}(W'.\theta_1)$. By assumption $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. Hence also $(S_1, m') \triangleright W'.\theta_1$. Therefore in particular $(S_1(l''), W'.\theta_1, m') \in \lceil W'.\theta_1(l'')\rceil_{\mathcal{V}}$. Because $l'' \neq l$ this is equivalent to $(S_1 \cup \{l \rightarrowtail (v,\tau)\}(l''), W'.\theta_1, m') \in \lceil W'.\theta_1 \cup \{l,\tau\}(l'')\rceil_{\mathcal{V}}$. We get the claim by Lemma 8.4.

    (b) $l'' = l$. In this case the goal simplifies to $(v, W'.\theta_1 \cup \{l,\tau\}, m') \in \lceil\tau\rceil_{\mathcal{V}}$. By assumption $(v, v', W, m) \in [\![B^{p'}]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.22 therefore $(v, W.\theta_1, m) \in \lceil B^{p'}\rceil_{\mathcal{V}}$. By the definitions of $\lceil B^{p'}\rceil_{\mathcal{V}}$ we directly get $(v, W.\theta_1, m) \in \lceil B\rceil_{\mathcal{V}}$. From that we get $(v, W.\theta_1, m) \in \lceil A\rceil_{\mathcal{V}}$ by Lemma 8.6. We get $(v, W.\theta_1, m) \in \lceil A^p\rceil_{\mathcal{V}}$ by definition. The goal follows from Lemma 8.4 and Lemma 7.2.
  * $\forall l'' \in \mathrm{dom}(W'.\theta_1 \cup \{l,\tau\}).W'.\theta_1 \cup \{l,\tau\}(l'') = \mathtt{type}(S_1 \cup \{l \rightarrowtail (v,\tau)\}, l'')$.
    Let $l'' \in \mathrm{dom}(W'.\theta_1 \cup \{l,\tau\})$. There are two cases:

    (a) $l'' \neq l$. In this case $l'' \in \mathrm{dom}(W'.\theta_1)$. By assumption $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. Hence $W'.\theta_1(l'') = \mathtt{type}(S_1, l'')$. Because $l'' \neq l$ this is equivalent to the goal.

    (b) $l'' = l$. In this case the goal simplifies to $\tau = \tau$. This is clearly the case.

– $(S_2 \cup \{l' \rightarrowtail (v',\tau)\}, m') \triangleright W'.\theta_2 \cup \{l',\tau\}$. For this we have to show
  * $\mathrm{dom}(W'.\theta_2 \cup \{l',\tau\}) \subseteq \mathrm{dom}(S_2 \cup \{l' \rightarrowtail (v',\tau)\})$.

    $\mathrm{dom}(W'.\theta_2 \cup \{l',\tau\}) = \mathrm{dom}(W'.\theta_2) \cup \{l'\} \overset{(S_1,S_2,m') \overset{\mathcal{A}}{\triangleright} W'}{\subseteq} \mathrm{dom}(S_2) \cup \{l'\} = \mathrm{dom}(S_2 \cup \{l' \rightarrowtail (v',\tau)\})$.
  * $\forall l'' \in \mathrm{dom}(W'.\theta_2 \cup \{l',\tau\}).(S_2 \cup \{l' \rightarrowtail (v',\tau)\}(l''), W'.\theta_2 \cup \{l',\tau\}, m') \in \lceil W'.\theta_2 \cup \{l',\tau\}(l'')\rceil_{\mathcal{V}}$. Let $l'' \in \mathrm{dom}(W'.\theta_2 \cup \{l',\tau\})$. There are two cases:

    (a) $l'' \neq l'$. In this case $l'' \in \mathrm{dom}(W'.\theta_2)$. By assumption $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. Hence also $(S_2, m') \triangleright W'.\theta_2$. Therefore in particular $(S_2(l''), W'.\theta_2, m') \in \lceil W'.\theta_2(l'')\rceil_{\mathcal{V}}$. Because $l'' \neq l'$ this is equivalent to $(S_1 \cup \{l' \rightarrowtail (v',\tau)\}(l''), W'.\theta_2, m') \in \lceil W'.\theta_2 \cup \{l',\tau\}(l'')\rceil_{\mathcal{V}}$. We get the claim by Lemma 8.4.

    (b) $l'' = l'$. In this case the goal simplifies to $(v', W'.\theta_2 \cup \{l',\tau\}, m') \in \lceil\tau\rceil_{\mathcal{V}}$. By assumption $(v, v', W, m) \in [\![B^{p'}]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.22 therefore $(v', W.\theta_2, m) \in \lceil B^{p'}\rceil_{\mathcal{V}}$.By the definitions of $\lceil B^{p'}\rceil_{\mathcal{V}}$ we directly get $(v', W.\theta_2, m) \in \lceil B\rceil_{\mathcal{V}}$. From that we get $(v', W.\theta_2, m) \in \lceil A\rceil_{\mathcal{V}}$ by Lemma 8.6. We get $(v', W.\theta_2, m) \in \lceil A^p\rceil_{\mathcal{V}}$ by definition. The goal follows from Lemma 8.4 and Lemma 7.2.
  * $\forall l'' \in \mathrm{dom}(W'.\theta_2 \cup \{l',\tau\}).W'.\theta_2 \cup \{l',\tau\}(l'') = \mathtt{type}(S_2 \cup \{l' \rightarrowtail (v',p)\}, l'')$.
    Let $l'' \in \mathrm{dom}(W'.\theta_2 \cup \{l',\tau\})$. There are two cases:

    (a) $l'' \neq l'$. In this case $l'' \in \mathrm{dom}(W'.\theta_2)$. By assumption $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. Hence $W'.\theta_2(l'') = \mathtt{type}(S_2, l'')$. Because $l'' \neq l'$ this is equivalent to the goal.

    (b) $l'' = l'$. In this case the goal simplifies to $\tau = \tau$. This is clearly the case.

- $l_\tau(v) \approx^{\mathcal{A}}_{W'.\beta \cup \{(l,l')\}} l'_\tau(v')$.
  We do case analysis on the visibility of p.

  (a) $p \not\sqsubseteq \mathcal{A}$. Because $\mathtt{pol}(\tau) = p$ we get the claim by **high**.

  (b) $p \sqsubseteq \mathcal{A}$: By **extend-τ** it suffices to show
  – $(l, l') \in W'.\beta \cup \{(l, l')\}$. This is obvious.
  – $v \,{}^{W'.\beta \cup \{(l,l')\}}\!\simeq^{\mathcal{A}}_{\tau} v'$. By Lemma 8.45 it suffices to show $v \,{}^{W'.\beta}\!\simeq^{\mathcal{A}}_{\tau} v'$. We do case analysis on $l_\tau(v) \approx^{\mathcal{A}}_{W'.\beta} l'_\tau(v') \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.
    i. $l_\tau(v) \approx^{\mathcal{A}}_{W'.\beta} l'_\tau(v')$. This must have been derived by **extend-τ**. Because $\tau = A^p$. We get the claim by inversion.
    ii. $\Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.

    First we show that $p' \sqsubseteq \mathcal{A}$: By assumption $\Sigma_1 \supseteq \Sigma$, $\Sigma_2 \supseteq \Sigma'$, $p'(\Sigma) \sqsubseteq p$ and $p'(\Sigma') \sqsubseteq p$. Hence by Lemma 4.3 and transitivity (Lemma 4.1)

☞ $p'(\Sigma_1) \sqsubseteq p$ and
☞ $p'(\Sigma_2) \sqsubseteq p$.
In both cases ($\Sigma_1 \sqsubseteq \mathcal{A}$ and $\Sigma_2 \sqsubseteq \mathcal{A}$) we get $p' \sqsubseteq \mathcal{A}$ by Lemma 8.46.

Remember that by assumption $\mathtt{firstorder}(\tau)$. Hence by Lemma 8.44 it suffices to show $(v, v', W', m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.25 it suffices to show $(v, v', W, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. We already know $(v, v', W, m) \in [\![\tau']\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\tau' = B^{p'}$ this gives us $(v, v', W, m) \in [\![B^{p'}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $p' \sqsubseteq \mathcal{A}$ we have $(v, v', W, m) \in [\![B]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.31 we get $(v, v', W, m) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$. $(v, v', W, m) \in [\![A^p]\!]^{\mathcal{A}}_{\mathcal{V}}$ follows because $p \sqsubseteq \mathcal{A}$. As $\tau = A^p$ this shows the goal.

- $(l, l', (W'.\theta_1 \cup \{l, \tau\}, W'.\theta_2 \cup \{l', \tau\}, W'.\beta \cup \{(l, l')\}), \Sigma, \Sigma', m') \in [\![(\mathtt{ref}(\tau))^{\perp}]\!]^{\mathcal{A}}_{E}$.
  It suffices to show $(l, l', (W'.\theta_1 \cup \{l, A^p\}, W'.\theta_2 \cup \{l', A^p\}, W'.\beta \cup \{(l, l')\}), m') \in [\![(\mathtt{ref}(A^p))^{\perp}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\perp \sqsubseteq \mathcal{A}$ (Lemma 4.19) it suffices to show $(l, l', (W'.\theta_1 \cup \{l, A^p\}, W'.\theta_2 \cup \{l', A^p\}, W'.\beta \cup \{(l, l')\}), m') \in [\![\mathtt{ref}(A^p)]\!]^{\mathcal{A}}_{\mathcal{V}}$. This means we need to show
  - $W'.\theta_1 \cup \{l, A^p\}(l) = A^p = W'.\theta_2 \cup \{l', A^p\}(l')$. This is clearly the case.
  - $(l, l') \in W'.\beta \cup \{(l, l')\}$. This is clearly the case.

□

Lemma 8.48. If $(e, e', W, \Sigma, \Sigma', m) \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_{E}$, $\Sigma \approx_{\mathcal{A}} \Sigma'$, $p \sqsubseteq \tau$ and $\tau' <: \tau$, then $(!\,e, !\,e', W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$.

Proof. By induction on m. It suffices to show $(!e, !e', W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{E_\beta}$. We already have $\Sigma \approx_{\mathcal{A}} \Sigma'$ by assumption. Let Σ_1, Σ_2 such that

- $\Sigma_1 \supseteq \Sigma$,
- $\Sigma_2 \supseteq \Sigma'$,
- $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

W', m' such that

- $m' < m$,
- $W' \sqsupseteq W$,

and S_1, S_2 such that

- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

There are two cases:

1. $(e, e', W, \Sigma, \Sigma', m) \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_{E_\beta}$. There are three additional cases:

(a) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \ \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\ S_1' \ \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2',\ S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \ \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

In this case it is suffices to show

$(!e, !e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \ \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\ S_1' \ \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2',\ S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \ \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

Clearly neither $!e$ nor $!e'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $!e, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $!e', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Because e and e' are not values the reductions must have happened with **EDeref**. Hence by inversion

- $e, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e', \Sigma_2, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
- $e_\beta = !e_0$
- $e_\beta' = !e_0'$

Also assume $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \ \vee \ \Sigma_2' \sqsubseteq \mathcal{A}$. This directly gives us a W'' such that

- $W'' \sqsupseteq W'$,
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
- $(e_0, e_0', W'', \Sigma, \Sigma', m') \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_E$.

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
- $(!e_0, !e_0', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E$ We get this by induction.

(b) $$(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\, S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_E) \end{array} \right\}$$

In this case it suffices to show

$$(!e, !e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\, S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E) \end{array} \right\}$$

It is clear that $!e$ is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $!e, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

Because e is not a value, the reduction must have happened with **EDeref**. By inversion

- $e, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e_\beta = !e_0$

Hence

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_0, e', W'', \Sigma, \Sigma', m') \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_E)$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(!e_0, !e', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E$. We get this using the induction hypothesis.

(c) $$(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \overset{\omega;\Sigma_2'}{\Longrightarrow} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_E) \end{array} \right\}$$

In this case it suffices to show

$$(!e, !e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$$

It is clear that $!e'$ is not a value. So let $\omega', e'_\beta, \Sigma_2', S_2'$ such that

- $!e', \Sigma_2, S_2 \succ e'_\beta, S_2', \omega', \Sigma_2'$

The reduction must have happened with **EDeref**. By inversion

- $e', \Sigma_2, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
- $e'_\beta = !e_0'$

Hence

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e, e_0', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\mathsf{ref}\ \tau')^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathsf{E}}$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(!e, !e_0', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this using the induction hypothesis.

(d) $(e, e', W, \Sigma, \Sigma', \mathfrak{m}) \in \left\{ (v, v', W, \Sigma_1, \Sigma_2, \mathfrak{m}) \;\middle|\; (v, v', W, \mathfrak{m}) \in [\![(\mathsf{ref}\ \tau')^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathcal{V}} \right\}$

Consequently e and e' are values v and v', respectively and $(v, v', W, \mathfrak{m}) \in [\![(\mathsf{ref}\ \tau')^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathcal{V}}$.
In this case it is suffices to show

$$(!v, !v') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\, S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge\; (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \cong^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$$

Clearly neither $!v$ nor $!v'$ is a value. So let $\omega, \omega', e_\beta, e'_\beta, \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $!v, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $!v', \Sigma_2, S_2 \succ e'_\beta, S_2', \omega', \Sigma_2'$

Because v and v' are values the reductions must have happened with **EDerefBeta**. Hence by inversion there are $l, l', v_0, v_0', \tau'', \tau'''$ such that

- $l \rightarrowtail (v_0, \tau'') \in S_1$
- $l' \rightarrowtail (v_0', \tau''') \in S_2$
- $S_1' = S_1$
- $S_2' = S_2$
- $\Sigma_1' = \Sigma_1$
- $\Sigma_2' = \Sigma_2$
- $e_\beta = v_0$
- $e'_\beta = v_0'$
- $\omega = \epsilon = \omega'$
- $v = l$
- $v' = l'$

So the reductions are really

- $!l, \Sigma_1, S_1 \succ v_0, S_1, \epsilon, \Sigma_1$

- $!l', \Sigma_2, S_2 \succ v_0', S_2, \epsilon, \Sigma_2$

Also assume $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon \vee \Sigma_1' \sqsubseteq \mathcal{A} \ \vee \ \Sigma_2' \sqsubseteq \mathcal{A}$. It suffices to show

- $W' \sqsupseteq W'$. We get this by Lemma 7.2.
- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. We already know that.
- $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon$. We get this by **refl**.
- $(v_0, v_0', W', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. It suffices to show $(v_0, v_0', W', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. By assumption $(l, l', W, m) \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_{\mathcal{V}}$. We do case analysis on whether $p \sqsubseteq \mathcal{A}$ or not:
  i. $p \sqsubseteq \mathcal{A}$: In this case $(l, l', W, m) \in [\![\mathsf{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.25 also $(l, l', W', m') \in [\![\mathsf{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$. Therefore
     – $W'.\theta_1(l) = \tau' = W'.\theta_2(l')$.
     – $(l, l') \in W'.\beta$.

     Because $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ in particular
     – $(S_1(l), S_2(l'), W', m') \in [\![\tau']\!]^{\mathcal{A}}_{\mathcal{V}}$.

     By assumption $l \rightarrowtail (v_0, \tau'') \in S_1$ and $l' \rightarrowtail (v_0', \tau''') \in S_2$. So this simplifies to
     – $(v_0, v_0', W', m') \in [\![\tau']\!]^{\mathcal{A}}_{\mathcal{V}}$

     We get the goal by Lemma 8.31.
  ii. $p \not\sqsubseteq \mathcal{A}$: τ has the form A^q. We get
     – $(l, l', W', m') \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_{\mathcal{V}}$ by Lemma 8.25 and Lemma 8.24.

     Because $p \not\sqsubseteq \mathcal{A}$ this means
     – $(l, W'.\theta_1, m') \in \lceil \mathsf{ref}\ \tau' \rceil_{\mathcal{V}}$ and
     – $(l', W'.\theta_2, m') \in \lceil \mathsf{ref}\ \tau' \rceil_{\mathcal{V}}$.

     Hence
     – $W'.\theta_1(l) = \tau'$ and
     – $W'.\theta_2(l') = \tau'$

     We know $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. In particular this means
     – $(S_1, m') \triangleright W'.\theta_1$ and
     – $(S_2, m') \triangleright W'.\theta_2$.

     Because $W'.\theta_1(l) = \tau' = W'.\theta_2(l')$ in particular $l \in \mathrm{dom}(W'.\theta_1)$ and $l' \in \mathrm{dom}(W'.\theta_2)$. Therefore the well formedness gives us
     – $(S_1(l), W'.\theta_1, m') \in \lceil W'.\theta_1(l) \rceil_{\mathcal{V}}$ and
     – $(S_2(l'), W'.\theta_2, m') \in \lceil W'.\theta_2(l') \rceil_{\mathcal{V}}$.

     With the knowledge we already have this simplifies to
     – $(v_0, W'.\theta_1, m') \in \lceil \tau' \rceil_{\mathcal{V}}$ and
     – $(v_0', W'.\theta_2, m') \in \lceil \tau' \rceil_{\mathcal{V}}$.

     Because $\tau' <: \tau$ and $\tau = A^q$ we get by inversion of **sub-policy**
     – $\tau' = B^{q'}$,
     – $B <: A$, and
     – $q' \sqsubseteq q$.

     So the definition of $\lceil B^{q'} \rceil_{\mathcal{V}}$ we get
     – $(v_0, W'.\theta_1, m') \in \lceil B \rceil_{\mathcal{V}}$ and
     – $(v_0', W'.\theta_2, m') \in \lceil B \rceil_{\mathcal{V}}$.

     By assumption $p \sqsubseteq \tau$. Hence also $\tau \not\sqsubseteq \mathcal{A}$, because otherwise we would have $p \sqsubseteq \mathcal{A}$ by transitivity Lemma 4.1. This means $q \not\sqsubseteq \mathcal{A}$. Hence it suffices to show
     – $(v_0, W''.\theta_1, m') \in \lceil A \rceil_{\mathcal{V}}$.
       We get this by Lemma 8.6.
     – $(v_0', W''.\theta_2, m') \in \lceil A \rceil_{\mathcal{V}}$.
       We get this by Lemma 8.6.

□

Lemma 8.49. If $(e_1, e_1', W, \Sigma, \Sigma', m) \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_{\mathsf{E}}$, $(e_2, e_2', W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$, $p \sqsubseteq \tau'$, $\tau(\Sigma) <: \tau'$, $\tau(\Sigma') <: \tau'$ and $\Sigma \approx_{\mathcal{A}} \Sigma'$, then
$(e_1 := e_2, e_1' := e_2', W, \Sigma, \Sigma', m) \in [\![\mathsf{unit}^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$.

Proof. By induction on m. It suffices to show $(e_1 := e_2, e_1' := e_2', W, \Sigma, \Sigma', m) \in [\![\mathsf{unit}^\perp]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. We already have $\Sigma \approx_{\mathcal{A}} \Sigma'$ by assumption. Let Σ_1, Σ_2 such that

- $\Sigma_1 \supseteq \Sigma$,
- $\Sigma_2 \supseteq \Sigma'$,
- $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

W', m' such that

- $m' < m$,
- $W' \sqsupseteq W$,

and S_1, S_2 such that

- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

There are two cases:

1. $(e_1, e_1', W, \Sigma, \Sigma', m) \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. This leaves us with three further cases:

   (a) $(e_1, e_1') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\ S_1' \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2',\ S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![(\mathsf{ref}\tau')^p]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$

   In that case it suffices to show

   $(e_1 := e_2, e_1' := e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\ S_1' \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2',\ S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\mathsf{unit}^\perp]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$

   Neither $e_1 := e_2$ nor $e_1' := e_2'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

   - $e_1 := e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
   - $e_1' := e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

   Since neither e_1 nor e_1' is a value and therefore also not a location, the reductions must have happened with **Eassignl**. Hence by inversion

   - $e_1, \Sigma_1, S_1 \succ e_\iota, S_1', \omega, \Sigma_1'$
   - $e_1', \Sigma_2, S_2 \succ e_\iota', S_2', \omega', \Sigma_2'$
   - $e_\beta = e_\iota := e_2$
   - $e_\beta' = e_\iota' := e_2'$

   Also let $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \ \vee\ \Sigma_2' \sqsubseteq \mathcal{A}$. This directly gives us a W'' such that

   - $W'' \sqsupseteq W'$,
   - $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$,
   - $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
   - $(e_\iota, e_\iota', W'', \Sigma, \Sigma', m') \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_{\mathsf{E}}$

   It suffices to show

   - $W'' \sqsupseteq W'$. We already know that.
   - $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.

- $\omega \approx^{\mathcal{A}}_{W'',\beta} \omega'$. We already know that.
- $(e_\iota := e_2, e'_\iota := e'_2, W'', \Sigma, \Sigma', m') \in [\![\mathtt{unit}^\perp]\!]^{\mathcal{A}}_{\mathsf{E}}$ We have $W'' \sqsupseteq W$ by transitivity (Lemma 7.2). Hence we also have $(e_2, e'_2, W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ by Lemma 8.29. We get the claim by induction.

(b) $$(e_1, e'_1) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e'_1, S'_1, \Sigma'_1, \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma'_1} e'_1,\, S'_1 \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S'_1, S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e'_1, e_2, W'', \Sigma, \Sigma', m') \in [\![(\mathtt{ref}\ \tau')^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$$

In this case it suffices to show

$$(e_1 := e_2, e'_1 := e'_2) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e'_1, S'_1, \Sigma'_1, \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma'_1} e'_1,\, S'_1 \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S'_1, S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e'_1, e_2, W'', \Sigma, \Sigma', m') \in [\![\mathtt{unit}^\perp]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$$

It is clear that $e_1 := e_2$ is not a value. So let $\omega, e_\beta, \Sigma'_1, S'_1$ such that

- $e_1 := e_2, \Sigma_1, S_1 \succ e_\beta, S'_1, \omega, \Sigma'_1$

By assumption e_1 is not a value and therefore also not a location. Hence the reduction must have happened with **Eassignl**. By inversion

- $e_1, \Sigma_1, S_1 \succ e_\iota, S'_1, \omega, \Sigma'_1$
- $e_\beta = e_\iota := e_2$

From our assumption we get

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S'_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_\iota, e'_1, W'', \Sigma, \Sigma', m') \in [\![(\mathtt{ref}\ \tau')^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathsf{E}}$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S'_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(e_\iota := e_2, e'_1 := e'_2, \Sigma, \Sigma', m') \in [\![\mathtt{unit}^\perp]\!]^{\mathcal{A}}_{\mathsf{E}}$. We know $(e_\iota, e'_1, W'', \Sigma, \Sigma', m') \in [\![(\mathtt{ref}\ \tau')^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get $(e_2, e'_2, W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ by Lemma 8.29. The goal follows using the induction hypothesis.

(c) $$(e_1, e'_1) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e'_2, S'_2, \Sigma'_2, \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma'_2} e'_2,\, S'_2 \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S'_2, m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e'_2, W'', \Sigma, \Sigma', m') \in [\![(\mathtt{ref}\ \tau')^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$$

In this case it suffices to show

$$(e_1 := e_2, e'_1 := e'_2) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e'_2, S'_2, \Sigma'_2, \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma'_2} e'_2,\, S'_2 \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S'_2, m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e'_2, W'', \Sigma, \Sigma', m') \in [\![\mathtt{unit}^\perp]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$$

Clearly $e'_1 := e'_2$ is not a value. So let $\omega, e'_\beta, \Sigma'_2, S'_2$ such that

- $e'_1 := e'_2, \Sigma_2, S_2 \succ e'_\beta, S'_2, \omega, \Sigma'_2$

By assumption e'_1 is not a value and therefore also not a location. Hence the reduction must have happened with **Eassignl**. By inversion

- $e'_1, \Sigma_2, S_2 \succ e'_\iota, S'_2, \omega, \Sigma'_2$
- $e'_\beta = e'_\iota := e'_2$

From our assumption we get

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_1, e_\mathfrak{l}', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\mathtt{ref}\ \tau')^p]\!]^{\mathcal{A}}_E$

It suffices to show the following:

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(e_1 := e_2, e_\mathfrak{l}' := e_2', \Sigma, \mathfrak{m}') \in [\![\mathtt{unit}^\perp]\!]^{\mathcal{A}}_E$. We know $(e_1, e_\mathfrak{l}', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\mathtt{ref}\ \tau')^p]\!]^{\mathcal{A}}_E$. We get $(e_2, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_E$ by Lemma 8.29. The goal follows using the induction hypothesis.

2. $(e_1, e_1', W, \Sigma, \Sigma', \mathfrak{m}) \in \left\{(v, v', W, \Sigma_{c_1}, \Sigma_{c_2}, \mathfrak{m}) \,\middle|\, (v, v', W, \mathfrak{m}) \in [\![(\mathtt{ref}\ \tau')^p]\!]^{\mathcal{A}}_V\right\}$

Hence e_1 and e_1' are values v_1 and v_1' respectively such that $(v_1, v_1', W, \mathfrak{m}) \in [\![(\mathtt{ref}\ \tau')^p]\!]^{\mathcal{A}}_V$. Either $p \sqsubseteq \mathcal{A}$ or $p \not\sqsubseteq \mathcal{A}$. In the first case $(v_1, v_1', W, \mathfrak{m}) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_V$ and in the second case both $(v_1, W.\theta_1, \mathfrak{m}) \in \lceil \mathtt{ref}\ \tau' \rceil_V$ and $(v_1', W.\theta_2, \mathfrak{m}) \in \lceil \mathtt{ref}\ \tau' \rceil_V$. In both cases this means that there are locations $\mathfrak{l}$ and $\mathfrak{l}'$ such that

- $e_1 = \mathfrak{l}$,
- $e_1' = \mathfrak{l}'$ and
- $W.\theta_1(\mathfrak{l}) = \tau' = W.\theta_2(\mathfrak{l}')$.

This leaves us with two cases again:

(a) $(e_2, e_2', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{E_\beta}$. There are again further cases:

i. $(e_2, e_2') \in \left\{(e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \wedge \\ \Sigma_2 \vdash e_2, S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2', S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_E \end{array}\right\}$

In that case it suffices to show

$(\mathfrak{l} := e_2, \mathfrak{l}' := e_2') \in \left\{(e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \wedge \\ \Sigma_2 \vdash e_2, S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2', S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\mathtt{unit}^\perp]\!]^{\mathcal{A}}_E \end{array}\right\}$

Clearly $\mathfrak{l} := e_2$ and $\mathfrak{l}' := e_2'$ are not values. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $\mathfrak{l} := e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $\mathfrak{l}' := e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Since e_2 and e_2' are not values by assumption, the reductions must have happened with **Eassignr**. Hence by inversion

- $e_2, \Sigma_1, S_1 \succ e_r, S_1', \omega, \Sigma_1'$
- $e_2', \Sigma_2, S_2 \succ e_r', S_2', \omega', \Sigma_2'$
- $e_\beta = \mathfrak{l} := e_r$
- $e_\beta' = \mathfrak{l}' := e_r'$

Also let $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \ \vee\ \Sigma_2' \sqsubseteq \mathcal{A}$. This directly gives us a W'' such that

- $W'' \sqsupseteq W'$,
- $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
- $(e_r, e_r', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{E}$

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
- $(\mathfrak{l} := e_r, \mathfrak{l}' := e_r', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\mathtt{unit}^{\perp})]\!]^{\mathcal{A}}_{E}$ We have $W'' \sqsupseteq W$ by transitivity (Lemma 7.2). Hence we also have $(\mathfrak{l}, \mathfrak{l}', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\mathtt{ref}\ \tau')^{p}]\!]^{\mathcal{A}}_{E}$ by Lemma 8.29. We get the claim by induction.

ii. $$(e_2, e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma_1'} e_1', S_1' \rightarrow \neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$$

In this case it suffices to show

$$(\mathfrak{l} := e_2, \mathfrak{l}' := e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma_1'} e_1', S_1' \rightarrow \neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\mathtt{unit}^{\perp}]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$$

It is clear that $\mathfrak{l} := e_2$ is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $\mathfrak{l} := e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

Because e_2 is not a value the reduction must have happened with **Eassignr**. By inversion

- $e_2, \Sigma_1, S_1 \succ e_r, S_1', \omega, \Sigma_1'$
- $e_\beta = \mathfrak{l} := e_r$

From our assumption we get

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_r, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{E}$

It suffices to show the following:

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\mathfrak{l} := e_r, \mathfrak{l}' := e_2', \Sigma, \Sigma', \mathfrak{m}') \in [\![\mathtt{unit}^{\perp}]\!]^{\mathcal{A}}_{E}$. We know $(e_r, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{E})$. We get $(\mathfrak{l}, \mathfrak{l}', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\mathtt{ref}\ \tau')^{p}]\!]^{\mathcal{A}}_{E}$ by Lemma 8.29. The goal follows using the induction hypothesis.

iii. $$(e_2, e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega;\Sigma_2'} e_2', S_2' \rightarrow \neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$$

In this case it suffices to show

$$(\mathfrak{l} := e_2, \mathfrak{l}' := e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega;\Sigma_2'} e_2', S_2' \rightarrow \neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\mathtt{unit}^{\perp}]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$$

It is clear that $\mathfrak{l}' := e_2'$ is not a value. So let $\omega, e_\beta', \Sigma_2', S_2'$ such that

- $\mathfrak{l}' := e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega, \Sigma_2'$

Because e_2' is not a value, the reduction must have happened with **Eassignr**. By inversion

- $e_2', \Sigma_2, S_2 \succ e_r', S_2', \omega, \Sigma_2'$
- $e_\beta' = l' := e_r'$

From our assumption we get

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_2, e_r', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E$

It suffices to show the following:

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(l := e_2, l' := e_r', \Sigma, \Sigma', m') \in [\![\mathtt{unit}^\perp]\!]^{\mathcal{A}}_E$. We know $(e_2, e_r', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E$. We get $(l, l', W'', \Sigma, \Sigma', m') \in [\![(\mathtt{ref}\ \tau')^p]\!]^{\mathcal{A}}_E$ by Lemma 8.29. The goal follows using the induction hypothesis.

(b) $(e_2, e_2', W, \Sigma, \Sigma', m) \in \{(v, v', W, \Sigma_c, m) \mid (v, v', W, m) \in [\![\tau]\!]^{\mathcal{A}}_V\}$

In this case e_2 and e_2' are values v_2 and v_2', respectively such that $(v_2, v_2', W, m) \in [\![\tau]\!]^{\mathcal{A}}_V$.

It suffices to show

$$(l := v_2, l' := v_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1',\ S_1' \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2',\ S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E \end{array} \right\}$$

.

It is clear that both $l := v_2$ and $l' := v_2'$ are not values. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $l := v_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $l' := v_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Since v_2 and v_2' are values, the reductions must have happened with **Eassign**. Hence

- $l \in \mathtt{dom}(S_1)$
- $l' \in \mathtt{dom}(S_2)$
- $e_\beta = ()$
- $e_\beta' = ()$
- $\omega = l_{\mathtt{type}(S_1, l)}(v_2)$
- $\omega' = l'_{\mathtt{type}(S_2, l')}(v_2')$
- $S_1' = S_1[l \rightarrowtail (v_2, \mathtt{type}(S_1, l))]$
- $S_2' = S_2[l' \rightarrowtail (v_2', \mathtt{type}(S_2, l'))]$
- $\Sigma_1' = \Sigma_1$
- $\Sigma_2' = \Sigma_2$

So the reductions are really

- $l := v_2, \Sigma_1, S_1 \succ (), S_1[l \rightarrowtail (v_2, \mathtt{type}(S_1, l))], l_{\mathtt{type}(S_1, l)}(v_2), \Sigma_1$
- $l' := v_2', \Sigma_2, S_2 \succ (), S_2[l' \rightarrowtail (v_2', \mathtt{type}(S_2, l'))], l'_{\mathtt{type}(S_2, l')}(v_2'), \Sigma_2$

Also assume $l_{\mathtt{type}(S_1, l)}(v_2) \approx^{\mathcal{A}}_{W'.\beta} l'_{\mathtt{type}(S_2, l')}(v_2') \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$. We know $\tau(\Sigma) <: \tau'$, $\tau(\Sigma') <: \tau'$, and $p \sqsubseteq \tau'$. More specifically τ has the form A^q and τ' has the form B^r and therefore $A^q(\Sigma) <: B^r$, $A^q(\Sigma') <: B^r$, and $p \sqsubseteq B^r$. Hence

- $q(\Sigma) \sqsubseteq r$,
- $q(\Sigma') \sqsubseteq r$,

- $A <: B$, and
- $p \sqsubseteq r$.

By assumption

- $W.\theta_1(l) = \tau' = B^r$.

Because $W' \sqsupseteq W$ and $W'.\theta_1(l) = W'.\theta_2(l')$, also

- $W'.\theta_1(l) = B^r = W'.\theta_2(l')$.

From $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ we get $(S_1, m') \triangleright W'.\theta_1$ and $(S_2, m') \triangleright W'.\theta_2$. Consequently

- $W'.\theta_1(l) = \mathtt{type}(S_1, l)$ and
- $W'.\theta_2(l') = \mathtt{type}(S_2, l')$.

We already know what $W'.\theta_1(l)$ and $W'.\theta_2(l')$ are, namely B^r. Hence

- $\mathtt{type}(S_1, l) = B^r$ and
- $\mathtt{type}(S_2, l') = B^r$.

It suffices to show

- $W' \sqsupseteq W'$. We get this by reflexivity (Lemma 7.2).
- $(S_1[l \rightarrowtail (v_2, \mathtt{type}(S_1, l))], S_2[l' \rightarrowtail (v_2', \mathtt{type}(S_2, l'))], m') \overset{\mathcal{A}}{\triangleright} W'$.

  We have to show
  - $W'.\beta \subseteq W'.\theta_1 \times W'.\theta_2$.

    We get this from $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.
  - $\forall (l_1, l_2) \in W'.\beta.\ W'.\theta_1(l_1) = W'.\theta_2(l_2) \wedge$
    $(S_1[l \rightarrowtail (v_2, \mathtt{type}(S_1, l))](l_1), S_2[l' \rightarrowtail (v_2', \mathtt{type}(S_1', l'))](l_2), W', m') \in [\![W'.\theta_1(l_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$.

    Let $(l_1, l_2) \in W'.\beta$. We get $W'.\theta_1(l_1) = W'.\theta_2(l_2)$ from $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. All that remains to be shown is $(S_1[l \rightarrowtail (v_2, \mathtt{type}(S_1, l))](l_1), S_2[l' \rightarrowtail (v_2', \mathtt{type}(S_1', l'))](l_2), W', m') \in [\![W'.\theta_1(l_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$. There are four cases:

    i. $l_1 \neq l$ and $l_2 \neq l'$. Because $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ we know $W'.\beta \subseteq \mathtt{dom}(W.\theta_1) \times \mathtt{dom}(W.\theta_2)$. We also get
    - $(S_1(l_1), S_2(l_2), W', m') \in [\![W'.\theta_1(l_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$

    from $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. Because $l_1 \neq l$ and $l_2 \neq l'$ this is equivalent to the remaining subgoal.

    ii. $l_1 = l$ and $l_2 \neq l'$.
    In this case it suffices to show $(v_2, S_2(l_2), W', m') \in [\![B^r]\!]^{\mathcal{A}}_{\mathcal{V}}$. We do case analysis on the visibility of r.

    A. $r \sqsubseteq \mathcal{A}$: We will show that this is impossible.
    By transitivity Lemma 4.1 we get $p \sqsubseteq \mathcal{A}$. By assumption $(l, l', W, m) \in [\![(\mathtt{ref}\ \tau')^p]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $p \sqsubseteq \mathcal{A}$ $(l, l', W, m) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.25 $(l, l', W', m) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$.
    In particular this means
    ☞ $(l, l') \in W'.\beta$.
    By assumption $W'.\beta$ is an injection and therefore in particular a function. Hence there can be no other $l'' \neq l'$ such that $(l, l'') \in W'.\beta$. But by assumption $(l, l_2) \in W'.\beta$ and $l_2 \neq l'$. ↯.

    B. $r \not\sqsubseteq \mathcal{A}$ In this case it suffices to show
    ☞ $(v_2, W'.\theta_1, m') \in \lceil B \rceil_{\mathcal{V}}$. We already know $(v_2, v_2', W, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.22 and Lemma 8.4 we have $(v_2, W'.\theta_1, m') \in \lceil \tau \rceil_{\mathcal{V}}$. As $\tau = A^q$ this gives us $(v_2, W'.\theta_1, m') \in \lceil A \rceil_{\mathcal{V}}$. The goal follows by Lemma 8.6.
    ☞ $(S_2(l_2), W', m') \in \lceil B \rceil_{\mathcal{V}}$. Because $(S_2, m') \triangleright W'.\theta_2$ we have $(S_2(l_2), W'.\theta_2, m') \in \lceil W'.\theta_2(l_2) \rceil_{\mathcal{V}}$. By assumption $(l, l_2) \in W'.\beta$. Because $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ this means that $W'.\theta_1(l) = W'.\theta_2(l_2)$. We have already seen that $W'.\theta_1(l) = B^r$. Hence $(S_2(l_2), W'.\theta_2, m') \in \lceil B^r \rceil_{\mathcal{V}}$. The goal follows by the definition of $\lceil B^r \rceil_{\mathcal{V}}$.

iii. $\mathsf{l}_1 \neq \mathsf{l}$ and $\mathsf{l}_2 = \mathsf{l}'$. By assumption $(\mathsf{l}_1, \mathsf{l}') \in W'.\beta$. Because $(\mathsf{S}_1, \mathsf{S}_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$ this means that $W'.\theta_1(\mathsf{l}_1) = W'.\theta_2(\mathsf{l}')$. We have already seen that $W'.\theta_2(\mathsf{l}') = \mathsf{B}^{\mathsf{r}}$. Hence it suffices to show $(\mathsf{S}_1(\mathsf{l}_1), \nu_2', W', \mathfrak{m}') \in [\![\mathsf{B}^{\mathsf{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. We do case analysis on the visibility of r.

A. $\mathsf{r} \sqsubseteq \mathcal{A}$: We will show that this is impossible. By transitivity Lemma 4.1 we get $\mathsf{p} \sqsubseteq \mathcal{A}$.
By assumption $(\mathsf{l}, \mathsf{l}', W, \mathfrak{m}) \in [\![(\mathtt{ref}\ \tau')^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\mathsf{p} \sqsubseteq \mathcal{A}$ $(\mathsf{l}, \mathsf{l}', W, \mathfrak{m}) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$.
By Lemma 8.25 $(\mathsf{l}, \mathsf{l}', W', \mathfrak{m}) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$. In particular this means
☞ $(\mathsf{l}, \mathsf{l}') \in W'.\beta$.
By assumption $W'.\beta$ is an injection. Hence there can be no other $\mathsf{l}'' \neq \mathsf{l}$ such that $(\mathsf{l}'', \mathsf{l}') \in W'.\beta$. But by assumption $(\mathsf{l}_1, \mathsf{l}') \in W'.\beta$ and $\mathsf{l}_1 \neq \mathsf{l}$. ↯.

B. $\mathsf{r} \not\sqsubseteq \mathcal{A}$ In this case it suffices to show
☞ $(\mathsf{S}_1(\mathsf{l}_1), W', \mathfrak{m}') \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$.
Because $(\mathsf{S}_1, \mathfrak{m}') \triangleright W'.\theta_1$ we have $(\mathsf{S}_1(\mathsf{l}_1), W'.\theta_1, \mathfrak{m}') \in \lceil W'.\theta_1(\mathsf{l}_1) \rceil_{\mathcal{V}}$. $W'.\theta_1(\mathsf{l}_1) = \mathsf{B}^{\mathsf{r}}$. Hence $(\mathsf{S}_1(\mathsf{l}_1), W'.\theta_1, \mathfrak{m}') \in \lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$. The goal follows by the definition of $\lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$.
☞ $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$.
We already know $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.22 and Lemma 8.4 we have $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil \tau \rceil_{\mathcal{V}}$. As $\tau = \mathsf{A}^{\mathsf{q}}$ this gives us $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$. The goal follows by Lemma 8.6.

iv. $(\mathsf{l}_1, \mathsf{l}_2) = (\mathsf{l}, \mathsf{l}')$.
The goal simplifies to $(\nu_2, \nu_2', W', \mathfrak{m}') \in [\![\mathsf{B}^{\mathsf{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$.
We do case analysis on whether $\mathsf{r} \sqsubseteq \mathcal{A}$ or not:

A. $\mathsf{r} \sqsubseteq \mathcal{A}$.
We do case analysis on $\mathsf{l}_{\mathtt{type}(\mathsf{S}_1, \mathsf{l})}(\nu_2) \approx^{\mathcal{A}}_{W'.\beta} \mathsf{l}'_{\mathtt{type}(\mathsf{S}_2, \mathsf{l}')}(\nu_2') \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.
This is the same as $\mathsf{l}_{\mathsf{B}^{\mathsf{r}}}(\nu_2) \approx^{\mathcal{A}}_{W'.\beta} \mathsf{l}'_{\mathsf{B}^{\mathsf{r}}}(\nu_2') \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.
$\alpha : \mathsf{l}_{\mathsf{B}^{\mathsf{r}}}(\nu_2) \approx^{\mathcal{A}}_{W'.\beta} \mathsf{l}'_{\mathsf{B}^{\mathsf{r}}}(\nu_2')$.

From $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$ or rather $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{A}^{\mathsf{q}}]\!]^{\mathcal{A}}_{\mathcal{V}}$ we get
☞ $(\nu_2, W'.\theta_1, \mathfrak{m}') \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$ and
☞ $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$
by Lemma 8.22,the definition of $\lceil \mathsf{A}^{\mathsf{q}} \rceil_{\mathcal{V}}$ and Lemma 8.4. From this we get
☞ $(\nu_2, W'.\theta_1, \mathfrak{m}') \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$ and
☞ $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$
by Lemma 8.31.
☞ $(\nu_2, W'.\theta_1, \mathfrak{m}') \in \lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$ and
☞ $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$
follows directly from the definition of $\lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$. The only rule with which $\mathsf{l}_{\mathsf{B}^{\mathsf{r}}}(\nu_2) \approx^{\mathcal{A}}_{W'.\beta} \mathsf{l}'_{\mathsf{B}^{\mathsf{r}}}(\nu_2')$ can be derived is **extend-τ** as it is clear from the structure of the observations that neither **refl** is not applicable. **high** is also not applicable because $\mathsf{r} \sqsubseteq \mathcal{A}$ by assumption.

By inversion
☞ $\nu \overset{W'.\beta}{\simeq}{}^{\mathcal{A}}_{\mathsf{B}^{\mathsf{r}}} \nu'$.

Also remember that we have restricted ourselves to first order state. Therefore we also have $\mathtt{firstorder}(\mathsf{B}^{\mathsf{r}})$. Therefore Lemma 8.43 gives us $(\nu_2, \nu_2', W', \mathfrak{m}') \in [\![\mathsf{B}^{\mathsf{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$.

$\beta : \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.

First we show that $\mathsf{q} \sqsubseteq \mathcal{A}$: By assumption $\Sigma_1 \supseteq \Sigma$, $\Sigma_2 \supseteq \Sigma'$, $\mathsf{q}(\Sigma) \sqsubseteq \mathsf{r}$ and $\mathsf{q}(\Sigma') \sqsubseteq \mathsf{r}$. Hence by Lemma 4.3 and transitivity (Lemma 4.1)
☞ $\mathsf{q}(\Sigma_1) \sqsubseteq \mathsf{r}$ and
☞ $\mathsf{q}(\Sigma_2) \sqsubseteq \mathsf{r}$.
In both cases ($\Sigma_1 \sqsubseteq \mathcal{A}$ and $\Sigma_2 \sqsubseteq \mathcal{A}$) we get $\mathsf{q} \sqsubseteq \mathcal{A}$ by Lemma 8.46.

Now we can continue with the main proof. We already know $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{A}^{\mathsf{q}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\mathsf{q} \sqsubseteq \mathcal{A}$, this means that $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{A}]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.31 $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{B}]\!]^{\mathcal{A}}_{\mathcal{V}}$. From this we can directly follow $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{B}^{\mathsf{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$

because $\mathsf{r} \sqsubseteq \mathcal{A}$ by assumption. The goal follows by Lemma 8.25 and Lemma 8.24.

B. $\mathsf{r} \not\sqsubseteq \mathcal{A}$.
Because $\mathsf{r} \not\sqsubseteq \mathcal{A}$, it suffices to show
☞ $(\nu_2, W'.\theta_1, \mathfrak{m}') \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$ and
☞ $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$.
From $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{A}^{\mathsf{q}}]\!]^{\mathcal{A}}_{\mathcal{V}}$ we get
☞ $(\nu_2, W'.\theta_1, \mathfrak{m}') \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$ and
☞ $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$
by Lemma 8.22, the definition of $\lceil \mathsf{A}^{\mathsf{q}} \rceil_{\mathcal{V}}$, Lemma 8.4. We get the remaining subgoals by Lemma 8.6.

– $(\mathsf{S}_1[\mathsf{l} \rightarrowtail (\nu_2, \mathtt{type}(\mathsf{S}_1, \mathsf{l}))], \mathfrak{m}') \triangleright W'.\theta_1$. For this we have to show
* $\mathtt{dom}(W'.\theta_1) \subseteq \mathtt{dom}(\mathsf{S}_1[\mathsf{l} \rightarrowtail (\nu_2, \mathtt{type}(\mathsf{S}_1, \mathsf{l}))])$.
$\mathtt{dom}(W'.\theta_1) \overset{(\mathsf{S}_1, \mathsf{S}_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'}{\subseteq} \mathtt{dom}(\mathsf{S}_1) \subseteq \mathtt{dom}(\mathsf{S}_1[\mathsf{l} \rightarrowtail (\nu_2, \mathtt{type}(\mathsf{S}_1, \mathsf{l}))])$.
* $\forall \mathsf{l}'' \in \mathtt{dom}(W'.\theta_1).(\mathsf{S}_1[\mathsf{l} \rightarrowtail (\nu_2, \mathtt{type}(\mathsf{S}_1, \mathsf{l}))](\mathsf{l}''), W'.\theta_1, \mathfrak{m}') \in \lceil W'.\theta_1(\mathsf{l}'') \rceil_{\mathcal{V}}$. Let $\mathsf{l}'' \in \mathtt{dom}(W'.\theta_1)$. There are two cases:
  i. $\mathsf{l}'' \neq \mathsf{l}$. By assumption $(\mathsf{S}_1, \mathsf{S}_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence also $(\mathsf{S}_1, \mathfrak{m}') \triangleright W'.\theta_1$. Therefore in particular $(\mathsf{S}_1(\mathsf{l}''), W'.\theta_1, \mathfrak{m}') \in \lceil W'.\theta_1(\mathsf{l}'') \rceil_{\mathcal{V}}$. Because $\mathsf{l}'' \neq \mathsf{l}$ this is equivalent to $(\mathsf{S}_1[\mathsf{l} \rightarrowtail (\nu_2, \mathtt{type}(\mathsf{S}_1, \mathsf{l}))](\mathsf{l}''), W'.\theta_1, \mathfrak{m}') \in \lceil W'.\theta_1(\mathsf{l}'') \rceil_{\mathcal{V}}$.
  ii. $\mathsf{l}'' = \mathsf{l}$. In this case the goal simplifies to $(\nu_2, W'.\theta_1, \mathfrak{m}') \in \lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$. By assumption $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{A}^{\mathsf{q}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.22 therefore $(\nu_2, W.\theta_1, \mathfrak{m}) \in \lceil \mathsf{A}^{\mathsf{q}} \rceil_{\mathcal{V}}$. By the definitions of $\lceil \mathsf{A}^{\mathsf{q}} \rceil_{\mathcal{V}}$ we directly get $(\nu_2, W.\theta_1, \mathfrak{m}) \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$. From that we get $(\nu_2, W.\theta_1, \mathfrak{m}) \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$ by Lemma 8.6. We get $(\nu_2, W.\theta_1, \mathfrak{m}) \in \lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$ by definition. The goal follows from Lemma 8.4 and Lemma 7.2.
* $\forall \mathsf{l}'' \in \mathtt{dom}(W'.\theta_1).W'.\theta_1(\mathsf{l}'') = \mathtt{type}(\mathsf{S}_1[\mathsf{l} \rightarrowtail (\nu_2, \mathtt{type}(\mathsf{S}_1, \mathsf{l}))], \mathsf{l}'')$.
Let $\mathsf{l}'' \in \mathtt{dom}(W'.\theta_1)$. There are two cases:
  i. $\mathsf{l}'' \neq \mathsf{l}$. By assumption $(\mathsf{S}_1, \mathsf{S}_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence $W'.\theta_1(\mathsf{l}'') = \mathtt{type}(\mathsf{S}_1, \mathsf{l}'')$. Because $\mathsf{l}'' \neq \mathsf{l}$ this is equivalent to the goal.
  ii. $\mathsf{l}'' = \mathsf{l}$. In this case the goal simplifies to $W'.\theta_1(\mathsf{l}) = \mathtt{type}(\mathsf{S}_1, \mathsf{l})$. We get this from $(\mathsf{S}_1, \mathsf{S}_2, \mathfrak{m}'), \mathsf{l} \overset{\mathcal{A}}{\triangleright} W'$.

– $(\mathsf{S}_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{type}(\mathsf{S}_1', \mathsf{l}'))], \mathfrak{m}') \triangleright W'.\theta_2$. For this we have to show
* $\mathtt{dom}(W'.\theta_2) \subseteq \mathtt{dom}(\mathsf{S}_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{type}(\mathsf{S}_1', \mathsf{l}'))])$.
$\mathtt{dom}(W'.\theta_2) \overset{(\mathsf{S}_1, \mathsf{S}_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'}{\subseteq} \mathtt{dom}(\mathsf{S}_2) \subseteq \mathtt{dom}(\mathsf{S}_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{type}(\mathsf{S}_1', \mathsf{l}'))])$.
* $\forall \mathsf{l}'' \in \mathtt{dom}(W'.\theta_2).(\mathsf{S}_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{type}(\mathsf{S}_1', \mathsf{l}'))](\mathsf{l}''), W'.\theta_2, \mathfrak{m}') \in \lceil W'.\theta_2(\mathsf{l}'') \rceil_{\mathcal{V}}$. Let $\mathsf{l}'' \in \mathtt{dom}(W'.\theta_2)$. There are two cases:
  i. $\mathsf{l}'' \neq \mathsf{l}'$. By assumption $(\mathsf{S}_1, \mathsf{S}_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence also $(\mathsf{S}_2, \mathfrak{m}') \triangleright W'.\theta_2$. Therefore in particular $(\mathsf{S}_2(\mathsf{l}''), W'.\theta_2, \mathfrak{m}') \in \lceil W'.\theta_2(\mathsf{l}'') \rceil_{\mathcal{V}}$. Because $\mathsf{l}'' \neq \mathsf{l}'$ this is equivalent to $(\mathsf{S}_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{type}(\mathsf{S}_1', \mathsf{l}'))](\mathsf{l}''), W'.\theta_2, \mathfrak{m}') \in \lceil W'.\theta_2(\mathsf{l}'') \rceil_{\mathcal{V}}$.
  ii. $\mathsf{l}'' = \mathsf{l}'$. In this case the goal simplifies to $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$. By assumption $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{A}^{\mathsf{q}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.22 therefore $(\nu_2', W.\theta_2, \mathfrak{m}) \in \lceil \mathsf{A}^{\mathsf{q}} \rceil_{\mathcal{V}}$. By the definitions of $\lceil \mathsf{A}^{\mathsf{q}} \rceil_{\mathcal{V}}$ we directly get $(\nu_2', W.\theta_2, \mathfrak{m}) \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$. From that we get $(\nu_2', W.\theta_2, \mathfrak{m}) \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$ by Lemma 8.6. We get $(\nu_2', W.\theta_2, \mathfrak{m}) \in \lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$ by definition. The goal follows from Lemma 8.4 and Lemma 7.2.
* $\forall \mathsf{l}'' \in \mathtt{dom}(W'.\theta_2).W'.\theta_2(\mathsf{l}'') = \mathtt{type}(\mathsf{S}_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{pol}(\mathsf{S}_1', \mathsf{l}'))], \mathsf{l}'')$.
Let $\mathsf{l}'' \in \mathtt{dom}(W'.\theta_2)$. There are two cases:
  i. $\mathsf{l}'' \neq \mathsf{l}'$. By assumption $(\mathsf{S}_1, \mathsf{S}_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence $W'.\theta_2(\mathsf{l}'') = \mathtt{type}(\mathsf{S}_2, \mathsf{l}'')$. Because $\mathsf{l}'' \neq \mathsf{l}'$ this is equivalent to the goal.
  ii. $\mathsf{l}'' = \mathsf{l}'$. In this case the goal simplifies to $W'.\theta_2(\mathsf{l}') = \mathtt{type}(\mathsf{S}_2, \mathsf{l}')$. We get this from $(\mathsf{S}_1, \mathsf{S}_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$.

• $\mathsf{l}_{\mathtt{type}(\mathsf{S}_1, \mathsf{l})}(\nu_2) \approx^{\mathcal{A}}_{W'.\beta} \mathsf{l}'_{\mathtt{type}(\mathsf{S}_2, \mathsf{l}')}(\nu_2')$.

This is the same as showing $\mathsf{l}_{\mathsf{B}^{\mathsf{r}}}(\nu_2) \approx^{\mathcal{A}}_{W'.\beta} \mathsf{l}'_{\mathsf{B}^{\mathsf{r}}}(\nu_2')$. We do case analysis on the visibility of r.

i. $\mathsf{r} \not\sqsubseteq \mathcal{A}$: In this case we get the claim by **high**.

ii. $\mathsf{r} \sqsubseteq \mathcal{A}$: By **extend-τ** it suffices to show
   - $(\mathsf{l}, \mathsf{l}') \in W'.\beta$. By transitivity Lemma 4.1 we get $\mathsf{p} \sqsubseteq \mathcal{A}$.
     By assumption $(\mathsf{l}, \mathsf{l}', W, \mathfrak{m}) \in [\![(\mathtt{ref}\ \tau')^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\mathsf{p} \sqsubseteq \mathcal{A}$ $(\mathsf{l}, \mathsf{l}', W, \mathfrak{m}) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$.
     By Lemma 8.25 $(\mathsf{l}, \mathsf{l}', W', \mathfrak{m}) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$. In particular this means
     ☞ $(\mathsf{l}, \mathsf{l}') \in W'.\beta$.
   - $\nu_2 \overset{W'.\beta}{\simeq}{}^{\mathcal{A}}_{\mathsf{B}^{\mathsf{r}}} \nu_2'$. We do another case analysis:
     A. $\mathsf{l}_{\mathtt{type}(\mathsf{S}_1,\mathsf{l})}(\nu_2) \approx^{\mathcal{A}}_{W'.\beta} \mathsf{l}'_{\mathtt{type}(\mathsf{S}_2,\mathsf{l}')}(\nu_2')$. This is the same as $\mathsf{l}_{\mathsf{B}^{\mathsf{r}}}(\nu_2) \approx^{\mathcal{A}}_{W'.\beta} \mathsf{l}'_{\mathsf{B}^{\mathsf{r}}}(\nu_2')$. This must have been derived by **extend-τ** because **refl** is syntactically not applicable and $\mathsf{r} \sqsubseteq \mathcal{A}$ rules out **high**. Hence by inversion
     ☞ $\nu_2 \overset{W'.\beta}{\simeq}{}^{\mathcal{A}}_{\mathsf{B}^{\mathsf{r}}} \nu_2'$
     which is what we needed to show.
     B. $\Sigma_1 \sqsubseteq \mathcal{A}$ or $\Sigma_2 \sqsubseteq \mathcal{A}$: We first show $\mathsf{q} \sqsubseteq \mathcal{A}$.
     By assumption $\Sigma_1 \supseteq \Sigma$, $\Sigma_2 \supseteq \Sigma'$, $\mathsf{q}(\Sigma) \sqsubseteq \mathsf{r}$ and $\mathsf{q}(\Sigma') \sqsubseteq \mathsf{r}$. Hence by Lemma 4.3 and transitivity (Lemma 4.1)
     ☞ $\mathsf{q}(\Sigma_1) \sqsubseteq \mathsf{r}$ and
     ☞ $\mathsf{q}(\Sigma_2) \sqsubseteq \mathsf{r}$.
     In both cases ($\Sigma_1 \sqsubseteq \mathcal{A}$ and $\Sigma_2 \sqsubseteq \mathcal{A}$) we get $\mathsf{q} \sqsubseteq \mathcal{A}$ by Lemma 8.46.

     Remember that by assumption $\mathtt{firstorder}(\mathsf{B}^{\mathsf{r}})$. Hence by Lemma 8.44 it suffices to show $(\nu_2, \nu_2', W', \mathfrak{m}) \in [\![\mathsf{B}^{\mathsf{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.25 it suffices to show $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{B}^{\mathsf{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. We already know $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{A}^{\mathsf{q}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\mathsf{q} \sqsubseteq \mathcal{A}$ we have $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{A}]\!]^{\mathcal{A}}_{\mathcal{V}}$. We get $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{B}]\!]^{\mathcal{A}}_{\mathcal{V}}$ by Lemma 8.31. The goal follows because $\mathsf{p} \sqsubseteq \mathcal{A}$.

- $((), (), W', \Sigma, \Sigma', \mathfrak{m}') \in [\![\mathtt{unit}^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$.
  It suffices to show $((), (), W', \mathfrak{m}') \in [\![\mathtt{unit}^{\perp}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\perp \sqsubseteq \mathcal{A}$ it suffices to show $((), (), W', \mathfrak{m}') \in [\![\mathtt{unit}]\!]^{\mathcal{A}}_{\mathcal{V}}$. This is clearly the case.

□

Lemma 8.50. If $(e, e', W, \Sigma\backslash\{\sigma\}, \Sigma'\backslash\{\sigma\}, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ and $\Sigma \approx_{\mathcal{A}} \Sigma'$, then $(e\ \mathtt{then\ unclose}\ \sigma, e'\ \mathtt{then\ unclose}\ \sigma, W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.

Proof. By induction on $\mathfrak{m}$. It suffices to show $(\mathtt{closed}\ \sigma\ \mathtt{in}\ e, \mathtt{closed}\ \sigma\ \mathtt{in}\ e', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. We already have $\Sigma \approx_{\mathcal{A}} \Sigma'$ by assumption. Let Σ_1, Σ_2 such that

- $\Sigma_1 \supseteq \Sigma$,
- $\Sigma_2 \supseteq \Sigma'$,
- $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

$W', \mathfrak{m}'$ such that

- $\mathfrak{m}' < \mathfrak{m}$,
- $W' \sqsupseteq W$,

and $\mathsf{S}_1, \mathsf{S}_2$ such that

- $(\mathsf{S}_1, \mathsf{S}_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$.

There are two cases:

1. $(e, e', W, \Sigma\backslash\{\sigma\}, \Sigma'\backslash\{\sigma\}, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. Clearly
   - $\Sigma\backslash\{\sigma\} \subseteq \Sigma_1\backslash\{\sigma\}$,
   - $\Sigma'\backslash\{\sigma\} \subseteq \Sigma_2\backslash\{\sigma\}$, and
   - $\Sigma_1\backslash\{\sigma\} \approx_{\mathcal{A}} \Sigma_2\backslash\{\sigma\}$.

   Hence there are three cases:

(a) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \backslash \{\sigma\} \vdash e_1,\, S_1 \xrightarrow{\omega;\Sigma_1'} e_1',\, S_1' \wedge \\ \Sigma_2 \backslash \{\sigma\} \vdash e_2,\, S_2 \xrightarrow{\omega';\Sigma_2'} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''. W'' \sqsupseteq W' \wedge\; (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma \backslash \{\sigma\}, \Sigma' \backslash \{\sigma\}, m') \in [\![\tau]\!]^{\mathcal{A}}_{E} \end{array} \right\}$

In this case it is suffices to show

$(\mathtt{closed}\ \sigma\ \mathtt{in}\ e, \mathtt{closed}\ \sigma\ \mathtt{in}\ e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xrightarrow{\omega;\Sigma_1'} e_1',\, S_1' \wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xrightarrow{\omega';\Sigma_2'} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''. W'' \sqsupseteq W' \wedge\; (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E} \end{array} \right\}.$

It is clear that neither $\mathtt{closed}\ \sigma\ \mathtt{in}\ e$ nor $\mathtt{closed}\ \sigma\ \mathtt{in}\ e'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $\mathtt{closed}\ \sigma\ \mathtt{in}\ e, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $\mathtt{closed}\ \sigma\ \mathtt{in}\ e', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

By assumption neither e nor e' are values. Hence the reductions must have happened with **Eclosed**. Hence by inversion

- $e, \Sigma_1 \backslash \{\sigma\}, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e', \Sigma_2 \backslash \{\sigma\}, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
- $e_\beta = \mathtt{closed}\ \sigma\ \mathtt{in}\ e_0$
- $e_\beta' = \mathtt{closed}\ \sigma\ \mathtt{in}\ e_0'$

Also assume $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \;\vee\; \Sigma_2' \sqsubseteq \mathcal{A}$.
We get a W'' such that

- $W'' \sqsupseteq W'$,
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
- $(e_0, e_0', W'', \Sigma \backslash \{\sigma\}, \Sigma' \backslash \{\sigma\}, m') \in [\![\tau]\!]^{\mathcal{A}}_{E}$

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
- $(\mathtt{closed}\ \sigma\ \mathtt{in}\ e_0, \mathtt{closed}\ \sigma\ \mathtt{in}\ e_0', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E}$ We get this by induction.

(b) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \backslash \{\sigma\} \vdash e_1,\, S_1 \xrightarrow{\omega;\Sigma_1'} e_1',\, S_1' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma \backslash \{\sigma\}, \Sigma' \backslash \{\sigma\}, m') \in [\![\tau]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$

In this case it suffices to show

$(\mathtt{closed}\ \sigma\ \mathtt{in}\ e, \mathtt{closed}\ \sigma\ \mathtt{in}\ e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xrightarrow{\omega;\Sigma_1'} e_1',\, S_1' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$

It is clear that $\mathtt{closed}\ \sigma\ \mathtt{in}\ e$ is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $\mathtt{closed}\ \sigma\ \mathtt{in}\ e, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

By assumption e is not a value. Hence the reduction must have happened with **Eclosed**. By inversion

- $e, \Sigma_1 \backslash \{\sigma\}, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e_\beta = \texttt{closed}\ \sigma\ \texttt{in}\ e_0$

Hence

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_0, e', W'', \Sigma\backslash\{\sigma\}, \Sigma'\backslash\{\sigma\}, m') \in [\![\tau]\!]_E^{\mathcal{A}}$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\texttt{closed}\ \sigma\ \texttt{in}\ e_0, \texttt{closed}\ \sigma\ \texttt{in}\ e', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]_E^{\mathcal{A}}$. We get this using the induction hypothesis.

(c) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2\backslash\{\sigma\} \vdash e_2,\ S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\ S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma\backslash\{\sigma\}, \Sigma'\backslash\{\sigma\}, m') \in [\![\tau]\!]_E^{\mathcal{A}}) \end{array} \right\}$

In this case it suffices to show

$(\texttt{closed}\ \sigma\ \texttt{in}\ e, \texttt{closed}\ \sigma\ \texttt{in}\ e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\ S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\ S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]_E^{\mathcal{A}}) \end{array} \right\}$

It is clear that $\texttt{closed}\ \sigma\ \texttt{in}\ e'$ is not a value. So let $\omega', e_\beta', \Sigma_2', S_2'$ such that

- $\texttt{closed}\ \sigma\ \texttt{in}\ e', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

By assumption e' is not a value. Hence the reduction must have happened with **Eclose**. By inversion

- $e', \Sigma_2\backslash\{\sigma\}, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
- $e_\beta' = \texttt{closed}\ \sigma\ \texttt{in}\ e_0'$

Hence

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e, e_0', W'', \Sigma\backslash\{\sigma\}, \Sigma'\backslash\{\sigma\}, m') \in [\![\tau]\!]_E^{\mathcal{A}}$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\texttt{closed}\ \sigma\ \texttt{in}\ e, \texttt{closed}\ \sigma\ \texttt{in}\ e_0', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]_E^{\mathcal{A}}$. We get this using the induction hypothesis.

2. $(e, e', W, \Sigma\backslash\{\sigma\}, \Sigma'\backslash\{\sigma\}, m) \in \left\{ (v, v', W, \Sigma_1, \Sigma_2, m) \;\middle|\; (v, v', W, m) \in [\![\tau]\!]_{\mathcal{V}}^{\mathcal{A}} \right\}$
   In particular this means that there are v, v' such that $e = v$ and $e' = v'$. In this case it suffices to show

$$(\mathbf{closed}\ \sigma\ \mathbf{in}\ v, \mathbf{closed}\ \sigma\ \mathbf{in}\ v') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \ \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\ S_1' \ \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\ S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \ \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E} \end{array} \right\}$$

It is clear that neither $\mathbf{closed}\ \sigma\ \mathbf{in}\ v$ nor $\mathbf{closed}\ \sigma\ \mathbf{in}\ v'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $\mathbf{closed}\ \sigma\ \mathbf{in}\ v, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $\mathbf{closed}\ \sigma\ \mathbf{in}\ v', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

By assumption both e and e' are values v and v', respectively. Hence the reductions must have happened with **EclosedBeta**. Consequently

- $e_\beta = v$
- $e_\beta' = v'$
- $S_1' = S_1$
- $S_2' = S_2$
- $\omega = \mathrm{unclose}(\sigma) = \omega'$
- $\Sigma_1' = \Sigma_1$
- $\Sigma_2' = \Sigma_2$

Hence the reductions are really

- $\mathbf{closed}\ \sigma\ \mathbf{in}\ v, \Sigma_1, S_1 \succ v, S_1, \mathrm{unclose}(\sigma), \Sigma_1$
- $\mathbf{closed}\ \sigma\ \mathbf{in}\ v', \Sigma_2, S_2 \succ v', S_2, \mathrm{unclose}(\sigma), \Sigma_2$

Also assume $\mathrm{unclose}(\sigma) \approx^{\mathcal{A}}_{W'.\beta} \mathrm{unclose}(\sigma) \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$. It suffices to show

- $W' \sqsupseteq W'$. We get this by Lemma 7.2.
- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. We already know this.
- $\mathrm{unclose}(\sigma) \cong^{\mathcal{A}}_{W'.\beta} \mathrm{unclose}(\sigma)$. We get this with **refl**.
- $(v, v', W', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E}$. We already know $(v, v', W, m) \in [\![\tau]\!]^{\mathcal{A}}_{V}$. By Lemma 8.24 and Lemma 8.25 we get $(v, v', W', m') \in [\![\tau]\!]^{\mathcal{A}}_{V}$ which implies the subgoal.

□

Lemma 8.51. If $(e, e', W, \Sigma\backslash\{\sigma\}, \Sigma'\backslash\{\sigma\}, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$ and $\Sigma \approx_{\mathcal{A}} \Sigma'$, then $(\mathsf{close}\ \sigma\ \mathsf{in}\ e, \mathsf{close}\ \sigma\ \mathsf{in}\ e', W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$.

Proof. It suffices to show $(\mathbf{closed}\ \sigma\ \mathbf{in}\ e, \mathbf{closed}\ \sigma\ \mathbf{in}\ e', W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{E_\beta}$. We already have $\Sigma \approx_{\mathcal{A}} \Sigma'$ by assumption. Let Σ_1, Σ_2 such that

- $\Sigma_1 \supseteq \Sigma$,
- $\Sigma_2 \supseteq \Sigma'$,
- $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

W', m' such that

- $m' < m$,
- $W' \sqsupseteq W$,

and S_1, S_2 such that

- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

It is sufficient to show

$$(\mathsf{close}\ \sigma\ \mathsf{in}\ e, \mathsf{close}\ \sigma\ \mathsf{in}\ e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \ \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \ \wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \ \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E} \end{array} \right\}$$

It is clear that neither $\mathsf{close}\ \sigma\ \mathsf{in}\ e$ nor $\mathsf{close}\ \sigma\ \mathsf{in}\ e'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $\mathsf{close}\ \sigma\ \mathsf{in}\ e, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $\mathsf{close}\ \sigma\ \mathsf{in}\ e', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

The reduction must have happened with **Eclose**. Consequently

- $e_\beta = \mathsf{closed}\ \sigma\ \mathsf{in}\ e$
- $e_\beta' = \mathsf{closed}\ \sigma\ \mathsf{in}\ e'$
- $S_1' = S_1$
- $S_2' = S_2$
- $\omega = \mathsf{close}(\sigma) = \omega'$
- $\Sigma_1' = \Sigma_1$
- $\Sigma_2' = \Sigma_2$

Hence the reductions are really

- $\mathsf{close}\ \sigma\ \mathsf{in}\ e, \Sigma_1, S_1 \succ \mathsf{closed}\ \sigma\ \mathsf{in}\ e, S_1, \mathsf{close}(\sigma), \Sigma_1$
- $\mathsf{close}\ \sigma\ \mathsf{in}\ v', \Sigma_2, S_2 \succ \mathsf{closed}\ \sigma\ \mathsf{in}\ e', S_2, \mathsf{close}(\sigma), \Sigma_2$

Also assume $\mathsf{close}(\sigma) \approx^{\mathcal{A}}_{W'.\beta} \mathsf{close}(\sigma) \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$. It suffices to show

- $W' \sqsupseteq W'$. We get this by Lemma 7.2.
- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. We already know this.
- $\mathsf{close}(\sigma) \approx^{\mathcal{A}}_{W'.\beta} \mathsf{close}(\sigma)$. We get this with **refl**.
- $(\mathsf{closed}\ \sigma\ \mathsf{in}\ e, \mathsf{closed}\ \sigma\ \mathsf{in}\ e', W', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E}$. By assumption we have $(e, e', \Sigma\backslash\{\sigma\}, \Sigma'\backslash\{\sigma\}, W, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$. By Lemma 8.24 and Lemma 8.25 this gives us $(e, e', \Sigma\backslash\{\sigma\}, \Sigma'\backslash\{\sigma\}, W', m') \in [\![\tau]\!]^{\mathcal{A}}_{E}$. We get the remaining subgoal with Lemma 8.50.

□

Lemma 8.52. If $(e, \theta, m) \in \lceil\tau\rceil^{pc}_{E}$ and $(S, m') \triangleright \theta'$, $\theta' \sqsupseteq \theta$, $m' < m$ and $\Sigma \vdash e, S \xRightarrow{\omega;\Sigma'} e', S'$, then $(e', \theta', m') \in \lceil\tau\rceil^{pc}_{E}$.

Proof. Because e reduces e cannot be a value. Hence we must have $(e, \theta, m) \in \lceil\tau\rceil^{pc}_{E_\beta}$. Because $\theta' \supseteq \theta$, $(S, m') \triangleright \theta'$, $m' < m$ and $\Sigma \vdash e, S \xRightarrow{\omega;\Sigma'} e', S'$ the goal follows directly from the definition of $\lceil\tau\rceil^{pc}_{E_\beta}$. □

Lemma 8.53. Let $i \in \{1, 2\}$. If $(e, W.\theta_i, m) \in \lceil\tau\rceil^{pc}_{E}$ and $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$, $W' \sqsupseteq W$, $m' < m$ and $\Sigma \vdash e, S_i \xRightarrow{\omega;\Sigma'} e', S'$, then $\forall W''.W'' \sqsupseteq W'.(e', W''.\theta_i, m') \in \lceil\tau\rceil^{pc}_{E}$.

Proof. Because $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$, we have $(S_i, m') \triangleright W'.\theta_i$. Because $W' \sqsupseteq W$ also $W'.\theta_i \sqsupseteq W.\theta_i$. Hence we have $(e, W'.\theta_i, m') \in \lceil\tau\rceil^{pc}_{E}$ by Lemma 8.52. Let $W'' \sqsupseteq W'$. Then $W''.\theta_i \sqsupseteq W'.\theta_i$. We get $(e, W''.\theta_i, m')$ by Lemma 8.5. □

Lemma 8.54. If

- $(e_1, e_1', W, \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$,
- $(e_2, e_2', W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$,
- $(e_1, W.\theta_1, m) \in \lceil\tau\rceil^{pol(\sigma)}_{E}$,
- $(e_1', W.\theta_2, m) \in \lceil\tau\rceil^{pol(\sigma)}_{E}$,
- $(e_2, W.\theta_1, m) \in \lceil\tau\rceil^{pol(\sigma)}_{E}$,
- $(e_2', W.\theta_2, m) \in \lceil\tau\rceil^{pol(\sigma)}_{E}$,
- $pol(\sigma) \sqsubseteq \tau$ and
- $\Sigma \approx_{\mathcal{A}} \Sigma'$,

then $(\mathsf{when}\ \sigma\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2, \mathsf{when}\ \sigma\ \mathsf{then}\ e_1'\ \mathsf{else}\ e_2', W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$.

Proof. By induction on m. We do case analysis on the visibility of σ

1. $pol(\sigma) \not\sqsubseteq \mathcal{A}$: By Lemma 8.30 it suffices to show
   - $((\mathsf{when}\ \sigma\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2, W.\theta_1, m) \in \lceil\tau\rceil^{pol(\sigma)}_{E}$. By Lemma 8.19 it suffices to show
     - $(e_1, W.\theta_1, m) \in \lceil\tau\rceil^{pol(\sigma)\sqcup pol(\sigma)}_{E}$. By Lemma 4.10, we have $pol(\sigma) \sqcup pol(\sigma) \approx pol(\sigma)$. By Lemma 8.5 it therefore suffices to show $(e_1, W.\theta_1, m) \in \lceil\tau\rceil^{pol(\sigma)}_{E}$ which we have by assumption.
     - $(e_2, W.\theta_1, m) \in \lceil\tau\rceil^{pol(\sigma)\sqcup pol(\sigma)}_{E}$. By Lemma 4.10, we have $pol(\sigma) \sqcup pol(\sigma) \approx pol(\sigma)$. By Lemma 8.5 it therefore suffices to show $(e_2, W.\theta_1, m) \in \lceil\tau\rceil^{pol(\sigma)}_{E}$ which we have by assumption.
   - $((\mathsf{when}\ \sigma\ \mathsf{then}\ e_1'\ \mathsf{else}\ e_2', W.\theta_2, m) \in \lceil\tau\rceil^{pol(\sigma)}_{E}$. By Lemma 8.19 it suffices to show
     - $(e_1', W.\theta_2, m) \in \lceil\tau\rceil^{pol(\sigma)\sqcup pol(\sigma)}_{E}$. By Lemma 4.10, we have $pol(\sigma) \sqcup pol(\sigma) \approx pol(\sigma)$. By Lemma 8.5 it therefore suffices to show $(e_1', W.\theta_2, m) \in \lceil\tau\rceil^{pol(\sigma)}_{E}$ which we have by assumption.
     - $(e_2', W.\theta_2, m) \in \lceil\tau\rceil^{pol(\sigma)\sqcup pol(\sigma)}_{E}$. By Lemma 4.10, we have $pol(\sigma) \sqcup pol(\sigma) \approx pol(\sigma)$. By Lemma 8.5 it therefore suffices to show $(e_2', W.\theta_2, m) \in \lceil\tau\rceil^{pol(\sigma)}_{E}$ which we have by assumption.
   - $\tau \not\sqsubseteq \mathcal{A}$. Assume $\tau \sqsubseteq \mathcal{A}$. Because $pol(\sigma) \sqsubseteq \tau$ we have $pol(\sigma) \sqsubseteq \mathcal{A}$ by transitivity (Lemma 4.1). $\lightning$.
   - $pol(\sigma) \not\sqsubseteq \mathcal{A}$. We have this by assumption.
   - $\Sigma \approx_{\mathcal{A}} \Sigma'$. We have this by assumption.
2. $pol(\sigma) \sqsubseteq \mathcal{A}$: It suffices to show $(\mathsf{when}\ \sigma\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2, \mathsf{when}\ \sigma\ \mathsf{then}\ e_1'\ \mathsf{else}\ e_2', W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{E_\beta}$. We already have $\Sigma \approx_{\mathcal{A}} \Sigma'$ by assumption. Let Σ_1, Σ_2 such that
   - $\Sigma_1 \supseteq \Sigma$,
   - $\Sigma_2 \supseteq \Sigma'$,
   - $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

   W', m' such that
   - $m' < m$,
   - $W' \sqsupseteq W$,

   and S_1, S_2 such that
   - $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

   We do case analysis on whether $\sigma \in \Sigma_1$:

(a) $\sigma \in \Sigma_1$. Because $\mathtt{pol}(\sigma) \sqsubseteq \mathcal{A}$ by assumption, also $\sigma \in (\Sigma_1)_{\mathcal{A}}$. By assumption $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$. Hence also $\sigma \in (\Sigma_2)_{\mathcal{A}}$. Consequently also $\sigma \in \Sigma_2$. There are two cases:

i. $(e_1, e_1', W, \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. Because $\sigma \in \Sigma_1$ and $\sigma \in \Sigma_2$ we have

- $\Sigma_1 \supseteq \Sigma_1 \cup \{\sigma\} \supseteq \Sigma \cup \{\sigma\}$
- $\Sigma_2 \supseteq \Sigma_2 \cup \{\sigma\} \supseteq \Sigma' \cup \{\sigma\}$.

Hence there are three further cases

A. $(e_1, e_1') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \;\wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\; (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \;\wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$

In this case it is suffices to show

$(\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2, \mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2') \in$

$\left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \;\wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\; (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \;\wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$.

It is clear that neither $\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2$ nor $\mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $\mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

By assumption neither e_1 nor e_1' is a value. Hence the reductions must have happened with **EWhenOpen**. Hence by inversion

- $e_1, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e_1', \Sigma_2, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
- $e_\beta = \mathit{when}\ \sigma\ \mathit{then}\ e_0\ \mathit{else}\ e_2$
- $e_\beta' = \mathit{when}\ \sigma\ \mathit{then}\ e_0'\ \mathit{else}\ e_2'$

Also assume $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \;\vee\; \Sigma_2' \sqsubseteq \mathcal{A}$.
We get a W'' such that

- $W'' \sqsupseteq W'$,
- $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
- $(e_0, e_0', W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.
- $(\mathit{when}\ \sigma\ \mathit{then}\ e_0\ \mathit{else}\ e_2, \mathit{when}\ \sigma\ \mathit{then}\ e_0'\ \mathit{else}\ e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. Note that by transitivity (Lemma 7.2) we have $W'' \sqsupseteq W$. We get this by induction if we can show
  - $(e_0, e_0', W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We already know that.
  - $(e_2, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this by Lemma 8.29.
  - $(e_0, W''.\theta_1, \mathfrak{m}') \in \lceil\tau\rceil^{\mathtt{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.53.
  - $(e_0', W''.\theta_2, \mathfrak{m}') \in \lceil\tau\rceil^{\mathtt{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.53.
  - $(e_2, W''.\theta_1, \mathfrak{m}') \in \lceil\tau\rceil^{\mathtt{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.5.

- $(e_2', W''.\theta_2, \mathfrak{m}') \in \lceil\tau\rceil_{\mathsf{E}}^{\mathsf{pol}(\sigma)}$. We get this by Lemma 8.5.
- $\mathsf{pol}(\sigma) \sqsubseteq \tau$. We already know this.
- $\Sigma \approx_{\mathcal{A}} \Sigma'$. We already know this.

B. $(e_1, e_1') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \rightarrow \neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}) \end{array} \right\}$

In this case it suffices to show

$(\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2, \mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2') \in$

$\left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \rightarrow \neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}) \end{array} \right\}$

It is clear that $\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2$ is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

By assumption e_1 is not a value. Hence the reduction must have happened with **EWhenOpen**. By inversion

- $e_1, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e_\beta = \mathit{when}\ \sigma\ \mathit{then}\ e_0\ \mathit{else}\ e_2$

Hence

- $\neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_0, e_1', W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}})$

It suffices to show the following:

- $\neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\mathit{when}\ \sigma\ \mathit{then}\ e_0\ \mathit{else}\ e_2, \mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}$. Note that by transitivity (Lemma 7.2) we have $W'' \sqsupseteq W$. We get this by induction if we can show
  - $(e_0, e_1', W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}$. We already know that.
  - $(e_2, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}$. We get this by Lemma 8.29.
  - $(e_0, W''.\theta_1, \mathfrak{m}') \in \lceil\tau\rceil_{\mathsf{E}}^{\mathsf{pol}(\sigma)}$. We get this by Lemma 8.53.
  - $(e_1', W''.\theta_2, \mathfrak{m}') \in \lceil\tau\rceil_{\mathsf{E}}^{\mathsf{pol}(\sigma)}$. We get this by Lemma 8.5.
  - $(e_2, W''.\theta_1, \mathfrak{m}') \in \lceil\tau\rceil_{\mathsf{E}}^{\mathsf{pol}(\sigma)}$. We get this by Lemma 8.5.
  - $(e_2', W''.\theta_2, \mathfrak{m}') \in \lceil\tau\rceil_{\mathsf{E}}^{\mathsf{pol}(\sigma)}$. We get this by Lemma 8.5.
  - $\mathsf{pol}(\sigma) \sqsubseteq \tau$. We already know this.
  - $\Sigma \approx_{\mathcal{A}} \Sigma'$. We already know this.

C. $(e_1, e_1') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \rightarrow \neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}) \end{array} \right\}$

In this case it suffices to show

$(\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2, \mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2') \in$

$\left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \rightarrow \neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}) \end{array} \right\}$

It is clear that $\mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2'$ is not a value. So let $\omega, e_\beta, \Sigma_2', S_2'$ such that

- $\mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2', \Sigma_2, S_2 \succ e_\beta, S_2', \omega, \Sigma_2'$

By assumption e_1' is not a value. Hence the reduction must have happened with **EWhenOpen**. By inversion

- $e_1', \Sigma_2, S_2 \succ e_0, S_2', \omega, \Sigma_2'$
- $e_\beta = \mathit{when}\ \sigma\ \mathit{then}\ e_0\ \mathit{else}\ e_2'$

Hence

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_1, e_0, W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}})$

It suffices to show the following:

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2, \mathit{when}\ \sigma\ \mathit{then}\ e_0\ \mathit{else}\ e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}$. Note that by transitivity (Lemma 7.2) we have $W'' \sqsupseteq W$. We get this by induction if we can show
  - $(e_1, e_0, W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}$. We already know that.
  - $(e_2, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}$. We get this by Lemma 8.29.
  - $(e_1, W''.\theta_1, \mathfrak{m}') \in \lceil\tau\rceil_{\mathsf{E}}^{\mathtt{pol}(\sigma)}$. We get this by Lemma 8.5
  - $(e_0, W''.\theta_2, \mathfrak{m}') \in \lceil\tau\rceil_{\mathsf{E}}^{\mathtt{pol}(\sigma)}$. We get this by Lemma 8.53..
  - $(e_2, W''.\theta_1, \mathfrak{m}') \in \lceil\tau\rceil_{\mathsf{E}}^{\mathtt{pol}(\sigma)}$. We get this by Lemma 8.5.
  - $(e_2', W''.\theta_2, \mathfrak{m}') \in \lceil\tau\rceil_{\mathsf{E}}^{\mathtt{pol}(\sigma)}$. We get this by Lemma 8.5.
  - $\mathtt{pol}(\sigma) \sqsubseteq \tau$. We already know this.
  - $\Sigma \approx_{\mathcal{A}} \Sigma'$. We already know this.

ii. $(e_1, e_1', W, \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}) \in \left\{(v, v', W, \Sigma_1, \Sigma_2, \mathfrak{m}) \,\middle|\, (v, v', W, \mathfrak{m}) \in [\![\tau]\!]_{\mathcal{V}}^{\mathcal{A}}\right\}$ In this case there are values v_1, v_1' such that $e_1 = v_1$ and $e_1' = v_1'$ and $(v_1, v_1', W, \mathfrak{m}) \in [\![\tau]\!]_{\mathcal{V}}^{\mathcal{A}}$. It is suffices to show

$(\mathit{when}\ \sigma\ \mathit{then}\ v_1\ \mathit{else}\ e_2, \mathit{when}\ \sigma\ \mathit{then}\ v_1'\ \mathit{else}\ e_2') \in$

$$\left\{(e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\ S_1' \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\ S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}} \end{array} \right\}.$$

It is clear that neither $\mathit{when}\ \sigma\ \mathit{then}\ v_1\ \mathit{else}\ e_2$ nor $\mathit{when}\ \sigma\ \mathit{then}\ v_1'\ \mathit{else}\ e_2'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $\mathit{when}\ \sigma\ \mathit{then}\ v_1\ \mathit{else}\ e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $\mathit{when}\ \sigma\ \mathit{then}\ v_1'\ \mathit{else}\ e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Because v_1 and v_1' are values, the reductions must have happened with **EWhenOpenBeta**. Hence

- $e_\beta = v_1$,
- $e_\beta' = v_1'$,
- $S_1' = S_1$,
- $S_2' = S_2$,
- $\omega = \epsilon = \omega'$,
- $\Sigma_1' = \Sigma_1$ and
- $\Sigma_2' = \Sigma_2$.

So the reductions are really

- $\mathit{when}\ \sigma\ \mathit{then}\ v_1\ \mathit{else}\ e_2, \Sigma_1, S_1 \succ v_1, S_1, \epsilon, \Sigma_1$
- $\mathit{when}\ \sigma\ \mathit{then}\ v_1'\ \mathit{else}\ e_2', \Sigma_2, S_2 \succ v_1', S_2, \epsilon, \Sigma_2$

Let $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon \vee \Sigma_1 \sqsupseteq \mathcal{A} \vee \Sigma_2 \sqsupseteq \mathcal{A}$. It suffices to show

- $W' \sqsupseteq W'$. We have this by Lemma 7.2.
- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. We already know this.
- $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon$. We have this by **refl**.
- $(v_1, v_1', W, \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. It suffices to show $(v_1, v_1', W, m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. We get this by Lemma 8.25 and Lemma 8.24.

(b) $\sigma \notin \Sigma_1$.

We show $\sigma \notin \Sigma_2$. Assume $\sigma \in \Sigma_2$. Then because $\mathtt{pol}(\sigma) \sqsubseteq \mathcal{A}$ by assumption, also $\sigma \in (\Sigma_2)_{\mathcal{A}}$. By assumption $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$. Hence also $\sigma \in (\Sigma_1)_{\mathcal{A}}$. But then $\sigma \in \Sigma_1$. $\lightning$.

There are two cases:

i. $(e_2, e_2', W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. There are three further cases

A. $(e_2, e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \wedge \\ \Sigma_2 \vdash e_2, S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2', S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$

In this case it is suffices to show

$(\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2, \mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2') \in$

$\left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \wedge \\ \Sigma_2 \vdash e_2, S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2', S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}.$

It is clear that neither $\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2$ nor $\mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $\mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

By assumption neither e_2 nor e_2' is a value. Hence the reductions must have happened with **EWhenClosed**. Hence by inversion

- $e_2, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e_2', \Sigma_2, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
- $e_\beta = \mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_0$
- $e_\beta' = \mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_0'$

Also assume $\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \ \vee\ \Sigma_2' \sqsubseteq \mathcal{A}$.

We get a W'' such that

- $W'' \sqsupseteq W'$,
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$, and
- $(e_0, e_0', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{W''.\beta} \omega'$. We already know that.

- $(\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_0, \mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_0', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. Note that by transitivity (Lemma 7.2) we have $W'' \sqsupseteq W$. We get this by induction if we can show
  - $(e_1, e_1', W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this by Lemma 8.29.
  - $(e_0, e_0', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We already know that.
  - $(e_0, W''.\theta_1, \mathfrak{m}') \in \lceil\tau\rceil^{\mathsf{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.53.
  - $(e_0', W''.\theta_2, \mathfrak{m}') \in \lceil\tau\rceil^{\mathsf{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.53.
  - $(e_1, W''.\theta_1, \mathfrak{m}') \in \lceil\tau\rceil^{\mathsf{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.5.
  - $(e_1', W''.\theta_2, \mathfrak{m}') \in \lceil\tau\rceil^{\mathsf{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.5.
  - $\mathsf{pol}(\sigma) \sqsubseteq \tau$. We already know this.
  - $\Sigma \approx_{\mathcal{A}} \Sigma'$. We already know this.

B. $(e_2, e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\ S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\ S_1' \rightarrow \neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'')) \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

In this case it suffices to show

$(\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2, \mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2') \in$
$\left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\ S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\ S_1' \rightarrow \neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''.W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'')) \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

It is clear that $\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2$ is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

By assumption e_2 is not a value. Hence the reduction must have happened with **EWhen-Closed**. By inversion

- $e_2, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e_\beta = \mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_0$

Hence

- $\neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_0, e_1', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}})$

It suffices to show the following:

- $\neg(\mathsf{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_0, \mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. Note that by transitivity (Lemma 7.2) we have $W'' \sqsupseteq W$. We get this by induction if we can show
  - $(e_1, e_1', W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this by Lemma 8.29.
  - $(e_0, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We already know that.
  - $(e_0, W''.\theta_1, \mathfrak{m}') \in \lceil\tau\rceil^{\mathsf{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.53.
  - $(e_2', W''.\theta_2, \mathfrak{m}') \in \lceil\tau\rceil^{\mathsf{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.5.
  - $(e_1, W''.\theta_1, \mathfrak{m}') \in \lceil\tau\rceil^{\mathsf{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.5.
  - $(e_1', W''.\theta_2, \mathfrak{m}') \in \lceil\tau\rceil^{\mathsf{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.5.
  - $\mathsf{pol}(\sigma) \sqsubseteq \tau$. We already know this.
  - $\Sigma \approx_{\mathcal{A}} \Sigma'$. We already know this.

C. $(e_2, e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

In this case it suffices to show

$(\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2, \mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2') \in$

$\left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

It is clear that $\mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2'$ is not a value. So let $\omega, e_\beta, \Sigma_2', S_2'$ such that

- $\mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_2', \Sigma_2, S_2 \succ e_\beta, S_2', \omega, \Sigma_2'$

By assumption e_2' is not a value. Hence the reduction must have happened with **EWhen-Closed**. By inversion

- $e_2', \Sigma_2, S_2 \succ e_0, S_2', \omega, \Sigma_2'$
- $e_\beta = \mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_0$

Hence

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_2, e_0, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$)

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ e_2, \mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ e_0, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. Note that by transitivity (Lemma 7.2) we have $W'' \sqsupseteq W$. We get this by induction if we can show
  - $(e_1, e_1', W'', \Sigma \cup \{\sigma\}, \Sigma' \cup \{\sigma\}, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this by Lemma 8.29.
  - $(e_2, e_0, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We already know that.
  - $(e_2, W''.\theta_1, \mathfrak{m}') \in \lceil\tau\rceil^{\mathrm{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.5
  - $(e_0, W''.\theta_2, \mathfrak{m}') \in \lceil\tau\rceil^{\mathrm{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.53..
  - $(e_1, W''.\theta_1, \mathfrak{m}') \in \lceil\tau\rceil^{\mathrm{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.5.
  - $(e_1', W''.\theta_2, \mathfrak{m}') \in \lceil\tau\rceil^{\mathrm{pol}(\sigma)}_{\mathsf{E}}$. We get this by Lemma 8.5.
  - $\mathrm{pol}(\sigma) \sqsubseteq \tau$. We already know this.
  - $\Sigma \approx_{\mathcal{A}} \Sigma'$. We already know this.

ii. $(e_2, e_2', W, \Sigma, \Sigma', \mathfrak{m}) \in \left\{ (v, v', W, \Sigma_1, \Sigma_2, \mathfrak{m}) \;\middle|\; (v, v', W, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}} \right\}$ In this case there are values v_2, v_2' such that $e_2 = v_2$ and $e_2' = v_2'$ and $(v_2, v_2', W, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. It is suffices to show

$(\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ v_2, \mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ v_2') \in$

$\left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\, S_2' \to \\ (\omega \approx^{\mathcal{A}}_{W'.\beta} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''. W'' \sqsupseteq W' \wedge\; (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{W''.\beta} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}.$

It is clear that neither $\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ v_2$ nor $\mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ v_2'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ v_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $\mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ v_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Because v_2 and v_2' are values, the reductions must have happened with **EWhenClosedBeta**. Hence

- $e_\beta = v_2$,
- $e_\beta' = v_2'$,
- $S_1' = S_1$,
- $S_2' = S_2$,
- $\omega = \epsilon = \omega'$,
- $\Sigma_1' = \Sigma_1$ and
- $\Sigma_2' = \Sigma_2$.

So the reductions are really

- $\mathit{when}\ \sigma\ \mathit{then}\ e_1\ \mathit{else}\ v_2, \Sigma_1, S_1 \succ v_2, S_1, \epsilon, \Sigma_1$
- $\mathit{when}\ \sigma\ \mathit{then}\ e_1'\ \mathit{else}\ v_2', \Sigma_2, S_2 \succ v_2', S_2, \epsilon, \Sigma_2$

Let $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon \vee \Sigma_1 \sqsupseteq \mathcal{A} \vee \Sigma_2 \sqsupseteq \mathcal{A}$. It suffices to show

- $W' \sqsupseteq W'$. We have this by Lemma 7.2.
- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. We already know this.
- $\epsilon \approx^{\mathcal{A}}_{W'.\beta} \epsilon$. We have this by **refl**.
- $(v_2, v_2', W, \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. It suffices to show $(v_2, v_2', W, m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{V}}$. We get this by Lemma 8.25 and Lemma 8.24.

□

Theorem 8.2 (Binary Fundamental Lemma)**.**
If $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau$ and $(\gamma, W, m) \in [\![\Gamma]\!]^{\mathcal{A}}_{\mathsf{V}}$ and $W.\theta_1 \sqsupseteq \theta \sqsubseteq W.\theta_2$ and $\forall l \in \mathrm{dom}(\theta).(l, l) \in W.\beta$, then $\forall \mathcal{A}, m.(\gamma_1(e), \gamma_2(e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.

Proof. Let $\mathcal{A}$ be an attacker. By induction on $\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau$.

- **var:**

$$\frac{}{\Gamma', x : \tau, \Gamma''; \Sigma; \theta \vdash_{\mathsf{pc}} x : \tau}\ \mathbf{var}$$

We have to show $(\gamma_1(x), \gamma_2(x), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. By assumption $(\gamma, W, m) \in \lceil \Gamma', x : \tau, \Gamma'' \rceil_{\mathsf{V}}$. Therefore since $x \in \mathrm{dom}(\Gamma', x : \tau, \Gamma'')$ we have $(\gamma_1(x), \gamma_2(x), W, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{V}}$. The goal follows directly from the construction of $[\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.

- **nat:**

$$\frac{n \in \mathbb{N}}{\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} n : \mathcal{N}^{\perp}}\ \mathbf{nat}$$

We have to show $(\gamma_1(n), \gamma_2(n), W, \Sigma, \Sigma, m) \in [\![\mathcal{N}^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$. This is equivalent to showing $(n, n, W, m) \in [\![\mathcal{N}^{\perp}]\!]^{\mathcal{A}}_{\mathsf{V}}$. Because $\perp \sqsubseteq \mathcal{A}$ by Lemma 4.19, it suffices to show $(n, n, W, m) \in [\![\mathcal{N}]\!]^{\mathcal{A}}_{\mathsf{V}}$. This follows directly from the definition of $[\![\mathcal{N}]\!]^{\mathcal{A}}_{\mathsf{V}}$.

- **open**

$$\frac{\Gamma; \Sigma \cup \{\sigma\}; \theta \vdash_{\mathsf{pc}} e : \tau \qquad \mathsf{pc} \sqsubseteq \mathrm{pol}(\sigma)}{\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} \mathit{open}(\sigma)\ \mathit{in}\ e : \tau}\ \mathbf{open}$$

We have to show $(\gamma_1(\mathit{open}(\sigma)\ \mathit{in}\ e), \gamma_2(\mathit{open}(\sigma)\ \mathit{in}\ e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ which is equivalent to showing $(\mathit{open}(\sigma)\ \mathit{in}\ \gamma_1(e), \mathit{open}(\sigma)\ \mathit{in}\ \gamma_2(e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. By induction $(\gamma_1(e), \gamma_2(e), W, \Sigma \cup \{\sigma\}, \Sigma \cup \{\sigma\}, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.
We get $(\mathit{open}(\sigma)\ \mathit{in}\ \gamma_1(e), \mathit{open}(\sigma)\ \mathit{in}\ \gamma_2(e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ by Lemma 8.35 if we can also show $\Sigma \approx_{\mathcal{A}} \Sigma$. This is clearly the case.

- **opened**:

$$\frac{\Gamma; \Sigma \cup \{\sigma\}; \theta \vdash_{\mathsf{pc}} e : \tau \qquad \mathsf{pc} \sqsubseteq \mathrm{pol}(\sigma)}{\Gamma; \Sigma; \theta \vdash_{\mathsf{pc}} \mathit{opened}(\sigma)\ \mathit{in}\ e : \tau}\ \mathbf{opened}$$

We have to show $(\gamma_1(\mathit{opened}(\sigma)\ \mathit{in}\ e), \gamma_2(\mathit{opened}(\sigma)\ \mathit{in}\ e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ which is equivalent to showing $(\mathit{opened}(\sigma)\ \mathit{in}\ \gamma_1(e), \mathit{opened}(\sigma)\ \mathit{in}\ \gamma_2(e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. By induction $(\gamma_1(e), \gamma_2(e), W, \Sigma \cup \{\sigma\}, \Sigma \cup \{\sigma\}, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We also clearly have $\Sigma \approx_{\mathcal{A}} \Sigma$.
Hence by Lemma 8.34 $(\mathit{opened}(\sigma)\ \mathit{in}\ \gamma_1(e), \mathit{opened}(\sigma)\ \mathit{in}\ \gamma_2(e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.

- λ:

$$\frac{\Gamma, x : \tau_1; \Sigma'; \theta \vdash_{p_e} e' : \tau_2}{\Gamma; \Sigma; \theta \vdash_{pc} \lambda x.e' : (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^{\perp}}\ \lambda$$

In this case $\tau = (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^{\perp}$. It suffices to show $(\gamma_1(\lambda x.e'), \gamma_2(\lambda x.e'), W, m) \in \llbracket (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^{\perp} \rrbracket^{\mathcal{A}}_{\mathcal{V}}$
It is clear that $\perp \sqsubseteq \mathcal{A}$ by Lemma 4.19. Because of this and because of the way substitutions work on functions it suffices to show $(\lambda x.\gamma_1(e'), \lambda x.\gamma_2(e'), W, m) \in \llbracket \tau_1 \xrightarrow{\Sigma', p_e} \tau_2 \rrbracket^{\mathcal{A}}_{\mathcal{V}}$. By the Unary Fundamental Lemma and the definition of substitution $(\lambda x.\gamma_1(e'), \theta, m) \in \lceil \tau \rceil^{pc}_{E}$ and $(\lambda x.\gamma_2(e'), \theta, m) \in \lceil \tau \rceil^{pc}_{E}$. So let

  - $W' \sqsupseteq W$,
  - $m' < m$,
  - $\Sigma_0 \supseteq \Sigma' \subseteq \Sigma_1$,
  - $(v, v', W', m') \in \lceil \tau_1 \rceil_{\mathcal{V}}$.

We need to prove $([v/x]\gamma_1(e'), [v'/x]\gamma_2(e'), W', \Sigma_0, \Sigma_1, m') \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_{E}$.

Remember that we assume that the variables replaced by γ are distinct from x and that x is distinct from the free variables in the expressions of the codomain of γ. Hence by Lemma 7.1 $[v/x]\gamma_1(e') = \gamma_1 \cup \{(x, v)\}(e')$ and $[v'/x]\gamma_2(e') = \gamma_2 \cup \{(x, v')\}(e')$. So it suffices to show $(\gamma_1 \cup \{(x, v)\}(e'), \gamma_1 \cup \{(x, v')\}(e'), W', \Sigma_0, \Sigma_1, m') \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_{E}$.

We show

  - $((\gamma_1 \cup \{(x, v)\}, \gamma_2 \cup \{(x, v')\}), W', m') \in \lceil \Gamma, x : \tau_1 \rceil_{\mathcal{V}}$.
    By Lemma 8.26 we get $(\gamma, W', m') \in \llbracket \Gamma \rrbracket^{\mathcal{A}}_{\mathcal{V}}$. The claim follows by Lemma 8.2.
  - $W'.\theta_1 \sqsupseteq \theta \sqsubseteq W'.\theta_2$. We already know $W' \sqsubseteq W$ and hence $W'.\theta_1 \sqsupseteq W.\theta_1$ and $W'.\theta_2 \sqsupseteq W.\theta_2$.
    The claim follows by transitivity Lemma 6.2.

Hence we get $(\gamma_1 \cup \{(x, v)\}(e'), \gamma_1 \cup \{(x, v')\}(e'), W', \Sigma', \Sigma', m') \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_{E}$ by induction. $(\gamma_1 \cup \{(x, v)\}(e'), \gamma_1 \cup \{(x, v')\}(e'), W', \Sigma_0, \Sigma_1, m') \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_{E}$ follows by Lemma 8.29.

- **prod**:

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e_1 : \tau_1 \qquad \Gamma; \Sigma; \theta \vdash_{pc} e_2 : \tau_2}{\Gamma; \Sigma; \theta \vdash_{pc} (e_1, e_2) : (\tau_1 \times \tau_2)^{\perp}}\ \textbf{prod}$$

In this case $\tau = (\tau_1 \times \tau_2)^{\perp}$. We have to show $(\gamma_1((e_1, e_2)), \gamma_2((e_1, e_2)), W, \Sigma, \Sigma, m) \in \llbracket (\tau_1 \times \tau_2)^{\perp} \rrbracket^{\mathcal{A}}_{E}$ which is equivalent to showing $((\gamma_1(e_1), \gamma_1(e_2)), (\gamma_2(e_1), \gamma_2(e_2)), W, \Sigma, \Sigma, m) \in \llbracket (\tau_1 \times \tau_2)^{\perp} \rrbracket^{\mathcal{A}}_{E}$. By induction $(\gamma_1(e_1), \gamma_2(e_1), W, \Sigma, \Sigma, m) \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_{E}$ and $(\gamma_1(e_2), \gamma_2(e_2), W, \Sigma, \Sigma, m) \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_{E}$. We get the claim by Lemma 8.36.

- **app**:

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e_1 : (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^{p} \qquad \Gamma; \Sigma; \theta \vdash_{pc} e_2 : \tau_1' \qquad p \sqsubseteq \tau_2 \qquad pc \sqcup p \sqsubseteq p_e \qquad \tau_1' <: \tau_1 \qquad \Sigma \supseteq \Sigma'}{\Gamma; \Sigma; \theta \vdash_{pc} e_1\ e_2 : \tau_2}\ \textbf{app}$$

In this case $\tau = \tau_2$. We have to show $(\gamma_1(e_1\ e_2), \gamma_2(e_1\ e_2), W, \Sigma, \Sigma, m) \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_{E}$ which is equivalent to showing $(\gamma_1(e_1)\ \gamma_1(e_2), \gamma_2(e_1)\ \gamma_2(e_2), W, \Sigma, \Sigma, m) \in \llbracket \tau_2 \rrbracket^{\mathcal{A}}_{E}$. By induction $(\gamma_1(e_1), \gamma_2(e_1), W, \Sigma, \Sigma, m) \in \llbracket (\tau_1 \xrightarrow{\Sigma', p_e} \tau_2)^{p} \rrbracket^{\mathcal{A}}_{E}$ and $(\gamma_1(e_2), \gamma_2(e_2), W, \Sigma, \Sigma, m) \in \llbracket \tau_1' \rrbracket^{\mathcal{A}}_{E}$. By Lemma 8.31 we have $(\gamma_1(e_2), \gamma_2(e_2), W, \Sigma, \Sigma, m) \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_{E}$. We already have $p \sqsubseteq \tau_2$ and get $p \sqsubseteq p_e$ by Lemma 4.13. We also clearly have $\Sigma \approx_{\mathcal{A}} \Sigma$. Hence we get the goal by Lemma 8.37.

- **fst**:

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e : (\tau_1 \times \tau_2)^{p} \qquad p \sqsubseteq \tau_1}{\Gamma; \Sigma; \theta \vdash_{pc} \mathsf{fst}(e) : \tau_1}\ \textbf{fst}$$

In this case $\tau = \tau_1$. We have to show $(\gamma_1(\mathsf{fst}(e)), \gamma_2(\mathsf{fst}(e)), W, \Sigma, \Sigma, m) \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_{E}$ which is equivalent to showing $(\mathsf{fst}(\gamma_1(e)), \mathsf{fst}(\gamma_2(e)), W, \Sigma, \Sigma, m) \in \llbracket \tau_1 \rrbracket^{\mathcal{A}}_{E}$. By induction $(\gamma_1(e), \gamma_2(e), W, \Sigma, \Sigma, m) \in \llbracket (\tau_1 \times \tau_2)^{p} \rrbracket^{\mathcal{A}}_{E}$. We also clearly have $\Sigma \approx_{\mathcal{A}} \Sigma$. We get the claim by Lemma 8.38.

- **snd**:

$$\frac{\Gamma;\Sigma;\theta \vdash_{\mathsf{pc}} e : (\tau_1 \times \tau_2)^{\mathfrak{p}} \qquad \mathfrak{p} \sqsubseteq \tau_2}{\Gamma;\Sigma;\theta \vdash_{\mathsf{pc}} \mathtt{snd}(e) : \tau_2}\ \textbf{snd}$$

  In this case $\tau = \tau_2$. We have to show $(\gamma_1(\mathtt{snd}(e)), \gamma_2(\mathtt{snd}(e)), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}}$ which is equivalent to showing $(\mathtt{snd}(\gamma_1(e)), \mathtt{snd}(\gamma_2(e)), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}}$. By induction $(\gamma_1(e), \gamma_2(e), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![(\tau_1 \times \tau_2)^{\mathfrak{p}}]\!]^{\mathcal{A}}_{\mathsf{E}}$. We also clearly have $\Sigma \approx_{\mathcal{A}} \Sigma$. We get the claim by Lemma 8.39.

- **inl:**

$$\frac{\Gamma;\Sigma;\theta \vdash_{\mathsf{pc}} e : \tau_1}{\Gamma;\Sigma;\theta \vdash_{\mathsf{pc}} \mathtt{inl}(e) : (\tau_1 + \tau_2)^{\perp}}\ \textbf{inl}$$

  In this case $\tau = (\tau_1 + \tau_2)^{\perp}$. We have to show $(\gamma_1(\mathtt{inl}\ e), \gamma_2(\mathtt{inl}\ e), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![(\tau_1 + \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$ which is equivalent to showing $(\mathtt{inl}\ \gamma_1(e), \mathtt{inl}\ \gamma_2(e), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![(\tau_1 + \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$. By induction $(\gamma_1(e), \gamma_2(e), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get the claim by Lemma 8.40.

- **inr:**

$$\frac{\Gamma;\Sigma;\theta \vdash_{\mathsf{pc}} e : \tau_2}{\Gamma;\Sigma;\theta \vdash_{\mathsf{pc}} \mathtt{inr}(e) : (\tau_1 + \tau_2)^{\perp}}\ \textbf{inr}$$

  In this case $\tau = (\tau_1 + \tau_2)^{\perp}$. We have to show $(\gamma_1(\mathtt{inr}\ e), \gamma_2(\mathtt{inr}\ e), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![(\tau_1 + \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$ which is equivalent to showing $(\mathtt{inr}\ \gamma_1(e), \mathtt{inr}\ \gamma_2(e), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![(\tau_1 + \tau_2)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$. By induction $(\gamma_1(e), \gamma_2(e), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get the claim by Lemma 8.41.

- **case:**

$$\frac{\begin{array}{c}\Gamma;\Sigma;\theta \vdash_{\mathsf{pc}} e : (\tau_1 + \tau_2)^{\mathfrak{p}} \\ \mathfrak{p} \sqsubseteq \tau \qquad \Gamma, x : \tau_1';\Sigma;\theta \vdash_{\mathsf{pc}\sqcup\mathfrak{p}} e_1 : \tau \qquad \Gamma, y : \tau_2';\Sigma;\theta \vdash_{\mathsf{pc}\sqcup\mathfrak{p}} e_2 : \tau \qquad \tau_1 <: \tau_1' \qquad \tau_2 <: \tau_2'\end{array}}{\Gamma;\Sigma;\theta \vdash_{\mathsf{pc}} \mathtt{case}(e, x.e_1, y.e_2) : \tau}\ \textbf{case}$$

  We have to show $(\gamma_1(\mathtt{case}(e, x.e_1, y.e_2)), \gamma_2(\mathtt{case}(e, x.e_1, y.e_2)), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. By our assumptions about variables $x \notin \mathtt{dom}(\gamma)$ and $y \notin \mathtt{dom}(\gamma)$. Hence this is equivalent to showing $(\mathtt{case}(\gamma_1(e), x.\gamma_1(e_1), y.\gamma_1(e_2)), \mathtt{case}(\gamma_2(e), x.\gamma_2(e_1), y.\gamma_2(e_2)), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. By Lemma 8.42 it suffices to show:

  - $(\gamma_1(e), \gamma_2(e), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![(\tau_1 + \tau_2)^{\mathfrak{p}}]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this by induction.
  - $\mathfrak{p} \sqsubseteq \tau$. We already know that.
  - $\Sigma \approx_{\mathcal{A}} \Sigma$. This is clearly the case.
  - $\forall W', \mathfrak{m}'. W' \sqsupseteq W \wedge \mathfrak{m}' \leqslant \mathfrak{m} \to \forall v, v'(v, v', W', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}} \to ([v/x]\gamma_1(e_1), [v'/x]\gamma_2(e_1), W', \Sigma, \Sigma, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.
    Let $W' \sqsupseteq W$, $\mathfrak{m}' \leqslant \mathfrak{m}$ and v, v' such that
    - $(v, v', W', \mathfrak{m}') \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$.

    By Lemma 7.1 it suffices to show $(\{x, v\} \cup \gamma_1(e_1), \{(x, v')\} \cup \gamma_2(e_1), W', \Sigma, \Sigma, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ By Lemma 8.31 also
    - $(v, v', W', \mathfrak{m}') \in [\![\tau_1']\!]^{\mathcal{A}}_{\mathcal{V}}$.

    By Lemma 8.26 also
    - $(\gamma, W', \mathfrak{m}') \in [\![\Gamma]\!]^{\mathcal{A}}_{\mathcal{V}}$.

    Therefore by Lemma 8.2 $((\{x, v\} \cup \gamma_1, \{(x, v')\} \cup \gamma_2), W', \mathfrak{m}') \in [\![\Gamma, x : \tau_1']\!]^{\mathcal{A}}_{\mathcal{V}}$ and by Lemma 6.2 $W.\theta_1 \sqsupseteq \theta \sqsubseteq W'.\theta_2$.
    $(\{x, v\} \cup \gamma_1(e_1), \{(x, v')\} \cup \gamma_2(e_1), W', \Sigma, \Sigma, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ follows by induction.
  - $\forall W', \mathfrak{m}'. W' \sqsupseteq W \wedge \mathfrak{m}' \leqslant \mathfrak{m} \to \forall w, w'(w, w', W', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}. ([w/y]\gamma_1(e_2), [w'/y]\gamma_2(e_2), W', \Sigma, \Sigma, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. Let $W' \sqsupseteq W$, $\mathfrak{m}' \leqslant \mathfrak{m}$ and w, w' such that
    - $(w, w', W', \mathfrak{m}') \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$.

    By Lemma 7.1 it suffices to show $(\{x, w\} \cup \gamma_1(e_2), \{(x, w')\} \cup \gamma_2(e_2), W', \Sigma, \Sigma, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ By Lemma 8.31 also
    - $(w, w', W', \mathfrak{m}') \in [\![\tau_2']\!]^{\mathcal{A}}_{\mathcal{V}}$.

By Lemma 8.26 also

* $(\gamma, W', \mathfrak{m}') \in [\![\Gamma]\!]^{\mathcal{A}}_{\mathcal{V}}$.

Therefore by Lemma 8.2 $((\{x, w\} \cup \gamma_1, \{(x, w')\} \cup \gamma_2), W', \mathfrak{m}') \in [\![\Gamma, x : \tau_2']\!]^{\mathcal{A}}_{\mathcal{V}}$ and by Lemma 6.2 $W.\theta_1 \sqsupseteq \theta \sqsubseteq W'.\theta_2$. $(\{x, w\} \cup \gamma_1(e_2), \{(x, w')\} \cup \gamma_2(e_2), W', \Sigma, \Sigma, \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ follows by induction.

– $\forall W', \mathfrak{m}'. W' \sqsupseteq W \wedge \mathfrak{m}' \leqslant \mathfrak{m} \to \forall v. (v, W'.\theta_1, \mathfrak{m}') \in \lceil \tau_1 \rceil_{\mathcal{V}} \to ([v/x]\gamma_1(e_1), W'.\theta_1, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$.
Let $W' \sqsupseteq W$, $\mathfrak{m}' \leqslant \mathfrak{m}$ and v such that

* $(v, W'.\theta_1, \mathfrak{m}') \in \lceil \tau_1 \rceil_{\mathcal{V}}$

By Lemma 7.1 it suffices to show $(\gamma_1 \cup \{(x, v)\}(e_1), W.'\theta_1, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$. By Lemma 8.6 also

* $(v, W'.\theta_1, \mathfrak{m}') \in [\![\tau_1']\!]^{\mathcal{A}}_{\mathcal{V}}$.

. By Lemma 8.32 and Lemma 8.23

* $(\gamma_1, W'.\theta_1, \mathfrak{m}') \in \lceil \Gamma \rceil_{\mathcal{V}}$.

Therefore by Lemma 8.1 $(\gamma_1 \cup \{(x, v)\}, W'.\theta_1, \mathfrak{m}') \in \lceil \Gamma, x : \tau_1' \rceil_{\mathcal{V}}$ and by Lemma 6.2 $W'.\theta_1 \sqsupseteq \theta$. We get $(\gamma_1 \cup \{(x, v)\}(e_1), W'.\theta_1, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$ by the Unary Fundamental Lemma.

– $\forall W', \mathfrak{m}'. W' \sqsupseteq W \wedge \mathfrak{m}' \leqslant \mathfrak{m} \to \forall v. (v, W'.\theta_2, \mathfrak{m}') \in \lceil \tau_1 \rceil_{\mathcal{V}} \to ([v/x]\gamma_2(e_1), W'.\theta_2, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$.
Let $W' \sqsupseteq W$, $\mathfrak{m}' \leqslant \mathfrak{m}$ and v such that

* $(v, W'.\theta_2, \mathfrak{m}') \in \lceil \tau_1 \rceil_{\mathcal{V}}$

By Lemma 7.1 it suffices to show $(\gamma_2 \cup \{(x, v)\}(e_1), W'.\theta_2, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$. By Lemma 8.6 also

* $(v, W'.\theta_2, \mathfrak{m}') \in [\![\tau_1']\!]^{\mathcal{A}}_{\mathcal{V}}$.

. By Lemma 8.32 and Lemma 8.23

* $(\gamma_2, W'.\theta_2, \mathfrak{m})' \in \lceil \Gamma \rceil_{\mathcal{V}}$.

Therefore by Lemma 8.1 $(\gamma_2 \cup \{(x, v)\}, W'.\theta_2, \mathfrak{m}') \in \lceil \Gamma, x : \tau_1' \rceil_{\mathcal{V}}$ and by Lemma 6.2 $W'.\theta_2 \sqsupseteq \theta$. We get $(\gamma_2 \cup \{(x, v)\}(e_1), W'.\theta_2, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$ by the Unary Fundamental Lemma.

– $\forall W', \mathfrak{m}'. W' \sqsupseteq W \wedge \mathfrak{m}' \leqslant \mathfrak{m} \to \forall v. (v, W'.\theta_1, \mathfrak{m}') \in \lceil \tau_2 \rceil_{\mathcal{V}} \to ([v/y]\gamma_1(e_2), W'.\theta_1, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$.
Let $W' \sqsupseteq W$, $\mathfrak{m}' \leqslant \mathfrak{m}$ and v such that

* $(v, W'.\theta_1, \mathfrak{m}') \in \lceil \tau_2 \rceil_{\mathcal{V}}$

By Lemma 7.1 it suffices to show $(\gamma_1 \cup \{(x, v)\}(e_2), W'.\theta_1, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$. By Lemma 8.6 also

* $(v, W'.\theta_1, \mathfrak{m}') \in [\![\tau_2']\!]^{\mathcal{A}}_{\mathcal{V}}$.

. By Lemma 8.32 and Lemma 8.23

* $(\gamma_1, W'.\theta_1, \mathfrak{m}') \in \lceil \Gamma \rceil_{\mathcal{V}}$.

Therefore by Lemma 8.1 $(\gamma_1 \cup \{(x, v)\}, W'.\theta_1, \mathfrak{m}') \in \lceil \Gamma, x : \tau_2' \rceil_{\mathcal{V}}$ and by Lemma 6.2 $W'.\theta_1 \sqsupseteq \theta$. We get $(\gamma_1 \cup \{(x, v)\}(e_2), W'.\theta_1, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$ by the Unary Fundamental Lemma.

– $\forall W', \mathfrak{m}'. W' \sqsupseteq W \wedge \mathfrak{m}' \leqslant \mathfrak{m} \to \forall v. (v, W'.\theta_2, \mathfrak{m}') \in \lceil \tau_2 \rceil_{\mathcal{V}} \to ([v/y]\gamma_2(e_2), W'.\theta_2, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$.
Let $W' \sqsupseteq W$, $\mathfrak{m}' \leqslant \mathfrak{m}$ and v such that

* $(v, W'.\theta_2, \mathfrak{m}') \in \lceil \tau_2 \rceil_{\mathcal{V}}$

By Lemma 7.1 it suffices to show $(\gamma_2 \cup \{(x, v)\}(e_2), W'.\theta_2, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$. By Lemma 8.6 also

* $(v, W'.\theta_2, \mathfrak{m}') \in [\![\tau_2']\!]^{\mathcal{A}}_{\mathcal{V}}$.

. By Lemma 8.32 and Lemma 8.23

* $(\gamma_2, W'.\theta_2, \mathfrak{m}') \in \lceil \Gamma \rceil_{\mathcal{V}}$.

Therefore by Lemma 8.1 $(\gamma_2 \cup \{(x, v)\}, W'.\theta_2, \mathfrak{m}') \in \lceil \Gamma, x : \tau_2' \rceil_{\mathcal{V}}$ and by Lemma 6.2 $W'.\theta_2 \sqsupseteq \theta$. We get $(\gamma_2 \cup \{(x, v)\}(e_2), W'.\theta_2, \mathfrak{m}') \in \lceil \tau \rceil^{pc \sqcup p}_{\mathsf{E}}$ by the Unary Fundamental Lemma.

- **new**:

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e : \tau' \qquad pc \sqsubseteq \tau \qquad \tau'(\Sigma) <: \tau}{\Gamma; \Sigma; \theta \vdash_{pc} new\,(e, \tau) : (ref\ \tau)^{\perp}}\ \textbf{new}$$

We have to show $(\gamma_1(new(e, \tau)), \gamma_2(new(e, \tau)), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![(ref(\tau))^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$ which is equivalent to showing $(new\,(\gamma_1(e), \tau), new\,(\gamma_2(e), \tau), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![(ref(\tau))^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$. By induction $(\gamma_1(e), \gamma_2(e), W, \Sigma, \Sigma, \mathfrak{m}) \in [\![\tau']\!]^{\mathcal{A}}_{\mathsf{E}}$. We get the claim by Lemma 8.47 if we can show $\Sigma \approx_{\mathcal{A}} \Sigma$. This is clearly the case.

- **loc:**

$$\frac{\theta(l) = \tau'}{\Gamma; \Sigma; \theta \vdash_{pc} l : (\mathsf{ref}\ \tau')^{\perp}}\ \textbf{loc}$$

$\gamma_1(l) = l = \gamma_2(l)$. Since l is a value it suffices to show $(l, l, W, m) \in [\![(\mathsf{ref}\ \tau')^{\perp}]\!]^{\mathcal{A}}_{V}$. Because $\perp \sqsubseteq \mathcal{A}$ by Lemma 4.19, it suffices to show $(l, l, W, m) \in [\![\mathsf{ref}\ \tau']\!]^{\mathcal{A}}_{V}$. To show this we have to show

  - $W.\theta_1(l) = \tau' = W.\theta_2(l)$. By assumption $W.\theta_1 \sqsupseteq \theta \sqsubseteq W.\theta_2$. And by assumption of the rule $\theta(l) = \tau'$. Hence $W.\theta_1(l) = \tau' = W.\theta_2(l)$.
  - $(l, l) \in W.\beta$. Clearly $l \in \mathrm{dom}(\theta)$ and therefore by assumption $(l, l) \in W.\beta$.

- **sub:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc'} e : \tau' \qquad pc \sqsubseteq pc' \qquad \tau' <: \tau}{\Gamma; \Sigma; \theta \vdash_{pc} e : \tau}\ \textbf{sub}$$

By induction we have $(\gamma_1(e), \gamma_2(e), W, \Sigma, \Sigma, m) \in [\![\tau']\!]^{\mathcal{A}}_{E}$. We get the goal by Lemma 8.31.

- **deref:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e' : (\mathsf{ref}\ \tau')^{p} \qquad p \sqsubseteq \tau \qquad \tau' <: \tau}{\Gamma; \Sigma; \theta \vdash_{pc} !e' : \tau}\ \textbf{deref}$$

We have to show $(\gamma_1(!e), \gamma_2(!e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$ which is equivalent to showing $(!(\gamma_1(e)), !(\gamma_2(e)), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$. By induction $(\gamma_1(e), \gamma_2(e), W, \Sigma, \Sigma, m) \in [\![(\mathsf{ref}\ \tau')^{p}]\!]^{\mathcal{A}}_{E}$. By Lemma 4.13 $p \sqsubseteq \tau$. We also clearly have $\Sigma \approx_{\mathcal{A}} \Sigma$. We get the claim by Lemma 8.48.

- **assign:**

$$\frac{\Gamma; \Sigma; \theta \vdash_{pc} e : (\mathsf{ref}\ \tau')^{p} \qquad \tau(\Sigma) <: \tau' \qquad \Gamma; \Sigma; \theta \vdash_{pc} e' : \tau \qquad pc \sqcup p \sqsubseteq \tau'}{\Gamma; \Sigma; \theta \vdash_{pc} e := e' : \mathsf{unit}^{\perp}}\ \textbf{assign}$$

We have to show $(\gamma_1(e := e'), \gamma_2(e := e'), W, \Sigma, \Sigma, m) \in [\![\mathtt{unit}^{\perp}]\!]^{\mathcal{A}}_{E}$ which is equivalent to showing $(\gamma_1(e) := \gamma_1(e'), \gamma_2(e) := \gamma_2(e'), W, \Sigma, \Sigma, m) \in [\![\mathtt{unit}^{\perp}]\!]^{\mathcal{A}}_{E}$. By induction $(\gamma_1(e), \gamma_2(e), W, \Sigma, \Sigma, m) \in [\![(\mathsf{ref}\ \tau')^{p}]\!]^{\mathcal{A}}_{E}$ and $(\gamma_1(e'), \gamma_2(e'), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$. We get the claim by Lemma 8.49 if we can show

  - $\Sigma \approx_{\mathcal{A}} \Sigma$. This is clearly the case.
  - $\tau(\Sigma) <: \tau'$. This is a premiss of the rule.
  - $p \sqsubseteq \tau'$. We get this by Lemma 4.13.

- **unit:**

$$\frac{}{\Gamma; \Sigma; \theta \vdash_{pc} () : \mathsf{unit}^{\perp}}\ \textbf{unit}$$

We have to show $(\gamma_1(()), \gamma_2(()), W, \Sigma, \Sigma, m) \in [\![\mathtt{unit}^{\perp}]\!]^{\mathcal{A}}_{E}$. This is equivalent to showing $((), (), W, m) \in [\![\mathtt{unit}^{\perp}]\!]^{\mathcal{A}}_{V}$. Because $\perp \sqsubseteq \mathcal{A}$ by Lemma 4.19, it suffices to show $((), (), W, m) \in [\![\mathtt{unit}]\!]^{\mathcal{A}}_{V}$. This follows directly from the definition of $[\![\mathtt{unit}]\!]^{\mathcal{A}}_{V}$.

- **close:**

$$\frac{\Gamma; \Sigma\backslash\{\sigma\}; \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq \mathrm{pol}(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} \mathsf{close}\ \sigma\ \mathsf{in}\ e : \tau}\ \textbf{close}$$

We have to show $(\gamma_1(\mathtt{close}\ \sigma\ \mathtt{in}\ e), \gamma_2(\mathtt{close}\ \sigma\ \mathtt{in}\ e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$. This is equivalent to showing $(\mathtt{close}\ \sigma\ \mathtt{in}\ \gamma_1(e), \mathtt{close}\ \sigma\ \mathtt{in}\ \gamma_2(e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$. By induction $(\gamma_1(e), \gamma_2(e), W, \Sigma\backslash\{\sigma\}, \Sigma\backslash\{\sigma\}, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$. We also clearly have $\Sigma \approx_{\mathcal{A}} \Sigma$.
Hence by Lemma 8.51 $(\mathtt{close}\ \sigma\ \mathtt{in}\ \gamma_1(e), \mathtt{close}\ \sigma\ \mathtt{in}\ \gamma_2(e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$.

- **closed:**

$$\frac{\Gamma; \Sigma\backslash\{\sigma\}; \theta \vdash_{pc} e : \tau \qquad pc \sqsubseteq \mathrm{pol}(\sigma)}{\Gamma; \Sigma; \theta \vdash_{pc} e\ \mathsf{then\ unclose}\ \sigma : \tau}\ \textbf{closed}$$

We have to show $(\gamma_1(\mathtt{closed}(\sigma)\ \mathtt{in}\ e), \gamma_2(\mathtt{closed}(\sigma)\ \mathtt{in}\ e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$ which is equivalent to showing $(\mathtt{closed}(\sigma)\ \mathtt{in}\ \gamma_1(e), \mathtt{closed}(\sigma)\ \mathtt{in}\ \gamma_2(e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$. By induction $(\gamma_1(e), \gamma_2(e), W, \Sigma\backslash\{\sigma\}, \Sigma\backslash\{\sigma\}, m$
$[\![\tau]\!]^{\mathcal{A}}_{E}$. We also clearly have $\Sigma \approx_{\mathcal{A}} \Sigma$.
Hence by Lemma 8.50 $(\mathtt{closed}(\sigma)\ \mathtt{in}\ \gamma_1(e), \mathtt{closed}(\sigma)\ \mathtt{in}\ \gamma_2(e), W, \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$.

- **when:**

$$\frac{\Gamma;\Sigma\cup\{\sigma\};\theta\vdash_{\mathsf{pc}\sqcup\mathsf{pol}(\sigma)} e_1:\tau \qquad \Gamma;\Sigma;\theta\vdash_{\mathsf{pc}\sqcup\mathsf{pol}(\sigma)} e_2:\tau \qquad \mathsf{pol}(\sigma)\sqsubseteq\tau}{\Gamma;\Sigma;\theta\vdash_{\mathsf{pc}} \mathsf{when}\ \sigma\ \mathsf{then}\ e_1\ \mathsf{else}\ e_2:\tau}\ \textbf{when}$$

  We have to show $(\gamma_1(\mathit{when}\ (\sigma)\ \mathit{then}\ e_1\ \mathit{else}\ e_2),\gamma_2(\mathit{when}\ (\sigma)\ \mathit{then}\ e_1\ \mathit{else}\ e_2),W,\Sigma,\Sigma,\mathfrak{m})\in[\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ which is equivalent to showing

  $(\mathit{when}\ (\sigma)\ \mathit{then}\ \gamma_1(e_1)\ \mathit{else}\ \gamma_1(e_2),\mathit{when}\ (\sigma)\ \mathit{then}\ \gamma_2(e_1)\ \mathit{else}\ \gamma_2(e_2),W,\Sigma,\Sigma,\mathfrak{m})\in[\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. By Lemma 8.54 it suffices to show

  - $(\gamma_1(e_1),\gamma_2(e_1),W,\Sigma\cup\{\sigma\},\Sigma\cup\{\sigma\},\mathfrak{m})\in[\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this by induction.
  - $(\gamma_1(e_2),\gamma_2(e_2),W,\Sigma,\Sigma,\mathfrak{m})\in[\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this by induction.
  - $(\gamma_1(e_1),W.\theta_1,\mathfrak{m})\in\lceil\tau\rceil^{\mathtt{pol}(\sigma)}_{\mathsf{E}}$. By Lemma 4.6 $\mathtt{pol}(\sigma)\sqsubseteq\mathtt{pc}\sqcup\mathtt{pol}(\sigma)$. Hence by Lemma 8.5 it suffices to show $(\gamma_1(e_1),W.\theta_1,\mathfrak{m})\in\lceil\tau\rceil^{\mathtt{pc}\sqcup\mathtt{pol}(\sigma)}_{\mathsf{E}}$. We get this by Unary Fundamental Lemma if $(\gamma_1,W.\theta_1,\mathfrak{m})\in\lceil\Gamma\rceil_{\mathcal{V}}$. By Lemma 8.32 this is the case.
  - $(\gamma_2(e_1),W.\theta_2,\mathfrak{m})\in\lceil\tau\rceil^{\mathtt{pol}(\sigma)}_{\mathsf{E}}$. By Lemma 4.6 $\mathtt{pol}(\sigma)\sqsubseteq\mathtt{pc}\sqcup\mathtt{pol}(\sigma)$. Hence by Lemma 8.5 it suffices to show $(\gamma_2(e_1),W.\theta_2,\mathfrak{m})\in\lceil\tau\rceil^{\mathtt{pc}\sqcup\mathtt{pol}(\sigma)}_{\mathsf{E}}$. We get this by Unary Fundamental Lemma if $(\gamma_2,W.\theta_2,\mathfrak{m})\in\lceil\Gamma\rceil_{\mathcal{V}}$. By Lemma 8.32 this is the case.
  - $(\gamma_1(e_2),W.\theta_1,\mathfrak{m})\in\lceil\tau\rceil^{\mathtt{pol}(\sigma)}_{\mathsf{E}}$. By Lemma 4.6 $\mathtt{pol}(\sigma)\sqsubseteq\mathtt{pc}\sqcup\mathtt{pol}(\sigma)$. Hence by Lemma 8.5 it suffices to show $(\gamma_1(e_2),W.\theta_1,\mathfrak{m})\in\lceil\tau\rceil^{\mathtt{pc}\sqcup\mathtt{pol}(\sigma)}_{\mathsf{E}}$. We get this by Unary Fundamental Lemma if $(\gamma_1,W.\theta_1,\mathfrak{m})\in\lceil\Gamma\rceil_{\mathcal{V}}$. By Lemma 8.32 this is the case.
  - $(\gamma_2(e_2),W.\theta_2,\mathfrak{m})\in\lceil\tau\rceil^{\mathtt{pol}(\sigma)}_{\mathsf{E}}$. By Lemma 4.6 $\mathtt{pol}(\sigma)\sqsubseteq\mathtt{pc}\sqcup\mathtt{pol}(\sigma)$. Hence by Lemma 8.5 it suffices to show $(\gamma_2(e_2),W.\theta_2,\mathfrak{m})\in\lceil\tau\rceil^{\mathtt{pc}\sqcup\mathtt{pol}(\sigma)}_{\mathsf{E}}$. We get this by Unary Fundamental Lemma if $(\gamma_2,W.\theta_2,\mathfrak{m})\in\lceil\Gamma\rceil_{\mathcal{V}}$. By Lemma 8.32 this is the case.
  - $\mathtt{pol}(\sigma)\sqsubseteq\tau$. This is an assumption of the rule.
  - $\Sigma\approx_{\mathcal{A}}\Sigma$. This is clearly the case.

□

9 Higher order observations:

Note that, in the paper, for reasons of explainability, we used a slightly different formulation of the logical relation, that is logically equivalent to the one used in our proofs (modulo the additional features we have to deal with here). In particular the condition that *we either have a relevant declassification or we continue to enforce relatedness* is formulated as the implication *if there is no relevant declassification, then we continue to enforce relatedness* here. The part of this condition not related to the active lock set is captured by the relation $\approx^{\mathcal{A}}_{(W,\mathfrak{m})}$ defined below.

If we want to have higher order observations we need some notion of equivalence of functions. The obvious notions is to take the logical relation again. Because all other notions of equivalence on values used in the equivalence of observations coincide with the logical relations as well, we can just replace the equivalence with being in the logical relation. Note that this means that equivalence of observations is now step-indexed.

$$\frac{\forall\mathfrak{l},\tau,\nu.\omega\neq\mathfrak{l}_\tau(\nu)}{\omega\approx^{\mathcal{A}}_{(W,\mathfrak{m})}\omega}\ \textbf{refl} \qquad \frac{\neg(\mathrm{pol}(\omega)\sqsubseteq\mathcal{A})\vee\neg(\mathrm{pol}(\omega')\sqsubseteq\mathcal{A})}{\omega\approx^{\mathcal{A}}_{(W,\mathfrak{m})}\omega'}\ \textbf{high} \qquad \frac{(\nu,\nu',W,\mathfrak{m})\in[\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}}{\mathfrak{l}_\tau(\nu)\approx^{\mathcal{A}}_{(W,\mathfrak{m})}\mathfrak{l}'_\tau(\nu')}\ \textbf{extend-}\tau$$

and

$$\frac{\mathrm{pol}(\omega)\not\sqsubseteq\mathcal{A} \qquad \mathrm{pol}(\omega')\not\sqsubseteq\mathcal{A}}{\omega\approx^{\mathcal{A}}_{(W,\mathfrak{m})}\omega'}\ \textbf{high} \qquad \frac{\forall\mathfrak{l},\tau,\nu.\omega\neq\mathfrak{l}_\tau(\nu)}{\omega\approx^{\mathcal{A}}_{(W,\mathfrak{m})}\omega}\ \textbf{refl}$$

$$\frac{(\nu,\nu',W,\mathfrak{m})\in[\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}} \qquad (\mathfrak{l},\mathfrak{l}')\in W.\beta}{\mathfrak{l}_\tau(\nu)\approx^{\mathcal{A}}_{(W,\mathfrak{m})}\mathfrak{l}'_\tau(\nu')}\ \textbf{extend-}\tau$$

The unary relations and the binary value relation stay exactly the same. In the binary expression relation we have to use the step-indexed notion of equivalence of observations now.

$\llbracket \tau \rrbracket^{\mathcal{A}}_{\mathrm{E}} := \llbracket \tau \rrbracket^{\mathcal{A}}_{\mathrm{E}_\beta} \cup \left\{ (v, v', W, \Sigma_{c_1}, \Sigma_{c_2}, m) \,\middle|\, (v, v', W, m) \in \llbracket \tau \rrbracket^{\mathcal{A}}_{\mathcal{V}} \right\}$ where:

$$
\llbracket \tau \rrbracket^{\mathcal{A}}_{\mathrm{E}_\beta} := \left\{ (e_1, e_2, W, \Sigma, \Sigma', m) \;\middle|\; \begin{array}{l}
\Sigma \approx_{\mathcal{A}} \Sigma' \wedge \forall \Sigma_1, \Sigma_2 . \Sigma \subseteq \Sigma_1 \wedge \Sigma' \subseteq \Sigma_2 \wedge \Sigma_1 \approx_{\mathcal{A}} \Sigma_2 \rightarrow \\
\\
\forall W', m', S_1, S_2 . m' < m \wedge W' \sqsupseteq W \wedge (S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W' \rightarrow (e_1, e_2) \in \\
\\
\left(\begin{array}{l}
C_{par} = \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l}
e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\
\forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega' . \\
\Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega; \Sigma_1'} e_1', S_1' \wedge \\
\Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega'; \Sigma_2'} e_2', S_2' \rightarrow \\
(\omega \approx^{\mathcal{A}}_{(W', m')} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\
\exists W'' . W'' \sqsupseteq W' \wedge (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\
\omega \approx^{\mathcal{A}}_{(W'', m')} \omega' \wedge (e_1', e_2', W'', \Sigma, \Sigma', m') \in \llbracket \tau \rrbracket^{\mathcal{A}}_{\mathrm{E}}
\end{array} \right\} \cup \\
\\
C_L = \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l}
e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega . \\
\Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega; \Sigma_1'} e_1', S_1' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\
(\exists W'' . W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\
(e_1', e_2, W'', \Sigma, \Sigma', m') \in \llbracket \tau \rrbracket^{\mathcal{A}}_{\mathrm{E}})
\end{array} \right\} \cup \\
\\
C_R = \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l}
e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega . \\
\Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega; \Sigma_2'} e_2', S_2' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\
(\exists W'' . W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\
(e_1, e_2', W'', \Sigma, \Sigma', m') \in \llbracket \tau \rrbracket^{\mathcal{A}}_{\mathrm{E}})
\end{array} \right\}
\end{array} \right)
\end{array} \right\}
$$

The only compatibility lemmas that change significantly are those dealing with references:

Lemma 9.1. If $(e, e', W, \Sigma, \Sigma', m) \in \llbracket \tau' \rrbracket^{\mathcal{A}}_{\mathrm{E}}$, $\Sigma \approx_{\mathcal{A}} \Sigma'$ and $\tau'(\Sigma) <: \tau$ and $\tau'(\Sigma') <: \tau$, then $(\mathsf{new}\,(e, \tau)\,, \mathsf{new}\,(e', \tau)\,, W, \Sigma, \Sigma', m) \in \llbracket (\mathsf{ref}\,(\tau))^{\perp} \rrbracket^{\mathcal{A}}_{\mathrm{E}}$.

Proof. By induction on m. It suffices to show $(new(e, \tau), new(e', \tau), W, \Sigma, \Sigma', m) \in \llbracket (\mathrm{ref}(\tau))^{\perp} \rrbracket^{\mathcal{A}}_{\mathrm{E}_\beta}$. We already have $\Sigma \approx_{\mathcal{A}} \Sigma'$ by assumption. Let Σ_1, Σ_2 such that

- $\Sigma_1 \supseteq \Sigma$,
- $\Sigma_2 \supseteq \Sigma'$,
- $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

W', m' such that

- $m' < m$,
- $W' \sqsupseteq W$,

and S_1, S_2 such that

- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

There are two cases:

1. $(e, e', W, \Sigma, \Sigma', m) \in \llbracket \tau' \rrbracket^{\mathcal{A}}_{\mathrm{E}_\beta}$. In this case there are three further cases:

(a) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \;\wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{(W',\mathfrak{m}')} \;\omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''. W'' \sqsupseteq W' \wedge\; (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \;\wedge \\ \omega \approx^{\mathcal{A}}_{(W'',\mathfrak{m}')} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau']\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$

In this case it is suffices to show

$(new(e, \tau), new(e', \tau)) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \;\wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{(W',\mathfrak{m}')} \;\omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''. W'' \sqsupseteq W' \wedge\; (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \;\wedge \\ \omega \approx^{\mathcal{A}}_{(W'',\mathfrak{m}')} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\mathsf{ref}(\tau))^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$

It is clear that neither $new(e, \tau)$ nor $new(e', \tau)$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $new(e, \tau), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $new(e', \tau), \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

By assumption neither e nor e' are values. Hence the reductions must have happened with **ENew**. Hence by inversion

- $e, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e', \Sigma_2, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
- $e_\beta = new(e_0, \tau)$
- $e_\beta' = new(e_0', \tau)$

Also assume $\omega \approx^{\mathcal{A}}_{(W',\mathfrak{m}')} \;\omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \;\vee\; \Sigma_2' \sqsubseteq \mathcal{A}$. This directly gives us a W'' such that

- $W'' \sqsupseteq W'$,
- $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{(W'',\mathfrak{m}')} \omega'$, and
- $(e_0, e_0', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau']\!]^{\mathcal{A}}_{\mathsf{E}}$

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{(W'',\mathfrak{m}')} \omega'$. We already know that.
- $(new(e_0, p), new(e_0', p), W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\mathsf{ref}\ \tau)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$. We get this by induction.

(b) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \;\wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \;\wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau']\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$

In this case it suffices to show

$(new(e, \tau), new(e', \tau)) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \rightarrow \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \;\wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \;\wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\mathsf{ref}\ \tau)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$.

It is clear that $new(e, \tau)$ is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $new(e, \tau), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

By assumption e is not a value. Hence the reduction must have happened with **ENew**. By inversion

- $e, \Sigma_1, S_1 \succ e_0, S_1', \omega, \Sigma_1'$
- $e_\beta = new(e_0, \tau)$

Hence

- $\neg(pol(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_0, e', W'', \Sigma, \Sigma', m') \in [\![\tau']\!]^{\mathcal{A}}_{E}$

It suffices to show the following:

- $\neg(pol(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(new(e_0, \tau), new(e', \tau), W'', \Sigma, \Sigma', m') \in [\![(\text{ref } \tau)^{\perp}]\!]^{\mathcal{A}}_{E}$. We get this using the induction hypothesis.

(c) $(e, e') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \rightarrow \neg(pol(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![\tau']\!]^{\mathcal{A}}_{E}) \end{array} \right\}$

In this case it suffices to show

$(new(e, \tau), new(e', \tau)) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega;\Sigma_2'} e_2',\, S_2' \rightarrow \neg(pol(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![(\text{ref } \tau)^{\perp}]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$

It is clear that $new(e', \tau)$ is not a value. So let $\omega', e_\beta', \Sigma_2', S_2'$ such that

- $new(e', \tau), \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

By assumption e' is not a value. Hence the reduction must have happened with **ENew**. By inversion

- $e', \Sigma_2, S_2 \succ e_0', S_2', \omega', \Sigma_2'$
- $e_\beta' = new(e_0', \tau)$

Hence

- $\neg(pol(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e, e_0', W'', \Sigma, \Sigma', m') \in [\![\tau']\!]^{\mathcal{A}}_{E}$

It suffices to show the following:

- $\neg(pol(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(new(e, \tau), new(e_0', \tau), W'', \Sigma, \Sigma', m') \in [\![(\text{ref } \tau)^{\perp}]\!]^{\mathcal{A}}_{E}$. We get this using the induction hypothesis.

2. $(e, e', W, \Sigma, \Sigma', m) \in \left\{ (v, v', W, \Sigma_{c_1}, \Sigma_{c_2}, m) \;\middle|\; (v, v', W, m) \in [\![\tau']\!]^{\mathcal{A}}_{\mathcal{V}} \right\}$

So there are v and v' such that $e = v$ and $e' = v'$ and $(v, v', W, m) \in [\![\tau']\!]^{\mathcal{A}}_{\mathcal{V}}$.

It suffices to show

$$(new(v,\tau), new(v',\tau)) \in \left\{ (e_1,e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \;\wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\, S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\, S_1' \;\wedge \\ \Sigma_2 \vdash e_2,\, S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\, S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{(W',\mathfrak{m}')} \;\omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''.W'' \sqsupseteq W' \wedge\; (S_1', S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{(W'',\mathfrak{m}')} \omega' \wedge\; (e_1', e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\mathrm{ref}\ \tau)^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}$$

It is clear that neither $new(v,\tau)$ nor $new(v',\tau)$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $new(v,\tau), \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $new(v',\tau), \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

The reductions must have happened with **ENewBeta**. Hence there are A, p, l, l' such that

- $\tau = A^p$
- $e_\beta = l$
- $e_\beta' = l'$
- $l \notin dom(S_1)$
- $l' \notin dom(S_2)$
- $\Sigma_1' = \Sigma_1$
- $\Sigma_2' = \Sigma_2$
- $S_1' = S_1 \cup \{l \rightarrowtail (v,\tau)\}$
- $S_2' = S_2 \cup \{l' \rightarrowtail (v',\tau)\}$
- $\omega = l_\tau(v)$
- $\omega' = l'_\tau(v')$

Hence the reductions are really

- $new(v,\tau), \Sigma_1, S_1 \succ l, S_1 \cup \{l \rightarrowtail (v,p)\}, l_\tau(v), \Sigma_1$
- $new(v',\tau), \Sigma_2, S_2 \succ l', S_2 \cup \{l' \rightarrowtail (v',p)\}, l'_\tau(v'), \Sigma_2$

Also assume $l_\tau(v) \approx^{\mathcal{A}}_{(W',\mathfrak{m}')} l'_\tau(v') \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$. We know $\tau'(\Sigma) <: \tau$ and $\tau'(\Sigma') <: \tau$ or more specifically $\tau'(\Sigma) <: A^p$ and $\tau'(\Sigma') <: A^p$. Hence there must be a type B and policy p' such that

- $\tau' = B^{p'}$,
- $p'(\Sigma) \sqsubseteq p$,
- $p'(\Sigma') \sqsubseteq p$ and
- $B <: A$.

It is clear that $W'.\beta \cup \{(l,l')\}$ is an injective partial function because $l \notin dom(S_1)$ and $l' \notin dom(S_2)$. Hence it suffices to show

- $(W'.\theta_1 \cup \{l,\tau\}, W'.\theta_2 \cup \{l',\tau\}, W'.\beta \cup \{(l,l')\}) \sqsupseteq W'$ We have to show
  - $W'.\theta_1 \cup \{l,\tau\} \sqsupseteq W'.\theta_1$. Let $l'' \in dom(W'.\theta_1)$. Then clearly also $l'' \in dom(W'.\theta_1 \cup \{l,\tau\})$. We still have to show $W'.\theta_1(l'') = W'.\theta_1 \cup \{l,\tau\}(l'')$ This is the case if $l'' \neq l$.

    We show $l'' \neq l$: By assumption $l \notin dom(S_1)$ and $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence in particular $dom(W'.\theta_1) \subseteq dom(S_1)$. Because $l \notin dom(S_1)$ therefore also $l \notin dom(W'.\theta_1)$. But $l'' \in dom(W'.\theta_1)$. Hence we must have $l'' \neq l$.
  - $W'.\theta_2 \cup \{l',\tau\} \sqsupseteq W'.\theta_2$. Let $l'' \in dom(W'.\theta_2)$. Then clearly also $l'' \in dom(W'.\theta_2 \cup \{l',\tau\})$. We still have to show $W'.\theta_2(l'') = W'.\theta_2 \cup \{l',\tau\}(l'')$ This is the case if $l'' \neq l'$.

    We show $l'' \neq l'$: By assumption $l' \notin dom(S_2)$ and $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence in particular $dom(W'.\theta_2) \subseteq dom(S_2)$. Because $l' \notin dom(S_2)$ therefore also $l' \notin dom(W'.\theta_2)$. But $l'' \in dom(W'.\theta_2)$. Hence we must have $l'' \neq l'$.
  - $W'.\beta \cup \{(l,l')\} \supseteq W'.\beta$. This is obvious.

- $(S_1 \cup \{l \rightarrowtail (\nu, \tau)\}, S_2 \cup \{l' \rightarrowtail (\nu', \tau)\}, m') \overset{\mathcal{A}}{\triangleright} (W'.\theta_1 \cup \{l, \tau\}, W'.\theta_2 \cup \{l', \tau\}, W'.\beta \cup \{(l, l')\})$.
  We have to show
  - $W'.\beta \cup \{(l, l')\} \subseteq \mathbf{dom}(W'.\theta_1 \cup \{l, \tau\}) \times \mathbf{dom}(W'.\theta_2 \cup \{l', \tau\})$.
    Let $(l_1, l_2) \in W'.\beta \cup \{(l, l')\}$. There are two options:
    (a) $(l_1, l_2) \neq (l, l')$. In this case $(l_1, l_2) \in W'.\beta$. By assumption $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. Hence $W'.\beta \subseteq \mathbf{dom}(W'.\theta_1) \times \mathbf{dom}(W'.\theta_2)$. Therefore $(l_1, l_2) \in \mathbf{dom}(W'.\theta_1) \times \mathbf{dom}(W'.\theta_2)$. Then also $(l_1, l_2) \in \mathbf{dom}(W'.\theta_1 \cup \{l, \tau\}) \times \mathbf{dom}(W'.\theta_2 \cup \{l', \tau\})$.
    (b) $(l_1, l_2) = (l, l')$. It suffices to show $(l, l') \in \mathbf{dom}(W'.\theta_1 \cup \{l, \tau\}) \times \mathbf{dom}(W'.\theta_2 \cup \{l', \tau\})$ which is clearly the case.
  - $\forall (l_1, l_2) \in W'.\beta \cup \{(l, l')\}.W'.\theta_1 \cup \{l, \tau\}(l_1) = W'.\theta_2 \cup \{l', \tau\}(l_2) \wedge$
    $(S_1 \cup \{l \rightarrowtail (\nu, \tau)\}(l_1), S_2 \cup \{l' \rightarrowtail (\nu', \tau)\}(l_2), (W'.\theta_1 \cup \{l, \tau\}, W'.\theta_2 \cup \{l', \tau\}, W'.\beta \cup \{(l, l')\}), m') \in [\![W'.\theta_1 \cup \{l, \tau\}(l_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$.
    Let $(l_1, l_2) \in W'.\beta \cup \{(l, l')\}$. There are two cases:
    (a) $(l_1, l_2) \neq (l, l')$. Then $(l_1, l_2) \in W'.\beta$. Because $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ we know $W'.\beta \subseteq \mathbf{dom}(W.\theta_1) \times \mathbf{dom}(W.\theta_2)$. Hence
    * $l_1 \in \mathbf{dom}(W.\theta_1)$ and
    * $l_2 \in \mathbf{dom}(W.\theta_2)$.

    By the same argument as in the previous case this means that
    * $l_1 \neq l$
    * $l_2 \neq l'$.

    Therefore

$$W'.\theta_1 \cup (l, \tau)(l_1) = W'.\theta_1(l_1) \overset{(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'}{=} W'.\theta_2(l_2) = W'.\theta_2 \cup \{l', \tau\}(l_2)$$

    .
    We also get
    * $(S_1(l_1), S_2(l_2), W', m') \in [\![W'.\theta_1(l_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$

    from $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$. We have already shown in a previous case that $(W'.\theta_1 \cup \{l, \tau\}, W'.\theta_2 \cup \{l', \tau\}, W'.\beta \cup \{(l, l')\}) \sqsupseteq W'$. Hence we get
    * $(S_1(l_1), S_2(l_2), (W'.\theta_1 \cup \{l, \tau\}, W'.\theta_2 \cup \{l', \tau\}, W'.\beta \cup \{(l, l')\}), m') \in [\![W'.\theta_1(l_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$

    by Lemma 8.25. Because $l_1 \neq l$ and $l_2 \neq l'$ this is equivalent to the remaining subgoal.
    (b) $(l_1, l_2) = (l, l')$. In this case

$$W'.\theta_1 \cup (l, \tau)(l_1) = W'.\theta_1 \cup (l, \tau)(l) = \tau = W'.\theta_2 \cup (l', \tau)(l') = W'.\theta_2 \cup (l', \tau)(l_2)$$

    .
    The second subgoal simplifies to $(\nu, \nu', (W'.\theta_1 \cup \{l, \tau\}, W'.\theta_2 \cup \{l', \tau\}, W'.\beta \cup \{(l, l')\}), m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$.
    τ has the form A^p. We do case analysis on whether $p \sqsubseteq \mathcal{A}$ or not:
    i. $p \sqsubseteq \mathcal{A}$.
    We do case analysis on $l_\tau(\nu) \approx^{\mathcal{A}}_{(W', m')} l'_\tau(\nu') \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.
    A. $l_\tau(\nu) \approx^{\mathcal{A}}_{(W', m')} l'_\tau(\nu')$.

    The only rule with which $l_\tau(\nu) \approx^{\mathcal{A}}_{(W', m')} l'_\tau(\nu')$ can be derived is **extend-τ** as it is clear from the structure of the observations that neither **refl** nor **extend** is applicable. **high** is also not applicable because $p \sqsubseteq \mathcal{A}$ by assumption.

    By inversion
    ☞ $(\nu, \nu', W', m') \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$.
    The goal follows by Lemma 8.25.
    B. $\Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.

    First we show that $p' \sqsubseteq \mathcal{A}$: By assumption $\Sigma_1 \supseteq \Sigma$, $\Sigma_2 \supseteq \Sigma'$, $p'(\Sigma) \sqsubseteq p$ and $p'(\Sigma') \sqsubseteq p$. Hence by Lemma 4.3 and transitivity (Lemma 4.1)
    ☞ $p'(\Sigma_1) \sqsubseteq p$ and
    ☞ $p'(\Sigma_2) \sqsubseteq p$.

In both cases ($\Sigma_1 \sqsubseteq \mathcal{A}$ and $\Sigma_2 \sqsubseteq \mathcal{A}$) we get $\mathfrak{p}' \sqsubseteq \mathcal{A}$ by Lemma 8.46.

Now we can continue with the main proof. We already know $(\nu, \nu', W, \mathfrak{m}) \in [\![\mathsf{B}^{\mathfrak{p}'}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\mathfrak{p}' \sqsubseteq \mathcal{A}$, this means that $(\nu, \nu', W, \mathfrak{m}) \in [\![\mathsf{B}]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.31 $(\nu, \nu', W, \mathfrak{m}) \in [\![\mathsf{A}]\!]^{\mathcal{A}}_{\mathcal{V}}$. From this we can directly follow $(\nu, \nu', W, \mathfrak{m}) \in [\![\mathsf{A}^{\mathfrak{p}}]\!]^{\mathcal{A}}_{\mathcal{V}}$ because $\mathfrak{p} \sqsubseteq \mathcal{A}$ by assumption. The goal follows by Lemma 8.25 and Lemma 8.24.

ii. $\mathfrak{p} \not\sqsubseteq \mathcal{A}$.
Because $\mathfrak{p} \not\sqsubseteq \mathcal{A}$, it suffices to show
* $(\nu, W'.\theta_1 \cup \{\mathfrak{l}, \tau\}, \mathfrak{m}') \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$ and

* $(\nu', W'.\theta_2 \cup \{\mathfrak{l}', \tau\}\, \mathfrak{m}') \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$.

By Lemma 8.4 it suffices to show
* $(\nu, W'.\theta_1, \mathfrak{m}') \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$ and

* $(\nu', W'.\theta_2, \mathfrak{m}') \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$.

From $(\nu, \nu', W, \mathfrak{m}) \in [\![\mathsf{B}^{\mathfrak{p}'}]\!]^{\mathcal{A}}_{\mathcal{V}}$ we get
* $(\nu, W'.\theta_1, \mathfrak{m}') \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$ and

* $(\nu', W'.\theta_2, \mathfrak{m}') \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$

by Lemma 8.22, the definition of $\lceil \mathsf{B}^{\mathfrak{p}'} \rceil_{\mathcal{V}}$ and Lemma 8.4. We get the remaining subgoals by Lemma 8.6.

– $(\Sigma_1 \cup \{\mathfrak{l} \rightarrowtail (\nu, \tau)\}, \mathfrak{m}') \triangleright W'.\theta_1 \cup \{\mathfrak{l}, \tau\}$. For this we have to show
* $\mathsf{dom}(W'.\theta_1 \cup \{\mathfrak{l}, \tau\}) \subseteq \mathsf{dom}(\Sigma_1 \cup \{\mathfrak{l} \rightarrowtail (\nu, \tau)\})$.
$\mathsf{dom}(W'.\theta_1 \cup \{\mathfrak{l}, \tau\}) = \mathsf{dom}(W'.\theta_1) \cup \{\mathfrak{l}\} \overset{(\Sigma_1, \Sigma_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'}{\subseteq} \mathsf{dom}(\Sigma_1) \cup \{\mathfrak{l}\} = \mathsf{dom}(\Sigma_1 \cup \{\mathfrak{l} \rightarrowtail (\nu, \tau)\})$.
* $\forall \mathfrak{l}'' \in \mathsf{dom}(W'.\theta_1 \cup \{\mathfrak{l}, \tau\}).(\Sigma_1 \cup \{\mathfrak{l} \rightarrowtail (\nu, \tau)\}(\mathfrak{l}''), W'.\theta_1 \cup \{\mathfrak{l}, \tau\}, \mathfrak{m}') \in \lceil W'.\theta_1 \cup \{\mathfrak{l}, \tau\}(\mathfrak{l}'') \rceil_{\mathcal{V}}$.
Let $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_1 \cup \{\mathfrak{l}, \tau\})$. There are two cases:

(a) $\mathfrak{l}'' \neq \mathfrak{l}$. In this case $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_1)$. By assumption $(\Sigma_1, \Sigma_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence also $(\Sigma_1, \mathfrak{m}') \triangleright W'.\theta_1$. Therefore in particular $(\Sigma_1(\mathfrak{l}''), W'.\theta_1, \mathfrak{m}') \in \lceil W'.\theta_1(\mathfrak{l}'') \rceil_{\mathcal{V}}$. Because $\mathfrak{l}'' \neq \mathfrak{l}$ this is equivalent to $(\Sigma_1 \cup \{\mathfrak{l} \rightarrowtail (\nu, \tau)\}(\mathfrak{l}''), W'.\theta_1, \mathfrak{m}') \in \lceil W'.\theta_1 \cup \{\mathfrak{l}, \tau\}(\mathfrak{l}'') \rceil_{\mathcal{V}}$. We get the claim by Lemma 8.4.

(b) $\mathfrak{l}'' = \mathfrak{l}$. In this case the goal simplifies to $(\nu, W'.\theta_1 \cup \{\mathfrak{l}, \tau\}, \mathfrak{m}') \in \lceil \tau \rceil_{\mathcal{V}}$. By assumption $(\nu, \nu', W, \mathfrak{m}) \in [\![\mathsf{B}^{\mathfrak{p}'}]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.22 therefore $(\nu, W.\theta_1, \mathfrak{m}) \in \lceil \mathsf{B}^{\mathfrak{p}'} \rceil_{\mathcal{V}}$. By the definitions of $\lceil \mathsf{B}^{\mathfrak{p}'} \rceil_{\mathcal{V}}$ we directly get $(\nu, W.\theta_1, \mathfrak{m}) \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$. From that we get $(\nu, W.\theta_1, \mathfrak{m}) \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$ by Lemma 8.6. We get $(\nu, W.\theta_1, \mathfrak{m}) \in \lceil \mathsf{A}^{\mathfrak{p}} \rceil_{\mathcal{V}}$ by definition. The goal follows from Lemma 8.4 and Lemma 7.2.

* $\forall \mathfrak{l}'' \in \mathsf{dom}(W'.\theta_1 \cup \{\mathfrak{l}, \tau\}).W'.\theta_1 \cup \{\mathfrak{l}, \tau\}(\mathfrak{l}'') = \mathsf{type}(\Sigma_1 \cup \{\mathfrak{l} \rightarrowtail (\nu, \tau)\}, \mathfrak{l}'')$.
Let $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_1 \cup \{\mathfrak{l}, \tau\})$. There are two cases:

(a) $\mathfrak{l}'' \neq \mathfrak{l}$. In this case $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_1)$. By assumption $(\Sigma_1, \Sigma_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence $W'.\theta_1(\mathfrak{l}'') = \mathsf{type}(\Sigma_1, \mathfrak{l}'')$. Because $\mathfrak{l}'' \neq \mathfrak{l}$ this is equivalent to the goal.

(b) $\mathfrak{l}'' = \mathfrak{l}$. In this case the goal simplifies to $\tau = \tau$. This is clearly the case.

– $(\Sigma_2 \cup \{\mathfrak{l}' \rightarrowtail (\nu', \tau)\}, \mathfrak{m}') \triangleright W'.\theta_2 \cup \{\mathfrak{l}', \tau\}$. For this we have to show
* $\mathsf{dom}(W'.\theta_2 \cup \{\mathfrak{l}', \tau\}) \subseteq \mathsf{dom}(\Sigma_2 \cup \{\mathfrak{l}' \rightarrowtail (\nu', \tau)\})$.
$\mathsf{dom}(W'.\theta_2 \cup \{\mathfrak{l}', \tau\}) = \mathsf{dom}(W'.\theta_2) \cup \{\mathfrak{l}'\} \overset{(\Sigma_1, \Sigma_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'}{\subseteq} \mathsf{dom}(\Sigma_2) \cup \{\mathfrak{l}'\} = \mathsf{dom}(\Sigma_2 \cup \{\mathfrak{l}' \rightarrowtail (\nu', \tau)\})$.
* $\forall \mathfrak{l}'' \in \mathsf{dom}(W'.\theta_2 \cup \{\mathfrak{l}', \tau\}).(\Sigma_2 \cup \{\mathfrak{l}' \rightarrowtail (\nu', \tau)\}(\mathfrak{l}''), W'.\theta_2 \cup \{\mathfrak{l}', \tau\}, \mathfrak{m}') \in \lceil W'.\theta_2 \cup \{\mathfrak{l}', \tau\}(\mathfrak{l}'') \rceil_{\mathcal{V}}$. Let $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_2 \cup \{\mathfrak{l}', \tau\})$. There are two cases:

(a) $\mathfrak{l}'' \neq \mathfrak{l}'$. In this case $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_2)$. By assumption $(\Sigma_1, \Sigma_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence also $(\Sigma_2, \mathfrak{m}') \triangleright W'.\theta_2$. Therefore in particular $(\Sigma_2(\mathfrak{l}''), W'.\theta_2, \mathfrak{m}') \in \lceil W'.\theta_2(\mathfrak{l}'') \rceil_{\mathcal{V}}$. Because $\mathfrak{l}'' \neq \mathfrak{l}'$ this is equivalent to $(\Sigma_1 \cup \{\mathfrak{l}' \rightarrowtail (\nu', \tau)\}(\mathfrak{l}''), W'.\theta_2, \mathfrak{m}') \in \lceil W'.\theta_2 \cup \{\mathfrak{l}', \tau\}(\mathfrak{l}'') \rceil_{\mathcal{V}}$. We get the claim by Lemma 8.4.

(b) $\mathfrak{l}'' = \mathfrak{l}'$. In this case the goal simplifies to $(\nu', W'.\theta_2 \cup \{\mathfrak{l}', \tau\}, \mathfrak{m}') \in \lceil \tau \rceil_{\mathcal{V}}$. By assumption $(\nu, \nu', W, \mathfrak{m}) \in [\![\mathsf{B}^{\mathfrak{p}'}]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.22 therefore $(\nu', W.\theta_2, \mathfrak{m}) \in \lceil \mathsf{B}^{\mathfrak{p}'} \rceil_{\mathcal{V}}$.By

the definitions of $\lceil \mathsf{B}^{\mathsf{p}'} \rceil_\nu$ we directly get $(\nu', W.\theta_2, \mathfrak{m}) \in \lceil \mathsf{B} \rceil_\nu$. From that we get $(\nu', W.\theta_2, \mathfrak{m}) \in \lceil \mathsf{A} \rceil_\nu$ by Lemma 8.6. We get $(\nu', W.\theta_2, \mathfrak{m}) \in \lceil \mathsf{A}^{\mathsf{p}} \rceil_\nu$ by definition. The goal follows from Lemma 8.4 and Lemma 7.2.

* $\forall \mathfrak{l}'' \in \mathsf{dom}(W'.\theta_2 \cup \{\mathfrak{l}', \tau\}). W'.\theta_2 \cup \{\mathfrak{l}', \tau\}(\mathfrak{l}'') = \mathsf{type}(S_2 \cup \{\mathfrak{l}' \rightarrowtail (\nu', \mathsf{p})\}, \mathfrak{l}'')$.
  Let $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_2 \cup \{\mathfrak{l}', \tau\})$. There are two cases:

  (a) $\mathfrak{l}'' \neq \mathfrak{l}'$. In this case $\mathfrak{l}'' \in \mathsf{dom}(W'.\theta_2)$. By assumption $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence $W'.\theta_2(\mathfrak{l}'') = \mathsf{type}(S_2, \mathfrak{l}'')$. Because $\mathfrak{l}'' \neq \mathfrak{l}'$ this is equivalent to the goal.

  (b) $\mathfrak{l}'' = \mathfrak{l}'$. In this case the goal simplifies to $\tau = \tau$. This is clearly the case.

- $\mathfrak{l}_\tau(\nu) \approx^{\mathcal{A}}_{((W'.\theta_1 \cup \{\mathfrak{l},\tau\}, W'.\theta_2 \cup \{\mathfrak{l}',\tau\}, W'.\beta \cup \{(\mathfrak{l},\mathfrak{l}')\}), \mathfrak{m}')} \mathfrak{l}'_\tau(\nu')$.
  We do case analysis on the visibility of p.

  (a) $\mathsf{p} \not\sqsubseteq \mathcal{A}$. Because $\mathsf{pol}(\tau) = \mathsf{p}$ we get the claim by **high**.

  (b) $\mathsf{p} \sqsubseteq \mathcal{A}$: By **extend-τ** it suffices to show

  – $(\mathfrak{l}, \mathfrak{l}') \in W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}$. This is obvious.

  – $(\nu, \nu', (W'.\theta_1 \cup \{\mathfrak{l}, \tau\}, W'.\theta_2 \cup \{\mathfrak{l}', \tau\}, W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}), \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_\nu$.
  By Lemma 8.25 it suffices to how Lemma 8.45 it suffices to show $(\nu, \nu', W', \mathfrak{m}') \in [\![\tau]\!]^{\mathcal{A}}_\nu$.
  We do case analysis on $\mathfrak{l}_\tau(\nu) \approx^{\mathcal{A}}_{(W', \mathfrak{m}')} \mathfrak{l}'_\tau(\nu') \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.

  i. $\mathfrak{l}_\tau(\nu) \approx^{\mathcal{A}}_{(W', \mathfrak{m}')} \mathfrak{l}'_\tau(\nu')$. This must have been derived by **extend-τ**. We get the goal by inversion.

  ii. $\Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.

  First we show that $\mathsf{p}' \sqsubseteq \mathcal{A}$: By assumption $\Sigma_1 \supseteq \Sigma$, $\Sigma_2 \supseteq \Sigma'$, $\mathsf{p}'(\Sigma) \sqsubseteq \mathsf{p}$ and $\mathsf{p}'(\Sigma') \sqsubseteq \mathsf{p}$. Hence by Lemma 4.3 and transitivity (Lemma 4.1)
  ☞ $\mathsf{p}'(\Sigma_1) \sqsubseteq \mathsf{p}$ and
  ☞ $\mathsf{p}'(\Sigma_2) \sqsubseteq \mathsf{p}$.
  In both cases ($\Sigma_1 \sqsubseteq \mathcal{A}$ and $\Sigma_2 \sqsubseteq \mathcal{A}$) we get $\mathsf{p}' \sqsubseteq \mathcal{A}$ by Lemma 8.46.

  By Lemma 8.25 it suffices to show $(\nu, \nu', W, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_\nu$. We already know $(\nu, \nu', W, \mathfrak{m}) \in [\![\tau']\!]^{\mathcal{A}}_\nu$. Because $\tau' = \mathsf{B}^{\mathsf{p}'}$ this gives us $(\nu, \nu', W, \mathfrak{m}) \in [\![\mathsf{B}^{\mathsf{p}'}]\!]^{\mathcal{A}}_\nu$. Because $\mathsf{p}' \sqsubseteq \mathcal{A}$ we have $(\nu, \nu', W, \mathfrak{m}) \in [\![\mathsf{B}]\!]^{\mathcal{A}}_\nu$. By Lemma 8.31 we get $(\nu, \nu', W, \mathfrak{m}) \in [\![\mathsf{A}]\!]^{\mathcal{A}}_\nu$. $(\nu, \nu', W, \mathfrak{m}) \in [\![\mathsf{A}^{\mathsf{p}}]\!]^{\mathcal{A}}_\nu$ follows because $\mathsf{p} \sqsubseteq \mathcal{A}$. As $\tau = \mathsf{A}^{\mathsf{p}}$ this shows the goal.

- $(\mathfrak{l}, \mathfrak{l}', (W'.\theta_1 \cup \{\mathfrak{l}, \tau\}, W'.\theta_2 \cup \{\mathfrak{l}', \tau\}, W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}), \Sigma, \Sigma', \mathfrak{m}') \in [\![(\mathsf{ref}(\tau))^\perp]\!]^{\mathcal{A}}_{\mathsf{E}}$.
  It suffices to show $(\mathfrak{l}, \mathfrak{l}', (W'.\theta_1 \cup \{\mathfrak{l}, \mathsf{A}^{\mathsf{p}}\}, W'.\theta_2 \cup \{\mathfrak{l}', \mathsf{A}^{\mathsf{p}}\}, W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}), \mathfrak{m}') \in [\![(\mathsf{ref}(\mathsf{A}^{\mathsf{p}}))^\perp]\!]^{\mathcal{A}}_\nu$.
  Because $\perp \sqsubseteq \mathcal{A}$ (Lemma 4.19) it suffices to show $(\mathfrak{l}, \mathfrak{l}', (W'.\theta_1 \cup \{\mathfrak{l}, \mathsf{A}^{\mathsf{p}}\}, W'.\theta_2 \cup \{\mathfrak{l}', \mathsf{A}^{\mathsf{p}}\}, W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}), \mathfrak{m}') \in [\![\mathsf{ref}(\mathsf{A}^{\mathsf{p}})]\!]^{\mathcal{A}}_\nu$. This means we need to show
  – $W'.\theta_1 \cup \{\mathfrak{l}, \mathsf{A}^{\mathsf{p}}\}(\mathfrak{l}) = \mathsf{A}^{\mathsf{p}} = W'.\theta_2 \cup \{\mathfrak{l}', \mathsf{A}^{\mathsf{p}}\}(\mathfrak{l}')$. This is clearly the case.
  – $(\mathfrak{l}, \mathfrak{l}') \in W'.\beta \cup \{(\mathfrak{l}, \mathfrak{l}')\}$. This is clearly the case.

□

Lemma 9.2. If $(e_1, e_1', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![(\mathsf{ref}\,\tau')^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathsf{E}}$, $(e_2, e_2', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$, $\mathsf{p} \sqsubseteq \tau'$, $\tau(\Sigma) <: \tau'$, $\tau(\Sigma') <: \tau'$ and $\Sigma \approx_{\mathcal{A}} \Sigma'$, then
$(e_1 := e_2, e_1' := e_2', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\mathsf{unit}^\perp]\!]^{\mathcal{A}}_{\mathsf{E}}$.

Proof. By induction on $\mathfrak{m}$. It suffices to show $(e_1 := e_2, e_1' := e_2', W, \Sigma, \Sigma', \mathfrak{m}) \in [\![\mathsf{unit}^\perp]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. We already have $\Sigma \approx_{\mathcal{A}} \Sigma'$ by assumption. Let Σ_1, Σ_2 such that

- $\Sigma_1 \supseteq \Sigma$,
- $\Sigma_2 \supseteq \Sigma'$,
- $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$,

$W', \mathfrak{m}'$ such that

- $\mathfrak{m}' < \mathfrak{m}$,
- $W' \sqsupseteq W$,

and S_1, S_2 such that

- $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$.

There are two cases:

1. $(e_1, e_1', W, \Sigma, \Sigma', m) \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_{E_\beta}$. This leaves us with three further cases:

(a) $(e_1, e_1') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \wedge \\ \Sigma_2 \vdash e_2, S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2', S_2' \to \\ (\omega \approx^{\mathcal{A}}_{(W',m')} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''. W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{(W'',m')} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![(\mathsf{ref}\tau')^p]\!]^{\mathcal{A}}_E \end{array} \right\}$

In that case it suffices to show

$(e_1 := e_2, e_1' := e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \wedge \\ \Sigma_2 \vdash e_2, S_2 \overset{\omega';\Sigma_2'}{\Longrightarrow} e_2', S_2' \to \\ (\omega \approx^{\mathcal{A}}_{(W',m')} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''. W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{(W'',m')} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\mathsf{unit}^\perp]\!]^{\mathcal{A}}_E \end{array} \right\}$

Neither $e_1 := e_2$ nor $e_1' := e_2'$ is a value. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $e_1 := e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $e_1' := e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Since neither e_1 nor e_1' is a value and therefore also not a location, the reductions must have happened with **Eassignl**. Hence by inversion

- $e_1, \Sigma_1, S_1 \succ e_l, S_1', \omega, \Sigma_1'$
- $e_1', \Sigma_2, S_2 \succ e_l', S_2', \omega', \Sigma_2'$
- $e_\beta = e_l := e_2$
- $e_\beta' = e_l' := e_2'$

Also let $\omega \approx^{\mathcal{A}}_{(W',m')} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \ \vee\ \Sigma_2' \sqsubseteq \mathcal{A}$. This directly gives us a W'' such that

- $W'' \sqsupseteq W'$,
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{(W'',m')} \omega'$, and
- $(e_l, e_l', W'', \Sigma, \Sigma', m') \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_E$

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{(W'',m')} \omega'$. We already know that.
- $(e_l := e_2, e_l' := e_2', W'', \Sigma, \Sigma', m') \in [\![\mathsf{unit}^\perp]\!]^{\mathcal{A}}_E$ We have $W'' \sqsupseteq W$ by transitivity (Lemma 7.2). Hence we also have $(e_2, e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_E$ by Lemma 8.29. We get the claim by induction.

(b) $(e_1, e_1') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_E) \end{array} \right\}$

In this case it suffices to show

$(e_1 := e_2, e_1' := e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1, S_1 \overset{\omega;\Sigma_1'}{\Longrightarrow} e_1', S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', m') \in [\![\mathsf{unit}^\perp]\!]^{\mathcal{A}}_E) \end{array} \right\}$

It is clear that $e_1 := e_2$ is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $e_1 := e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

By assumption e_1 is not a value and therefore also not a location. Hence the reduction must have happened with **Eassignl**. By inversion

- $e_1, \Sigma_1, S_1 \succ e_l, S_1', \omega, \Sigma_1'$
- $e_\beta = e_l := e_2$

From our assumption we get

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_l, e_1', W'', \Sigma, \Sigma', m') \in [\![(\mathtt{ref}\ \tau')^p]\!]_E^{\mathcal{A}}$

It suffices to show the following:

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(e_l := e_2, e_1' := e_2', \Sigma, \Sigma', m') \in [\![\mathtt{unit}^\perp]\!]_E^{\mathcal{A}}$. We know $(e_l, e_1', W'', \Sigma, \Sigma', m') \in [\![(\mathtt{ref}\ \tau')^p]\!]_E^{\mathcal{A}}$. We get $(e_2, e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]_E^{\mathcal{A}}$ by Lemma 8.29. The goal follows using the induction hypothesis.

(c) $(e_1, e_1') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\ S_2 \overset{\omega;\Sigma_2'}{\Longrightarrow} e_2',\ S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![(\mathtt{ref}\ \tau')^p]\!]_E^{\mathcal{A}}) \end{array} \right\}$

In this case it suffices to show

$(e_1 := e_2, e_1' := e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\ S_2 \overset{\omega;\Sigma_2'}{\Longrightarrow} e_2',\ S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', m') \in [\![\mathtt{unit}^\perp]\!]_E^{\mathcal{A}}) \end{array} \right\}$

Clearly $e_1' := e_2'$ is not a value. So let $\omega, e_\beta', \Sigma_2', S_2'$ such that

- $e_1' := e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega, \Sigma_2'$

By assumption e_1' is not a value and therefore also not a location. Hence the reduction must have happened with **Eassignl**. By inversion

- $e_1', \Sigma_2, S_2 \succ e_l', S_2', \omega, \Sigma_2'$
- $e_\beta' = e_l' := e_2'$

From our assumption we get

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_1, e_l', W'', \Sigma, \Sigma', m') \in [\![(\mathtt{ref}\ \tau')^p]\!]_E^{\mathcal{A}}$

It suffices to show the following:

- $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(e_1 := e_2, e_l' := e_2', \Sigma, m') \in [\![\mathtt{unit}^\perp]\!]_E^{\mathcal{A}}$. We know $(e_1, e_l', W'', \Sigma, \Sigma', m') \in [\![(\mathtt{ref}\ \tau')^p]\!]_E^{\mathcal{A}}$. We get $(e_2, e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]_E^{\mathcal{A}}$ by Lemma 8.29. The goal follows using the induction hypothesis.

2. $(e_1, e_1', W, \Sigma, \Sigma', m) \in \left\{(v, v', W, \Sigma_{c_1}, \Sigma_{c_2}, m) \,\middle|\, (v, v', W, m) \in [\![(\text{ref } \tau')^p]\!]^{\mathcal{A}}_{\mathcal{V}}\right\}$

Hence e_1 and e_1' are values v_1 and v_1' respectively such that $(v_1, v_1', W, m) \in [\![(\text{ref } \tau')^p]\!]^{\mathcal{A}}_{\mathcal{V}}$. Either $p \sqsubseteq \mathcal{A}$ or $p \not\sqsubseteq \mathcal{A}$. In the first case $(v_1, v_1', W, m) \in [\![\text{ref } \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$ and in the second case both $(v_1, W.\theta_1, m) \in \lceil \text{ref } \tau' \rceil_{\mathcal{V}}$ and $(v_1', W.\theta_2, m) \in \lceil \text{ref } \tau' \rceil_{\mathcal{V}}$. In both cases this means that there are locations l and l' such that

- $e_1 = l$,
- $e_1' = l'$ and
- $W.\theta_1(l) = \tau' = W.\theta_2(l')$.

This leaves us with two cases again:

(a) $(e_2, e_2', W, \Sigma, \Sigma', m) \in [\![\tau]\!]^{\mathcal{A}}_{E_\beta}$. There are again further cases:

i. $(e_2, e_2') \in \left\{(e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma_1'} e_1', S_1' \wedge \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega';\Sigma_2'} e_2', S_2' \to \\ (\omega \approx^{\mathcal{A}}_{(W',m')} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{(W'',m')} \omega' \wedge (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E} \end{array}\right\}$

In that case it suffices to show

$(l := e_2, l' := e_2') \in \left\{(e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma_1'} e_1', S_1' \wedge \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega';\Sigma_2'} e_2', S_2' \to \\ (\omega \approx^{\mathcal{A}}_{(W',m')} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \to \\ \exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{(W'',m')} \omega' \wedge (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\text{unit}^\perp]\!]^{\mathcal{A}}_{E} \end{array}\right\}$

Clearly $l := e_2$ and $l' := e_2'$ are not values. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $l := e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $l' := e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Since e_2 and e_2' are not values by assumption, the reductions must have happened with **Eassignr**. Hence by inversion

- $e_2, \Sigma_1, S_1 \succ e_r, S_1', \omega, \Sigma_1'$
- $e_2', \Sigma_2, S_2 \succ e_r', S_2', \omega', \Sigma_2'$
- $e_\beta = l := e_r$
- $e_\beta' = l' := e_r'$

Also let $\omega \approx^{\mathcal{A}}_{(W',m')} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \;\vee\; \Sigma_2' \sqsubseteq \mathcal{A}$. This directly gives us a W'' such that

- $W'' \sqsupseteq W'$,
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$,
- $\omega \approx^{\mathcal{A}}_{(W'',m')} \omega'$, and
- $(e_r, e_r', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E}$

It suffices to show

- $W'' \sqsupseteq W'$. We already know that.
- $(S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know that.
- $\omega \approx^{\mathcal{A}}_{(W'',m')} \omega'$. We already know that.
- $(l := e_r, l' := e_r', W'', \Sigma, \Sigma', m') \in [\![\text{unit}^\perp]\!]^{\mathcal{A}}_{E}$ We have $W'' \sqsupseteq W$ by transitivity (Lemma 7.2). Hence we also have $(l, l', W'', \Sigma, \Sigma', m') \in [\![(\text{ref } \tau')^p]\!]^{\mathcal{A}}_{E}$ by Lemma 8.29. We get the claim by induction.

ii. $(e_2, e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xrightarrow{\omega;\Sigma_1'} e_1',\, S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}) \end{array} \right\}$

In this case it suffices to show

$(\mathfrak{l} := e_2, \mathfrak{l}' := e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1,\, S_1 \xrightarrow{\omega;\Sigma_1'} e_1',\, S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ (e_1', e_2, W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\mathtt{unit}^{\perp}]\!]_{\mathsf{E}}^{\mathcal{A}}) \end{array} \right\}$

It is clear that $\mathfrak{l} := e_2$ is not a value. So let $\omega, e_\beta, \Sigma_1', S_1'$ such that

- $\mathfrak{l} := e_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$

Because e_2 is not a value the reduction must have happened with **Eassignr**. By inversion

- $e_2, \Sigma_1, S_1 \succ e_r, S_1', \omega, \Sigma_1'$
- $e_\beta = \mathfrak{l} := e_r$

From our assumption we get

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_r, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.
- $(S_1', S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(\mathfrak{l} := e_r, \mathfrak{l}' := e_2', \Sigma, \Sigma', \mathfrak{m}') \in [\![\mathtt{unit}^{\perp}]\!]_{\mathsf{E}}^{\mathcal{A}}$. We know $(e_r, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}$. We get $(\mathfrak{l}, \mathfrak{l}', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![(\mathtt{ref}\ \tau')^{\mathsf{p}}]\!]_{\mathsf{E}}^{\mathcal{A}}$ by Lemma 8.29. The goal follows using the induction hypothesis.

iii. $(e_2, e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xrightarrow{\omega;\Sigma_2'} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}) \end{array} \right\}$

In this case it suffices to show

$(\mathfrak{l} := e_2, \mathfrak{l}' := e_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2,\, S_2 \xrightarrow{\omega;\Sigma_2'} e_2',\, S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W''. W'' \sqsupseteq W' \wedge (S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'' \wedge \\ (e_1, e_2', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\mathtt{unit}^{\perp}]\!]_{\mathsf{E}}^{\mathcal{A}}) \end{array} \right\}$

It is clear that $\mathfrak{l}' := e_2'$ is not a value. So let $\omega, e_\beta', \Sigma_2', S_2'$ such that

- $\mathfrak{l}' := e_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega, \Sigma_2'$

Because e_2' is not a value, the reduction must have happened with **Eassignr**. By inversion

- $e_2', \Sigma_2, S_2 \succ e_r', S_2', \omega, \Sigma_2'$
- $e_\beta' = \mathfrak{l}' := e_r'$

From our assumption we get

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$

and there is an W'' such that

- $W'' \sqsupseteq W'$
- $(S_1, S_2', \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W''$
- $(e_2, e_r', W'', \Sigma, \Sigma', \mathfrak{m}') \in [\![\tau]\!]_{\mathsf{E}}^{\mathcal{A}}$

It suffices to show the following:

- $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$. We already know this
- $W'' \sqsupseteq W'$. We already know this.

- $(S_1, S_2', m') \overset{\mathcal{A}}{\triangleright} W''$. We already know this.
- $(l := e_2, l' := e_r', \Sigma, \Sigma', m') \in [\![\mathsf{unit}^{\perp}]\!]^{\mathcal{A}}_{E}$. We know $(e_2, e_r', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E}$. We get $(l, l', W'', \Sigma, \Sigma', m') \in [\![(\mathsf{ref}\ \tau')^p]\!]^{\mathcal{A}}_{E}$ by Lemma 8.29. The goal follows using the induction hypothesis.

(b) $(e_2, e_2', W, \Sigma, \Sigma', m) \in \{(v, v', W, \Sigma_c, m) \mid (v, v', W, m) \in [\![\tau]\!]^{\mathcal{A}}_{V}\}$

In this case e_2 and e_2' are values v_2 and v_2', respectively such that $(v_2, v_2', W, m) \in [\![\tau]\!]^{\mathcal{A}}_{V}$.
It suffices to show

$$(l := v_2, l' := v_2') \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1,\ S_1 \xRightarrow{\omega;\Sigma_1'} e_1',\ S_1' \wedge \\ \Sigma_2 \vdash e_2,\ S_2 \xRightarrow{\omega';\Sigma_2'} e_2',\ S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{(W',m')} \ \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W''. W'' \sqsupseteq W' \wedge\ (S_1', S_2', m') \overset{\mathcal{A}}{\triangleright} (W'') \wedge \\ \omega \approx^{\mathcal{A}}_{(W'',m')} \omega' \wedge\ (e_1', e_2', W'', \Sigma, \Sigma', m') \in [\![\tau]\!]^{\mathcal{A}}_{E} \end{array} \right\}$$

.

It is clear that both $l := v_2$ and $l' := v_2'$ are not values. So let $\omega, \omega', e_\beta, e_\beta', \Sigma_1', \Sigma_2', S_1', S_2'$ such that

- $l := v_2, \Sigma_1, S_1 \succ e_\beta, S_1', \omega, \Sigma_1'$
- $l' := v_2', \Sigma_2, S_2 \succ e_\beta', S_2', \omega', \Sigma_2'$

Since v_2 and v_2' are values, the reductions must have happened with **Eassign**. Hence

- $l \in \mathrm{dom}(S_1)$
- $l' \in \mathrm{dom}(S_2)$
- $e_\beta = ()$
- $e_\beta' = ()$
- $\omega = l_{\mathsf{type}(S_1,l)}(v_2)$
- $\omega' = l'_{\mathsf{type}(S_2,l')}(v_2')$
- $S_1' = S_1[l \rightarrowtail (v_2, \mathsf{type}(S_1, l))]$
- $S_2' = S_2[l' \rightarrowtail (v_2', \mathsf{type}(S_2, l'))]$
- $\Sigma_1' = \Sigma_1$
- $\Sigma_2' = \Sigma_2$

So the reductions are really

- $l := v_2, \Sigma_1, S_1 \succ (), S_1[l \rightarrowtail (v_2, \mathsf{type}(S_1, l))], l_{\mathsf{type}(S_1,l)}(v_2), \Sigma_1$
- $l' := v_2', \Sigma_2, S_2 \succ (), S_2[l' \rightarrowtail (v_2', \mathsf{type}(S_2, l'))], l'_{\mathsf{type}(S_2,l')}(v_2'), \Sigma_2$

Also assume $l_{\mathsf{type}(S_1,l)}(v_2) \approx^{\mathcal{A}}_{(W',m')} l'_{\mathsf{type}(S_2,l')}(v_2') \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$. We know $\tau(\Sigma) <: \tau'$, $\tau(\Sigma') <: \tau'$, and $p \sqsubseteq \tau'$. More specifically τ has the form A^q and τ' has the form B^r and therefore $A^q(\Sigma) <: B^r$, $A^q(\Sigma') <: B^r$, and $p \sqsubseteq B^r$. Hence

- $q(\Sigma) \sqsubseteq r$,
- $q(\Sigma') \sqsubseteq r$,
- $A <: B$, and
- $p \sqsubseteq r$.

By assumption

- $W.\theta_1(l) = \tau' = B^r$.

Because $W' \sqsupseteq W$ and $W'.\theta_1(l) = W'.\theta_2(l')$, also

- $W'.\theta_1(l) = B^r = W'.\theta_2(l')$.

From $(S_1, S_2, m') \overset{\mathcal{A}}{\triangleright} W'$ we get $(S_1, m') \triangleright W'.\theta_1$ and $(S_2, m') \triangleright W'.\theta_2$. Consequently

- $W'.\theta_1(l) = \mathsf{type}(S_1, l)$ and
- $W'.\theta_2(l') = \mathsf{type}(S_2, l')$.

We already know what $W'.\theta_1(l)$ and $W'.\theta_2(l')$ are, namely B^r. Hence

- $\mathtt{type}(\mathsf{S}_1, \mathsf{l}) = \mathsf{B}^{\mathsf{r}}$ and
- $\mathtt{type}(\mathsf{S}_2, \mathsf{l}') = \mathsf{B}^{\mathsf{r}}$.

It suffices to show

- $W' \sqsupseteq W'$. We get this by reflexivity (Lemma 7.2).
- $(\mathsf{S}_1[\mathsf{l} \rightarrowtail (\nu_2, \mathtt{type}(\mathsf{S}_1, \mathsf{l}))], \mathsf{S}_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{type}(\mathsf{S}_2, \mathsf{l}'))], \mathsf{m}') \overset{\mathcal{A}}{\triangleright} W'$.

  We have to show
  - $W'.\beta \subseteq W'.\theta_1 \times W'.\theta_2$.

    We get this from $(\mathsf{S}_1, \mathsf{S}_2, \mathsf{m}') \overset{\mathcal{A}}{\triangleright} W'$.
  - $\forall (\mathsf{l}_1, \mathsf{l}_2) \in W'.\beta.\ W'.\theta_1(\mathsf{l}_1) = W'.\theta_2(\mathsf{l}_2) \wedge$
    $(\mathsf{S}_1[\mathsf{l} \rightarrowtail (\nu_2, \mathtt{type}(\mathsf{S}_1, \mathsf{l}))](\mathsf{l}_1), \mathsf{S}_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{type}(\mathsf{S}_1', \mathsf{l}'))](\mathsf{l}_2), W', \mathsf{m}') \in [\![W'.\theta_1(\mathsf{l}_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$.

    Let $(\mathsf{l}_1, \mathsf{l}_2) \in W'.\beta$. We get $W'.\theta_1(\mathsf{l}_1) = W'.\theta_2(\mathsf{l}_2)$ from $(\mathsf{S}_1, \mathsf{S}_2, \mathsf{m}') \overset{\mathcal{A}}{\triangleright} W'$. All that remains to be shown is $(\mathsf{S}_1[\mathsf{l} \rightarrowtail (\nu_2, \mathtt{type}(\mathsf{S}_1, \mathsf{l}))](\mathsf{l}_1), \mathsf{S}_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{type}(\mathsf{S}_1', \mathsf{l}'))](\mathsf{l}_2), W', \mathsf{m}') \in [\![W'.\theta_1(\mathsf{l}_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$. There are four cases:

    i. $\mathsf{l}_1 \neq \mathsf{l}$ and $\mathsf{l}_2 \neq \mathsf{l}'$. Because $(\mathsf{S}_1, \mathsf{S}_2, \mathsf{m}') \overset{\mathcal{A}}{\triangleright} W'$ we know $W'.\beta \subseteq \mathtt{dom}(W.\theta_1) \times \mathtt{dom}(W.\theta_2)$. We also get
    - $(\mathsf{S}_1(\mathsf{l}_1), \mathsf{S}_2(\mathsf{l}_2), W', \mathsf{m}') \in [\![W'.\theta_1(\mathsf{l}_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$

    from $(\mathsf{S}_1, \mathsf{S}_2, \mathsf{m}') \overset{\mathcal{A}}{\triangleright} W'$. Because $\mathsf{l}_1 \neq \mathsf{l}$ and $\mathsf{l}_2 \neq \mathsf{l}'$ this is equivalent to the remaining subgoal.

    ii. $\mathsf{l}_1 = \mathsf{l}$ and $\mathsf{l}_2 \neq \mathsf{l}'$.
    In this case it suffices to show $(\nu_2, \mathsf{S}_2(\mathsf{l}_2), W', \mathsf{m}') \in [\![\mathsf{B}^{\mathsf{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. We do case analysis on the visibility of r.
    A. $\mathsf{r} \sqsubseteq \mathcal{A}$: We will show that this is impossible.
    By transitivity Lemma 4.1 we get $\mathsf{p} \sqsubseteq \mathcal{A}$. By assumption $(\mathsf{l}, \mathsf{l}', W, \mathsf{m}) \in [\![(\mathtt{ref}\ \tau')^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\mathsf{p} \sqsubseteq \mathcal{A}$ $(\mathsf{l}, \mathsf{l}', W, \mathsf{m}) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.25 $(\mathsf{l}, \mathsf{l}', W', \mathsf{m}) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$. In particular this means
    ☞ $(\mathsf{l}, \mathsf{l}') \in W'.\beta$.
    By assumption $W'.\beta$ is an injection and therefore in particular a function. Hence there can be no other $\mathsf{l}'' \neq \mathsf{l}'$ such that $(\mathsf{l}, \mathsf{l}'') \in W'.\beta$. But by assumption $(\mathsf{l}, \mathsf{l}_2) \in W'.\beta$ and $\mathsf{l}_2 \neq \mathsf{l}'$. ↯.

    B. $\mathsf{r} \not\sqsubseteq \mathcal{A}$ In this case it suffices to show
    ☞ $(\nu_2, W'.\theta_1, \mathsf{m}') \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$. We already know $(\nu_2, \nu_2', W, \mathsf{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.22 and Lemma 8.4 we have $(\nu_2, W'.\theta_1, \mathsf{m}') \in \lceil \tau \rceil_{\mathcal{V}}$. As $\tau = \mathsf{A}^{\mathsf{q}}$ this gives us $(\nu_2, W'.\theta_1, \mathsf{m}') \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$. The goal follows by Lemma 8.6.
    ☞ $(\mathsf{S}_2(\mathsf{l}_2), W', \mathsf{m}') \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$. Because $(\mathsf{S}_2, \mathsf{m}') \triangleright W'.\theta_2$ we have $(\mathsf{S}_2(\mathsf{l}_2), W'.\theta_2, \mathsf{m}') \in \lceil W'.\theta_2(\mathsf{l}_2) \rceil_{\mathcal{V}}$. By assumption $(\mathsf{l}, \mathsf{l}_2) \in W'.\beta$. Because $(\mathsf{S}_1, \mathsf{S}_2, \mathsf{m}') \overset{\mathcal{A}}{\triangleright} W'$ this means that $W'.\theta_1(\mathsf{l}) = W'.\theta_2(\mathsf{l}_2)$. We have already seen that $W'.\theta_1(\mathsf{l}) = \mathsf{B}^{\mathsf{r}}$. Hence $(\mathsf{S}_2(\mathsf{l}_2), W'.\theta_2, \mathsf{m}') \in \lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$. The goal follows by the definition of $\lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$.

    iii. $\mathsf{l}_1 \neq \mathsf{l}$ and $\mathsf{l}_2 = \mathsf{l}'$. By assumption $(\mathsf{l}_1, \mathsf{l}') \in W'.\beta$. Because $(\mathsf{S}_1, \mathsf{S}_2, \mathsf{m}') \overset{\mathcal{A}}{\triangleright} W'$ this means that $W'.\theta_1(\mathsf{l}_1) = W'.\theta_2(\mathsf{l}')$. We have already seen that $W'.\theta_2(\mathsf{l}') = \mathsf{B}^{\mathsf{r}}$. Hence it suffices to show $(\mathsf{S}_1(\mathsf{l}_1), \nu_2', W', \mathsf{m}') \in [\![\mathsf{B}^{\mathsf{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. We do case analysis on the visibility of r.
    A. $\mathsf{r} \sqsubseteq \mathcal{A}$: We will show that this is impossible. By transitivity Lemma 4.1 we get $\mathsf{p} \sqsubseteq \mathcal{A}$.
    By assumption $(\mathsf{l}, \mathsf{l}', W, \mathsf{m}) \in [\![(\mathtt{ref}\ \tau')^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\mathsf{p} \sqsubseteq \mathcal{A}$ $(\mathsf{l}, \mathsf{l}', W, \mathsf{m}) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.25 $(\mathsf{l}, \mathsf{l}', W', \mathsf{m}) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$. In particular this means
    ☞ $(\mathsf{l}, \mathsf{l}') \in W'.\beta$.
    By assumption $W'.\beta$ is an injection. Hence there can be no other $\mathsf{l}'' \neq \mathsf{l}$ such that $(\mathsf{l}'', \mathsf{l}') \in W'.\beta$. But by assumption $(\mathsf{l}_1, \mathsf{l}') \in W'.\beta$ and $\mathsf{l}_1 \neq \mathsf{l}$. ↯.

    B. $\mathsf{r} \not\sqsubseteq \mathcal{A}$ In this case it suffices to show
    ☞ $(\mathsf{S}_1(\mathsf{l}_1), W', \mathsf{m}') \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$.
    Because $(\mathsf{S}_1, \mathsf{m}') \triangleright W'.\theta_1$ we have $(\mathsf{S}_1(\mathsf{l}_1), W'.\theta_1, \mathsf{m}') \in \lceil W'.\theta_1(\mathsf{l}_1) \rceil_{\mathcal{V}}$. $W'.\theta_1(\mathsf{l}_1) = \mathsf{B}^{\mathsf{r}}$. Hence $(\mathsf{S}_1(\mathsf{l}_1), W'.\theta_1, \mathsf{m}') \in \lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$. The goal follows by the definition of $\lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$.
    ☞ $(\nu_2', W'.\theta_2, \mathsf{m}') \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$.

We already know $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.22 and Lemma 8.4 we have $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil\tau\rceil_{\mathcal{V}}$. As $\tau = A^{\mathfrak{q}}$ this gives us $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil A\rceil_{\mathcal{V}}$. The goal follows by Lemma 8.6.

iv. $(l_1, l_2) = (l, l')$.
The goal simplifies to $(\nu_2, \nu_2', W', \mathfrak{m}') \in [\![B^{\mathfrak{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$.
We do case analysis on whether $\mathfrak{r} \sqsubseteq \mathcal{A}$ or not:

A. $\mathfrak{r} \sqsubseteq \mathcal{A}$.
We do case analysis on $l_{\mathtt{type}(S_1,l)}(\nu_2) \approx^{\mathcal{A}}_{(W',\mathfrak{m}')} l'_{\mathtt{type}(S_2,l')}(\nu_2') \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.
This is the same as $l_{B^{\mathfrak{r}}}(\nu_2) \approx^{\mathcal{A}}_{(W',\mathfrak{m}')} l'_{B^{\mathfrak{r}}}(\nu_2') \vee \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.
$\alpha : l_{B^{\mathfrak{r}}}(\nu_2) \approx^{\mathcal{A}}_{(W',\mathfrak{m}')} l'_{B^{\mathfrak{r}}}(\nu_2')$.

of $\lceil B^{\mathfrak{r}}\rceil_{\mathcal{V}}$. The only rule with which $l_{B^{\mathfrak{r}}}(\nu_2) \approx^{\mathcal{A}}_{(W',\mathfrak{m}')} l'_{B^{\mathfrak{r}}}(\nu_2')$ can be derived is **extend-τ** as it is clear from the structure of the observations that neither **refl** is not applicable. **high** is also not applicable because $\mathfrak{r} \sqsubseteq \mathcal{A}$ by assumption.

By inversion
☞ $(\nu_2, \nu_2', W', \mathfrak{m}') \in [\![B^{\mathfrak{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$.
This was the goal.

$\beta : \Sigma_1 \sqsubseteq \mathcal{A} \vee \Sigma_2 \sqsubseteq \mathcal{A}$.

First we show that $\mathfrak{q} \sqsubseteq \mathcal{A}$: By assumption $\Sigma_1 \supseteq \Sigma$, $\Sigma_2 \supseteq \Sigma'$, $\mathfrak{q}(\Sigma) \sqsubseteq \mathfrak{r}$ and $\mathfrak{q}(\Sigma') \sqsubseteq \mathfrak{r}$. Hence by Lemma 4.3 and transitivity (Lemma 4.1)
☞ $\mathfrak{q}(\Sigma_1) \sqsubseteq \mathfrak{r}$ and
☞ $\mathfrak{q}(\Sigma_2) \sqsubseteq \mathfrak{r}$.
In both cases ($\Sigma_1 \sqsubseteq \mathcal{A}$ and $\Sigma_2 \sqsubseteq \mathcal{A}$) we get $\mathfrak{q} \sqsubseteq \mathcal{A}$ by Lemma 8.46.

Now we can continue with the main proof. We already know $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![A^{\mathfrak{q}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\mathfrak{q} \sqsubseteq \mathcal{A}$, this means that $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.31 $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![B]\!]^{\mathcal{A}}_{\mathcal{V}}$. From this we can directly follow $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![B^{\mathfrak{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$ because $\mathfrak{r} \sqsubseteq \mathcal{A}$ by assumption. The goal follows by Lemma 8.25 and Lemma 8.24.

B. $\mathfrak{r} \not\sqsubseteq \mathcal{A}$.
Because $\mathfrak{r} \not\sqsubseteq \mathcal{A}$, it suffices to show
☞ $(\nu_2, W'.\theta_1, \mathfrak{m}') \in \lceil B\rceil_{\mathcal{V}}$ and
☞ $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil B\rceil_{\mathcal{V}}$.
From $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![A^{\mathfrak{q}}]\!]^{\mathcal{A}}_{\mathcal{V}}$ we get
☞ $(\nu_2, W'.\theta_1, \mathfrak{m}') \in \lceil A\rceil_{\mathcal{V}}$ and
☞ $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil A\rceil_{\mathcal{V}}$
by Lemma 8.22, the definition of $\lceil A^{\mathfrak{q}}\rceil_{\mathcal{V}}$, Lemma 8.4. We get the remaining subgoals by Lemma 8.6.

– $(S_1[l \rightarrowtail (\nu_2, \mathtt{type}(S_1, l))], \mathfrak{m}') \triangleright W'.\theta_1$. For this we have to show
  * $\mathtt{dom}(W'.\theta_1) \subseteq \mathtt{dom}(S_1[l \rightarrowtail (\nu_2, \mathtt{type}(S_1, l))])$.
  $\mathtt{dom}(W'.\theta_1) \overset{(S_1,S_2,\mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'}{\subseteq} \mathtt{dom}(S_1) \subseteq \mathtt{dom}(S_1[l \rightarrowtail (\nu_2, \mathtt{type}(S_1, l))])$.
  * $\forall l'' \in \mathtt{dom}(W'.\theta_1).(S_1[l \rightarrowtail (\nu_2, \mathtt{type}(S_1, l))])(l''), W'.\theta_1, \mathfrak{m}') \in \lceil W'.\theta_1(l'')\rceil_{\mathcal{V}}$. Let $l'' \in \mathtt{dom}(W'.\theta_1)$. There are two cases:
    i. $l'' \neq l$. By assumption $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence also $(S_1, \mathfrak{m}') \triangleright W'.\theta_1$. Therefore in particular $(S_1(l''), W'.\theta_1, \mathfrak{m}') \in \lceil W'.\theta_1(l'')\rceil_{\mathcal{V}}$. Because $l'' \neq l$ this is equivalent to $(S_1[l \rightarrowtail (\nu_2, \mathtt{type}(S_1, l))](l''), W'.\theta_1, \mathfrak{m}') \in \lceil W'.\theta_1(l'')\rceil_{\mathcal{V}}$.
    ii. $l'' = l$. In this case the goal simplifies to $(\nu_2, W'.\theta_1, \mathfrak{m}') \in \lceil B^{\mathfrak{r}}\rceil_{\mathcal{V}}$. By assumption $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![A^{\mathfrak{q}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.22 therefore $(\nu_2, W.\theta_1, \mathfrak{m}) \in \lceil A^{\mathfrak{q}}\rceil_{\mathcal{V}}$. By the definitions of $\lceil A^{\mathfrak{q}}\rceil_{\mathcal{V}}$ we directly get $(\nu_2, W.\theta_1, \mathfrak{m}) \in \lceil A\rceil_{\mathcal{V}}$. From that we get $(\nu_2, W.\theta_1, \mathfrak{m}) \in \lceil B\rceil_{\mathcal{V}}$ by Lemma 8.6. We get $(\nu_2, W.\theta_1, \mathfrak{m}) \in \lceil B^{\mathfrak{r}}\rceil_{\mathcal{V}}$ by definition. The goal follows from Lemma 8.4 and Lemma 7.2.
  * $\forall l'' \in \mathtt{dom}(W'.\theta_1).W'.\theta_1(l'') = \mathtt{type}(S_1[l \rightarrowtail (\nu_2, \mathtt{type}(S_1, l))], l'')$.
  Let $l'' \in \mathtt{dom}(W'.\theta_1)$. There are two cases:
    i. $l'' \neq l$. By assumption $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence $W'.\theta_1(l'') = \mathtt{type}(S_1, l'')$. Because

$\mathsf{l}'' \neq \mathsf{l}$ this is equivalent to the goal.

ii. $\mathsf{l}'' = \mathsf{l}$. In this case the goal simplifies to $W'.\theta_1(\mathsf{l}) = \mathtt{type}(S_1, \mathsf{l})$. We get this from $(S_1, S_2, \mathfrak{m}'), \mathsf{l} \overset{\mathcal{A}}{\triangleright} W'$.

– $(S_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{type}(S_1', \mathsf{l}'))], \mathfrak{m}') \triangleright W'.\theta_2$. For this we have to show

* $\mathtt{dom}(W'.\theta_2) \subseteq \mathtt{dom}(S_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{type}(S_1', \mathsf{l}'))])$.
  $\mathtt{dom}(W'.\theta_2) \overset{(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'}{\subseteq} \mathtt{dom}(S_2) \subseteq \mathtt{dom}(S_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{type}(S_1', \mathsf{l}'))])$.
* $\forall \mathsf{l}'' \in \mathtt{dom}(W'.\theta_2).(S_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{type}(S_1', \mathsf{l}'))](\mathsf{l}''), W'.\theta_2, \mathfrak{m}') \in \lceil W'.\theta_2(\mathsf{l}'') \rceil_{\mathcal{V}}$. Let $\mathsf{l}'' \in \mathtt{dom}(W'.\theta_2)$. There are two cases:

  i. $\mathsf{l}'' \neq \mathsf{l}'$. By assumption $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence also $(S_2, \mathfrak{m}') \triangleright W'.\theta_2$. Therefore in particular $(S_2(\mathsf{l}''), W'.\theta_2, \mathfrak{m}') \in \lceil W'.\theta_2(\mathsf{l}'') \rceil_{\mathcal{V}}$. Because $\mathsf{l}'' \neq \mathsf{l}'$ this is equivalent to $(S_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{type}(S_1', \mathsf{l}'))](\mathsf{l}''), W'.\theta_2, \mathfrak{m}') \in \lceil W'.\theta_2(\mathsf{l}'') \rceil_{\mathcal{V}}$.

  ii. $\mathsf{l}'' = \mathsf{l}'$. In this case the goal simplifies to $(\nu_2', W'.\theta_2, \mathfrak{m}') \in \lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$. By assumption $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{A}^{\mathsf{q}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.22 therefore $(\nu_2', W.\theta_2, \mathfrak{m}) \in \lceil \mathsf{A}^{\mathsf{q}} \rceil_{\mathcal{V}}$. By the definitions of $\lceil \mathsf{A}^{\mathsf{q}} \rceil_{\mathcal{V}}$ we directly get $(\nu_2', W.\theta_2, \mathfrak{m}) \in \lceil \mathsf{A} \rceil_{\mathcal{V}}$. From that we get $(\nu_2', W.\theta_2, \mathfrak{m}) \in \lceil \mathsf{B} \rceil_{\mathcal{V}}$ by Lemma 8.6. We get $(\nu_2', W.\theta_2, \mathfrak{m}) \in \lceil \mathsf{B}^{\mathsf{r}} \rceil_{\mathcal{V}}$ by definition. The goal follows from Lemma 8.4 and Lemma 7.2.

* $\forall \mathsf{l}'' \in \mathtt{dom}(W'.\theta_2).W'.\theta_2(\mathsf{l}'') = \mathtt{type}(S_2[\mathsf{l}' \rightarrowtail (\nu_2', \mathtt{pol}(S_1', \mathsf{l}'))], \mathsf{l}'')$.
  Let $\mathsf{l}'' \in \mathtt{dom}(W'.\theta_2)$. There are two cases:

  i. $\mathsf{l}'' \neq \mathsf{l}'$. By assumption $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$. Hence $W'.\theta_2(\mathsf{l}'') = \mathtt{type}(S_2, \mathsf{l}'')$. Because $\mathsf{l}'' \neq \mathsf{l}'$ this is equivalent to the goal.

  ii. $\mathsf{l}'' = \mathsf{l}'$. In this case the goal simplifies to $W'.\theta_2(\mathsf{l}') = \mathtt{type}(S_2, \mathsf{l}')$. We get this from $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W'$.

- $\mathsf{l}_{\mathtt{type}(S_1, \mathsf{l})}(\nu_2) \approx^{\mathcal{A}}_{(W', \mathfrak{m}')} \mathsf{l}'_{\mathtt{type}(S_2, \mathsf{l}')}(\nu_2')$.

  This is the same as showing $\mathsf{l}_{\mathsf{B}^{\mathsf{r}}}(\nu_2) \approx^{\mathcal{A}}_{(W', \mathfrak{m}')} \mathsf{l}'_{\mathsf{B}^{\mathsf{r}}}(\nu_2')$. We do case analysis on the visibility of r.

  i. $\mathsf{r} \not\sqsubseteq \mathcal{A}$: In this case we get the claim by **high**.

  ii. $\mathsf{r} \sqsubseteq \mathcal{A}$: By **extend-τ** it suffices to show

  – $(\mathsf{l}, \mathsf{l}') \in W'.\beta$. By transitivity Lemma 4.1 we get $\mathsf{p} \sqsubseteq \mathcal{A}$.
  By assumption $(\mathsf{l}, \mathsf{l}', W, \mathfrak{m}) \in [\![(\mathtt{ref}\ \tau')^{\mathsf{p}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\mathsf{p} \sqsubseteq \mathcal{A}$ $(\mathsf{l}, \mathsf{l}', W, \mathfrak{m}) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.25 $(\mathsf{l}, \mathsf{l}', W', \mathfrak{m}) \in [\![\mathtt{ref}\ \tau']\!]^{\mathcal{A}}_{\mathcal{V}}$. In particular this means
  ☞ $(\mathsf{l}, \mathsf{l}') \in W'.\beta$.

  – $(\nu_2, \nu_2', W', \mathfrak{m}') \in [\![\mathsf{B}^{\mathsf{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. We do another case analysis:

  A. $\mathsf{l}_{\mathtt{type}(S_1, \mathsf{l})}(\nu_2) \approx^{\mathcal{A}}_{(W', \mathfrak{m}')} \mathsf{l}'_{\mathtt{type}(S_2, \mathsf{l}')}(\nu_2')$. This is the same as $\mathsf{l}_{\mathsf{B}^{\mathsf{r}}}(\nu_2) \approx^{\mathcal{A}}_{(W', \mathfrak{m}')} \mathsf{l}'_{\mathsf{B}^{\mathsf{r}}}(\nu_2')$. This must have been derived by **extend-τ** because **refl** is syntactically not applicable and $\mathsf{r} \sqsubseteq \mathcal{A}$ rules out **high**. Hence by inversion
  ☞ $(\nu_2, \nu_2', W', \mathfrak{m}') \in [\![\mathsf{B}^{\mathsf{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$
  which is what we needed to show.

  B. $\Sigma_1 \sqsubseteq \mathcal{A}$ or $\Sigma_2 \sqsubseteq \mathcal{A}$: We first show $\mathsf{q} \sqsubseteq \mathcal{A}$.
  By assumption $\Sigma_1 \supseteq \Sigma$, $\Sigma_2 \supseteq \Sigma'$, $\mathsf{q}(\Sigma) \sqsubseteq \mathsf{r}$ and $\mathsf{q}(\Sigma') \sqsubseteq \mathsf{r}$. Hence by Lemma 4.3 and transitivity (Lemma 4.1)
  ☞ $\mathsf{q}(\Sigma_1) \sqsubseteq \mathsf{r}$ and
  ☞ $\mathsf{q}(\Sigma_2) \sqsubseteq \mathsf{r}$.
  In both cases ($\Sigma_1 \sqsubseteq \mathcal{A}$ and $\Sigma_2 \sqsubseteq \mathcal{A}$) we get $\mathsf{q} \sqsubseteq \mathcal{A}$ by Lemma 8.46.

  Remember that by assumption $\mathtt{firstorder}(\mathsf{B}^{\mathsf{r}})$. Hence by Lemma 8.44 it suffices to show $(\nu_2, \nu_2', W', \mathfrak{m}) \in [\![\mathsf{B}^{\mathsf{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. By Lemma 8.25 it suffices to show $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{B}^{\mathsf{r}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. We already know $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{A}^{\mathsf{q}}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\mathsf{q} \sqsubseteq \mathcal{A}$ we have $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{A}]\!]^{\mathcal{A}}_{\mathcal{V}}$. We get $(\nu_2, \nu_2', W, \mathfrak{m}) \in [\![\mathsf{B}]\!]^{\mathcal{A}}_{\mathcal{V}}$ by Lemma 8.31. The goal follows because $\mathsf{p} \sqsubseteq \mathcal{A}$.

- $((), (), W', \Sigma, \Sigma', \mathfrak{m}') \in [\![\mathtt{unit}^{\perp}]\!]^{\mathcal{A}}_{\mathsf{E}}$.
It suffices to show $((), (), W', \mathfrak{m}') \in [\![\mathtt{unit}^{\perp}]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $\perp \sqsubseteq \mathcal{A}$ it suffices to show $((), (), W', \mathfrak{m}') \in [\![\mathtt{unit}]\!]^{\mathcal{A}}_{\mathcal{V}}$. This is clearly the case.

□

10 Knowledge based security

Note that while we use the more general logical relation to prove security here, we still need to restrict ourselves to firstorder-observations and therefore firstorder-state for the reasons described in the paper.

We formally define firstorder observations:

Definition 10.1. Firstorder observations are formally defined as follows

$$\frac{}{\mathtt{firstorder}(\mathsf{open}(\sigma))}\ \textbf{Fopen} \qquad \frac{}{\mathtt{firstorder}(\mathsf{close}(\sigma))}\ \textbf{Fclose} \qquad \frac{}{\mathtt{firstorder}(\mathsf{unopen}(\sigma))}\ \textbf{Funopen}$$

$$\frac{}{\mathtt{firstorder}(\mathsf{unclose}(\sigma))}\ \textbf{Funclose} \qquad \frac{\mathtt{firstorder}(\tau)}{\mathtt{firstorder}(\mathsf{l}_\tau(v))}\ \textbf{Fwrite}$$

Definition 10.2. For a state S we define θ_S pointwise in the following way:

$$\theta_S(l) := \mathrm{type}(S, l)$$

Definition 10.3 (Low States and Low Equivalence)**.** For a state S and attacker $\mathcal{A}$ we define the low-state $S_\mathcal{A}$ of S:

$$S_\mathcal{A} = \{l \rightarrowtail (v, \tau) \in S \mid \tau \sqsubseteq \mathcal{A}\}$$

We also define $S \approx_\mathcal{A} S'$ as

$$\mathrm{dom}(S_\mathcal{A}) = \mathrm{dom}(S'_\mathcal{A}) \wedge \forall m.\ (S_\mathcal{A}, S'_\mathcal{A}, m) \overset{\mathcal{A}}{\triangleright} (\theta_{S_\mathcal{A}}, \theta_{S'_\mathcal{A}}, \mathrm{id}_{\mathrm{dom}(S_\mathcal{A})})$$

Note that $\mathrm{dom}(S_\mathcal{A}) = \mathrm{dom}(S'_\mathcal{A})$ also means that $\theta_{S_\mathcal{A}} = \theta_{S'_\mathcal{A}}$.

Note that in the paper we define low equivalence as

$$\mathrm{dom}(S_\mathcal{A}) = \mathrm{dom}(S'_\mathcal{A}) \wedge \forall m.\ (S, S', m) \overset{\mathcal{A}}{\triangleright} (\theta_{S_\mathcal{A}}, \theta_{S'_\mathcal{A}}, \mathrm{id}_{\mathrm{dom}(S_\mathcal{A})})$$

So we are using the original worlds instead of the low worlds. These two formalisations are equivalent because the world only puts a restriction on the low locations. We use the first definition here, because it corresponds closer to the definition in flow-locks. We use the other definition in the paper because it allows us to avoid having to explicitly define low states.

Lemma 10.1 (Low idempotence)**.** $(S_\mathcal{A})_\mathcal{A} = S_\mathcal{A}$.

Proof.

- $\subseteq$: Let $(l \rightarrowtail (v, \tau)) \in (S_\mathcal{A})_\mathcal{A}$. Then by definition $(l \rightarrowtail (v, \tau)) \in S_\mathcal{A}$.
- $\supseteq$: Let $(l \rightarrowtail (v, \tau)) \in S_\mathcal{A}$. Then clearly
  - $(l \rightarrowtail (v, \tau)) \in S_\mathcal{A}$ and
  - $\tau \sqsubseteq \mathcal{A}$.

  Hence $(l \rightarrowtail (v, \tau)) \in (S_\mathcal{A})_\mathcal{A}$.

□

Lemma 10.2 (Low preserves order)**.**

1. If $S \supseteq S'$, then $S_\mathcal{A} \supseteq S'_\mathcal{A}$.
2. If $S \supseteq S'_\mathcal{A}$, then $S_\mathcal{A} \supseteq S'_\mathcal{A}$.

Proof.

1. Let $S \supseteq S'$. Let $(l \rightarrowtail (v, \tau)) \in S'_\mathcal{A}$. Then $(l \rightarrowtail (v, \tau)) \in S'$ and $\tau \sqsubseteq \mathcal{A}$. Because $S \supseteq S'$ we have $(l \rightarrowtail (v, \tau)) \in S$ and hence $(l \rightarrowtail (v, \tau)) \in S_\mathcal{A}$.
2. By 1. $S_\mathcal{A} \supseteq (S'_\mathcal{A})_\mathcal{A}$. By Lemma 10.1 $(S'_\mathcal{A})_\mathcal{A} = S'_\mathcal{A}$. The goal follows by transitivity.

□

Lemma 10.3. $(S_1 \cup S_2)_\mathcal{A} = (S_1)_\mathcal{A} \cup (S_2)_\mathcal{A}$.

Proof. $\sqsubseteq$: Let $(l \rightarrowtail (v, \tau)) \in (S_1 \cup S_2)_\mathcal{A}$. Then

- $p \sqsubseteq \mathcal{A}$ and

– $(l \rightarrowtail (v, \tau)) \in S_1 \cup S_2$.

If $(l \rightarrowtail (v, \tau)) \in S_1$, then $(l \rightarrowtail (v, \tau)) \in (S_1)_{\mathcal{A}}$ and hence $(l \rightarrowtail (v, \tau)) \in (S_1)_{\mathcal{A}} \cup (S_2)_{\mathcal{A}}$. Alternatively if $(l \rightarrowtail (v, \tau)) \in S_2$, then $(l \rightarrowtail (v, \tau)) \in (S_2)_{\mathcal{A}}$ and hence $(l \rightarrowtail (v, \tau)) \in (S_1)_{\mathcal{A}} \cup (S_2)_{\mathcal{A}}$.

$\supseteq$: Let $(l \rightarrowtail (v, \tau)) \in (S_1)_{\mathcal{A}} \cup (S_2)_{\mathcal{A}}$. There are two cases:

1. $(l \rightarrowtail (v, \tau)) \in (S_1)_{\mathcal{A}}$: Then
   – $(l \rightarrowtail (v, \tau)) \in S_1$
   – $\tau \sqsubseteq \mathcal{A}$.

   Then also $(l \rightarrowtail (v, \tau)) \in S_1 \cup S_2$ and hence $(l \rightarrowtail (v, \tau)) \in (S_1 \cup S_2)_{\mathcal{A}}$.
2. $(l \rightarrowtail (v, \tau)) \in (S_1)_{\mathcal{A}}$: Then
   – $(l \rightarrowtail (v, \tau)) \in S_2$
   – $\tau \sqsubseteq \mathcal{A}$.

   Then also $(l \rightarrowtail (v, \tau)) \in S_1 \cup S_2$ and hence $(l \rightarrowtail (v, \tau)) \in (S_1 \cup S_2)_{\mathcal{A}}$.

□

Lemma 10.4. If $\Sigma \vdash e, S \xrightarrow{\omega;\Sigma'} e', S'$ and $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$, then $S_{\mathcal{A}} = S'_{\mathcal{A}}$.

Proof. By induction on the derivation of the reduction. In most cases either $S = S'$ anyway, which makes the statement trivial, or we get the claim by induction. The only interesting cases are

- **ENewBeta**

$$\frac{l \notin \mathrm{dom}(S)}{\Sigma \vdash \mathsf{new}(v, \tau), S \xrightarrow{l_\tau(v);\Sigma} l, S \cup \{l \rightarrowtail (v, \tau)\}}\ \textbf{ENewBeta}$$

  Since $\Sigma = \Sigma'$ it is clear that $\Sigma_{\mathcal{A}} = \Sigma'_{\mathcal{A}}$. We have to show $S_{\mathcal{A}} = (S \cup \{l \rightarrowtail (v, \tau)\})_{\mathcal{A}}$. By Lemma 10.3 it suffices to show $S_{\mathcal{A}} = S_{\mathcal{A}} \cup \{l \rightarrowtail (v, \tau)\}_{\mathcal{A}}$. By assumption $\neg(\mathtt{pol}(l_\tau(v)) \sqsubseteq \mathcal{A})$ and $\mathtt{pol}(l_\tau(v)) = \mathtt{pol}(\tau)$. Hence $\neg(\tau \sqsubseteq \mathcal{A})$ and therefore $\{l \rightarrowtail (v, \tau)\}_{\mathcal{A}} = \emptyset$. So the goal simplifies to $S_{\mathcal{A}} = S_{\mathcal{A}}$ which we get by reflexivity.

- **Eassign**

$$\frac{l \in \mathrm{dom}(S) \qquad \mathtt{type}(S, l) = \tau}{\Sigma \vdash l := v, S \xrightarrow{l_\tau(v);\Sigma} (), S[l \rightarrowtail (v, \tau)]}\ \textbf{Eassign}$$

  Since $\Sigma = \Sigma'$ it is clear that $\Sigma_{\mathcal{A}} = \Sigma'_{\mathcal{A}}$. We have to show $S_{\mathcal{A}} = (S[l \rightarrowtail (v, \tau)])_{\mathcal{A}}$. By assumption $\neg(\mathtt{pol}(l_\tau(v)) \sqsubseteq \mathcal{A})$. Hence $\neg(\tau \sqsubseteq \mathcal{A})$.

  Let $(l' \rightarrowtail (v', \tau')) \in S_{\mathcal{A}}$ We show $l' \neq l$: Assume $l' = l$. By assumption $\mathtt{type}(S, l) = \tau$. Hence we would have $(l \rightarrowtail (v', \tau)) \in S_{\mathcal{A}}$. This would give us $\tau \sqsubseteq \mathcal{A}$. But $\tau \not\sqsubseteq \mathcal{A}$. ↯.

  Since $l' \neq l$ we have $(l' \rightarrowtail (v', \tau')) \in S[l \rightarrowtail (v, \tau)]_{\mathcal{A}}$.

  Now let $(l' \rightarrowtail (v', \tau')) \in S[l \rightarrowtail (v, \tau)]_{\mathcal{A}}$. Because $\tau \not\sqsubseteq \mathcal{A}$ we have $l' \neq l$. Hence $(l' \rightarrowtail (v', \tau')) \in S_{\mathcal{A}}$.

□

Definition 10.4 (Visible and invisible observations)**.** An observation ω is considered to be invisible to attacker $\mathcal{A}$ ($\mathrm{inv}_{\mathcal{A}}(\omega)$), if $\omega = \epsilon$ or $\mathrm{pol}(\omega) \not\sqsubseteq \mathcal{A}$. If an observation is not invisible it is visible.

Remark. *Note that if* $\mathrm{inv}_{\mathcal{A}}(\omega)$*, in particular* $\neg(pol(\omega) \sqsubseteq \mathcal{A})$*, because we either have this anyway or* $\omega = \epsilon$ *and the policy of* ϵ *is undefined.*

Definition 10.5 (Traces)**.** A finite trace $\vec{\omega}$ is a series of observations $\omega_1, \omega_2, \ldots \omega_n$. We also define the length of a trace $\mathtt{len}(\omega_1, \ldots, \omega_n) = n$. A trace $\omega_1, \ldots, \omega_n$ is called an $\mathcal{A}$-low trace if all observations ω_i with $1 \leqslant i \leqslant n$ are visible to $\mathcal{A}$. The empty trace with length 0 is called ε. To avoid confusion with the trace containing just the single observation ϵ we will write (ϵ) to denote the trace containing just the single observation ϵ.

Note that in the paper we use captial Ω for traces because the arrow did not render properly.

Definition 10.6 (Trace reduction)**.**

$$\frac{\Sigma \vdash e, S \xRightarrow{\omega;\Sigma'} e', S'}{\Sigma \vdash e, S \xRightarrow{\omega;\Sigma'}{}^{*} e', S'}\ \textbf{single} \qquad \frac{\Sigma \vdash e, S \xRightarrow{\omega;\Sigma'} e', S' \qquad \Sigma \vdash e', S' \xRightarrow{\vec{\omega}';\Sigma''}{}^{*} e'', S''}{\Sigma \vdash e, S \xRightarrow{\omega,\vec{\omega}';\Sigma''}{}^{*} e'', S''}\ \textbf{continue}$$

Note that below we sometimes still use the deprecated notation $e, S, \Sigma \overset{\vec{\omega}}{\Rightarrow} e', S', \Sigma'$ instead of $\Sigma \vdash e, S \xRightarrow{\vec{\omega};\Sigma'}{}^{*} e', S'$.

Definition 10.7 (Trace equivalence)**.** We lift the relation $\approx^{\mathcal{A}}_{(W,m)}$ to traces in the following way: For traces $\vec{\omega} := \omega_1 \dots \omega_n$ and $\vec{\omega}' := \omega'_1 \dots \omega'_n$ we have

$$\vec{\omega} \approx^{\mathcal{A}}_{(W,m)} \vec{\omega}'$$

if for all $0 \leqslant i \leqslant n$ we have $\omega_i \approx^{\mathcal{A}}_{(W,m)} \omega'_i$.

Lemma 10.5. If $(e_1, e_2, W, \Sigma_1, \Sigma_2, m) \in [\![\tau]\!]^{\mathcal{A}}_{E}$, and $\Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma'_1}{}^{*} e'_1, S'_1$, and $\Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega';\Sigma'_2}{}^{*} e'_2, S'_2$, $(S_1, S_2, m-1) \overset{\mathcal{A}}{\triangleright} W$, $m > 0$, and both $\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}$ and $\mathrm{pol}(\omega') \sqsubseteq \mathcal{A}$, and if then also $\omega \approx^{\mathcal{A}}_{(W,m-1)} \omega'$ or $\Sigma'_1 \sqsubseteq \mathcal{A}$ or $\Sigma'_2 \sqsubseteq \mathcal{A}$, then $\exists W' \sqsupseteq W.\ (e'_1, e'_2, W', \Sigma_1, \Sigma_2, m-1) \in [\![\tau]\!]^{\mathcal{A}}_{E}$, $(S'_1, S'_2, m-1) \overset{\mathcal{A}}{\triangleright} W'$ and $\omega \approx^{\mathcal{A}}_{(W',m-1)} \omega'$.

Proof. Because e_1 and e_2 reduce they are no values. Hence $(e_1, e_2, W, \Sigma_1, \Sigma_2, m) \in [\![\tau]\!]^{\mathcal{A}}_{E_\beta}$. Clearly $\Sigma_1 \subseteq \Sigma_1$, $\Sigma_2 \subseteq \Sigma_2$, $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$ (we get this from $(e_1, e_2, W, \Sigma_1, \Sigma_2, m) \in [\![\tau]\!]^{\mathcal{A}}_{E_\beta}$), $W \sqsupseteq W$ (Lemma 7.2), $m - 1 < m$ and $(S_1, S_2, m-1) \overset{\mathcal{A}}{\triangleright} W$. There are three cases:

1. $(e_1, e_2) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge\ e_2 \notin \mathcal{V} \wedge \\ \forall e'_1, S'_1, \Sigma'_1, \omega, e'_2, \Sigma'_2, S'_2, \omega'. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma'_1} e'_1, S'_1 \wedge \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega';\Sigma'_2} e'_2, S'_2 \to \\ (\omega \approx^{\mathcal{A}}_{(W,m-1)} \omega' \vee \Sigma'_1 \sqsubseteq \mathcal{A} \vee \Sigma'_2 \sqsubseteq \mathcal{A}) \to \\ \exists W'.W' \sqsupseteq W \wedge\ (S'_1, S'_2, m-1) \overset{\mathcal{A}}{\triangleright} (W') \wedge \\ \omega \approx^{\mathcal{A}}_{(W',m-1)} \omega' \wedge\ (e'_1, e'_2, W', \Sigma_1, \Sigma_2, m-1) \in [\![\tau]\!]^{\mathcal{A}}_{E} \end{array} \right\}$.

   By inversion of $e_1, S_1, \Sigma_1 \overset{\omega}{\Rightarrow} e'_1, S'_1, \Sigma'_1$, and $e_2, S_2, \Sigma_2 \overset{\omega'}{\Rightarrow} e'_2, S'_2, \Sigma'_2$ we get

   - $e_1, \Sigma_1, S_1 \succ e'_1, S'_1, \omega, \Sigma'_1$
   - $e_2, \Sigma_2, S_2 \succ e'_2, S'_2, \omega', \Sigma'_2$.

   Because we also have $\omega \approx^{\mathcal{A}}_{(W,m-1)} \omega'$ or $\Sigma'_1 \sqsubseteq \mathcal{A}$ or $\Sigma'_2 \sqsubseteq \mathcal{A}$ by assumption, this gives us an $W' \sqsupseteq W$ with the desired properties.

2. $(e_1, e_2) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \ \wedge \forall e'_1, S'_1, \Sigma'_1, \omega. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma'_1} e'_1, S'_1 \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W'.W' \sqsupseteq W \wedge (S'_1, S_2, m-1) \overset{\mathcal{A}}{\triangleright} (W') \wedge \\ (e'_1, e_2, W', \Sigma_1, \Sigma_2, m-1) \in [\![\tau]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$. By inversion of $e_1, S_1, \Sigma_1 \overset{\omega}{\Rightarrow} e'_1, S'_1, \Sigma'_1$ we get

   - $e_1, \Sigma_1, S_1 \succ e'_1, S'_1, \omega, \Sigma'_1$

   This gives us $\neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A})$ which contradicts our assumption. ↯

3. $(e_1, e_2) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \ \wedge \forall e'_2, S'_2, \Sigma'_2, \omega. \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega;\Sigma'_2} e'_2, S'_2 \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W'.W' \sqsupseteq W \wedge (S_1, S'_2, m-1) \overset{\mathcal{A}}{\triangleright} W' \wedge \\ (e_1, e'_2, W', \Sigma_1, \Sigma_2, m-1) \in [\![\tau]\!]^{\mathcal{A}}_{E}) \end{array} \right\}$. By inversion of $e_2, S_2, \Sigma_2 \overset{\omega'}{\Rightarrow} e'_2, S'_2, \Sigma'_2$ we get

- $e_2, \Sigma_2, S_2 \succ e_2', S_2', \omega', \Sigma_2'$

This gives us $\neg(\mathtt{pol}(\omega') \sqsubseteq \mathcal{A})$ which contradicts our assumption. $\lightning$

□

Lemma 10.6. If $(S, \mathfrak{m}) \triangleright \theta$ and $\mathfrak{m}' < \mathfrak{m}$, then $(S, \mathfrak{m}') \triangleright \theta$.

Proof. We have to show

- $\mathtt{dom}(\theta) \subseteq \mathtt{dom}(S)$. We get this from $(S, \mathfrak{m}) \triangleright \theta$.
- $\forall l \in \mathtt{dom}(\theta).(S(l), \theta, \mathfrak{m}') \in \lceil \theta(l) \rceil_{\mathcal{V}}$.
  Let $l \in \mathtt{dom}(\theta)$. We get $(S(l), \theta, \mathfrak{m}) \in \lceil \theta(l) \rceil_{\mathcal{V}}$ from $(S, \mathfrak{m}) \triangleright \theta$. The goal follows by Lemma 8.4.
- $\forall l \in \mathtt{dom}(\theta).\theta(l) = \mathtt{type}(S, l)$. We get this from $(S, \mathfrak{m}) \triangleright \theta$.

□

Lemma 10.7. If $(S_1, S_2, \mathfrak{m}) \overset{\mathcal{A}}{\triangleright} W$ and $\mathfrak{m}' < \mathfrak{m}$, then $(S_1, S_2, \mathfrak{m}') \overset{\mathcal{A}}{\triangleright} W$.

Proof. We need to show

- $W.\beta \subseteq \mathtt{dom}(W.\theta_1) \times \mathtt{dom}(W.\theta_2)$. We already know this from $(S_1, S_2, \mathfrak{m}) \overset{\mathcal{A}}{\triangleright} W$.
- $\forall (l, l') \in W.\beta.W.\theta_1(l) = W.\theta_2(l') \wedge (S_1(l), S_2(l'), W, \mathfrak{m}') \in [\![W.\theta_1(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$. Let $(l, l') \in W.\beta$. We get $W.\theta_1(l) = W.\theta_2(l')$ from $(S_1, S_2, \mathfrak{m}) \overset{\mathcal{A}}{\triangleright} W$. This also gives us $(S_1(l), S_2(l'), W, \mathfrak{m}') \in [\![W.\theta_1(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$. We get the claim by Lemma 8.24.
- $(S_1, \mathfrak{m}') \triangleright W.\theta_1$. We get the claim by Lemma 10.6.
- $(S_2, \mathfrak{m}') \triangleright W.\theta_2$. We get the claim by Lemma 10.6.

□

Lemma 10.8.
If $\omega \approx^{\mathcal{A}}_{(W,\mathfrak{m})} \omega'$, and $W' \sqsupseteq W$ and $\mathfrak{m}' \leqslant \mathfrak{m}$, then $\omega \approx^{\mathcal{A}}_{(W',\mathfrak{m}')} \omega'$.

Proof. By case analysis on the derivation of $\omega \approx^{\mathcal{A}}_{(W,\mathfrak{m})} \omega'$. If the rule used was **refl** or **high** we get the claim with the same rule. If the rule used was **extend-τ** we get they claim by using Lemma 8.25 and Lemma 8.24 on the premiss and using the same rule with the result. □

Lemma 10.9. If $(e_1, e_2, W, \Sigma_1, \Sigma_2, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$, and $\Sigma_1 \vdash e_1, S_1 \xrightarrow{\omega_1,\ldots\omega_n,\omega;\Sigma_1'}{}^{*} e_1', S_1'$, and $\Sigma_2 \vdash e_2, S_2 \xrightarrow{\omega_1',\ldots\omega_l',\omega';\Sigma_2'}{}^{*}$ e_2', S_2', $(S_1, S_2, \mathfrak{m}-1) \overset{\mathcal{A}}{\triangleright} W$, $\mathfrak{m} > \mathfrak{n}+\mathfrak{l}$, $\forall i.\mathit{inv}_{\mathcal{A}}(\omega_i')$, $\forall j.\mathit{inv}_{\mathcal{A}}(\omega_j')$ and both $\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}$ and $\mathrm{pol}(\omega') \sqsubseteq \mathcal{A}$, and if then also , $\omega \approx^{\mathcal{A}}_{(W,\mathfrak{m}-1)} \omega'$ or $\Sigma_1' \sqsubseteq \mathcal{A}$ or $\Sigma_2' \sqsubseteq \mathcal{A}$, then $\exists W' \sqsupseteq W.(e_1', e_2', W', \Sigma, \Sigma_2, \mathfrak{m}-\mathfrak{n}-\mathfrak{l}-1) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$, $(S_1', S_2', \mathfrak{m}-\mathfrak{n}-\mathfrak{l}-1) \overset{\mathcal{A}}{\triangleright} W'$ and $\omega \approx^{\mathcal{A}}_{(W',\mathfrak{m}-\mathfrak{n}-\mathfrak{l}-1)} \omega'$.

Proof. By induction on $\mathfrak{n}+\mathfrak{l}$. Because e_1 and e_2 reduce they are no values. Hence $(e_1, e_2, W, \Sigma_1, \Sigma_2, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$. Clearly $\Sigma_1 \subseteq \Sigma_1$, $\Sigma_2 \subseteq \Sigma_2$, $\Sigma_1 \approx_{\mathcal{A}} \Sigma_2$ (we get this from $(e_1, e_2, W, \Sigma_1, \Sigma_2, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}_\beta}$), $W \sqsupseteq W$ (Lemma 7.2), $\mathfrak{m}-1 < \mathfrak{m}$ and $(S_1, S_2, \mathfrak{m}-1) \overset{\mathcal{A}}{\triangleright} W$. There are three cases:

1. $(e_1, e_2) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge\; e_2 \notin \mathcal{V} \wedge \\ \forall e_1', S_1', \Sigma_1', \omega, e_2', \Sigma_2', S_2', \omega'. \\ \Sigma_1 \vdash e_1, S_1 \xrightarrow{\omega;\Sigma_1'} e_1', S_1' \wedge \\ \Sigma_2 \vdash e_2, S_2 \xrightarrow{\omega';\Sigma_2'} e_2', S_2' \rightarrow \\ (\omega \approx^{\mathcal{A}}_{(W,\mathfrak{m}-1)} \omega' \vee \Sigma_1' \sqsubseteq \mathcal{A} \vee \Sigma_2' \sqsubseteq \mathcal{A}) \rightarrow \\ \exists W'.W' \sqsupseteq W \wedge\; (S_1', S_2', \mathfrak{m}-1) \overset{\mathcal{A}}{\triangleright} (W') \wedge \\ \omega \approx^{\mathcal{A}}_{(W',\mathfrak{m}-1)} \omega' \wedge\; (e_1', e_2', W', \Sigma_1, \Sigma_2, \mathfrak{m}-1) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}} \end{array} \right\}.$

   We do case analysis

   (a) $\mathfrak{n} = 0 = \mathfrak{l}$: Then $\mathfrak{m}-\mathfrak{n}-\mathfrak{l}-1 = \mathfrak{m}-1$. We get the goal by Lemma 10.5.

(b) $\mathfrak{n} > 0$ and $\mathfrak{l} = 0$: By inversion of $\mathsf{e}_1, \mathsf{S}_1, \Sigma_1 \overset{\omega_1,\ldots\omega_\mathfrak{n},\omega}{\Rightarrow} \mathsf{e}_1', \mathsf{S}_1', \Sigma_1'$, and $\mathsf{e}_2, \mathsf{S}_2, \Sigma_2 \overset{\omega'}{\Rightarrow} \mathsf{e}_2', \mathsf{S}_2', \Sigma_2'$ we get that there are $\mathsf{e}_1'', \mathsf{S}_1'', \Sigma_1''$ such that

- $\mathsf{e}_1, \Sigma_1, \mathsf{S}_1 \succ \mathsf{e}_1'', \mathsf{S}_1'', \omega_1, \Sigma_1''$
- $\mathsf{e}_2, \Sigma_2, \mathsf{S}_2 \succ \mathsf{e}_2', \mathsf{S}_2', \omega', \Sigma_2'$.

By assumption $\mathit{inv}_\mathcal{A}(\omega_1)$. Hence we have $\neg(\mathtt{pol}(\omega_1) \sqsubseteq \mathcal{A})$. Consequently $\omega_1 \approx^\mathcal{A}_{(W,\mathfrak{m}-1)} \omega'$ by **high**. Hence there exists a $W' \sqsupseteq W$ such that among other things

- $\omega_1 \approx^\mathcal{A}_{(W',\mathfrak{m}-1)} \omega'$.

We show that this is a contradiction by doing cases analysis on the derivation of $\omega_1 \approx^\mathcal{A}_{W'.\beta} \omega'$.

i. **refl**: In this case $\omega_1 = \omega'$. In particular therefore $\mathtt{pol}(\omega_1) = \mathtt{pol}(\omega')$. But we already know that $\mathtt{pol}(\omega') \sqsubseteq \mathcal{A}$ and $\neg(\mathtt{pol}(\omega_1) \subseteq \mathcal{A})$ ↯.

ii. **extend-τ**: In this case $\mathtt{pol}(\omega_1) = \mathtt{pol}(\omega')$. But we already know that $\mathtt{pol}(\omega') \sqsubseteq \mathcal{A}$ and $\neg(\mathtt{pol}(\omega_1) \subseteq \mathcal{A})$ ↯.

iii. **high**: In this case $\mathtt{pol}(\omega') \not\sqsubseteq \mathcal{A}$. But we already know $\mathtt{pol}(\omega') \sqsubseteq \mathcal{A}$. ↯.

(c) $\mathfrak{n} = 0$ and $\mathfrak{l} > 0$. By inversion of $\mathsf{e}_1, \mathsf{S}_1, \Sigma_1 \overset{\omega}{\Rightarrow} \mathsf{e}_1', \mathsf{S}_1', \Sigma_1'$, and $\mathsf{e}_2, \mathsf{S}_2, \Sigma_2 \overset{\omega_1',\ldots\omega_\mathfrak{l}',\omega'}{\Rightarrow} \mathsf{e}_2', \mathsf{S}_2', \Sigma_2'$ we get that there are $\mathsf{e}_2'', \mathsf{S}_2'', \Sigma_2''$ such that

- $\mathsf{e}_1, \Sigma_1, \mathsf{S}_1 \succ \mathsf{e}_1', \mathsf{S}_1', \omega, \Sigma_1'$
- $\mathsf{e}_2, \Sigma_2, \mathsf{S}_2 \succ \mathsf{e}_2'', \mathsf{S}_2'', \omega_1', \Sigma_2''$.

By assumption $\mathit{inv}_\mathcal{A}(\omega_1')$. Hence we have $\neg(\mathtt{pol}(\omega_1') \sqsubseteq \mathcal{A})$. Consequently $\omega_1' \approx^\mathcal{A}_{(W,\mathfrak{m}-1)} \omega$ by **high**. Hence there exists a $W' \sqsupseteq W$ such that among other things

- $\omega_1' \approx^\mathcal{A}_{(W',\mathfrak{m}-1)} \omega$.

We show that this is a contradiction by doing cases analysis on the derivation of $\omega_1' \approx^\mathcal{A}_{W'.\beta} \omega$.

i. **refl**: In this case $\omega_1' = \omega$. In particular therefore $\mathtt{pol}(\omega_1') = \mathtt{pol}(\omega)$. But we already know that $\mathtt{pol}(\omega) \sqsubseteq \mathcal{A}$ and $\neg(\mathtt{pol}(\omega_1') \subseteq \mathcal{A})$ ↯.

ii. **extend-τ**: In this case $\mathtt{pol}(\omega_1') = \mathtt{pol}(\omega)$. But we already know that $\mathtt{pol}(\omega) \sqsubseteq \mathcal{A}$ and $\neg(\mathtt{pol}(\omega_1') \subseteq \mathcal{A})$ ↯.

iii. **high**: In this case $\mathtt{pol}(\omega) \not\sqsubseteq \mathcal{A}$. But we already know $\mathtt{pol}(\omega) \sqsubseteq \mathcal{A}$. ↯.

(d) $\mathfrak{n} > 0$ and $\mathfrak{l} > 0$: By inversion of $\mathsf{e}_1, \mathsf{S}_1, \Sigma_1 \overset{\omega_1,\ldots\omega_\mathfrak{n},\omega}{\Rightarrow} \mathsf{e}_1', \mathsf{S}_1', \Sigma_1'$, and $\mathsf{e}_2, \mathsf{S}_2, \Sigma_2 \overset{\omega_1',\ldots\omega_\mathfrak{l}',\omega'}{\Rightarrow} \mathsf{e}_2', \mathsf{S}_2', \Sigma_2'$ we get that there are $\mathsf{e}_1'', \mathsf{e}_2'', \mathsf{S}_1'', \mathsf{S}_2'', \Sigma_1'', \Sigma_2''$ such that

- $\mathsf{e}_1, \Sigma_1, \mathsf{S}_1 \succ \mathsf{e}_1'', \mathsf{S}_1'', \omega_1, \Sigma_1''$
- $\mathsf{e}_1'', \Sigma_1, \mathsf{S}_1'' \overset{\omega_2,\ldots,\omega_\mathfrak{n},\omega}{\Rightarrow} \mathsf{e}_1', \mathsf{S}_1', \Sigma_1'$,
- $\mathsf{e}_2, \Sigma_2, \mathsf{S}_2 \succ \mathsf{e}_2'', \mathsf{S}_2'', \omega_1', \Sigma_2''$,
- $\mathsf{e}_2'', \Sigma_2, \mathsf{S}_2'' \overset{\omega_2',\ldots,\omega_\mathfrak{l}',\omega}{\Rightarrow} \mathsf{e}_2', \mathsf{S}_2', \Sigma_2'$.

By assumption $\mathit{inv}_\mathcal{A}(\omega_1')$. Hence we have $\neg(\mathtt{pol}(\omega_1') \sqsubseteq \mathcal{A})$. Consequently $\omega_1' \approx^\mathcal{A}_{(W,\mathfrak{m}-1)} \omega_1'$ by **high**. Hence there is a W' such that

- $W' \sqsupseteq W$,
- $(\mathsf{S}_1'', \mathsf{S}_2'', \mathfrak{m}-1) \overset{\mathcal{A}}{\triangleright} W'$,
- $\omega_1 \approx^\mathcal{A}_{(W',\mathfrak{m}-1)} \omega_1'$ and
- $(\mathsf{e}_1'', \mathsf{e}_2'', W', \Sigma_1, \Sigma_2, \mathfrak{m}-1) \in [\![\tau]\!]^\mathcal{A}_\mathsf{E}$.

By Lemma 10.7 we get

- $(\mathsf{S}_1'', \mathsf{S}_2'', \mathfrak{m}-2) \overset{\mathcal{A}}{\triangleright} W'$.

Note that $\mathfrak{m}-2 > 0$ because $\mathfrak{m} > \mathfrak{n}+\mathfrak{l}$ and both $\mathfrak{n}$ and $\mathfrak{l}$ are at least 1. We also have $\mathfrak{m}-1 > \mathfrak{n}+\mathfrak{l}-1 > (\mathfrak{n}-1)+(\mathfrak{l}-1)$. We also get by Lemma 10.8 that

- $\omega \approx^\mathcal{A}_{(W',(\mathfrak{m}-1)-1)} \omega'$

Hence we get by induction that there is a W'' such that

- $W'' \sqsupseteq W'$,
- $(\mathsf{e}_1', \mathsf{e}_2', W'', \Sigma_1, \Sigma_2, (\mathfrak{m}-1)-(\mathfrak{n}-1)-(\mathfrak{l}-1)-1) \in [\![\tau]\!]^\mathcal{A}_\mathsf{E}$ and
- $(\mathsf{S}_1', \mathsf{S}_2', (\mathfrak{m}-1)-(\mathfrak{n}-1)-(\mathfrak{l}-1)-1) \overset{\mathcal{A}}{\triangleright} W''$.

- $\omega \approx^{\mathcal{A}}_{(W'',(m-1)-(n-1)-(l-1)-1)} \omega'$

To show the goal it suffices to show

- $W'' \sqsupseteq W$. We get this by transitivity (Lemma 7.2).
- $(e_1', e_2', W'', \Sigma_1, \Sigma_2, m-n-l-1) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. Because $m-n-l-1 < m-n-l = (m-1)-(n-1)-(l-1)-1$ we get this by Lemma 8.29.
- $(S_1', S_2', m-n-l-1) \overset{\mathcal{A}}{\triangleright} W''$. Because $m-n-l-1 < m-n-l = (m-1)-(n-1)-(l-1)-1$ we get this by Lemma 10.7.
- $\omega \approx^{\mathcal{A}}_{(W'',m-n-l-1)} \omega'$. Because $m-n-l-1 < m-n-l = (m-1)-(n-1)-(l-1)-1$ we get this by Lemma 10.8.

2. $(e_1, e_2) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_1 \notin \mathcal{V} \;\wedge \forall e_1', S_1', \Sigma_1', \omega. \\ \Sigma_1 \vdash e_1, S_1 \xRightarrow{\omega;\Sigma_1'} e_1', S_1' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W'. W' \sqsupseteq W \wedge (S_1', S_2, m-1) \overset{\mathcal{A}}{\triangleright} (W') \wedge \\ (e_1', e_2, W', \Sigma_1, \Sigma_2, m-1) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}.$

We have to consider two cases

(a) $n = 0$. By inversion of $e_1, S_1, \Sigma_1 \overset{\omega}{\Rightarrow} e_1', S_1', \Sigma_1'$ we get

- $e_1, \Sigma_1, S_1 \succ e_1', S_1', \omega, \Sigma_1'$

This gives us $\neg(\mathtt{pol}(\omega) \sqsubseteq \mathcal{A})$ which contradicts our assumption. ↯

(b) $n > 0$. By inversion of $e_1, S_1, \Sigma_1 \overset{\omega_1,\ldots\omega_n,\omega}{\Rightarrow} e_1', S_1', \Sigma_1'$ we get that there are e_1'', S_1'', Σ_1'' such that

- $e_1, \Sigma_1, S_1 \succ e_1'', S_1'', \omega_1, \Sigma_1''$
- $e_1'', \Sigma_1, S_1'' \overset{\omega_2,\ldots,\omega_n,\omega}{\Rightarrow} e_1', S_1', \Sigma_1'$.

Hence there is a W' such that

- $W' \sqsupseteq W$,
- $(S_1'', S_2, m-1) \overset{\mathcal{A}}{\triangleright} W'$,
- $(e_1'', e_2, W', \Sigma_1, \Sigma_2, m-1) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.

By Lemma 10.7 we get

- $(S_1'', S_2, m-2) \overset{\mathcal{A}}{\triangleright} W'$.

Note that $m-2 \geqslant 0$ because $m > n+l$ and n is at least 1. We also have $m-1 > (n+l)-1 = (n-1)+l$. We also get by Lemma 10.8 that

- $\omega \approx^{\mathcal{A}}_{(W',(m-1)-1)} \omega'$

Hence we get by induction that there is a W'' such that

- $W'' \sqsupseteq W'$,
- $(e_1', e_2', W'', \Sigma_1, \Sigma_2, (m-1)-(n-1)-l-1) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ and
- $(S_1', S_2', (m-1)-(n-1)-l-1) \overset{\mathcal{A}}{\triangleright} W''$.
- $\omega \approx^{\mathcal{A}}_{(W'',(m-1)-(n-1)-l-1)} \omega'$

To show the goal it suffices to show

- $W'' \sqsupseteq W$. We get this by transitivity (Lemma 7.2).
- $(e_1', e_2', W'', \Sigma_1, \Sigma_2, m-n-l-1) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$.
  $m-n-l-1 = (m-1)-(n-1)-l-1$, so we already know this.
- $(S_1', S_2', m-n-l-1) \overset{\mathcal{A}}{\triangleright} W''$.
  $m-n-l-1 = (m-1)-(n-1)-l-1$, so we already know this.
- $\omega \approx^{\mathcal{A}}_{(W'',m-n-l-1)} \omega'$. $m-n-l-1 = (m-1)-(n-1)-l-1$, so we already know this.

3. $(e_1, e_2) \in \left\{ (e_1, e_2) \;\middle|\; \begin{array}{l} e_2 \notin \mathcal{V} \;\wedge \forall e_2', S_2', \Sigma_2', \omega. \\ \Sigma_2 \vdash e_2, S_2 \xRightarrow{\omega;\Sigma_2'} e_2', S_2' \to \neg(\mathrm{pol}(\omega) \sqsubseteq \mathcal{A}) \wedge \\ (\exists W'. W' \sqsupseteq W \wedge (S_1, S_2', m-1) \overset{\mathcal{A}}{\triangleright} W' \wedge \\ (e_1, e_2', W', \Sigma_1, \Sigma_2, m-1) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}) \end{array} \right\}$. We have to consider two cases

(a) $l = 0$. By inversion of $e_2, S_2, \Sigma_2 \overset{\omega'}{\Rightarrow} e_2', S_2', \Sigma_2'$ we get

- $e_2, \Sigma_2, S_2 \succ e_2', S_2', \omega', \Sigma_2'$

This gives us $\neg(\mathsf{pol}(\omega') \sqsubseteq \mathcal{A})$ which contradicts our assumption. ↯

(b) $l > 0$. By inversion of $e_2, S_2, \Sigma_2 \overset{\omega_1', \ldots \omega_n', \omega'}{\Rightarrow} e_2', S_2', \Sigma_2'$ we get that there are e_2'', S_2'', Σ_2'' such that

- $e_2, \Sigma_2, S_2 \succ e_2'', S_2'', \omega_1', \Sigma_2''$
- $e_2'', \Sigma_2, S_2'' \overset{\omega_2', \ldots, \omega_n', \omega'}{\Rightarrow} e_2', S_2', \Sigma_2'$.

Hence there is a W' such that

- $W' \sqsupseteq W$,
- $(S_1, S_2'', m - 1) \overset{\mathcal{A}}{\triangleright} W'$,
- $(e_1, e_2'', W', \Sigma_1, \Sigma_2, m - 1) \in [\![\tau]\!]_E^{\mathcal{A}}$.

By Lemma 10.7 we get

- $(S_1, S_2'', m - 2) \overset{\mathcal{A}}{\triangleright} W'$.

Note that $m - 2 \geqslant 0$ because $m > n + l$ and l is at least 1. We also have $m - 1 > (n + l) - 1 = n + (l - 1)$. We also get by Lemma 10.8 that

- $\omega \approx^{\mathcal{A}}_{(W', (m-1)-1)} \omega'$

Hence we get by induction that there is a W'' such that

- $W'' \sqsupseteq W'$,
- $(e_1', e_2', W'', \Sigma_1, \Sigma_2, (m - 1) - n - (l - 1) - 1) \in [\![\tau]\!]_E^{\mathcal{A}}$ and
- $(S_1', S_2', (m - 1) - n - (l - 1) - 1) \overset{\mathcal{A}}{\triangleright} W''$.
- $\omega \approx^{\mathcal{A}}_{(W'', (m-1)-n-(l-1)-1)} \omega'$

To show the goal it suffices to show

- $W'' \sqsupseteq W$. We get this by transitivity (Lemma 7.2).
- $(e_1', e_2', W'', \Sigma_1, \Sigma_2, m - n - l - 1) \in [\![\tau]\!]_E^{\mathcal{A}}$.
  $m - n - l - 1 = (m - 1) - n - (l - 1) - 1$, so we already know this.
- $(S_1', S_2', m - n - l - 1) \overset{\mathcal{A}}{\triangleright} W''$.
  $m - n - l - 1 = (m - 1) - n - (l - 1) - 1$, so we already know this.
- $\omega \approx^{\mathcal{A}}_{(W'', m-n-l-1)} \omega'$. $m - n - l - 1 = (m - 1) - n - (l - 1) - 1$, so we already know this.

□

Definition 10.8 (Low projection of a trace)**.** We define $\vec{\omega}_{\mathcal{A}}$ in the following way:

$$\omega_{\mathcal{A}} := \begin{cases} \varepsilon & \text{, if } \mathsf{inv}_{\mathcal{A}}(\omega) \\ \omega & \text{, otherwise} \end{cases} \qquad (\omega, \vec{\omega'})_{\mathcal{A}} := \begin{cases} \vec{\omega'}_{\mathcal{A}} & \text{, if } \mathsf{inv}_{\mathcal{A}}(\omega) \\ \omega, \vec{\omega'}_{\mathcal{A}} & \text{, otherwise} \end{cases}$$

We define reduction with $\mathcal{A}$-visible traces. Note that the reduction reports the active lock set of the last visible observation.

Definition 10.9 ($\mathcal{A}$-visible trace reduction)**.**

$$\frac{}{\Sigma \vdash e, S \overset{\varepsilon;\Sigma}{\Longrightarrow}^*_{\mathcal{A}} e, S}\ \textbf{no-red} \qquad \frac{\Sigma \vdash e, S \overset{\vec{\omega};\Sigma'}{\Longrightarrow}^*_{\mathcal{A}} e'', S'' \quad \Sigma \vdash e'', S'' \overset{\omega;\Sigma''}{\Longrightarrow} e', S' \quad \mathsf{inv}_{\mathcal{A}}(\omega)}{\Sigma \vdash e, S \overset{\vec{\omega};\Sigma'}{\Longrightarrow}^*_{\mathcal{A}} e', S'}\ \textbf{inv-red}$$

$$\frac{\Sigma \vdash e, S \overset{\vec{\omega};\Sigma''}{\Longrightarrow}^*_{\mathcal{A}} e'', S'' \quad \Sigma \vdash e'', S'' \overset{\omega;\Sigma'}{\Longrightarrow} e', S' \quad \neg\mathsf{inv}_{\mathcal{A}}(\omega)}{\Sigma \vdash e, S \overset{\vec{\omega},\omega;\Sigma'}{\Longrightarrow}^*_{\mathcal{A}} e', S'}\ \textbf{vis-red}$$

We sometimes still use the deprecated notation $e, S, \Sigma, \overset{\vec{\omega}}{\Longrightarrow}_{\mathcal{A}} e', S', \Sigma'$ in this document instead of $\Sigma \vdash e, S \overset{\vec{\omega};\Sigma'}{\Longrightarrow}^*_{\mathcal{A}} e', S'$.

We prove that there is a sensible connection between visible trace reduction and normal trace reduction.

Lemma 10.10. If $\Sigma \vdash e, S \xRightarrow{\omega;\Sigma''} e'', S''$ and $\Sigma \vdash e'', S'' \xRightarrow{\vec{\omega};\Sigma'}{}^{*}_{\mathcal{A}} e', S'$, then

- if $\mathit{inv}_{\mathcal{A}}(\omega)$, then $\Sigma \vdash e, S \xRightarrow{\vec{\omega};\Sigma'}{}^{*}_{\mathcal{A}} e', S'$
- if $\neg\mathit{inv}_{\mathcal{A}}(\omega)$ and
  - $\vec{\omega} = \varepsilon$, then $\Sigma \vdash e, S \xRightarrow{\omega;\Sigma''}{}^{*}_{\mathcal{A}} e', S'$
  - $\vec{\omega} \neq \varepsilon$, then $\Sigma \vdash e, S \xRightarrow{\omega,\vec{\omega};\Sigma'}{}^{*}_{\mathcal{A}} e', S'$.

Proof. By induction on $\Sigma \vdash e'', S'' \xRightarrow{\vec{\omega};\Sigma'}{}^{*}_{\mathcal{A}} e', S'$.

- **no-red**. In this case
  - $\vec{\omega} = \varepsilon$ and
  - $\Sigma' = \Sigma$
  - $e' = e''$
  - $S' = S''$

  We do case analysis on $\mathit{inv}_{\mathcal{A}}(\omega)$.

  1. $\mathit{inv}_{\mathcal{A}}(\omega)$. It suffices to show $\Sigma \vdash e, S \xRightarrow{\varepsilon;\Sigma}{}^{*}_{\mathcal{A}} e'', S''$ We get

$$\dfrac{\dfrac{}{\Sigma \vdash e, S \xRightarrow{\varepsilon;\Sigma}{}^{*}_{\mathcal{A}} e, S}\ \textbf{no-red} \qquad \Sigma \vdash e, S \xRightarrow{\omega;\Sigma''} e'', S'' \qquad \mathit{inv}_{\mathcal{A}}(\omega)}{\Sigma \vdash e, S \xRightarrow{\varepsilon;\Sigma}{}^{*}_{\mathcal{A}} e'', S''}\ \textbf{inv-red}$$

  2. $\neg\mathit{inv}_{\mathcal{A}}(\omega)$. It suffices to show $\Sigma \vdash e, S \xRightarrow{\omega;\Sigma''}{}^{*}_{\mathcal{A}} e'', S''$. We get

$$\dfrac{\dfrac{}{\Sigma \vdash e, S \xRightarrow{\varepsilon;\Sigma}{}^{*}_{\mathcal{A}} e, S}\ \textbf{no-red} \qquad e, \Sigma, S \succ e'', S'', \omega, \Sigma'' \qquad \neg\mathit{inv}_{\mathcal{A}}(\omega)}{e, S, \Sigma \xRightarrow{\omega}_{\mathcal{A}} e'', S'', \Sigma''}\ \textbf{vis-red}$$

- **inv-red**. In this case
  - $e'', S'', \Sigma \xRightarrow{\vec{\omega}}_{\mathcal{A}} e''', S''', \Sigma'$
  - $e''', S''', \Sigma \succ e', S', \omega', \Sigma'''$
  - $\mathit{inv}_{\mathcal{A}}(\omega)'$.

  We do case analysis on $\mathit{inv}_{\mathcal{A}}(\omega)$.

  1. $\mathit{inv}_{\mathcal{A}}(\omega)$. By induction
     - $e, S, \Sigma \xRightarrow{\vec{\omega}}_{\mathcal{A}} e''', S''', \Sigma'$

     Hence by **inv-red** $e, S, \Sigma \xRightarrow{\vec{\omega}}_{\mathcal{A}} e', S', \Sigma'$.
  2. $\neg\mathit{inv}_{\mathcal{A}}(\omega)$. We do another case analysis:
     (a) $\vec{\omega} = \varepsilon$. By induction
        - $e, S, \Sigma \xRightarrow{\omega}_{\mathcal{A}} e''', S''', \Sigma''$

        Hence by **inv-red** $e, S, \Sigma \xRightarrow{\omega}_{\mathcal{A}} e', S', \Sigma''$.
     (b) $\vec{\omega} \neq \varepsilon$. Then by induction
        - $e, S, \Sigma \xRightarrow{\omega,\vec{\omega}}_{\mathcal{A}} e''', S''', \Sigma'$

        Hence by **inv-red** $e, S, \Sigma \xRightarrow{\omega,\vec{\omega}}_{\mathcal{A}} e', S', \Sigma'$.

- **vis-red**. In this case
  - $e'', S'', \Sigma \xRightarrow{\vec{\omega}'}_{\mathcal{A}} e''', S''', \Sigma'''$
  - $e''', S''', \Sigma \succ e', S', \omega', \Sigma'$
  - $\neg \mathit{inv}_{\mathcal{A}}(\omega)'$
  - $\vec{\omega} = \vec{\omega}', \omega'$.

  We do case analysis on $\mathit{inv}_{\mathcal{A}}(\omega)$.

  1. $\mathit{inv}_{\mathcal{A}}(\omega)$. By induction
     - $e, S, \Sigma \xRightarrow{\vec{\omega}'}_{\mathcal{A}} e''', S''', \Sigma'''$

     We get $e, S, \Sigma \xRightarrow{\vec{\omega}', \omega'}_{\mathcal{A}} e', S', \Sigma'$ which is equivalent to the goal with **vis-red**.
  2. $\neg \mathit{inv}_{\mathcal{A}}(\omega)$. We do another case analysis:
     (a) $\vec{\omega}' = \varepsilon$. In this case $\vec{\omega} = \omega, \omega'$. By induction
     - $e, S, \Sigma \xRightarrow{\omega}_{\mathcal{A}} e''', S''', \Sigma''$

     We get $e, S, \Sigma \xRightarrow{\omega, \omega'}_{\mathcal{A}} e', S', \Sigma'$ by **vis-red**.
     (b) $\vec{\omega}' \neq \varepsilon$. By induction
     - $e, S, \Sigma \xRightarrow{\omega, \vec{\omega}'}_{\mathcal{A}} e''', S''', \Sigma'''$.

     $e, S, \Sigma \xRightarrow{\omega, \vec{\omega}', \omega'}_{\mathcal{A}}$ follows by **vis-red**.

□

Lemma 10.11.
If $\Sigma \vdash e,\ S \xRightarrow{\vec{\omega}; \Sigma'}{}^{*} e',\ S'$, then there is a Σ'' such that $\Sigma \vdash e,\ S \xRightarrow{\vec{\omega}_{\mathcal{A}}; \Sigma''}{}^{*}_{\mathcal{A}} e',\ S'$.

Proof. By induction on the derivation of $e, S, \Sigma \xRightarrow{\vec{\omega}} e', S', \Sigma'$.

- **single**: In this case there is some observation ω such that
  - $\vec{\omega} = \omega$ and
  - $e, \Sigma, S \succ e', S', \omega, \Sigma'$. We do case analysis:
    1. $\mathit{inv}_{\mathcal{A}}(\omega)$. In this case $\omega_{\mathcal{A}} = \varepsilon$. We get

$$\dfrac{\dfrac{}{\Sigma \vdash e,\ S \xRightarrow{\varepsilon; \Sigma}{}^{*}_{\mathcal{A}} e,\ S}\ \textbf{no-red} \qquad e, \Sigma, S \succ e', S', \omega, \Sigma' \qquad \mathit{inv}_{\mathcal{A}}(\omega)}{e, S, \Sigma \xRightarrow{\varepsilon}_{\mathcal{A}} e', S', \Sigma}\ \textbf{inv-red}$$

    2. $\neg \mathit{inv}_{\mathcal{A}}(\omega)$. In this case $\omega_{\mathcal{A}} = \omega$. We get

$$\dfrac{\dfrac{}{\Sigma \vdash e,\ S \xRightarrow{\varepsilon; \Sigma}{}^{*}_{\mathcal{A}} e,\ S}\ \textbf{no-red} \qquad e, \Sigma, S \succ e', S', \omega, \Sigma' \qquad \neg \mathit{inv}_{\mathcal{A}}(\omega)}{e, S, \Sigma \xRightarrow{\omega}_{\mathcal{A}} e', S', \Sigma'}\ \textbf{vis-red}$$

  - **continue**: In this case there is an observation ω and a trace $\vec{\omega}'$ such that
    * $\vec{\omega} = \omega, \vec{\omega}'$
    * $e, \Sigma, S \succ e'', S'', \omega, \Sigma''$
    * $e'', S'', \Sigma \xRightarrow{\vec{\omega}'} e', S', \Sigma'$.

    By induction there is a Σ''' such that
    * $e'', S'', \Sigma \xRightarrow{\vec{\omega}'_{\mathcal{A}}}_{\mathcal{A}} e', S', \Sigma'''$.

    We do case analysis on $\mathit{inv}_{\mathcal{A}}(\omega)$.
    1. $\mathit{inv}_{\mathcal{A}}(\omega)$. In that case by Lemma 10.10 we have $e, S, \Sigma \xRightarrow{\vec{\omega}'_{\mathcal{A}}}_{\mathcal{A}} e', S', \Sigma'''$. This is equivalent to the goal because we have $\vec{\omega}_{\mathcal{A}} = (\omega, \vec{\omega}')_{\mathcal{A}} = \vec{\omega}'_{\mathcal{A}}$ because $\mathit{inv}_{\mathcal{A}}(\omega)$.

2. $\neg \mathit{inv}_{\mathcal{A}}(\omega)$. We do another cases analysis
   (a) $\vec{\omega'}_{\mathcal{A}} = \varepsilon$. In this case we get by Lemma 10.10 that $e, S, \Sigma \overset{\omega}{\Longrightarrow}_{\mathcal{A}} e', S', \Sigma''$. This is equivalent to the goal because we have $\vec{\omega}_{\mathcal{A}} = (\omega, \vec{\omega'})_{\mathcal{A}} = \omega, \vec{\omega'}_{\mathcal{A}} = \omega, \epsilon = \omega$ because $\neg \mathit{inv}_{\mathcal{A}}(\omega)$.
   (b) $\vec{\omega'} \neq \varepsilon$. In this case we get by Lemma 10.10 that $e, S, \Sigma \overset{\omega, \vec{\omega'}_{\mathcal{A}}}{\Longrightarrow}_{\mathcal{A}} e', S', \Sigma'''$. This is equivalent to the goal because we have $\vec{\omega}_{\mathcal{A}} = (\omega, \vec{\omega'})_{\mathcal{A}} = \omega, \vec{\omega'}_{\mathcal{A}}$ because $\neg \mathit{inv}_{\mathcal{A}}(\omega)$.

□

Lemma 10.12. If $e, S, \Sigma \overset{\vec{\omega}}{\Rightarrow} e', S', \Sigma'$ and $e', S', \Sigma \overset{\vec{\omega'}}{\Rightarrow} e'', S'', \Sigma''$, then $e, S, \Sigma \overset{\vec{\omega}, \vec{\omega'}}{\Rightarrow} e'', S'', \Sigma''$.

Proof. By induction on $e, S, \Sigma \overset{\vec{\omega}}{\Rightarrow} e', S', \Sigma'$.

- **single**. In this case
  - $e, \Sigma, S \succ e', S', \omega, \Sigma'$ and
  - $\vec{\omega} = \omega$.

  We get $e, S, \Sigma \overset{\omega, \vec{\omega'}}{\Rightarrow} e'', S'', \Sigma''$ by **continue**. This is the goal because $\vec{\omega} = \omega$.
- **continue**. In this case there are $e''', S''', \Sigma''', \omega, \vec{\omega''}$ such that
  - $e, \Sigma, S \succ e''', S''', \omega, \Sigma'''$
  - $e''', S''', \Sigma \overset{\vec{\omega''}}{\Rightarrow} e', S', \Sigma'$
  - $\vec{\omega} = \omega, \vec{\omega''}$.

  By induction we have $e''', S''', \Sigma \overset{\vec{\omega''}, \vec{\omega'}}{\Rightarrow} e'', S'', \Sigma''$. We get $e, S, \Sigma \overset{\omega, \vec{\omega''}, \vec{\omega'}}{\Rightarrow} e'', S'', \Sigma''$ by **continue**. This is equal to the goal.

□

Lemma 10.13. If $\mathit{inv}_{\mathcal{A}}(\omega)$, then $(\vec{\omega}, \omega)_{\mathcal{A}} = \vec{\omega}_{\mathcal{A}}$

Proof. By induction on $\vec{\omega}$.

- $\mathrm{tr} = \omega'$. We do case analysis on $\mathit{inv}_{\mathcal{A}}(\omega')$.
  1. $\mathit{inv}_{\mathcal{A}}(\omega')$. In this case $(\vec{\omega}, \omega)_{\mathcal{A}} = (\omega', \omega)_{\mathcal{A}} = \omega_{\mathcal{A}} = \varepsilon = \omega'_{\mathcal{A}} = \vec{\omega}_{\mathcal{A}}$.
  2. $\neg \mathit{inv}_{\mathcal{A}}(\omega')$. In this case $(\vec{\omega}, \omega)_{\mathcal{A}} = (\omega', \omega)_{\mathcal{A}} = \omega', \omega_{\mathcal{A}} = \omega', \varepsilon = \omega' = \omega'_{\mathcal{A}} = \vec{\omega}_{\mathcal{A}}$.
- $\mathrm{tr} = \omega', \vec{\omega'}$. We do case analysis on $\mathit{inv}_{\mathcal{A}}(\omega')$.
  1. $\mathit{inv}_{\mathcal{A}}(\omega')$. In this case $(\vec{\omega}, \omega)_{\mathcal{A}} = (\omega', \vec{\omega'}, \omega)_{\mathcal{A}} = (\vec{\omega'}, \omega)_{\mathcal{A}} \overset{\text{Ind.}}{=} \vec{\omega'}_{\mathcal{A}} = (\omega', \vec{\omega'})_{\mathcal{A}} = \vec{\omega}_{\mathcal{A}}$.
  2. $\neg \mathit{inv}_{\mathcal{A}}(\omega')$. In this case $(\vec{\omega}, \omega)_{\mathcal{A}} = (\omega', \vec{\omega'}, \omega)_{\mathcal{A}} = \omega', (\vec{\omega'}, \omega)_{\mathcal{A}} \overset{\text{Ind.}}{=} \omega', \vec{\omega'}_{\mathcal{A}} = (\omega', \vec{\omega'})_{\mathcal{A}} = \vec{\omega}_{\mathcal{A}}$.

□

Lemma 10.14. Let $\vec{\omega}$ be a trace and ω an observation. If $\neg \mathit{inv}_{\mathcal{A}}(\omega)$, then $\vec{\omega} = \varepsilon$ or $(\vec{\omega}, \omega)_{\mathcal{A}} = \vec{\omega}_{\mathcal{A}}, \omega$

Proof. By induction on $\vec{\omega}$.

- $\vec{\omega} = \epsilon$. There is nothing to show.
- $\vec{\omega} = \omega'$. We do case analysis on $\mathit{inv}_{\mathcal{A}}(\omega')$.
  1. $\mathit{inv}_{\mathcal{A}}(\omega')$. In this case $(\vec{\omega}, \omega)_{\mathcal{A}} = (\omega', \omega)_{\mathcal{A}} = \omega_{\mathcal{A}} = \varepsilon, \omega = \omega'_{\mathcal{A}}, \omega = \vec{\omega}_{\mathcal{A}}, \omega$.
  2. $\neg \mathit{inv}_{\mathcal{A}}(\omega')$. In this case $(\vec{\omega}, \omega)_{\mathcal{A}} = (\omega', \omega)_{\mathcal{A}} = \omega', \omega_{\mathcal{A}} = \omega', \omega = \omega'_{\mathcal{A}}, \omega = \vec{\omega}_{\mathcal{A}}, \omega$.
- $\vec{\omega} = \omega', \vec{\omega'}$. We do case analysis on $\mathit{inv}_{\mathcal{A}}(\omega')$.
  1. $\mathit{inv}_{\mathcal{A}}(\omega')$. In this case $(\vec{\omega}, \omega)_{\mathcal{A}} = (\omega', \vec{\omega'}, \omega)_{\mathcal{A}} = (\vec{\omega'}, \omega)_{\mathcal{A}} \overset{\text{Ind.}}{=} \vec{\omega'}_{\mathcal{A}}, \omega = (\omega', \vec{\omega'})_{\mathcal{A}}, \omega = \vec{\omega}_{\mathcal{A}}, \omega$.

2. $\neg \mathit{inv}_{\mathcal{A}}(\omega')$. In this case $(\vec{\omega}, \omega)_{\mathcal{A}} = (\omega', \vec{\omega'}, \omega)_{\mathcal{A}} = \omega', (\vec{\omega'}, \omega)_{\mathcal{A}} \overset{\text{Ind.}}{=} \omega', \vec{\omega'}_{\mathcal{A}}, \omega = (\omega', \vec{\omega'})_{\mathcal{A}}, \omega = \vec{\omega}_{\mathcal{A}}, \omega$.

□

Lemma 10.15. If $\Sigma \vdash e, S \xrightarrow{\vec{\omega};\Sigma'}{}^{*}_{\mathcal{A}} e', S'$, then either $\vec{\omega} = \varepsilon$, $e' = e$, $\Sigma' = \Sigma$ and $S' = S$, or there are $\vec{\omega'}, \Sigma''$ such that $\Sigma \vdash e, S \xrightarrow{\vec{\omega'};\Sigma''}{}^{*} e', S'$ and $\vec{\omega'}_{\mathcal{A}} = \vec{\omega}$.

Proof. By induction on $e, S, \Sigma \overset{\vec{\omega}}{\Longrightarrow}_{\mathcal{A}} e', S', \Sigma'$.

- **no-red**. In this case $\vec{\omega} = \varepsilon$, $e' = e$, $\Sigma' = \Sigma$ and $S' = S$.
- **inv-red** In this case there are $e'', S'', \Sigma'', \omega$ such that
  - $e, S, \Sigma \overset{\vec{\omega}}{\Longrightarrow}_{\mathcal{A}} e'', S'', \Sigma'$,
  - $e'', \Sigma, S'' \succ e', S', \omega, \Sigma''$,
  - $\mathit{inv}_{\mathcal{A}}(\omega)$.

  By induction there are two cases:
  1. $\vec{\omega} = \varepsilon$, $e'' = e$,$\Sigma' = \Sigma$ and $S'' = S$. In this case it suffices to show
     - $e, S, \Sigma \overset{\omega}{\Rightarrow} e', S', \Sigma''$. We get this by **single** because of the known equalities.
     - $\omega_{\mathcal{A}} = \varepsilon$. We have this because $\mathit{inv}_{\mathcal{A}}(\omega)$.
  2. There are $\vec{\omega'}, \Sigma'''$ such that
     - $e, S, \Sigma \overset{\vec{\omega'}}{\Rightarrow} e'', S'', \Sigma'''$
     - $\vec{\omega'}_{\mathcal{A}} = \vec{\omega}$

     We get $e'', S'', \Sigma \overset{\omega}{\Rightarrow} e', S', \Sigma''$ by **single**. $e, S, \Sigma \overset{\vec{\omega'},\omega}{\Rightarrow} e', S', \Sigma''$ follows by Lemma 10.12. All that remains to be shown is that $(\vec{\omega'}, \omega)_{\mathcal{A}} = \vec{\omega}$. We get this by Lemma 10.13.
- **vis-red** In this case there are $e'', S'', \Sigma'', \omega, \vec{\omega'}$ such that
  - $e, S, \Sigma \overset{\vec{\omega'}}{\Longrightarrow}_{\mathcal{A}} e'', S'', \Sigma''$,
  - $e'', \Sigma, S'' \succ e', S', \omega, \Sigma'$,
  - $\neg \mathit{inv}_{\mathcal{A}}(\omega)$.
  - $\vec{\omega} = \vec{\omega'}, \omega$

  By induction there are two cases:
  1. $\vec{\omega'} = \varepsilon$, $e'' = e$, $\Sigma'' = \Sigma$ and $S'' = S$. In this case it suffices to show
     - $e, S, \Sigma \overset{\omega}{\Rightarrow} e', S', \Sigma''$. We get this by **single** because of the known equalities.
     - $\omega_{\mathcal{A}} = \omega$. We have this because $\neg \mathit{inv}_{\mathcal{A}}(\omega)$.
  2. There are $\vec{\omega''}, \Sigma'''$ such that
     - $e, S, \Sigma \overset{\vec{\omega''}}{\Rightarrow} e'', S'', \Sigma'''$
     - $\vec{\omega''}_{\mathcal{A}} = \vec{\omega'}$

     We get $e'', S'', \Sigma \overset{\omega}{\Rightarrow} e', S', \Sigma'$ by **single**. $e, S, \Sigma \overset{\vec{\omega''},\omega}{\Rightarrow} e', S', \Sigma'$ follows by Lemma 10.12.
     All that remains to be shown is that $(\vec{\omega''}, \omega)_{\mathcal{A}} = \vec{\omega}$. By Lemma 10.14 we get $(\vec{\omega''}, \omega)_{\mathcal{A}} = \vec{\omega''}_{\mathcal{A}}, \omega = \vec{\omega'}, \omega = \vec{\omega}$.

□

Lemma 10.16. If $\neg \mathit{inv}_{\mathcal{A}}(\omega)$, then $(\vec{\omega}, \omega)_{\mathcal{A}} \neq \varepsilon$

Proof. By induction on $\vec{\omega}$.

- $\vec{\omega} = \varepsilon$. In this case $(\vec{\omega}, \omega)_{\mathcal{A}} = \omega_{\mathcal{A}} = \omega$. And $\omega \neq \varepsilon$.
- $\vec{\omega} = \omega', \vec{\omega'}$. We do case analysis on $\mathit{inv}_{\mathcal{A}}(\omega')$

1. $\mathsf{inv}_{\mathcal{A}}(\omega')$. In this case $(\vec{\omega}, \omega)_{\mathcal{A}} = (\omega', \vec{\omega'}, \omega)_{\mathcal{A}} = (\vec{\omega'}, \omega)_{\mathcal{A}} \overset{\text{Ind.}}{\neq} \varepsilon$.
2. $\neg\mathsf{inv}_{\mathcal{A}}(\omega')$. In this case $(\vec{\omega}, \omega)_{\mathcal{A}} = (\omega', \vec{\omega'}, \omega)_{\mathcal{A}} = \omega', (\vec{\omega'}, \omega) \neq \varepsilon$.

□

Definition 10.10. A trace $\vec{\omega} := \omega_0, \omega_1, \ldots \omega_n$ is equivalent to a trace $\vec{\omega'} := \omega'_0, \omega'_1, \ldots \omega'_n$ (written $\vec{\omega} \approx^{\mathcal{A}}_{(W,m)} \vec{\omega'}$), when we have $\omega_i \approx^{\mathcal{A}}_{(W,m)} \omega'_i$ for all $0 \leqslant i \leqslant n$.

Lemma 10.17. If $\vec{\omega}_{\mathcal{A}} = \vec{\omega'}, \omega$, then $\neg\mathsf{inv}_{\mathcal{A}}(\omega)$.

Proof. By induction on $\vec{\omega}$.

- $\vec{\omega} = \omega'$. We do case analysis on $\mathsf{inv}_{\mathcal{A}}(\omega')$.
  1. $\mathsf{inv}_{\mathcal{A}}(\omega')$. In this case $\vec{\omega}_{\mathcal{A}} = \omega'_{\mathcal{A}} = \varepsilon \neq \vec{\omega'}, \omega$. ↯
  2. $\neg\mathsf{inv}_{\mathcal{A}}(\omega')$. In this case $\vec{\omega}_{\mathcal{A}} = \omega'_{\mathcal{A}} = \omega' = \vec{\omega'}, \omega$. This can only be the case if $\vec{\omega'} = \varepsilon$ and $\omega' = \omega$. Since $\neg\mathsf{inv}_{\mathcal{A}}(\omega')$ also $\neg\mathsf{inv}_{\mathcal{A}}(\omega)$.
- $\vec{\omega} = \omega', \vec{\omega''}$. We do case analysis on $\mathsf{inv}_{\mathcal{A}}(\omega')$.
  1. $\mathsf{inv}_{\mathcal{A}}(\omega')$. In this case $\mathsf{tr}_{\mathcal{A}} = (\omega', \vec{\omega''})_{\mathcal{A}} = \vec{\omega''}_{\mathcal{A}} = \vec{\omega'}, \omega$. We get the claim by induction.
  2. $\neg\mathsf{inv}_{\mathcal{A}}(\omega')$. In this case $\mathsf{tr}_{\mathcal{A}} = (\omega', \vec{\omega''})_{\mathcal{A}} = \omega', \vec{\omega''}_{\mathcal{A}} = \vec{\omega'}, \omega$. We do case analysis on $\vec{\omega'}$.
     (a) $\vec{\omega'} = \varepsilon$. In this case $\omega', \vec{\omega''}_{\mathcal{A}} = \omega$. This can only be the case if $\omega' = \omega$ and $\vec{\omega''}_{\mathcal{A}} = \varepsilon$. Since $\neg\mathsf{inv}_{\mathcal{A}}(\omega')$ we also have $\neg\mathsf{inv}_{\mathcal{A}}(\omega)$.
     (b) $\vec{\omega'} = \omega'', \vec{\omega'''}$. In this case $\omega', \vec{\omega''}_{\mathcal{A}} = \omega'', \vec{\omega'''}, \omega$. Hence $\omega' = \omega''$ and $\vec{\omega''}_{\mathcal{A}} = \vec{\omega'''}, \omega$. We get the claim by induction.

□

Lemma 10.18. If $(\vec{\omega}, \omega)_{\mathcal{A}} = \omega$, then there are $\omega_1, \ldots, \omega_n$ such that $\vec{\omega} = \omega_1, \ldots, \omega_n$ and $\forall 1 \leqslant i \leqslant n$, $\mathsf{inv}_{\mathcal{A}}(\omega_i)$ and $\mathsf{pol}(\omega) \sqsubseteq \mathcal{A}$.

Proof. By induction on $\vec{\omega}$.
$\vec{\omega} = \varepsilon$. There are two cases:

1. $\mathsf{inv}_{\mathcal{A}}(\omega)$. In this case $(\vec{\omega}, \omega)_{\mathcal{A}} = \omega_{\mathcal{A}} = \varepsilon$ ↯.
2. $\neg(\mathsf{inv}_{\mathcal{A}}(\omega))$. $\neg\mathsf{inv}_{\mathcal{A}}(\omega)$ implies $\mathtt{pol}(\omega) \sqsubseteq \mathcal{A}$. In this case $\vec{\omega}_{\mathcal{A}} = \omega_{\mathcal{A}} = \omega'$. Hence the claim is true if we set $n = 0$.

$\vec{\omega} = \omega', \vec{\omega'}$. There are two cases:

1. $\mathsf{inv}_{\mathcal{A}}(\omega')$. In this case $(\vec{\omega}, \omega)_{\mathcal{A}} = (\omega', \vec{\omega'}, \omega)_{\mathcal{A}} = (\vec{\omega'}, \omega)_{\mathcal{A}}$. By transitivity this gives us $(\vec{\omega'}, \omega)_{\mathcal{A}} = \omega$. By induction we get that there are $\omega_1, \ldots, \omega_n$ and such that $\vec{\omega'} = \omega_1, \ldots, \omega_n, \omega$ and $\forall 1 \leqslant i \leqslant n$, $\mathsf{inv}_{\mathcal{A}}(\omega_i)$ and $\mathtt{pol}(\omega) \sqsubseteq \mathcal{A}$. Then $\vec{\omega} = \omega', \omega_1, \ldots, \omega_n$ We already have $\mathsf{inv}_{\mathcal{A}}(\omega')$ so this shows the goal.
2. $\neg(\mathsf{inv}_{\mathcal{A}}(\omega'))$. In this case $\vec{\omega}_{\mathcal{A}} = (\omega', \vec{\omega''}, \omega)_{\mathcal{A}} = \omega', (\vec{\omega''}, \omega)_{\mathcal{A}}$. By transitivity $\omega = \omega', (\vec{\omega''}, \omega)_{\mathcal{A}}$. This can only be the case if $\omega = \omega'$ and $(\vec{\omega'}, \omega)_{\mathcal{A}} = \varepsilon$. Because $\omega = \omega'$ and $\neg\mathsf{inv}_{\mathcal{A}}(\omega')$ we also have $\neg\mathsf{inv}_{\mathcal{A}}(\omega)$. But then by Lemma 10.16 we have $\vec{\omega'}, \omega_{\mathcal{A}} \neq \varepsilon$. ↯.

□

Lemma 10.19. If $\vec{\omega}_{\mathcal{A}} = \omega, \vec{\omega'}$, then $\vec{\omega} = \omega_1, \ldots, \omega_n, \omega, \vec{\omega''}$ and $\vec{\omega''}_{\mathcal{A}} = \vec{\omega'}$ and $\forall 1 \leqslant i \leqslant n.\mathsf{inv}_{\mathcal{A}}(\omega_i)$ and $\neg\mathsf{inv}_{\mathcal{A}}(\omega)$.

Proof. By induction in $\vec{\omega}$.

- $\vec{\omega} = \varepsilon$. In this case $\vec{\omega}_{\mathcal{A}}$ is not even defined. So $\vec{\omega}_{\mathcal{A}} = \omega, \vec{\omega'}$ cannot be the case. ↯.
- $\vec{\omega} = \omega', \vec{\omega''}$. We do case analysis on $\mathsf{inv}_{\mathcal{A}}(\omega')$.
  1. $\mathsf{inv}_{\mathcal{A}}(\omega')$. In this case $\vec{\omega''}_{\mathcal{A}} = (\omega', \vec{\omega''})_{\mathcal{A}} = \vec{\omega}_{\mathcal{A}} = \omega, \vec{\omega'}$. Hence by induction there are $\omega_1, \ldots, \omega_n$ and $\vec{\omega'''}$ such that
     – $\vec{\omega''} = \omega_1, \ldots, \omega_n, \omega, \vec{\omega'''}$

- $\vec{\omega''}_{\mathcal{A}} = \vec{\omega'}$
- $\forall 1 \leqslant i \leqslant n. \mathit{inv}_{\mathcal{A}}(\omega_i)$
- $\neg \mathit{inv}_{\mathcal{A}}(\omega)$

We get the goal because also $\mathit{inv}_{\mathcal{A}}(\omega')$.

2. $\neg \mathit{inv}_{\mathcal{A}}(\omega')$. In this case $\vec{\omega}_{\mathcal{A}} = (\omega', \vec{\omega''})_{\mathcal{A}} = \omega', \vec{\omega''}_{\mathcal{A}}$. Hence $\omega', \vec{\omega''} = \omega, \vec{\omega'}$. This can only be the case of $\omega' = \omega$ and $\vec{\omega''}_{\mathcal{A}} = \vec{\omega'}$. So we have the goal with $n = 0$.

□

Lemma 10.20. If $\Sigma \vdash e, S \xRightarrow{\vec{\omega}, \vec{\omega'}; \Sigma'}{}^{*} e', S'$, there are e'', S'', Σ'' such that $\Sigma \vdash e, S \xRightarrow{\vec{\omega}; \Sigma''}{}^{*} e'', S''$ and $\Sigma \vdash e'', S'' \xRightarrow{\vec{\omega'}; \Sigma'}{}^{*} e', S'$.

Proof. By induction on $\vec{\omega}$.

- $\vec{\omega} = \omega$. In this case we get the claim by the definition of $e, S, \Sigma \overset{\omega, \vec{\omega'}}{\Rightarrow} e', S', \Sigma'$.
- $\vec{\omega} = \omega, \vec{\omega''}$. Then by definition of $e, S, \Sigma \overset{\omega, \vec{\omega''}, \vec{\omega'}}{\Rightarrow} e', S', \Sigma'$ there are e''', S''', Σ''' such that
  - $e, S, \Sigma \overset{\omega}{\Rightarrow} e''', S''', \Sigma'''$ and
  - $e''', S''', \Sigma \overset{\vec{\omega''}, \vec{\omega'}}{\Rightarrow} e', S', \Sigma'$.

  By induction we have e'', S'', Σ'' such that
  - $e''', S''', \Sigma \overset{\vec{\omega''}}{\Rightarrow} e'', S'', \Sigma''$ and
  - $e'', S'', \Sigma \overset{\vec{\omega'}}{\Rightarrow} e', S', \Sigma'$ which is part of our goal.

  By definition we get $e, S, \Sigma \overset{\omega, \vec{\omega''}}{\Rightarrow} e'', S'', \Sigma''$ which is all that remains to be shown.

□

Lemma 10.21. If $(\vec{\omega}, \omega)_{\mathcal{A}} = \vec{\omega'}, \omega$, then $\vec{\omega} = \varepsilon$ or $\vec{\omega}_{\mathcal{A}} = \vec{\omega'}$.

Proof. By Lemma 10.17 we have $\neg \mathit{inv}_{\mathcal{A}}(\omega)$. Hence by Lemma 10.14 we get two cases:

- $\vec{\omega} = \varepsilon$. This proves the goal.
- $(\vec{\omega}, \omega)_{\mathcal{A}} = \vec{\omega}_{\mathcal{A}}, \omega$. In this case $\vec{\omega}_{\mathcal{A}}, \omega = \vec{\omega'}, \omega$. This can only be the case if $\vec{\omega}_{\mathcal{A}} = \vec{\omega'}$.

□

Lemma 10.22. 1. If $\omega \approx^{\mathcal{A}}_{(W,m)} \omega'$ and $W' \sqsupseteq W$ and $m' \leqslant m$, then $\omega \approx^{\mathcal{A}}_{(W',m')} \omega'$.

2. If $\vec{\omega} \approx^{\mathcal{A}}_{(W,m)} \vec{\omega'}$ and $W' \supseteq W$ and $m' \leqslant m$, then $\vec{\omega} \approx^{\mathcal{A}}_{(W',m')} \vec{\omega'}$.

Proof. 1. By cases analysis on the derivation of $\omega \approx^{\mathcal{A}}_{(W,m)} \omega'$. For **refl** and **high** we get the claim by the same rule. For **extend-τ** ω and ω' have the form $l_\tau(v)$ and $l'_\tau(v')$, respectively. By inversion we get
   - $(v, v', W, m) \in [\![\tau]\!]^{\mathcal{A}}_V$
   - $(l, l') \in W.\beta$

   We get the claim by **extend-τ** if we can show
   - $(v, v', W', m') \in [\![\tau]\!]^{\mathcal{A}}_V$. We get this by Lemma 8.25 and Lemma 8.24.
   - $(l, l') \in W'.\beta$. This follows directly from $W' \supseteq W$.

2. We get this by pointwise application of 1. to each pair of observations in the traces.

□

Lemma 10.23. If $(e_1, e_2, W, \Sigma_1, \Sigma_2, m) \in [\![\tau]\!]^{\mathcal{A}}_E$, $\Sigma_1 \vdash e_1, S_1 \xrightarrow{\vec{\omega_1}, \omega_1; \Sigma_1'}{}^{*} e_1', S_1', \Sigma_2 \vdash e_2, S_2 \xrightarrow{\vec{\omega_2}, \omega_2; \Sigma_2'}{}^{*} e_2', S_2', \vec{\omega_1'}, \omega_1 = (\vec{\omega_1}, \omega_1)_{\mathcal{A}}, \vec{\omega_2'}, \omega_2 = (\vec{\omega_2}, \omega_2)_{\mathcal{A}}, \vec{\omega_1'} \approx^{\mathcal{A}}_{(W, m-1)} \vec{\omega_2'}, (S_1, S_2, m-1) \overset{\mathcal{A}}{\triangleright} W$, $m \geqslant \mathsf{len}(\vec{\omega_1}) + \mathsf{len}(\vec{\omega_2}) + 2$ and $\Sigma_1' \sqsubseteq \mathcal{A}$ or $\Sigma_2' \sqsubseteq \mathcal{A}$, then there is a $W' \sqsupseteq W$ such that $\vec{\omega_1'}, \omega_1 \approx^{\mathcal{A}}_{(W', m-\mathsf{len}(\vec{\omega_1})-\mathsf{len}(\vec{\omega_2})-1)} \vec{\omega_2'}, \omega_2$.

Proof. By induction on $\vec{\omega_1'}$.

- $\vec{\omega_1'} = \varepsilon$. In this case because $\vec{\omega_1'} \approx^{\mathcal{A}}_{(W, m-1)} \vec{\omega_2'}$ we have $\vec{\omega_2'} = \varepsilon$ as well. Hence $(\vec{\omega_1}, \omega_1)_{\mathcal{A}} = \omega_1$ and $(\vec{\omega_2}, \omega_2)_{\mathcal{A}} = \omega_2$. By Lemma 10.18 this means that there are $\omega_1', \ldots \omega_n'$ and $\omega_1'', \ldots, \omega_{n'}''$such that
  - $\vec{\omega_1} = \omega_1', \ldots \omega_n'$
  - $\vec{\omega_2} = \omega_1'', \ldots \omega_{n'}''$
  - $\forall 1 \leqslant i \leqslant n. \mathsf{inv}_{\mathcal{A}}(\omega_i')$
  - $\forall 1 \leqslant i \leqslant n'. \mathsf{inv}_{\mathcal{A}}(\omega_i'')$
  - $\mathsf{pol}(\omega_1) \sqsubseteq \mathcal{A}$
  - $\mathsf{pol}(\omega_2) \sqsubseteq \mathcal{A}$

  Clearly also $\mathsf{len}(\omega_1) = n$ and $\mathsf{len}(\omega_2) = n'$ and hence
  - $m \geqslant n + n' + 2$

  Hence
  - $e_1, S_1, \Sigma_1 \overset{\omega_1', \ldots \omega_n', \omega_1}{\Rightarrow} e_1', S_1', \Sigma_1'$
  - $e_2, S_2, \Sigma_2 \overset{\omega_1'', \ldots \omega_{n'}'', \omega_2}{\Rightarrow} e_2', S_2', \Sigma_2'$

  By Lemma 10.9 we get that there is a $W' \sqsupseteq W$ such that $\omega_1 \approx^{\mathcal{A}}_{(W', m-n-n'-1)} \omega_2$. This is the goal since $\vec{\omega_1'} = \varepsilon = \vec{\omega_2'}$.

- $\vec{\omega_1'} = \omega_1', \vec{\omega_1''}$. Then because of $\vec{\omega_1'} \approx^{\mathcal{A}}_{(W, m-1)} \vec{\omega_2'}$ we must have that there are ω_2' and $\vec{\omega_2''}$ such that $\vec{\omega_2'} = \omega_2', \vec{\omega_2''}$ and $\omega_1' \approx^{\mathcal{A}}_{(W, m-1)} \omega_2'$. Then also $\vec{\omega_1''} \approx^{\mathcal{A}}_{(W, m-1)} \vec{\omega_2''}$. Hence
  - $(\vec{\omega_1}, \omega_1)_{\mathcal{A}} = \omega_1', \vec{\omega_1''}, \omega_1$
  - $(\vec{\omega_2}, \omega_2)_{\mathcal{A}} = \omega_2', \vec{\omega_2''}, \omega_2$

  Hence by Lemma 10.21 we have one of two cases:
  - $\vec{\omega_1} = \epsilon$ or $\vec{\omega_2} = \epsilon$. This would mean that $(\vec{\omega_1}, \omega_1)_{\mathcal{A}} = (\omega_1)_{\mathcal{A}} = \omega_1 = \omega_1', \vec{\omega_1''}, \omega_1$. or $(\vec{\omega_2}, \omega_2)_{\mathcal{A}} = (\omega_2)_{\mathcal{A}} = \omega_2 = \omega_2', \vec{\omega_2''}, \omega_2$. This is clearly impossible.
  - $\vec{\omega_1}_{\mathcal{A}} = \omega_1', \vec{\omega_1''}$ and $\vec{\omega_2}_{\mathcal{A}} = \omega_2', \vec{\omega_2''}$.

    By Lemma 10.19 we get that there are $\bar{\omega_1}, \ldots, \bar{\omega_n}$, $\bar{\omega_1'}, \ldots, \bar{\omega_{n'}'}$,$\vec{\bar{\omega}}$ and $\vec{\bar{\omega}'}$ such that
    - $\vec{\omega_1} = \bar{\omega_1}, \ldots, \bar{\omega_n}, \omega_1', \vec{\bar{\omega}}$,
    - $\vec{\omega_2} = \bar{\omega_1'}, \ldots, \bar{\omega_{n'}'}, \omega_2', \vec{\bar{\omega}'}$,
    - $\vec{\bar{\omega}}_{\mathcal{A}} = \vec{\omega_1''}$
    - $\vec{\bar{\omega}'}_{\mathcal{A}} = \vec{\omega_2''}$
    - $\neg \mathsf{inv}_{\mathcal{A}}(\omega_1')$ and hence $\mathsf{pol}(\omega_1') \sqsubseteq \mathcal{A}$
    - $\neg \mathsf{inv}_{\mathcal{A}}(\omega_2')$ and hence $\mathsf{pol}(\omega_2') \sqsubseteq \mathcal{A}$
    - $\forall 1 \leqslant i \leqslant n. \mathsf{inv}_{\mathcal{A}}(\bar{\omega_i})$
    - $\forall 1 \leqslant i \leqslant n'. \mathsf{inv}_{\mathcal{A}}(\bar{\omega_i'})$

    Hence we have
    - $e_1, S_1, \Sigma_1 \overset{\bar{\omega_1}, \ldots, \bar{\omega_n}, \omega_1', \vec{\bar{\omega}}, \omega_1}{\Rightarrow} e_1', S_1', \Sigma_1'$
    - $e_2, S_2, \Sigma_2 \overset{\bar{\omega_1'}, \ldots, \bar{\omega_{n'}'}, \omega_2', \vec{\bar{\omega}'}, \omega_2}{\Rightarrow} e_2', S_2', \Sigma_2'$.

* $m \geqslant n + 1 + \mathsf{len}(\vec{\omega}) + n' + 1 + \mathsf{len}(\vec{\omega'}) + 2$

By Lemma 10.20 we have e_1'', S_1'', Σ_1'' and e_2'', S_2'', Σ_2'' such that

* $e_1, S_1, \Sigma_1 \overset{\omega_1, \ldots, \omega_n, \omega_1'}{\Rightarrow} e_1'', S_1'', \Sigma_1''$
* $e_1'', S_1'', \Sigma_1 \overset{\vec{\omega}, \omega_1}{\Rightarrow} e_1', S_1', \Sigma_1'$.
* $e_2, S_2, \Sigma_2 \overset{\omega_1', \ldots, \omega_{n'}', \omega_2'}{\Rightarrow} e_2'', S_2'', \Sigma_2''$.
* $e_2'', S_2'', \Sigma_2 \overset{\vec{\omega'}, \omega_2}{\Rightarrow} e_2', S_2', \Sigma_2'$.

By Lemma 10.9 there is are $W' \sqsupseteq W$ and $m' = m - n - n' - 1$ such that

* $(e_1'', e_2'', W', \Sigma_1, \Sigma_2, m') \in [\![\tau]\!]_E^{\mathcal{A}}$,
* $(S_1'', S_2'', m') \overset{\mathcal{A}}{\triangleright} W'$
* $\omega_1' \approx^{\mathcal{A}}_{(W', m')} \omega_2'$.
* $m' \geqslant \mathsf{len}(\vec{\omega}) + 1 + \mathsf{len}(\vec{\omega'}) + 2$.

By induction we get that there is an $W'' \sqsupseteq W'$ such that $\vec{\omega_1''}, \omega_1 \approx^{\mathcal{A}}_{(W'', m' - \mathsf{len}(\vec{\omega}) - \mathsf{len}(\vec{\omega'}) - 1)} \vec{\omega_2''}, \omega_2$, if we can show

* $(e_1'', e_2'', W', \Sigma_1, \Sigma_2 m') \in [\![\tau]\!]_E^{\mathcal{A}}$. We already know this.
* $e_1'', S_1'', \Sigma_1 \overset{\vec{\omega}, \omega_1}{\Rightarrow} e_1', S_1', \Sigma_1'$. We already know this.
* $e_2'', S_2'', \Sigma_2 \overset{\vec{\omega'}, \omega_2}{\Rightarrow} e_2', S_2', \Sigma_2'$. We already know this.
* $\vec{\omega_1''}, \omega_1 = (\vec{\omega}, \omega_1)_{\mathcal{A}}$. By Lemma 10.17 we have $\neg \mathsf{inv}_{\mathcal{A}}(\omega_1)$. Hence by Lemma 10.14 there are two cases:
  - $\vec{\omega} = \varepsilon$. This is impossible because $\vec{\omega}_{\mathcal{A}} = \vec{\omega_1''}$ which means in particular that $\vec{\omega}_{\mathcal{A}}$ is defined. But $\varepsilon_{\mathcal{A}}$ is undefined. ↯
  - $(\vec{\omega}, \omega_1)_{\mathcal{A}} = \vec{\omega}_{\mathcal{A}}, \omega_1$. This shows the goal because $\vec{\omega}_{\mathcal{A}} = \vec{\omega_1''}$.
* $\vec{\omega_2''}, \omega_2 = (\vec{\omega'}, \omega_2)_{\mathcal{A}}$. By Lemma 10.17 we have $\neg \mathsf{inv}_{\mathcal{A}}(\omega_2)$. Hence by Lemma 10.14 there are two cases:
  - $\vec{\omega'} = \varepsilon$. This is impossible because $\vec{\omega'}_{\mathcal{A}} = \vec{\omega_2''}$ which means in particular that $\vec{\omega'}_{\mathcal{A}}$ is defined. But $\varepsilon_{\mathcal{A}}$ is undefined. ↯
  - $(\vec{\omega'}, \omega_2)_{\mathcal{A}} = \vec{\omega'}_{\mathcal{A}}, \omega_2$. This shows the goal because $\vec{\omega'}_{\mathcal{A}} = \vec{\omega_2''}$.
* $\vec{\omega_1''} \approx^{\mathcal{A}}_{(W', m'-1)} \vec{\omega_2''}$. We get this by Lemma 10.8.
* $(S_1'', S_2'', m' - 1) \overset{\mathcal{A}}{\triangleright} W'$. We get this by Lemma 10.7.
* $m' \geqslant \mathsf{len}(\vec{\omega}) + \mathsf{len}(\vec{\omega'}) + 2$. This follows from $m' \geqslant \mathsf{len}(\vec{\omega}) + 1 + \mathsf{len}(\vec{\omega'}) + 2$.
* $\Sigma_1' \sqsubseteq \mathcal{A}$ or $\Sigma_2' \sqsubseteq \mathcal{A}$. We already know this.

It suffices to show $\omega_1', \vec{\omega_1''}, \omega_1 \approx^{\mathcal{A}}_{(W'', m-(n+1+\mathsf{len}(\vec{\omega}))-(n'+1+\mathsf{len}(\vec{\omega'}))-1)} \omega_2', \vec{\omega_2''}, \omega_2$. To show this it suffices to show

* $\omega_1' \approx^{\mathcal{A}}_{(W'', m-(n+1+\mathsf{len}(\vec{\omega}))-(n'+1+\mathsf{len}(\vec{\omega'}))-1)} \omega_2'$. We get this by Lemma 10.22 because $m' = m - n - n' - 1$.
* $\vec{\omega_1''}, \omega_1 \approx^{\mathcal{A}}_{(W'', m-(n+1+\mathsf{len}(\vec{\omega}))-(n'+1+\mathsf{len}(\vec{\omega'}))-1)} \vec{\omega_2''}, \omega_2$. We get this by Lemma 10.22 using the definition of m'.

□

Definition 10.11 (Low states)**.** A state L is called $\mathcal{A}$-low if $L_{\mathcal{A}} = L$.

Definition 10.12. For a state environment θ and state S we define a state environment $\theta^S : \mathsf{dom}(\theta) \cup \mathsf{dom}(S) \to \mathsf{Type}$.

$$\theta^S(l) := \begin{cases} \theta(l) & \text{if } l \in \mathrm{dom}(\theta) \\ \mathrm{type}(S, l) & \text{otherwise} \end{cases}$$

Definition 10.13 (Knowledge)**.** The knowledge of attacker $\mathcal{A}$ after observing expression e produce trace ω in $\mathcal{A}$-low state L and lock set Σ with locations in θ is defined in the following way:

$$k_{\mathcal{A}}(e;\vec{\omega};L;\Sigma) := \left\{ S \;\middle|\; S \approx_{\mathcal{A}} L \wedge \Sigma \vdash e, S \xRightarrow{\vec{\omega'};\Sigma'}{}^{*}_{\mathcal{A}} e', S' \wedge\ \exists W \supseteq (\theta_S, \theta_S, \mathrm{id}_{\mathrm{dom}(L)}).\forall m.\vec{\omega} \approx^{\mathcal{A}}_{(W,m)} \vec{\omega'} \right\}$$

This definition is slightly different from the definition of knowledge in [4] because we have to take care of the non-deterministic choice of locations. We define runs similarly to [4].

Definition 10.14 (Runs)**.** An $\mathcal{A}$-observable run is defined in the following way:

$$Run_{\mathcal{A}}(e, L, \Sigma, \theta) := \left\{ (\vec{\omega}, \Sigma') \;\middle|\; \exists S, S', e'.\ S \triangleright.\ \theta^{L} \wedge S \approx_{\mathcal{A}} L \wedge \Sigma \vdash e, S \xRightarrow{\vec{\omega};\Sigma'}{}^{*}_{\mathcal{A}} e', S' \right\}$$

Lemma 10.24. If $v\ \beta \simeq^{\mathcal{A}}_{\tau} v'$, then also $v'\ \beta^{-1} \simeq^{\mathcal{A}}_{\tau} v$ and if $v\ \beta \simeq^{\mathcal{A}}_{A} v'$, then also $v'\ \beta^{-1} \simeq^{\mathcal{A}}_{A} v$.

Proof. By mutual induction on τ and A.

- $\tau = A^{p}$: There derivation could have happened with one of these two rules:
  1. **eqHigh**. In this case $p \not\sqsubseteq \mathcal{A}$. We get $v'\ \beta^{-1} \simeq^{\mathcal{A}}_{A^{p}} v$ by **eqHigh**.
  2. **eqLow**. In this case $p \sqsubseteq \mathcal{A}$ and $v\ \beta \simeq^{\mathcal{A}}_{A} v'$. $v'\ \beta^{-1} \simeq^{\mathcal{A}}_{A} v$ by induction. We get the claim by **eqLow**.
- $A = \mathtt{unit}$: In this case $v\ \beta \simeq^{\mathcal{A}}_{\mathtt{unit}} v'$ must have been derived by **eqUnit**. By inversion we get $v = () = v'$. We get the claim by **eqUnit**.
- $A = \mathbb{N}$. In this case $v\ \beta \simeq^{\mathcal{A}}_{\mathbb{N}} v'$ must have been derived by **eqNat**. By inversion we get $v = n = v'$. We get the claim by **eqNat**.
- $A = \tau_1 + \tau_2$. In this case there are two rules with which $v\ \beta \simeq^{\mathcal{A}}_{\mathbb{N}} v'$ could have been derived:
  1. **eqInl**: In this case there are v_0, v_0' such that
     - $v = \mathtt{inl}\ v_0$,
     - $v' = \mathtt{inl}\ v_0'$ and
     - $v_0\ \beta \simeq^{\mathcal{A}}_{\tau_1} v_0'$.

     $v_0'\ \beta^{-1} \simeq^{\mathcal{A}}_{\tau_1} v_0$ by induction. The claim follows by **eqInl**.
  2. **eqInr:** Analogous to the previous case.
- $A = \tau_1 \times \tau_2$. In this case $v\ \beta \simeq^{\mathcal{A}}_{\tau_1\times\tau_2} v'$ must have been derived by **eqPair**. Hence there are v_1, v_2, v_1', v_2' such that
  - $v = (v_1, v_2)$,
  - $v' = (v_1', v_2')$,
  - $v_1\ \beta \simeq^{\mathcal{A}}_{\tau_1} v_1'$
  - $v_2\ \beta \simeq^{\mathcal{A}}_{\tau_2} v_2'$

  Hence by induction
  - $v_1'\ \beta^{-1} \simeq^{\mathcal{A}}_{\tau_1} v_1$ and
  - $v_2'\ \beta^{-1} \simeq^{\mathcal{A}}_{\tau_2} v_2$.

  We get $(v_1', v_2')\ \beta^{-1} \simeq^{\mathcal{A}}_{\tau_1\times\tau_2} (v_1'', v_2'')$ by **eqPair**.
- $A = \mathtt{ref}\ \tau$. In this case $v\ \beta \simeq^{\mathcal{A}}_{\mathtt{ref}\ \tau} v'$ must have been derived by **eqRef**. By inversion there are l, l' such that
  - $v = l$,
  - $v' = l'$
  - $(l, l') \in \beta$ and

  We have to show $l'\ \beta^{-1} \simeq^{\mathcal{A}}_{\mathtt{ref}\ \tau} l$. By **eqRef** it suffice to show $(l', l) \in \beta^{-1}$. This is clearly the case.

□

Lemma 10.25. If $(v, v', (\theta, \theta', \beta), m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$ and $\mathtt{firstorder}(\tau)$, then $(v', v, (\theta', \theta, \beta^{-1}), m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$.

Proof. By Lemma 8.44 we have $v \overset{\beta}{\simeq}{}^{\mathcal{A}}_{\tau} v'$. By Lemma 10.24 we have $v' \overset{\beta^{-1}}{\simeq}{}^{\mathcal{A}}_{\tau} v$. We also have $(v, \theta, m) \in \lceil\tau\rceil_{\mathcal{V}}$ and $(v', \theta', m) \in \lceil\tau\rceil_{\mathcal{V}}$ by Lemma 8.22. Hence by Lemma 8.43 we get $(v', v, (\theta', \theta, \beta^{-1}), m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. □

Lemma 10.26. If $v \overset{\beta}{\simeq}{}^{\mathcal{A}}_{\tau} v'$ and $v' \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{\tau} v''$, then $v \overset{\beta' \circ \beta}{\simeq}{}^{\mathcal{A}}_{\tau} v''$ and if $v \overset{\beta}{\simeq}{}^{\mathcal{A}}_{A} v'$ and $v' \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{A} v''$, then $v \overset{\beta' \circ \beta}{\simeq}{}^{\mathcal{A}}_{A} v''$.

Proof. By mutual induction on τ and A.

- $\tau = A^{\mathfrak{p}}$: There derivation could have happened with one of these two rules:
  1. **eqHigh**. In this case $\mathfrak{p} \not\sqsubseteq \mathcal{A}$. We get $v \overset{\beta' \circ \beta}{\simeq}{}^{\mathcal{A}}_{A^{\mathfrak{p}}} v''$ by **eqHigh**.
  2. **eqLow**. In this case $\mathfrak{p} \sqsubseteq \mathcal{A}$ and $v \overset{\beta}{\simeq}{}^{\mathcal{A}}_{A} v'$. We do inversion on $v' \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{A^{\mathfrak{p}}} v''$. Because $\mathfrak{p} \sqsubseteq \mathcal{A}$ the only applicable rule is **eqLow**. Hence $v' \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{A} v''$. We get $v \overset{\beta' \circ \beta}{\simeq}{}^{\mathcal{A}}_{A} v''$ by induction. We get the claim by **eqLow**.
- $A = \mathtt{unit}$. In this case both $v \overset{\beta}{\simeq}{}^{\mathcal{A}}_{\mathtt{unit}} v'$ and $v' \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{\mathtt{unit}} v''$ must have been derived by **eqUnit**. By inversion we get $v = v' = v'' = ()$. We get the claim by **eqUnit**.
- $A = \mathcal{N}$. In this case both $v \overset{\beta}{\simeq}{}^{\mathcal{A}}_{\mathcal{N}} v'$ and $v' \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{\mathcal{N}} v''$ must have been derived by **eqNat**. By inversion we get $v = v' = v'' = n$. We get the claim by **eqNat**.
- $A = \tau_1 + \tau_2$. In this case there are two rules with which $v \overset{\beta}{\simeq}{}^{\mathcal{A}}_{\mathcal{N}} v'$ could have been derived:
  1. **eqInl**: In this case there are v_0, v_0' such that
     - $v = \mathtt{inl}\ v_0$,
     - $v' = \mathtt{inl}\ v_0'$ and
     - $v_0 \overset{\beta}{\simeq}{}^{\mathcal{A}}_{\tau_1} v_0'$.

     We do inversion on $\mathtt{inl}\ v_0 \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{\tau_1+\tau_2} v''$. The only applicable rule is **eqInl**. Hence there is also a v_0'' such that
     - $v'' = \mathtt{inl}\ v_0''$ and
     - $v_0' \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{\tau_1} v_0''$.

     We get $v_0 \overset{\beta' \circ \beta}{\simeq}{}^{\mathcal{A}}_{\tau_1} v_0''$ by induction. The claim follows by **eqInl**.
  2. **eqInr:** Analogous to the previous case.
- $A = \tau_1 \times \tau_2$. In this case both $v \overset{\beta}{\simeq}{}^{\mathcal{A}}_{\tau_1 \times \tau_2} v'$ and $v' \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{\tau_1 \times \tau_2} v''$ must have been derived by **eqPair**. Hence there are $v_1, v_2, v_1', v_2', v_1'', v_2''$ such that
  - $v = (v_1, v_2)$,
  - $v' = (v_1', v_2')$,
  - $v'' = (v_1', v_2')$,
  - $v_1 \overset{\beta}{\simeq}{}^{\mathcal{A}}_{\tau_1} v_1'$
  - $v_2 \overset{\beta}{\simeq}{}^{\mathcal{A}}_{\tau_2} v_2'$
  - $v_1' \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{\tau_1} v_1''$
  - $v_2' \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{\tau_2} v_2''$

  Hence by induction
  - $v_1 \overset{\beta' \circ \beta}{\simeq}{}^{\mathcal{A}}_{\tau_1} v_1''$ and
  - $v_2 \overset{\beta' \circ \beta}{\simeq}{}^{\mathcal{A}}_{\tau_2} v_2''$.

  We get $(v_1, v_2) \overset{\beta' \circ \beta}{\simeq}{}^{\mathcal{A}}_{\tau_1 \times \tau_2} (v_1'', v_2'')$ by **eqPair**.
- $A = \mathtt{ref}\ \tau$. In this case both $v \overset{\beta}{\simeq}{}^{\mathcal{A}}_{\mathtt{ref}\ \tau} v'$ and $v' \overset{\beta'}{\simeq}{}^{\mathcal{A}}_{\mathtt{ref}\ \tau} v''$ must have been derived by **eqRef**. By inversion there are l, l', l'' such that
  - $v = l$,
  - $v' = l'$

– $\nu'' = \mathfrak{l}''$,
– $(\mathfrak{l}, \mathfrak{l}') \in \beta$ and
– $(\mathfrak{l}', \mathfrak{l}'') \in \beta'$.

We have to show $\mathfrak{l}\ {}^{\beta'\circ\beta}\simeq^{\mathcal{A}}_{\mathtt{ref}\ \tau}\ \mathfrak{l}''$. By **eqRef** it suffice to show $(\mathfrak{l}, \mathfrak{l}'') \in \beta' \circ \beta$. This is clearly the case.

□

Lemma 10.27. If $\mathtt{firstorder}(\tau)$, $(\nu, \nu', (\theta, \theta', \beta), \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$ and $(\nu', \nu'', (\theta'', \theta''', \beta'), \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$, then $(\nu, \nu'', (\theta, \theta''', \beta' \circ \beta), \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$.

Proof. By Lemma 8.44 we have $\nu\ {}^{\beta}\simeq^{\mathcal{A}}_{\tau}\ \nu'$ and $\nu'\ {}^{\beta'}\simeq^{\mathcal{A}}_{\tau}\ \nu''$. Hence by Lemma 10.26 $\nu\ {}^{\beta'\circ\beta}\simeq^{\mathcal{A}}_{\tau}\ \nu''$. We also have $(\nu, \theta, \mathfrak{m}) \in \lceil\tau\rceil_{\mathcal{V}}$ and $(\nu'', \theta''', \mathfrak{m}) \in \lceil\tau\rceil_{\mathcal{V}}$ by Lemma 8.22. Hence $(\nu, \nu'', (\theta, \theta''', \beta' \circ \beta), \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$ by Lemma 8.43. □

Lemma 10.28. If we consider only `firstorder` observations. Then

1. If $\omega \approx^{\mathcal{A}}_{((\theta,\theta',\beta),\mathfrak{m})} \omega'$, then $\omega' \approx^{\mathcal{A}}_{((\theta',\theta,\beta^{-1}),\mathfrak{m})} \omega$.
2. If $\vec{\omega} \approx^{\mathcal{A}}_{((\theta,\theta',\beta),\mathfrak{m})} \vec{\omega'}$, then $\vec{\omega'} \approx^{\mathcal{A}}_{((\theta',\theta,\beta^{-1}),\mathfrak{m})} \vec{\omega}$.

Proof. 1. We do case analysis on the derivation of $\omega \approx^{\mathcal{A}}_{((\theta,\theta',\beta),\mathfrak{m})} \omega'$.

(a) **refl**: In this case $\omega = \omega'$ and ω or ω' do not have the form $\mathfrak{l}_\tau(\nu)$. We get the goal by **refl**.

(b) **extend-τ**: In this case
- $\omega = \mathfrak{l}_\tau(\nu)$,
- $\omega' = \mathfrak{l}'_\tau(\nu')$,
- $(\mathfrak{l}, \mathfrak{l}') \in \beta$, and
- $(\nu, \nu', (\theta, \theta', \beta), \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$.

By **extend-τ** it suffices to show
- $(\mathfrak{l}', \mathfrak{l}) \in \beta^{-1}$. This follows directly from $(\mathfrak{l}, \mathfrak{l}') \in \beta$.
- $(\nu', \nu, (\theta', \theta, \beta^{-1}), \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. We get this by Lemma 10.25 because τ is firstorder by assumption.

(c) **high**:In this case by inversion
- $\mathtt{pol}(\omega) \not\sqsubseteq \mathcal{A}$.
- $\mathtt{pol}(\omega') \not\sqsubseteq \mathcal{A}$.

The claim follows by **high**.

2. By induction on the length $\mathfrak{n}$ of $\vec{\omega}$.

Base case: $\mathfrak{n} = 0$. In this case there is nothing to show. Induction case: $\mathfrak{n} > 0$. In this case $\vec{\omega} = \omega_0, \vec{\omega_{\mathfrak{tl}}}$ for some observation ω and trace $\vec{\omega_{\mathfrak{tl}}}$. Because $\vec{\omega} \approx^{\mathcal{A}}_{\beta} \vec{\omega'}$ we know that there are ω' and $\vec{\omega'_{\mathfrak{tl}}}$ such that $\vec{\omega'} = \omega', \vec{\omega'_{\mathfrak{tl}}}$ and $\omega \approx^{\mathcal{A}}_{\beta} \omega'$ and $\vec{\omega_{\mathfrak{tl}}} \approx^{\mathcal{A}}_{\beta} \vec{\omega'_{\mathfrak{tl}}}$. To show the goal it suffices to show
- $\omega' \approx^{\mathcal{A}}_{\beta^{-1}} \omega$. We get this by 1.
- $\vec{\omega'_{\mathfrak{tl}}} \approx^{\mathcal{A}}_{\beta^{-1}} \vec{\omega_{\mathfrak{tl}}}$. We get this by induction.

□

Lemma 10.29. If we consider only `firstorder` observations, then

1. If $\omega \approx^{\mathcal{A}}_{((\theta,\theta',\beta),\mathfrak{m})} \omega'$ and $\omega' \approx^{\mathcal{A}}_{((\theta'',\theta''',\beta'),\mathfrak{m})} \omega''$, then $\omega \approx^{\mathcal{A}}_{[((\theta,\theta''',\beta'\circ\beta),\mathfrak{m})} \omega''$.
2. If $\vec{\omega} \approx^{\mathcal{A}}_{((\theta,\theta',\beta),\mathfrak{m})} \vec{\omega'}$ and $\vec{\omega'} \approx^{\mathcal{A}}_{((\theta'',\theta''',\beta'),\mathfrak{m})} \vec{\omega''}$, then $\vec{\omega} \approx^{\mathcal{A}}_{[((\theta,\theta''',\beta'\circ\beta),\mathfrak{m})} \vec{\omega''}$.

Proof. 1. We do case analysis on the derivation of $\omega \approx^{\mathcal{A}}_{((\theta,\theta',\beta),\mathfrak{m})} \omega'$.

(a) **refl**: In this case $\omega = \omega'$ and ω or ω' do not have the form $\mathfrak{l}_\mathfrak{p}(\nu)$ or $\mathfrak{l}_\tau(\nu)$. Hence they must have one of the following forms:

i. $\mathtt{open}(\sigma)$.

In this case we have to show $\mathtt{open}(\sigma) \approx^{\mathcal{A}}_{((\theta,\theta''',\beta'\circ\beta),\mathfrak{m})} \omega''$. We already know

- $\mathtt{open}(\sigma) \approx^{\mathcal{A}}_{((\theta'',\theta''',\beta'),\mathfrak{m})} \omega''$.

This could only have been derived using **refl** or **high**. In both cases we can derived the goal with the same rule.

ii. $\mathtt{close}(\sigma)$. Analogous to the previous case.

iii. $\mathtt{unopen}(\sigma)$. Analogous to the previous cases.

iv. $\mathtt{unclose}(\sigma)$. Analogous to the previous cases.

(b) **extend-τ**: In this case

- $\omega = \mathfrak{l}_\tau(\nu)$,
- $\omega' = \mathfrak{l}'_\tau(\nu')$,
- $(\mathfrak{l},\mathfrak{l}') \in \beta$, and
- $(\nu,\nu',(\theta,\theta',\beta),\mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_V$

We do case analysis on the derivation of $\mathfrak{l}'_\tau(\nu') \approx^{\mathcal{A}}_{((\theta'',\theta''',\beta'),\mathfrak{m})} \omega''$.

i. **refl**: This rule is not applicable because $\mathfrak{l}'_\tau(\nu')$ violates a premiss of the rule.

ii. **extend-τ**: In this case there are $\mathfrak{l}''$ and ν'' such that

- $\omega'' = \mathfrak{l}''_\tau(\nu'')$,
- $(\mathfrak{l}',\mathfrak{l}'') \in \beta'$, and
- $(\nu',\nu'',(\theta'',\theta''',\beta'),\mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_V$

We have to show $\mathfrak{l}_\tau(\nu) \approx^{\mathcal{A}}_{[((\theta,\theta''',\beta'\circ\beta),\mathfrak{m})} \mathfrak{l}''_\tau(\nu'')$. By **extend-$\tau$** it suffices to show

- $(\mathfrak{l},\mathfrak{l}'') \in \beta'\circ\beta$. This is the case because $(\mathfrak{l},\mathfrak{l}') \in \beta$ and $(\mathfrak{l}',\mathfrak{l}'') \in \beta'$.
- $(\nu,\nu'',(\theta,\theta''',\beta'\circ\beta),\mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_V$. We get this by Lemma 10.27 because by assumption $\mathtt{firstorder}(\tau)$.

iii. **high**: In this case by inversion

- $\mathtt{pol}(\tau) = \mathtt{pol}(\mathfrak{l}'_\tau(\nu')) \not\sqsubseteq \mathcal{A}$.
- $\mathtt{pol}(\omega'') \not\sqsubseteq \mathcal{A}$.

We get the goal by **high**.

(c) **high**:In this case by inversion

- $\mathtt{pol}(\omega) \not\sqsubseteq \mathcal{A}$.
- $\mathtt{pol}(\omega') \not\sqsubseteq \mathcal{A}$.

We do case analysis on the derivation of $\omega' \approx^{\mathcal{A}}_{((\theta'',\theta''',\beta'),\mathfrak{m})} \omega''$.

i. **refl**. In this case $\omega'' = \omega'$. In particular $\mathtt{pol}(\omega'') \not\sqsubseteq \mathcal{A}$. We get the goal by **high**.

ii. **extend-τ**. By inversion there are $\mathfrak{l}',\mathfrak{l}'',\tau,\nu',\nu''$ such that

- $\omega' = \mathfrak{l}'_\tau(\nu')$ and
- $\omega'' = \mathfrak{l}''_\tau(\nu'')$.

Because $\mathtt{pol}(\omega') = \mathtt{pol}(\tau)$ we have $\tau \not\sqsubseteq \mathcal{A}$. Hence we get the goal by **high**.

iii. **high**: In this case by inversion also

- $\mathtt{pol}(\omega'') \not\sqsubseteq \mathcal{A}$.

We get the goal by **high**.

2. By induction on the length $\mathfrak{n}$ of $\vec{\omega}$.

Base case: $\mathfrak{n} = 0$. In this case there is nothing to show.

Induction case: $\mathfrak{n} > 0$. In this case $\vec{\omega} = \omega_0, \vec{\omega_{tl}}$ for some observation ω and trace $\vec{\omega_{tl}}$. Because $\vec{\omega} \approx^{\mathcal{A}}_{((\theta,\theta',\beta),\mathfrak{m})} \vec{\omega'}$ we know that there are ω' and $\vec{\omega'_{tl}}$ such that $\vec{\omega'} = \omega', \vec{\omega'_{tl}}$ and $\omega \approx^{\mathcal{A}}_{((\theta,\theta',\beta),\mathfrak{m})} \omega'$ and $\vec{\omega_{tl}} \approx^{\mathcal{A}}_{((\theta,\theta',\beta),\mathfrak{m})} \vec{\omega'_{tl}}$. By the same reasoning we get that there are ω'' and $\vec{\omega''_{tl}}$ such that $\vec{\omega''} = \omega'', \vec{\omega''_{tl}}$ and $\omega' \approx^{\mathcal{A}}_{((\theta'',\theta''',\beta'),\mathfrak{m})} \omega''$ and $\vec{\omega'_{tl}} \approx^{\mathcal{A}}_{((\theta'',\theta''',\beta'),\mathfrak{m})} \vec{\omega''_{tl}}$. To show the goal it suffices to show

- $\omega \approx^{\mathcal{A}}_{[((\theta,\theta''',\beta'\circ\beta),\mathfrak{m})} \omega''$. We get this by 1.
- $\vec{\omega_{tl}} \approx^{\mathcal{A}}_{[((\theta,\theta''',\beta'\circ\beta),\mathfrak{m})} \vec{\omega''_{tl}}$. We get this by induction.

□

Lemma 10.30. If we only consider firstorder observations and $\forall \mathfrak{m}, \vec{\omega} \approx^{\mathcal{A}}_{(W,\mathfrak{m})} \vec{\omega'}$ and $W \sqsupseteq (\theta_L, \theta_L, \mathrm{id}_{\mathrm{dom}(L)})$, then $k_{\mathcal{A}}(e; \vec{\omega}; L; \Sigma) = k_{\mathcal{A}}(e; \vec{\omega'}; L; \Sigma)$.

Proof. $\subseteq$: Let $S \in k_{\mathcal{A}}(e, \vec{\omega}, L, \Sigma)$. Then there are $e', S', \Sigma', \vec{\omega''}$ and W' such that

- $S \approx_{\mathcal{A}} L$,
- $e, S, \Sigma \Longrightarrow^{\vec{\omega''}}_{\mathcal{A}} e', S', \Sigma'$
- $W' \sqsupseteq (\theta_S, \theta_S, \mathrm{id}_{\mathrm{dom}(L)})$
- $\forall \mathfrak{m}, \vec{\omega} \approx^{\mathcal{A}}_{(W',\mathfrak{m})} \vec{\omega''}$.

W has the form (θ, θ', β) and W' has the form $(\theta'', \theta''', \beta')$
It suffice to show

- $S \approx_{\mathcal{A}} L$. We already know that.
- $e, S, \Sigma \Longrightarrow^{\vec{\omega''}}_{\mathcal{A}} e', S', \Sigma'$. We already know that.
- $(\theta', \theta''', \beta' \circ \beta^{-1}) \sqsupseteq (\theta_L, \theta_L, \mathrm{id}_{\mathrm{dom}(L)})$. This involves showing:
  - $\theta' \sqsupseteq \theta_L$. We already know this.
  - $\theta''' \sqsupseteq \theta_L$. We already know this.
  - $\beta' \circ \beta^{-1} \supseteq \mathrm{id}_{\mathrm{dom}(L)}$. Let $(l, l) \in \mathrm{id}_{\mathrm{dom}(L)}$. Then because $\beta \supseteq \mathrm{id}_{\mathrm{dom}(L)}$ and $\beta' \supseteq \mathrm{id}_{\mathrm{dom}(L)}$ we have
    - $(l, l) \in \beta$
    - $(l, l) \in \beta'$

    Hence also $(l, l) \in \beta^{-1}$ and therefore $(l, l) \in \beta' \circ \beta^{-1}$.
- $\forall \mathfrak{m}, \vec{\omega'} \approx^{\mathcal{A}}_{(\theta', \theta''', \beta' \circ \beta^{-1}), \mathfrak{m}} \vec{\omega''}$. Let $\mathfrak{m} \in \mathbb{N}$. By Lemma 10.28 we have $\vec{\omega'} \approx^{\mathcal{A}}_{((\theta', \theta, \beta^{-1}), \mathfrak{m})} \vec{\omega}$. By Lemma 10.29 this gives us the goal.

$\supseteq$: Let $S \in k_{\mathcal{A}}(e, \vec{\omega'}, L, \Sigma)$. Then there are $e', S', \Sigma', \vec{\omega''}$ and W' such that

- $S \approx_{\mathcal{A}} L$,
- $e, S, \Sigma \Longrightarrow^{\vec{\omega''}}_{\mathcal{A}} e', S', \Sigma'$
- $W' \sqsupseteq (\theta_L, \theta_L, \mathrm{id}_{\mathrm{dom}(L)})$
- $\forall \mathfrak{m}, \vec{\omega'} \approx^{\mathcal{A}}_{(W',\mathfrak{m})} \vec{\omega''}$.

W has the form (θ, θ', β) and W' has the form $(\theta'', \theta''', \beta')$. It suffice to show

- $S \approx_{\mathcal{A}} L$. We already know that.
- $e, S, \Sigma \Longrightarrow^{\vec{\omega''}}_{\mathcal{A}} e', S', \Sigma'$. We already know that.
- $(\theta, \theta''', \beta' \circ \beta) \sqsupseteq (\theta_S, \theta_S, \mathrm{id}_{\mathrm{dom}(L)})$. This involves showing:
  - $\theta \sqsupseteq \theta_L$. We already know this.
  - $\theta''' \sqsupseteq \theta_L$. We already know this.
  - $\beta' \circ \beta \supseteq \mathrm{id}_{\mathrm{dom}(L)}$. Let $(l, l) \in \mathrm{id}_{\mathrm{dom}(L)}$. Then because $\beta \supseteq \mathrm{id}_{\mathrm{dom}(L)}$ and $\beta' \supseteq \mathrm{id}_{\mathrm{dom}(L)}$ we have
    - $(l, l) \in \beta$
    - $(l, l) \in \beta'$

    Hence also $(l, l) \in \beta' \circ \beta$.
- $\forall \mathfrak{m}, \vec{\omega} \approx^{\mathcal{A}}_{((\theta, \theta''', \beta' \circ \beta), \mathfrak{m})} \vec{\omega''}$. We get this by Lemma 10.29.

□

Lemma 10.31 (Low equivalence symmetric)**.** If S, S' are firstorder states and $S \approx_{\mathcal{A}} S'$, then $S' \approx_{\mathcal{A}} S$.

Proof. Let S, S' such that $S \approx_{\mathcal{A}} S'$. Then in particular

- $\mathrm{dom}(S_{\mathcal{A}}) = \mathrm{dom}(S'_{\mathcal{A}})$
- $\forall m.(S_{\mathcal{A}}, S'_{\mathcal{A}}, m) \overset{\mathcal{A}}{\triangleright} (\theta_{S_{\mathcal{A}}}, \theta_{S'_{\mathcal{A}}}, \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})})$.

We have to show

1. $\mathrm{dom}(S'_{\mathcal{A}}) = \mathrm{dom}(S_{\mathcal{A}})$. We get this by symmetry of equality.
2. $\forall m.(S'_{\mathcal{A}}, S_{\mathcal{A}}, m) \overset{\mathcal{A}}{\triangleright} (\theta_{S'_{\mathcal{A}}}, \theta_{S_{\mathcal{A}}}, \mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})})$. Let $m \in \mathbb{N}$. We specialize our second assumption with m. By unfolding the definition (and using the fact that two location in the identity relatio are identical), this gives us
   - $(S_{\mathcal{A}}, m) \triangleright \theta_{S_{\mathcal{A}}}$
   - $(S'_{\mathcal{A}}, m) \triangleright \theta_{S'_{\mathcal{A}}}$
   - $\mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})} \subseteq \theta_{S_{\mathcal{A}}} \times \theta_{S'_{\mathcal{A}}}$.
   - $\forall (l, l) \in \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}.\theta_{S_{\mathcal{A}}} = \theta_{S'_{\mathcal{A}}} \wedge (S_{\mathcal{A}}(l), S'_{\mathcal{A}}(l), (\theta_{S_{\mathcal{A}}}, \theta_{S'_{\mathcal{A}}}, \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}), m) \in [\![\theta_{S_{\mathcal{A}}}(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$

   We need to show the following:

   (a) $(S', m) \triangleright \theta_{S'_{\mathcal{A}}}$. We already know this.

   (b) $(S, m) \triangleright \theta_{S_{\mathcal{A}}}$. We already know this.

   (c) $\mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})} \subseteq \theta_{S'_{\mathcal{A}}} \times \theta_{S_{\mathcal{A}}}$. Let $(l, l) \in \mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})}$. Since $\mathrm{dom}(S_{\mathcal{A}}) = \mathrm{dom}(S'_{\mathcal{A}})$, this mean
   - $(l, l) \in \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}$.

   From $\mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})} \subseteq \theta_{S_{\mathcal{A}}} \times \theta_{S'_{\mathcal{A}}}$ we can further deduce
   - $(l, l) \in \theta_{S_{\mathcal{A}}} \times \theta_{S'_{\mathcal{A}}}$.

   Hence in particular
   - $l \in \theta_{S_{\mathcal{A}}}$ and
   - $l \in \theta_{S'_{\mathcal{A}}}$.

   $(l, l) \in \theta_{S'_{\mathcal{A}}} \times \theta_{S_{\mathcal{A}}}$, which is what we need to show here, follows directly from these two facts.

   (d) $\forall (l, l) \in \mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})}.\theta_{S'_{\mathcal{A}}} = \theta_{S_{\mathcal{A}}} \wedge (S'_{\mathcal{A}}(l), S_{\mathcal{A}}(l), (\theta_{S'_{\mathcal{A}}}, \theta_{S_{\mathcal{A}}}, \mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})}), m) \in [\![\theta_{S'_{\mathcal{A}}}(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$. Let $(l, l) \in \mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})}$. Then because $\mathrm{dom}(S'_{\mathcal{A}}) = \mathrm{dom}(S_{\mathcal{A}})$, we also have
   - $(l, l) \in \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}$.

   This gives us
   - $\theta_{S_{\mathcal{A}}} = \theta_{S'_{\mathcal{A}}}$ and
   - $(S_{\mathcal{A}}(l), S'_{\mathcal{A}}(l), (\theta_{S_{\mathcal{A}}}, \theta_{S'_{\mathcal{A}}}, \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}), m) \in [\![\theta_{S_{\mathcal{A}}}(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$.

   We have to show

   i. $\theta_{S'_{\mathcal{A}}} = \theta_{S_{\mathcal{A}}}$. We get this by symmetry of equality.

   ii. $(S'_{\mathcal{A}}(l), S_{\mathcal{A}}(l), (\theta_{S'_{\mathcal{A}}}, \theta_{S_{\mathcal{A}}}, \mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})}), m) \in [\![\theta_{S'_{\mathcal{A}}}(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$. From $(S_{\mathcal{A}}, m) \triangleright \theta_{S_{\mathcal{A}}}$, we get that
   - $\theta_{S_{\mathcal{A}}}(l) = \mathrm{type}(S_{\mathcal{A}}, l)$.

   Because S and therefore also $S_{\mathcal{A}}$ is firstorder, this means
   - $\mathtt{firstorder}(\theta_{S_{\mathcal{A}}}(l))$

   This allows us to use Lemma 10.25 to get
   - $(S'_{\mathcal{A}}(l), S_{\mathcal{A}}(l), (\theta_{S'_{\mathcal{A}}}, \theta_{S_{\mathcal{A}}}, \mathtt{id}^{-1}_{\mathrm{dom}(S_{\mathcal{A}})}), m) \in [\![\theta_{S_{\mathcal{A}}}(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$.

   But since the inverse of the identity relation is the identity relation and because $\mathrm{dom}(S_{\mathcal{A}}) = \mathrm{dom}(S'_{\mathcal{A}})$, this gives us
   - $(S'_{\mathcal{A}}(l), S_{\mathcal{A}}(l), (\theta_{S'_{\mathcal{A}}}, \theta_{S_{\mathcal{A}}}, \mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})}), m) \in [\![\theta_{S_{\mathcal{A}}}(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$.

   The goal follows from $\theta_{S_{\mathcal{A}}} = \theta_{S'_{\mathcal{A}}}$.

□

Lemma 10.32 (Low equivalence transitive)**.**

1. If S, S', S'' are firstorder states and $S \approx_{\mathcal{A}} S'$ and $S' \approx_{\mathcal{A}} S''$, then $S \approx_{\mathcal{A}} S''$.
2. If $\Sigma \approx_{\mathcal{A}} \Sigma'$ and $\Sigma' \approx_{\mathcal{A}} \Sigma''$, then $\Sigma \approx_{\mathcal{A}} \Sigma''$.

Proof. 1. Because of $S \approx_{\mathcal{A}} S'$ and $S' \approx_{\mathcal{A}} S''$ we have

- $\mathtt{dom}(S_{\mathcal{A}}) = \mathtt{dom}(S'_{\mathcal{A}}) = \mathtt{dom}(S''_{\mathcal{A}})$.
- $\forall \mathfrak{m}.\ (S_{\mathcal{A}}, S'_{\mathcal{A}}, \mathfrak{m}) \overset{\mathcal{A}}{\triangleright} (\theta_{S_{\mathcal{A}}}, \theta_{S'_{\mathcal{A}}, \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}})$.
- $\forall \mathfrak{m}.\ (S'_{\mathcal{A}}, S''_{\mathcal{A}}, \mathfrak{m}) \overset{\mathcal{A}}{\triangleright} (\theta_{S'_{\mathcal{A}}}, \theta_{S''_{\mathcal{A}}, \mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})}})$.

We have to show:

- $\mathtt{dom}(S_{\mathcal{A}}) = \mathtt{dom}(S''_{\mathcal{A}})$. We already know this.
- $\forall \mathfrak{m}.(S, S'', \mathfrak{m}) \overset{\mathcal{A}}{\triangleright} (\theta_{S_{\mathcal{A}}}, \theta_{S''_{\mathcal{A}}, \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}})$. Let $\mathfrak{m} \in \mathbb{N}$. By insantiating our assumptions with $\mathfrak{m}$ and unfolding the definition of $\overset{\mathcal{A}}{\triangleright}$, we get:
  - $\mathrm{dom}(\theta_{S_{\mathcal{A}}}) \subseteq \mathrm{dom}(S_{\mathcal{A}})$.
  - $\mathrm{dom}(\theta_{S'_{\mathcal{A}}}) \subseteq \mathrm{dom}(S'_{\mathcal{A}})$.
  - $\forall \mathfrak{l} \in \mathrm{dom}(\theta_{S_{\mathcal{A}}}).\ \theta_{S_{\mathcal{A}}}(\mathfrak{l}) = \mathrm{type}(S_{\mathcal{A}}, \mathfrak{l})$.
  - $\forall \mathfrak{l} \in \mathrm{dom}(\theta_{S'_{\mathcal{A}}}).\ \theta_{S'_{\mathcal{A}}}(\mathfrak{l}) = \mathrm{type}(S'_{\mathcal{A}}, \mathfrak{l})$.
  - $\mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})} \subseteq \mathrm{dom}(\theta_{S_{\mathcal{A}}}) \times \mathrm{dom}(\theta_{S'_{\mathcal{A}}})$.
  - $\forall (\mathfrak{l}_1, \mathfrak{l}_2) \in \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}.\theta_{S_{\mathcal{A}}}(\mathfrak{l}_1) = \theta_{S'_{\mathcal{A}}}(\mathfrak{l}_2) \wedge (S_{\mathcal{A}}(\mathfrak{l}_1), S'_{\mathcal{A}}(\mathfrak{l}_2), (\theta_{S_{\mathcal{A}}}, \theta_{S'_{\mathcal{A}}, \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}}), \mathfrak{m}) \in [\![\theta_{S_{\mathcal{A}}}(\mathfrak{l}_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$.
  - $\mathrm{dom}(\theta_{S''_{\mathcal{A}}}) \subseteq \mathrm{dom}(S''_{\mathcal{A}})$.
  - $\forall \mathfrak{l} \in \mathrm{dom}(\theta_{S''_{\mathcal{A}}}).\ \theta_{S''_{\mathcal{A}}}(\mathfrak{l}) = \mathrm{type}(S''_{\mathcal{A}}, \mathfrak{l})$.
  - $\mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})} \subseteq \mathrm{dom}(\theta_{S'_{\mathcal{A}}}) \times \mathrm{dom}(\theta_{S''_{\mathcal{A}}})$.
  - $\forall (\mathfrak{l}_1, \mathfrak{l}_2) \in \mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})}.\theta_{S'_{\mathcal{A}}}(\mathfrak{l}_1) = \theta_{S''_{\mathcal{A}}}(\mathfrak{l}_2) \wedge (S'_{\mathcal{A}}(\mathfrak{l}_1), S''_{\mathcal{A}}(\mathfrak{l}_2), (\theta_{S'_{\mathcal{A}}}, \theta_{S''_{\mathcal{A}}, \mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})}}), \mathfrak{m}) \in [\![\theta_{S'_{\mathcal{A}}}(\mathfrak{l}_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$.

  From this we have to show:
  - $\mathrm{dom}(\theta_{S_{\mathcal{A}}}) \subseteq \mathrm{dom}(S_{\mathcal{A}})$. We already know this.
  - $\mathrm{dom}(\theta_{S''_{\mathcal{A}}}) \subseteq \mathrm{dom}(S''_{\mathcal{A}})$. We already know this.
  - $\forall \mathfrak{l} \in \mathrm{dom}(\theta_{S_{\mathcal{A}}}).\ \theta_{S_{\mathcal{A}}}(\mathfrak{l}) = \mathrm{type}(S_{\mathcal{A}}, \mathfrak{l})$. We already know this.
  - $\forall \mathfrak{l} \in \mathrm{dom}(\theta_{S''_{\mathcal{A}}}).\ \theta_{S''_{\mathcal{A}}}(\mathfrak{l}) = \mathrm{type}(S''_{\mathcal{A}}, \mathfrak{l})$. We already know this.
  - $\mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})} \subseteq \mathrm{dom}(\theta_{S_{\mathcal{A}}}) \times \mathrm{dom}(\theta_{S''_{\mathcal{A}}})$. Let $(\mathfrak{l}, \mathfrak{l}) \in \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}$. Then, because we know by assumption that $\mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})} \subseteq \mathrm{dom}(\theta_{S_{\mathcal{A}}}) \times \mathrm{dom}(\theta_{S'_{\mathcal{A}}})$, we have
    - $\mathfrak{l} \in \mathrm{dom}(\theta_{S_{\mathcal{A}}})$
    - $\mathfrak{l} \in \mathrm{dom}(\theta_{S'_{\mathcal{A}}})$

    Because $\mathrm{dom}(\theta_{S'_{\mathcal{A}}}) \subseteq \mathrm{dom}(S'_{\mathcal{A}})$, we also have
    - $(\mathfrak{l}, \mathfrak{l}) \in \mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})}$.

    From $\mathtt{id}_{\mathrm{dom}(S'_{\mathcal{A}})} \subseteq \mathrm{dom}(\theta_{S'_{\mathcal{A}}}) \times \mathrm{dom}(\theta_{S''_{\mathcal{A}}})$ we can further deduce that
    - $\mathfrak{l} \in \mathrm{dom}(\theta_{S''_{\mathcal{A}}})$.

    Since both $\mathfrak{l} \in \mathrm{dom}(\theta_{S_{\mathcal{A}}})$ and $\mathfrak{l} \in \mathrm{dom}(\theta_{S''_{\mathcal{A}}})$ we have
    - $(\mathfrak{l}, \mathfrak{l}) \in \mathrm{dom}(\theta_{S_{\mathcal{A}}}) \times \mathrm{dom}(\theta_{S''_{\mathcal{A}}})$.

    This is what we needed to show.
  - $\forall (\mathfrak{l}_1, \mathfrak{l}_2) \in \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}.\theta_{S_{\mathcal{A}}}(\mathfrak{l}_1) = \theta_{S''_{\mathcal{A}}}(\mathfrak{l}_2) \wedge (S_{\mathcal{A}}(\mathfrak{l}_1), S''_{\mathcal{A}}(\mathfrak{l}_2), (\theta_{S_{\mathcal{A}}}, \theta_{S''_{\mathcal{A}}, \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}}), \mathfrak{m}) \in [\![\theta_{S_{\mathcal{A}}}(\mathfrak{l}_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$.
    Let $(\mathfrak{l}_1, \mathfrak{l}_2) \in \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}$. Then
    - $\mathfrak{l}_1 = \mathfrak{l}_2$

    by the definition of the identity relation. We have to show
    (a) $\theta_{S_{\mathcal{A}}}(\mathfrak{l}_1) = \theta_{S''_{\mathcal{A}}}(\mathfrak{l}_2)$. Since $\mathfrak{l}_1 = \mathfrak{l}_2$, this is equivalent to showing $\theta_{S_{\mathcal{A}}}(\mathfrak{l}_1) = \theta_{S''_{\mathcal{A}}}(\mathfrak{l}_1)$. Since $(\mathfrak{l}_1, \mathfrak{l}_1) \in \mathtt{id}_{\mathrm{dom}(S_{\mathcal{A}})}$, we have that
    - $\theta_{S_{\mathcal{A}}}(\mathfrak{l}_1) = \theta_{S'_{\mathcal{A}}}(\mathfrak{l}_1)$

from one of our assumptions. Because $\mathrm{dom}(S_{\mathcal{A}}) = \mathrm{dom}(S'_{\mathcal{A}})$ and $l_1 \in \mathrm{dom}(S_{\mathcal{A}})$, we also have

* $l_1 \in \mathrm{dom}(S'_{\mathcal{A}})$.

This also gives us

* $(l_1, l_1) \in \mathrm{id}_{\mathrm{dom}(S'_{\mathcal{A}})}$.

Hence, we also get from one of our assumptions that

* $\theta_{S'_{\mathcal{A}}}(l_1) = \theta_{S''_{\mathcal{A}}}(l_1)$.

$\theta_{S_{\mathcal{A}}}(l_1) = \theta_{S''_{\mathcal{A}}}(l_1)$ follows by transitivity. This is what we needed to show.

(b) $(S_{\mathcal{A}}(l_1), S''_{\mathcal{A}}(l_2), (\theta_{S_{\mathcal{A}}}, \theta_{S''_{\mathcal{A}}, \mathrm{id}_{\mathrm{dom}(S_{\mathcal{A}})}}), m) \in [\![\theta_{S_{\mathcal{A}}}(l_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$. Because $l_1 = l_2$ it suffices to show $(S_{\mathcal{A}}(l_1), S''_{\mathcal{A}}(l_1), (\theta_{S_{\mathcal{A}}}, \theta_{S''_{\mathcal{A}}, \mathrm{id}_{\mathrm{dom}(S_{\mathcal{A}})}}), m) \in [\![\theta_{S_{\mathcal{A}}}(l_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$. From one of our assumptions we get

* $(S_{\mathcal{A}}(l_1), S'_{\mathcal{A}}(l_1), (\theta_{S_{\mathcal{A}}}, \theta_{S'_{\mathcal{A}}, \mathrm{id}_{\mathrm{dom}(S_{\mathcal{A}})}}), m) \in [\![\theta_{S_{\mathcal{A}}}(l_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$.

In the previous case we have already shown that

* $(l_1, l_1) \in \mathrm{id}_{\mathrm{dom}(S'_{\mathcal{A}})}$.

Hence we also get

* $(S'_{\mathcal{A}}(l_1), S''_{\mathcal{A}}(l_1), (\theta_{S'_{\mathcal{A}}}, \theta_{S''_{\mathcal{A}}, \mathrm{id}_{\mathrm{dom}(S'_{\mathcal{A}})}}), m) \in [\![\theta_{S'_{\mathcal{A}}}(l_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$.

Since $(l_1, l_1) \in \mathrm{id}_{\mathrm{dom}(S_{\mathcal{A}})}$, we also know

* $\theta_{S_{\mathcal{A}}}(l_1) = \theta_{S'_{\mathcal{A}}}(l_1)$.

Using this equation we get

* $(S'_{\mathcal{A}}(l_1), S''_{\mathcal{A}}(l_1), (\theta_{S'_{\mathcal{A}}}, \theta_{S''_{\mathcal{A}}, \mathrm{id}_{\mathrm{dom}(S'_{\mathcal{A}})}}), m) \in [\![\theta_{S_{\mathcal{A}}}(l_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$.

Because we know by assumption that $\mathrm{id}_{\mathrm{dom}(S_{\mathcal{A}})} \subseteq \mathrm{dom}(\theta_{S_{\mathcal{A}}}) \times \mathrm{dom}(\theta_{S'_{\mathcal{A}}})$, we also know

* $l_1 \in \mathrm{dom}(\theta_{S_{\mathcal{A}}})$.

Because $\forall l \in \mathrm{dom}(\theta_{S_{\mathcal{A}}})$. $\theta_{S_{\mathcal{A}}}(l) = \mathrm{type}(S_{\mathcal{A}}, l)$, this gives us

* $\theta_{S_{\mathcal{A}}}(l_1) = \mathrm{type}(S_{\mathcal{A}}, l_1)$.

Because by assumption S is a firstorder state and $\forall l \in \mathrm{dom}(S_{\mathcal{A}})$. $\mathrm{type}(S_{\mathcal{A}}, l) = \mathrm{type}(S, l)$, we have

* $\mathtt{firstorder}(\mathrm{type}(S_{\mathcal{A}}, l_1))$.

and therefore, exploting the equality from before, also

* $\theta_{S_{\mathcal{A}}}(l_1)$.

Hence we can use Lemma 10.27 to get

* $(S_{\mathcal{A}}(l_1), S''_{\mathcal{A}}(l_1), (\theta_{S_{\mathcal{A}}}, \theta_{S''_{\mathcal{A}}}, \mathrm{id}_{\mathrm{dom}(S'_{\mathcal{A}})} \circ \mathrm{id}_{\mathrm{dom}(S_{\mathcal{A}})}), m) \in [\![\theta_{S_{\mathcal{A}}}(l_1)]\!]^{\mathcal{A}}_{\mathcal{V}}$.

This is equivalent to the remaining subgoal because $\mathrm{id}(\mathrm{dom}(S'_{\mathcal{A}})) \circ \mathrm{id}(\mathrm{dom}(S_{\mathcal{A}})) = \mathrm{id}(\mathrm{dom}(S_{\mathcal{A}}))$ due to $\mathrm{dom}(S_{\mathcal{A}}) = \mathrm{dom}(S'_{\mathcal{A}})$.

□

Lemma 10.33. If $\Sigma \vdash e, S \xRightarrow{\vec{\omega}, \omega; \Sigma'}{}^{*}_{\mathcal{A}} e', S'$ there are e'', S'', ω' such that $\Sigma \vdash e, S \xRightarrow{\vec{\omega'}, \omega; \Sigma'}{}^{*} e'', S''$, and $\vec{\omega}, \omega = (\vec{\omega'}, \omega)_{\mathcal{A}}$.

Proof. By induction on $e, S, \Sigma \xRightarrow{\vec{\omega}; \omega}_{\mathcal{A}} e', S', \Sigma'$.

- **no-red**. In this case we would have $\vec{\omega}, \omega = \varepsilon$. This is obviously impossible. ↯.
- **inv-red**. In this case there are e'', S'' such that
  - $e, S, \Sigma \xRightarrow{\vec{\omega}; \omega}_{\mathcal{A}} e'', S'', \Sigma'$

  By induction there are e''', S''' such that $e, S, \Sigma \xRightarrow{\vec{\omega'}; \omega} e'', S'', \Sigma'$, and $\vec{\omega}, \omega = \vec{\omega'}, \omega_{\mathcal{A}}$.
- **vis-red**. In this case there are e'', S'', Σ'' such that
  - $e, S, \Sigma \xRightarrow{\vec{\omega}}_{\mathcal{A}} e'', S'', \Sigma''$
  - $e'', \Sigma, S'' \succ e', S', \omega, \Sigma'$
  - $\neg \mathit{inv}_{\mathcal{A}}(\omega)$

  By Lemma 10.15 we get two cases:

1. – $e'' = e$
   – $S'' = S$
   – $\Sigma'' = \Sigma$,
   – $\vec{\omega} = \varepsilon$

   Hence we already have $e, \Sigma, S \succ e', S', \omega, \Sigma'$. We get $e, S, \Sigma \overset{\omega}{\Rightarrow} e', S', \Sigma'$ by **single**. This suffices if $\vec{\omega}, \omega = \omega = \omega_{\mathcal{A}}$ This is the case because $\neg \mathsf{in}\nu_{\mathcal{A}}(\omega)$.

2. There are $\Sigma''', \vec{\omega'}$ such that

   – $e, S, \Sigma \overset{\vec{\omega'}}{\Rightarrow} e'', S'', \Sigma'''$ and
   – $\vec{\omega'}_{\mathcal{A}} = \vec{\omega}$.

   By **single** we get $e'', S'', \Sigma \overset{\omega}{\Rightarrow} e', S', \Sigma'$. Hence we get $e, S, \Sigma \overset{\vec{\omega'}, \omega}{\Rightarrow} e', S', \Sigma'$ by Lemma 10.12. This suffices because by Lemma 10.14 we have $(\vec{\omega'}, \omega)_{\mathcal{A}} = \vec{\omega'}_{\mathcal{A}}, \omega \overset{\vec{\omega'}_{\mathcal{A}} = \vec{\omega}}{=} \vec{\omega}, \omega$.

□

Lemma 10.34. If $S \triangleright \theta^L$ and L is low and $S \approx_{\mathcal{A}} L$, then $\theta^L \sqsupseteq \theta_L$.

Proof. Let $l \in \mathrm{dom}(\theta_L)$. By definition $l \in \mathrm{dom}(L)$. Hence also $l \in \mathrm{dom}(\theta^L)$. Then by $S \triangleright \theta^L$ we have $\theta^L(l) = \mathrm{type}(S, l)$.

Since L is low, $L = L_{\mathcal{A}}$. Hence $l \in \mathrm{dom}((_{\mathcal{A}}L))$ Since $S \approx_{\mathcal{A}} L$, this means that $\theta_L(l) = \mathrm{type}((_{\mathcal{A}}L), l) = \mathrm{type}(L, l)$.

Since $S \approx_{\mathcal{A}} L$, also $\mathrm{dom}((_{\mathcal{A}}S)) = \mathrm{dom}((_{\mathcal{A}}L)) = \mathrm{dom}(L)$. Since $l \in \mathrm{dom}(L)$ therefore in particular $l \in \mathrm{dom}((_{\mathcal{A}}S))$. Hence also $(l, l) \in \mathsf{id}(\mathrm{dom}(\theta_{S_{\mathcal{A}}}))$. Therefore by $S \approx_{\mathcal{A}} L$ we have $\mathrm{type}(S, l) = \theta_{S_{\mathcal{A}}}(l) = \theta_{L_{\mathcal{A}}}(l) = \theta_L(l) = \mathrm{type}(L, l)$. Hence $\theta_L(l) = \mathrm{type}(L, l) = \mathrm{type}(S, l) = \theta^L(l)$. □

Lemma 10.35. 1. If $\mathsf{firstorder}(\tau)$ and $(\nu, \theta, m) \in \lceil \tau \rceil_{\mathcal{V}}$, then $\forall n.\ (\nu, \theta, n) \in \lceil \tau \rceil_{\mathcal{V}}$.

2. If $\mathsf{firstorder}(A)$ and $(\nu, \theta, m) \in \lceil A \rceil_{\mathcal{V}}$, then $\forall n.\ (\nu, \theta, n) \in \lceil A \rceil_{\mathcal{V}}$.

Proof. By mutual induction on $\mathsf{firstorder}(\tau)$ and $\mathsf{firstorder}(A)$.

1. Let $n \in \mathbb{N}$. We have to show $(\nu, \theta, n) \in \lceil \tau \rceil_{\mathcal{V}}$. τ has the form A^{p} and $\mathsf{firstorder}(\tau)$ must have been derived by **FPol**. Hence by inversion

   - $\mathsf{firstorder}(A)$

   and by definition of $\lceil A^{\mathsf{p}} \rceil_{\mathcal{V}}$

   - $(\nu, \theta, m) \in \lceil A \rceil_{\mathcal{V}}$.

   By definition of $\lceil A^{\mathsf{p}} \rceil_{\mathcal{V}}$ it suffices to show $(\nu, \theta, n) \in \lceil A \rceil_{\mathcal{V}}$. We get this by induction.

2. Let $n \in \mathbb{N}$. We have to show $(\nu, \theta, n) \in \lceil A \rceil_{\mathcal{V}}$. We do case analysis on the derivation of $\mathsf{firstorder}(A)$.

   (a) **Funit:** In this case $A = \mathsf{unit}$. By definition of $\lceil \mathsf{unit} \rceil_{\mathcal{V}}$ we know that $\nu = ()$. Hence we have to show $((), \theta, n) \in \lceil \mathsf{unit} \rceil_{\mathcal{V}}$. We get this by definition of $\lceil \mathsf{unit} \rceil_{\mathcal{V}}$.

   (b) **Fnat:** In this case $A = \mathbb{N}$. By definition of $\lceil \mathbb{N} \rceil_{\mathcal{V}}$ we know that there is an n' such that $\nu = n'$ and $n' \in \mathbb{N}$. Hence we have to show $(n', \theta, n) \in \lceil \mathbb{N} \rceil_{\mathcal{V}}$. We get this by definition of $\lceil \mathbb{N} \rceil_{\mathcal{V}}$ because $n' \in \mathbb{N}$.

   (c) **FProd:** In this case there are τ_1 and τ_2 such that

   - $A = \tau_1 \times \tau_2$.
   - $\mathsf{firstorder}(\tau_1)$
   - $\mathsf{firstorder}(\tau_2)$

   By definition of $\lceil \tau_1 \times \tau_2 \rceil_{\mathcal{V}}$ we know that there are ν_1, ν_2 such that

   - $\nu = (\nu_1, \nu_2)$,
   - $(\nu_1, \theta, m) \in \lceil \tau_1 \rceil_{\mathcal{V}}$, and
   - $(\nu_2, \theta, m) \in \lceil \tau_2 \rceil_{\mathcal{V}}$.

   By definition of $\lceil \tau_1 \times \tau_2 \rceil_{\mathcal{V}}$ it suffices to show

   - $(\nu_1, \theta, n) \in \lceil \tau_1 \rceil_{\mathcal{V}}$. We get this by induction.

- $(v_2, \theta, n) \in \lceil \tau_2 \rceil_{\mathcal{V}}$. We get this by induction.

(d) **FSum:** In this case there are τ_1 and τ_2 such that

- $A = \tau_1 + \tau_2$.
- $\mathtt{firstorder}(\tau_1)$
- $\mathtt{firstorder}(\tau_2)$

By definition of $\lceil \tau_1 + \tau_2 \rceil_{\mathcal{V}}$ there are two cases

i. There is a v' such that
   - $v = \mathsf{inl}\,(v')$ and
   - $(v', \theta, m) \in \lceil \tau_1 \rceil_{\mathcal{V}}$.

   By definition of $\lceil \tau_1 + \tau_2 \rceil_{\mathcal{V}}$ it suffices to show
   - $(v', \theta, n) \in \lceil \tau_1 \rceil_{\mathcal{V}}$. We get this by induction.

ii. There is a v' such that
   - $v = \mathsf{inr}\,(v')$ and
   - $(v', \theta, m) \in \lceil \tau_2 \rceil_{\mathcal{V}}$.

   By definition of $\lceil \tau_1 + \tau_2 \rceil_{\mathcal{V}}$ it suffices to show
   - $(v', \theta, n) \in \lceil \tau_2 \rceil_{\mathcal{V}}$. We get this by induction.

(e) **FRef**: In this case there is τ, such that

- $A = \mathsf{ref}\,\tau$ and
- $\mathtt{firstorder}(\tau)$.

By definition of $\lceil \mathsf{ref}\,\tau \rceil_{\mathcal{V}}$ there is an l such that

- $v = l$ and
- $\theta(l) = \tau$.

By definition of $\lceil \mathsf{ref}\,\tau \rceil_{\mathcal{V}}$ it suffices to show $\theta(l) = \tau$, which we already know.

□

Lemma 10.36. 1. If $\mathtt{firstorder}(\tau)$ and $(v, v', W, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$, then $\forall n.\ (v, v', W, n) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$.

2. If $\mathtt{firstorder}(A)$ and $(v, v', W, m) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$, then $\forall n.\ (v, v', W, n) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$.

Proof. By mutual induction on $\mathtt{firstorder}(\tau)$ and $\mathtt{firstorder}(A)$.

1. Let $n \in \mathbb{N}$. We have to show $(v, v', W, n) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. τ has the form A^p and $\mathtt{firstorder}(\tau)$ must have been derived by **FPol**. Hence by inversion

   - $\mathtt{firstorder}(A)$.

   There are two cases:

   (a) $p \sqsubseteq \mathcal{A}$: In this case by definition of $[\![A^p]\!]^{\mathcal{A}}_{\mathcal{V}}$ we have
   - $(v, v', W, m) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$

   and it suffices to show $(v, v', W, n) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$. We get this by induction.

   (b) $p \not\sqsubseteq \mathcal{A}$: In this case by definition of $[\![A^p]\!]^{\mathcal{A}}_{\mathcal{V}}$ we have
   - $(v, W.\theta_1, m) \in \lceil A \rceil_{\mathcal{V}}$ and
   - $(v', W.\theta_2, m) \in \lceil A \rceil_{\mathcal{V}}$

   and it suffices to show $(v, W.\theta_1, n) \in \lceil A \rceil_{\mathcal{V}}$ and $(v', W.\theta_2, n) \in \lceil A \rceil_{\mathcal{V}}$. We get both by Lemma 10.35.

2. Let $n \in \mathbb{N}$. We have to show $(v, v', W, n) \in [\![A]\!]^{\mathcal{A}}_{\mathcal{V}}$. We do case analysis on the derivation of $\mathtt{firstorder}(A)$.

   (a) **Funit:** In this case $A = \mathsf{unit}$. By definition of $[\![\mathsf{unit}]\!]^{\mathcal{A}}_{\mathcal{V}}$ we know that $v = () = v'$. Hence we have to show $((), (), W, n) \in [\![\mathsf{unit}]\!]^{\mathcal{A}}_{\mathcal{V}}$. We get this by definition of $[\![\mathsf{unit}]\!]^{\mathcal{A}}_{\mathcal{V}}$.

   (b) **Fnat:** In this case $A = \mathbb{N}$. By definition of $[\![\mathbb{N}]\!]^{\mathcal{A}}_{\mathcal{V}}$ we know that there is an n' such that $v = n' = v'$ and $n' \in \mathbb{N}$. Hence we have to show $(n', n', W, n) \in \lceil \mathbb{N} \rceil_{\mathcal{V}}$. We get this by definition of $[\![\mathbb{N}]\!]^{\mathcal{A}}_{\mathcal{V}}$ because $n' \in \mathbb{N}$.

   (c) **FProd:** In this case there are τ_1 and τ_2 such that

- $A = \tau_1 \times \tau_2$.
- $\mathtt{firstorder}(\tau_1)$
- $\mathtt{firstorder}(\tau_2)$

By definition of $[\![\tau_1 \times \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$ we know that there are v_1, v_2, v_1', v_2' such that

- $v = (v_1, v_2)$,
- $v' = (v_1', v_2')$,
- $(v_1, v_1', W, \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$, and
- $(v_2, v_2', W, \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$.

By definition of $[\![\tau_1 \times \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$ it suffices to show

- $(v_1, v_1', W, \mathfrak{n}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$. We get this by induction.
- $(v_2, v_2', W, \mathfrak{n}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$. We get this by induction.

item **FSum:** In this case there are τ_1 and τ_2 such that

- $A = \tau_1 + \tau_2$.
- $\mathtt{firstorder}(\tau_1)$
- $\mathtt{firstorder}(\tau_2)$

By definition of $[\![\tau_1 + \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$ there are two cases

i. There are v_0, v_0' such that
   - $v = \mathsf{inl}\,(v_0)$,
   - $v' = \mathsf{inl}\,(v_0')$, and
   - $(v_0, v_0', W, \mathfrak{m}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$.

   By definition of $[\![\tau_1 + \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$ it suffices to show
   - $(v_0, v_0', W, \mathfrak{n}) \in [\![\tau_1]\!]^{\mathcal{A}}_{\mathcal{V}}$. We get this by induction.

ii. There are v_0, v_0' such that
   - $v = \mathsf{inr}\,(v_0)$,
   - $v' = \mathsf{inr}\,(v_0')$, and
   - $(v_0, v_0', W, \mathfrak{m}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$.

   By definition of $[\![\tau_1 + \tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$ it suffices to show
   - $(v_0, v_0', W, \mathfrak{n}) \in [\![\tau_2]\!]^{\mathcal{A}}_{\mathcal{V}}$. We get this by induction.

(d) **FRef**: In this case there is τ, such that

- $A = \mathsf{ref}\ \tau$ and
- $\mathtt{firstorder}(\tau)$.

By definition of $[\![\mathsf{ref}\ \tau]\!]^{\mathcal{A}}_{\mathcal{V}}$ there are $\mathfrak{l}, \mathfrak{l}'$ such that

- $v = \mathfrak{l}$,
- $v' = \mathfrak{l}'$,
- $W.\theta_1(\mathfrak{l}) = \tau = W.\theta_2(\mathfrak{l}')$, and
- $(\mathfrak{l}, \mathfrak{l}') \in W.\beta$.

By definition of $[\![\mathsf{ref}\ \tau]\!]^{\mathcal{A}}_{\mathcal{V}}$ it suffices to show $W.\theta_1(\mathfrak{l}) = \tau = W.\theta_2(\mathfrak{l}')$ and $(\mathfrak{l}, \mathfrak{l}') \in W.\beta$, both of which we already know.

□

Lemma 10.37. 1. If ω and ω' are firstorder observations and $\omega \approx^{\mathcal{A}}_{(W,\mathfrak{m})} \omega'$, then $\forall \mathfrak{n}.\ \omega \approx^{\mathcal{A}}_{(W,\mathfrak{n})} \omega'$.

2. If $\vec{\omega}$ and $\vec{\omega'}$ contain only firstorder observations and $\vec{\omega} \approx^{\mathcal{A}}_{(W,\mathfrak{m})} \vec{\omega'}$, then $\forall \mathfrak{n}.\ \vec{\omega} \approx^{\mathcal{A}}_{(W,\mathfrak{n})} \vec{\omega'}$.

Proof. 1. Let $\mathfrak{n} \in \mathbb{N}$. We have to show $\omega \approx^{\mathcal{A}}_{(W,\mathfrak{n})} \omega'$. We do case analysis on the derivation of $\omega \approx^{\mathcal{A}}_{(W,\mathfrak{m})} \omega'$.

(a) **refl**: We get the goal by **refl**.

(b) **high**: We get the goal by **high**.

(c) **extend-τ**: In this case there are $\mathfrak{l}, \mathfrak{l}', v, v'$ such that

- $\omega = \mathfrak{l}_\tau(v)$ and

- $\omega' = \mathsf{l}'_\tau(v')$
- $(\mathsf{l}, \mathsf{l}') \in W.\beta$
- $(v, v', W, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$.

By **extend-τ** it suffices to show

- $(\mathsf{l}, \mathsf{l}') \in W.\beta$. We already know this.
- $(v, v', W, \mathfrak{n}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathcal{V}}$. By assumption $\mathtt{firstorder}(\omega)$ and because $\omega = \mathsf{l}_\tau(v)$ this gives us
  - $\mathtt{firstorder}(\tau)$

  by inversion. We get the goal by Lemma 10.36.

2. We get this by pointwise application of 1. to each pair of observations in the traces.

□

Theorem 10.1 (Semantic typing implies flow-lock security)**.** Let e be in the language with just firstorder state. If $\forall \mathfrak{m}, (e, e, (\theta^{\mathsf{L}}, \theta^{\mathsf{L}}, \mathtt{id}_{\mathrm{dom}(\theta^{\mathsf{L}})}), \Sigma, \Sigma, \mathfrak{m}) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$ and $(\vec{\omega}, \omega; \Sigma') \in \mathtt{Run}_{\mathcal{A}}(e, \mathsf{L}, \Sigma, \theta)$ and $(\vec{\omega'}, \omega'; \Sigma'') \in \mathtt{Run}_{\mathcal{A}}(e, \mathsf{L}, \Sigma, \theta)$ and $\forall \mathfrak{m}, \vec{\omega} \approx^{\mathcal{A}}_{((\theta,\theta,\mathtt{id}_{\mathrm{dom}(\theta)}),\mathfrak{m}))} \vec{\omega'}$ and $\Sigma' \sqsubseteq \mathcal{A}$ or $\Sigma'' \sqsubseteq \mathcal{A}$, then $\mathsf{k}_{\mathcal{A}}(e; \vec{\omega}, \omega; \mathsf{L}; \Sigma) = \mathsf{k}_{\mathcal{A}}(e; \vec{\omega'}, \omega'; \mathsf{L}; \Sigma)$.

Proof. By Lemma 10.30 it suffices to show that there is a W', s.t. $W' \supseteq (\theta_{\mathsf{L}}, \theta_{\mathsf{L}}, \mathtt{id}_{\mathrm{dom}(\mathsf{L})})$ and $\forall \mathfrak{m}, \vec{\omega}, \omega \approx^{\mathcal{A}}_{W',\mathfrak{m}} \vec{\omega'}, \omega'$. By Lemma 10.37 the step-indexes are irrelevant in the first-order when we just have firstorder observations and it therefore suffices to show there is a $W' \supseteq (\theta_{\mathsf{L}}, \theta_{\mathsf{L}}, \mathtt{id}_{\mathrm{dom}(\mathsf{L})})$ such that $\vec{\omega}, \omega \approx^{\mathcal{A}}_{W',0} \vec{\omega'}, \omega'$.

Because $(\vec{\omega}, \omega; \Sigma') \in \mathtt{Run}_{\mathcal{A}}(e, \mathsf{L}, \Sigma, \theta)$ and $(\vec{\omega'}, \omega'; \Sigma'') \in \mathtt{Run}_{\mathcal{A}}(e, \mathsf{L}, \Sigma, \theta)$ there are $\mathsf{S}_1, \mathsf{S}'_1, e_1, \mathsf{S}_2, \mathsf{S}'_2, e_2$ such that

- $\mathsf{S}_1 \rhd_{\cdot} \theta^{\mathsf{L}}$
- $\mathsf{S}_2 \rhd_{\cdot} \theta^{\mathsf{L}}$
- $\mathsf{S}_1 \approx_{\mathcal{A}} \mathsf{L}$
- $\mathsf{S}_2 \approx_{\mathcal{A}} \mathsf{L}$
- $\Sigma \vdash e, \mathsf{S}_1 \xRightarrow{\vec{\omega},\omega;\Sigma'}{}^{*}_{\mathcal{A}} e_1, \mathsf{S}'_1$
- $\Sigma \vdash e, \mathsf{S}_2 \xRightarrow{\vec{\omega'},\omega';\Sigma''}{}^{*}_{\mathcal{A}} e_2, \mathsf{S}'_2$

So by Lemma 10.33 there are $\vec{\omega}, e'_1, \mathsf{S}''_1$ and $\vec{\omega'}, e'_2, \mathsf{S}''_2$ such that

- $\Sigma \vdash e, \mathsf{S}_1 \xRightarrow{\vec{\omega},\omega;\Sigma'}{}^{*} e'_1, \mathsf{S}''_1$
- $\Sigma \vdash e, \mathsf{S}_2 \xRightarrow{\vec{\omega'},\omega';\Sigma''}{}^{*} e'_2, \mathsf{S}''_2$
- $(\vec{\omega}, \omega)_{\mathcal{A}} = \vec{\omega}, \omega$
- $(\vec{\omega'}, \omega')_{\mathcal{A}} = \vec{\omega'}, \omega'$

Let l_1 be the length of $\vec{\omega}_{\mathcal{A}}$ and let l_2 be the length of $\vec{\omega'}_{\mathcal{A}}$. Because $(\theta^{\mathsf{L}}, \theta^{\mathsf{L}}, \mathtt{id}_{\mathrm{dom}(\theta^{\mathsf{L}})}) \sqsupseteq (\theta, \theta, \mathtt{id}_{\mathrm{dom}(\theta)})$ we get by monotonicity (10.8) that $\vec{\omega} \approx^{\mathcal{A}}_{((\theta^{\mathsf{L}},\theta^{\mathsf{L}},\mathtt{id}_{\mathrm{dom}(\theta^{\mathsf{L}})}),\mathsf{l}_1+\mathsf{l}_2+1))} \vec{\omega'}$.

We show $(\mathsf{S}_1, \mathsf{S}_2, \mathsf{l}_1 + \mathsf{l}_2 + 1) \overset{\mathcal{A}}{\rhd} (\theta^{\mathsf{L}}, \theta^{\mathsf{L}}, \mathtt{id}(\mathrm{dom}(\theta^{\mathsf{L}})))$. For this we have to show the following:

- $\mathtt{id}(\mathrm{dom}(\theta^{\mathsf{L}})) \subseteq \mathrm{dom}(\theta^{\mathsf{L}}) \times \mathrm{dom}(\theta^{\mathsf{L}})$. This is obviously the case.
- $(\mathsf{S}_1, \mathsf{l}_1 + \mathsf{l}_2 + 1) \rhd \theta^{\mathsf{L}}$. We have to show
  - $\mathrm{dom}(\theta^{\mathsf{L}}) \subseteq \mathrm{dom}(\mathsf{S}_1)$. We have this by $\mathsf{S}_1 \rhd_{\cdot} \theta^{\mathsf{L}}$
  - $\forall \mathsf{l} \in \mathrm{dom}(\theta^{\mathsf{L}}).(\mathsf{S}_1(\mathsf{l}), \theta^{\mathsf{L}}, \mathsf{l}_1 + \mathsf{l}_2 + 1) \in \lceil \theta^{\mathsf{L}}(\mathsf{l}) \rceil_{\mathcal{V}}$.
    Let $\mathsf{l} \in \mathrm{dom}(\theta^{\mathsf{L}})$. By $\mathsf{S}_1 \rhd_{\cdot} \theta^{\mathsf{L}}$ we have $\cdot; \emptyset; \theta^{\mathsf{L}} \vdash_{\perp} \mathsf{S}_1(\mathsf{l}) : \theta^{\mathsf{L}}(\mathsf{l})$. Because $\mathrm{dom}(\cdot) \subseteq \mathrm{dom}(\emptyset)$ and there are no $\mathsf{x} \in \mathrm{dom}(\cdot)$ we have $(\emptyset, \theta^{\mathsf{L}}, \mathsf{l}_1 + \mathsf{l}_2 + 1) \in \lceil \cdot \rceil_{\mathcal{V}}$. Hence we get $(\mathsf{S}_1(\mathsf{l}), \theta^{\mathsf{L}}, \mathsf{l}_1 + \mathsf{l}_2 + 1) \in \lceil \theta^{\mathsf{L}}(\mathsf{l}) \rceil^{\perp}_{\mathsf{E}}$ by the Unary Fundamental Lemma. The goal follows because $\mathsf{S}_1(\mathsf{l}) \in \mathcal{V}$ by $\mathsf{S}_1 \rhd_{\cdot} \theta^{\mathsf{L}}$.

– $\forall l \in \mathrm{dom}(\theta^L).\theta^L(l) = \mathtt{type}(S_1, l)$. We have this by $S_1 \triangleright \theta^L$.

- $(S_2, l_1 + l_2 + 1) \triangleright \theta^L$. We have to show
  – $\mathrm{dom}(\theta^L) \subseteq \mathrm{dom}(S_2)$. We have this by $S_2 \triangleright \theta^L$.
  – $\forall l \in \mathrm{dom}(\theta^L).(S_2(l), \theta^L, l_1 + l_2 + 1) \in \lceil \theta^L(l) \rceil_{\mathcal{V}}$.
  Let $l \in \mathrm{dom}(\theta^L)$. By $S_2 \triangleright \theta^L$ we have $\cdot; \emptyset; \theta^L \vdash_\perp S_2(l) : \theta^L(l)$. Because $\mathrm{dom}(\cdot) \subseteq \mathrm{dom}(\emptyset)$ and there are no $x \in \mathrm{dom}(\cdot)$ we have $(\emptyset, \theta^L, l_1 + l_2 + 1) \in \lceil \cdot \rceil_{\mathcal{V}}$. Hence we get $(S_2(l), \theta^L, l_1 + l_2 + 1) \in \lceil \theta^L(l) \rceil^{\perp}_{\mathsf{E}}$ by the Unary Fundamental Lemma. The goal follows because $S_2(l) \in \mathcal{V}$ by $S_2 \triangleright \theta^L$.
  – $\forall l \in \mathrm{dom}(\theta^L).\theta^L(l) = \mathtt{type}(S_2, l)$. We have this by $S_2 \triangleright \theta^L$.

- $\forall (l, l') \in \mathtt{id}(\mathrm{dom}(\theta^L)).\ \theta^L(l) = \theta^L(l') \wedge (S_1(l), S_2(l'), (\theta^L, \theta^L, \mathtt{id}(\mathrm{dom}(\theta^L))), l_1 + l_2 + 1) \in [\![\theta^L(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$.
  Let $(l, l') \in \mathtt{id}(\mathrm{dom}(\theta^L))$. Then $l = l'$. So it suffices to show
  – $\theta^L(l) = \theta^L(l)$. This is trivially true.
  – $(S_1(l), S_2(l), (\theta^L, \theta^L, \mathtt{id}(\mathrm{dom}(\theta^L))), l_1 + l_2 + 1) \in [\![\theta^L(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$.
  We have already seen that $\mathrm{dom}(\theta^L) \subseteq \mathrm{dom}(S_1)$ and $\mathrm{dom}(\theta^L) \subseteq \mathrm{dom}(S_2)$. Hence in particular
    * $l \in \mathrm{dom}(S_1)$ and
    * $l \in \mathrm{dom}(S_2)$.

  Hence there are v_1, v_2 and τ_1, τ_2 such that
    * $l \rightarrowtail (v_1, \tau_1) \in S_1$ and
    * $l \rightarrowtail (v_2, \tau_2) \in S_2$.

  As $l \in \mathtt{dom}(\theta^L)$ we have that $\mathtt{type}(S_1, l) = \theta^L(l) = \mathtt{type}(S_2, l)$. Hence
    * $l \rightarrowtail (v_1, \theta^L(l)) \in S_1$ and
    * $l \rightarrowtail (v_2, \theta^L(l)) \in S_2$.

  We have $\theta^L(l) = A^p$ for some type A and policy p. There are two cases:
  1. $p \sqsubseteq \mathcal{A}$:
  In this case $\theta^L(l) \sqsubseteq \mathcal{A}$ and hence
    * $l \rightarrowtail (v_1, \theta^L(l)) \in (S_1)_{\mathcal{A}}$ and
    * $l \rightarrowtail (v_2, \theta^L(l)) \in (S_2)_{\mathcal{A}}$.

  By Lemma 10.31 and Lemma 10.32 we have $S_1 \approx_{\mathcal{A}} S_2$. Because of this and because $(l, l) \in \mathrm{dom}((S_1)_{\mathcal{A}})$, we get
    * $(v_1, v_2, (\theta_{(S_1)_{\mathcal{A}}}, \theta_{(S_2)_{\mathcal{A}}}, \mathtt{id}_{(}\mathrm{dom}((S_1)_{\mathcal{A}}))), l_1 + l_2 + 1) \in [\![\theta^L(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$.

  Because $S_1 \approx_{\mathcal{A}} L$ and $S_2 \approx_{\mathcal{A}} L$, we also have $\theta_{(S_1)_{\mathcal{A}}} = \theta_{L_{\mathcal{A}}} = \theta_L = \theta_{L_{\mathcal{A}}} = \theta_{(S_2)_{\mathcal{A}}}$. and $\mathrm{dom}((S_1)_{\mathcal{A}}) = \mathrm{dom}(L_{\mathcal{A}}) = \mathrm{dom}(L)$. Hence
    * $(v_1, v_2, (\theta_L, \theta_L, \mathtt{id}_{(}\mathrm{dom}(L))), l_1 + l_2 + 1) \in [\![\theta^L(l)]\!]^{\mathcal{A}}_{\mathcal{V}}$.

  The goal follows by monotonicity (Lemma 8.25).
  2. $p \not\sqsubseteq \mathcal{A}$. In this case it suffices to show
    * $(S_1(l), \theta^L, l_1 + l_2 + 1) \in \lceil A \rceil_{\mathcal{V}}$. It suffices to show $(S_1(l), \theta^L, l_1 + l_2 + 1) \in \lceil A^p \rceil_{\mathcal{V}}$ which is the same as showing $(S_1(l), \theta^L, l_1 + l_2 + 1) \in \lceil \theta^L(l) \rceil_{\mathcal{V}}$. We get this from $(S_1, l_1 + l_2 + 1) \triangleright \theta^L$, which we have already shown, because $l \in \mathtt{dom}(\theta^L)$.
    * $(S_2(l), \theta^L, l_1 + l_2 + 1) \in \lceil A \rceil_{\mathcal{V}}$. It suffices to show $(S_2(l), \theta^L, l_1 + l_2 + 1) \in \lceil A^p \rceil_{\mathcal{V}}$ which is the same as showing $(S_2(l), \theta^L, l_1 + l_2 + 1) \in \lceil \theta^L(l) \rceil_{\mathcal{V}}$. We get this from $(S_2, l_1 + l_2 + 1) \triangleright \theta^L$, which we have already shown, because $l \in \mathtt{dom}(\theta^L)$.

From all of what we know we get by Lemma 10.23 that there is a world W such that $W \sqsupseteq (\theta^L, \theta^L, \mathtt{id}_{\mathrm{dom}(\theta^L)})$ and $\vec{\omega}, \omega \approx^{\mathcal{A}}_{(W,1)} \vec{\omega'}, \omega'$. Let W be this world. By monotonicity (Lemma 10.22) we also have $\vec{\omega}, \omega \approx^{\mathcal{A}}_{W,0} \vec{\omega'}, \omega'$. By transitivity $W \sqsupseteq (\theta_L, \theta_L, \mathtt{id}_{\mathrm{dom}(L)})$, so this suffices to show the goal.

□

Corollary 10.38 (Termination insensitive flow-lock security)**.**
Let e be in the language with just firstorder state. If $\cdot; \Sigma; \theta \vdash_{\mathsf{pc}} e : \tau$ and $(\vec{\omega}, \omega; \Sigma') \in \mathtt{Run}_{\mathcal{A}}(e, L, \Sigma, \theta)$ and $(\vec{\omega'}, \omega'; \Sigma'') \in \mathtt{Run}_{\mathcal{A}}(e, L, \Sigma, \theta)$ where L is an $\mathcal{A}$-low state and $\forall m, \vec{\omega} \approx^{\mathcal{A}}_{((\theta,\theta,\mathtt{id}_{\mathrm{dom}(\theta)}),m))} \vec{\omega'}$ and $\Sigma' \sqsubseteq \mathcal{A}$ or $\Sigma'' \sqsubseteq \mathcal{A}$, then $\mathrm{k}_{\mathcal{A}}(e; \vec{\omega}, \omega; L; \Sigma) = \mathrm{k}_{\mathcal{A}}(e; \vec{\omega'}, \omega'; L; \Sigma)$.

Proof. By Theorem 10.1 it suffices to show $\forall m, (e, e, (\theta^L, \theta^L, \mathtt{id}_{\mathrm{dom}(\theta^L)}), \Sigma, \Sigma, m) \in [\![\tau]\!]^{\mathcal{A}}_{\mathsf{E}}$. Let $m \in \mathbb{N}$. By the Binary Fundamental Lemma it suffices to show

1. $(\emptyset, (\theta^L, \theta^L, \mathtt{id}(\mathtt{dom}(\theta^L))), m) \in [\![\cdot]\!]^{\mathcal{A}}_{\mathcal{V}}$. We have this because $\mathtt{dom}(\cdot) \subseteq \mathtt{dom}(\emptyset)$ and there are no $x \in \mathtt{dom}(\cdot)$.
2. $\theta^L \sqsupseteq \theta$. This follows from the definition of θ^L.
3. $\forall l.l \in \mathrm{dom}(\theta)$. $(l, l) \in \mathtt{id}(\mathtt{dom}(\theta^L))$. Let $l \in \mathrm{dom}(\theta)$. Since $\mathrm{dom}(\theta^L) = \mathrm{dom}(\theta) \cup \mathrm{dom}(L)$, we get $(l, l) \in \mathtt{id}(\mathtt{dom}(\theta^L))$.

□

References

[1] H. P. Barendregt, *The Lambda Calculus : its Syntax and Semantics*, ser. Studies in Logic and the Foundations of Mathematics. North-Holland, 2001. [Online]. Available: https://www.sciencedirect.com/bookseries/studies-in-logic-and-the-foundations-of-mathematics/vol/103

[2] N. Broberg and D. Sands, "Flow locks: Towards a core calculus for dynamic flow policies," in *Programming Languages and Systems, 15th European Symposium on Programming, ESOP 2006, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2006, Vienna, Austria, March 27-28, 2006, Proceedings*, ser. Lecture Notes in Computer Science, P. Sestoft, Ed., vol. 3924. Springer, 2006, pp. 180–196. [Online]. Available: https://doi.org/10.1007/11693024_13

[3] ——, "Flow-sensitive semantics for dynamic information flow policies," in *Proceedings of the 2009 Workshop on Programming Languages and Analysis for Security, PLAS 2009, Dublin, Ireland, 15-21 June, 2009*, S. Chong and D. A. Naumann, Eds. ACM, 2009, pp. 101–112. [Online]. Available: https://doi.org/10.1145/1554339.1554352

[4] ——, "Paralocks: role-based information flow control and beyond," in *Proceedings of the 37th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages, POPL 2010, Madrid, Spain, January 17-23, 2010*, M. V. Hermenegildo and J. Palsberg, Eds. ACM, 2010, pp. 431–444. [Online]. Available: https://doi.org/10.1145/1706299.1706349

[5] V. Rajani and D. Garg, "Types for information flow control: Labeling granularity and semantic models," in *31st IEEE Computer Security Foundations Symposium, CSF 2018, Oxford, United Kingdom, July 9-12, 2018*. IEEE Computer Society, 2018, pp. 233–246. [Online]. Available: https://doi.org/10.1109/CSF.2018.00024