A SOUNDNESS

Lemma A.1. *For all* $n > 0, \epsilon \in \textsc{ErExit}, m_p, m_q, \mathsf{C}, \mathsf{C}'$*:*

$$\mathsf{C}, m_p \stackrel{n}{\Rightarrow} \epsilon, m_q \implies \mathsf{C}; \mathsf{C}', m_p \stackrel{n}{\Rightarrow} \epsilon, m_q$$

Proof. We proceed by natural induction on n.

Base case n=1
Pick arbitrary $\epsilon \in \textsc{ErExit}$, $m_p, m_q, \mathsf{C}, \mathsf{C}'$ such that $\mathsf{C}, m_p \stackrel{1}{\Rightarrow} \epsilon, m_q$. From the operational semantics we know there exist l, C'' such that $\mathsf{C} \xrightarrow{l} \mathsf{C}''$ and $(m_p, m_q) \in [\![l]\!]\epsilon$. Consequently, from the control flow transitions we have $\mathsf{C}; \mathsf{C}' \xrightarrow{l} \mathsf{C}''; \mathsf{C}'$. As such, from the operational semantics we have $\mathsf{C}; \mathsf{C}', m_p \stackrel{1}{\Rightarrow} \epsilon, m_q$.

Inductive case n=j+1 and $n > 1$

$$\forall \epsilon \in \textsc{ErExit}, m_1, m_2, \mathsf{C}_1, \mathsf{C}_2.\ \mathsf{C}_1, m_1 \stackrel{j}{\Rightarrow} \epsilon, m_2 \implies \mathsf{C}_1; \mathsf{C}_2, m_1 \stackrel{j}{\Rightarrow} \epsilon, m_2 \qquad \text{(I.H)}$$

Pick arbitrary $\epsilon \in \textsc{ErExit}$, $m_p, m_q, \mathsf{C}, \mathsf{C}'$ such that $\mathsf{C}, m_p \stackrel{n}{\Rightarrow} \epsilon, m_q$. As $n > 1$, from the operational semantics we know there exist l, C'', m such that, $\mathsf{C} \xrightarrow{l} \mathsf{C}''$, $(m_p, m) \in [\![l]\!]ok$, and $\mathsf{C}'', m \stackrel{j}{\Rightarrow} \epsilon, m_q$. Consequently, from the control flow transitions we have $\mathsf{C}; \mathsf{C}' \xrightarrow{l} \mathsf{C}''; \mathsf{C}'$. Moreover, from (I.H) we have $\mathsf{C}''; \mathsf{C}', m \stackrel{j}{\Rightarrow} \epsilon, m_q$. As such, since n=j+1, $\mathsf{C}; \mathsf{C}' \xrightarrow{l} \mathsf{C}''; \mathsf{C}'$, $(m_p, m) \in [\![l]\!]ok$ and $\mathsf{C}''; \mathsf{C}', m \stackrel{j}{\Rightarrow} \epsilon, m_q$ from the operational semantics we have $\mathsf{C}; \mathsf{C}', m_p \stackrel{n}{\Rightarrow} \epsilon, m_q$, as required. □

Lemma A.2. *For all* $n, k, \epsilon, m_p, m_r, m_q, \mathsf{C}_1, \mathsf{C}_2$*:*

$$\mathsf{C}_1, m_p \stackrel{n}{\Rightarrow} ok, m_r \land \mathsf{C}_2, m_r \stackrel{k}{\Rightarrow} \epsilon, m_q \implies \exists b.\ \mathsf{C}_1; \mathsf{C}_2, m_p \stackrel{b}{\Rightarrow} \epsilon, m_q$$

Proof. We proceed by natural induction on n.

Base case n=0
Pick arbitrary $k, \epsilon, m_p, m_r, m_q, \mathsf{C}_1, \mathsf{C}_2$ such that: $\mathsf{C}_1, m_p \stackrel{0}{\Rightarrow} ok, m_r$ and $\mathsf{C}_2, m_r \stackrel{k}{\Rightarrow} \epsilon, m_q$. As $\mathsf{C}_1, m_p \stackrel{0}{\Rightarrow} ok, m_r$, from the operational semantics we then know C_1=`skip` and m_r=m_p. Consequently, from the control flow transitions we have $\mathsf{C}_1; \mathsf{C}_2 \xrightarrow{\mathrm{id}} \mathsf{C}_2$. Moreover, from the definition of $[\![.]\!]$ ans since m_p=m_r we have $(m_p, m_r) \in [\![\mathrm{id}]\!]ok$. As such, since $\mathsf{C}_1; \mathsf{C}_2 \xrightarrow{\mathrm{id}} \mathsf{C}_2$, $(m_p, m_r) \in [\![\mathrm{id}]\!]ok$ and $\mathsf{C}_2, m_r \stackrel{k}{\Rightarrow} \epsilon, m_q$, from the operational semantics we have $\mathsf{C}_1; \mathsf{C}_2, m_p \stackrel{k+1}{\Longrightarrow} \epsilon, m_q$, as required.

Inductive case n=j+1

$$\begin{aligned}&\forall k, \epsilon, m_p, m_r, m_q, \mathsf{C}_1, \mathsf{C}_2.\\ &\qquad \mathsf{C}_1, m_p \stackrel{j}{\Rightarrow} ok, m_r \land \mathsf{C}_2, m_r \stackrel{k}{\Rightarrow} \epsilon, m_q \implies \exists b.\ \mathsf{C}_1; \mathsf{C}_2, m_p \stackrel{b}{\Rightarrow} \epsilon, m_q\end{aligned} \qquad \text{(I.H)}$$

Pick arbitrary k, ϵ, $m_p, m_q, m_r, \mathsf{C}_1, \mathsf{C}_2$ such that: $\mathsf{C}_1, m_p \stackrel{n}{\Rightarrow} ok, m_r$ and $\mathsf{C}_2, m_r \stackrel{k}{\Rightarrow} \epsilon, m_q$. As $n > 0$, from the operational semantics we know there exist l, C', m such that, $\mathsf{C}_1 \xrightarrow{l} \mathsf{C}'$, $(m_p, m) \in [\![l]\!]ok$, and $\mathsf{C}', m \stackrel{j}{\Rightarrow} \epsilon, m_r$. Consequently, from the control flow transitions we have $\mathsf{C}_1; \mathsf{C}_2 \xrightarrow{l} \mathsf{C}'; \mathsf{C}_2$. As $\mathsf{C}', m \stackrel{j}{\Rightarrow} \epsilon, m_r$ and $\mathsf{C}_2, m_r \stackrel{k}{\Rightarrow} \epsilon, m_q$, from (I.H) we know there exists b such that $\mathsf{C}'; \mathsf{C}_2, m \stackrel{b}{\Rightarrow} \epsilon, m_q$. As such, since $C_1; C_2 \xrightarrow{l} C'; C_2$, $(m_p, m) \in [\![l]\!]ok$ and $C_1; C_2, m \overset{b}{\Rightarrow} \epsilon, m_q$, from the operational semantics we have $C_1; C_2, m_p \overset{b+1}{\Longrightarrow} \epsilon, m_q$, as required. □

Lemma A.3. *For all* n, ϵ, m_p, m_q, C*:*

$$C, m_p \overset{n}{\Rightarrow} \epsilon, m_q \implies \texttt{skip} \,||\, C, m_p \overset{n+1}{\Longrightarrow} \epsilon, m_q \land C \,||\, \texttt{skip}, m_p \overset{n+1}{\Longrightarrow} \epsilon, m_q$$

Proof. From the operational semantics we then have $\texttt{skip} \,||\, C \xrightarrow{\mathrm{id}} C$ and $C \,||\, \texttt{skip} \xrightarrow{\mathrm{id}} C$. Moreover, from the definition of $[\![.]\!]$ we have $(m_p, m_p) \in [\![\mathrm{id}]\!]ok$. Consequently, as $C, m_p \overset{n}{\Rightarrow} \epsilon, m_q$, from the operational semantics we have $\texttt{skip} \,||\, C, m_p \overset{n+1}{\Longrightarrow} \epsilon, m_q$ and $C \,||\, \texttt{skip}, m_p \overset{n+1}{\Longrightarrow} \epsilon, m_q$, as required. □

Lemma A.4. *For all* $n, \epsilon, m_p, m_r, m_q, C_1, C_2$*:*

$$C_1, m_p \overset{n}{\Rightarrow} ok, m_r \land C_2, m_r \overset{k}{\Rightarrow} \epsilon, m_q \implies \exists j.\ C_1 \,||\, C_2, m_p \overset{j}{\Rightarrow} \epsilon, m_q \land C_2 \,||\, C_1, m_p \overset{j}{\Rightarrow} \epsilon, m_q$$

Proof. We proceed by natural induction on n.

Base case n=0
Pick arbitrary $k, \epsilon, m_p, m_q, m_r, C_1, C_2$ such that $C_1, m_p \overset{0}{\Rightarrow} ok, m_r$ and $C_2, m_r \overset{k}{\Rightarrow} \epsilon, m_q$. From the operational semantics we then know $C_1 = \texttt{skip}$ and $m_r{=}m_p$. As such, from Lemma A.3 we know $C_1 \,||\, C_2, m_p \overset{k+1}{\Longrightarrow} \epsilon, m_q$ and $C_2 \,||\, C_1, m_p \overset{k+1}{\Longrightarrow} \epsilon, m_q$, as required.

Inductive case n=j+1

$$\begin{array}{l}\forall k, \epsilon, m_1, m_2, m_3, C_1, C_2. \\ \quad C_1, m_1 \overset{j}{\Rightarrow} ok, m_3 \land C_2, m_3 \overset{k}{\Rightarrow} \epsilon, m_2 \implies \exists i.\ C_1 \,||\, C_2, m_1 \overset{i}{\Rightarrow} \epsilon, m_2 \land C_2 \,||\, C_1, m_1 \overset{i}{\Rightarrow} \epsilon, m_2\end{array} \tag{I.H}$$

Pick arbitrary $k, \epsilon, m_p, m_q, m_r, C_1, C_2$ such that $C_1, m_p \overset{n}{\Rightarrow} ok, m_r$ and $C_2, m_r \overset{k}{\Rightarrow} \epsilon, m_q$. As $n > 0$ and $C_1, m_p \overset{n}{\Rightarrow} ok, m_r$, from the operational semantics we know there exist l, C', m such that, $C_1 \xrightarrow{l} C'$, $(m_p, m) \in [\![l]\!]ok$, and $C', m \overset{j}{\Rightarrow} ok, m_r$. Consequently, as $C', m \overset{j}{\Rightarrow} ok, m_r$ and $C_2, m_r \overset{k}{\Rightarrow} \epsilon, m_q$, from (I.H) we know there exists i such that $C' \,||\, C_2, m \overset{i}{\Rightarrow} \epsilon, m_q$ and $C_2 \,||\, C', m \overset{i}{\Rightarrow} \epsilon, m_q$. Moreover, as $C_1 \xrightarrow{l} C'$, from the operational semantics we also have $C_1 \,||\, C_2 \xrightarrow{l} C' \,||\, C_2$ and $C_2 \,||\, C_1 \xrightarrow{l} C_2 \,||\, C'$. Consequently, as $C_1 \,||\, C_2 \xrightarrow{l} C' \,||\, C_2$, $C_2 \,||\, C_1 \xrightarrow{l} C_2 \,||\, C'$, $(m_p, m) \in [\![l]\!]ok$, $C' \,||\, C_2, m \overset{i}{\Rightarrow} \epsilon, m_q$ and $C_2 \,||\, C', m \overset{i}{\Rightarrow} \epsilon, m_q$, from the operational semantics we also have $C_1 \,||\, C_2, m \overset{i+1}{\Longrightarrow} \epsilon, m_q$ and $C_2 \,||\, C_1, m \overset{i+1}{\Longrightarrow} \epsilon, m_q$, as required. □

Lemma A.5. *For all* $n, \epsilon \in \textsc{ErExit}, m_p, m_q, C_1, C_2$*:*

$$C_1, m_p \overset{n}{\Rightarrow} \epsilon, m_q \implies C_1 \,||\, C_2, m_p \overset{n}{\Rightarrow} \epsilon, m_q \land C_2 \,||\, C_1, m_p \overset{n}{\Rightarrow} \epsilon, m_q$$

Proof. As $\epsilon \in \textsc{ErExit}$ and $C_1, m_p \overset{n}{\Rightarrow} \epsilon, m_q$, we know $n > 0$. We proceed by induction on n.

Base case n=1
Pick arbitrary $\epsilon \in \textsc{ErExit}, m_p, m_q, C_1, C_2$ such that $C_1, m_p \overset{1}{\Rightarrow} \epsilon, m_q$. From the operational semantics we then know there exists l, C' such that $C_1 \xrightarrow{l} C'$, $(m_p, m_q) \in [\![l]\!]\epsilon$. As $C_1 \xrightarrow{l} C'$, from the control flow transitions we then also have $C_1 \,||\, C_2 \xrightarrow{l} C' \,||\, C_2$ and $C_2 \,||\, C_1 \xrightarrow{l} C_2 \,||\, C'$. As such, since

$\epsilon \in \textsc{ErExit}$ and $(m_p, m_q) \in [\![l]\!]\epsilon$, from the operational semantics we have $C_1 \,||\, C_2, m_p \xRightarrow{1} \epsilon, m_q$ and $C_2 \,||\, C_1, m_p \xRightarrow{1} \epsilon, m_q$, as required.

Inductive case $n{=}j{+}1$ and $n > 1$

$$\begin{aligned} &\forall \epsilon \in \textsc{ErExit}, m_1, m_2, C_1, C_2. \\ &\quad C_1, m_1 \xRightarrow{j} \epsilon, m_2 \implies C_1 \,||\, C_2, m_1 \xRightarrow{j} \epsilon, m_2 \wedge C_2 \,||\, C_1, m_1 \xRightarrow{j} \epsilon, m_2 \end{aligned} \tag{I.H}$$

Pick arbitrary $\epsilon \in \textsc{ErExit}$, m_p, m_q, C_1, C_2 such that $C_1, m_p \xRightarrow{n} \epsilon, m_q$. As $n > 1$ and $C_1, m_p \xRightarrow{n} \mathit{ok}, m_r$, from the operational semantics we know there exist l, C', m such that, $C_1 \xrightarrow{l} C'$, $(m_p, m) \in [\![l]\!]\mathit{ok}$, and $C', m \xRightarrow{j} \epsilon, m_q$. As $C', m \xRightarrow{j} \epsilon, m_q$ and $\epsilon \in \textsc{ErExit}$, from (I.H) we know $C' \,||\, C_2, m \xRightarrow{j} \epsilon, m_q$ and $C_2 \,||\, C', m \xRightarrow{j} \epsilon, m_q$. Moreover, as $C \xrightarrow{l} C'$, from the control flow transitions we have $C_1 \,||\, C_2 \xrightarrow{l} C' \,||\, C_2$ and $C_2 \,||\, C_1 \xrightarrow{l} C_2 \,||\, C'$. Consequently, as $n = j{+}1$, $C_1 \,||\, C_2 \xrightarrow{l} C' \,||\, C_2$, $C_2 \,||\, C_1 \xrightarrow{l} C_2 \,||\, C'$, $(m_p, m) \in [\![l]\!]\mathit{ok}$, $C' \,||\, C_2, m \xRightarrow{j} \epsilon, m_q$ and $C_2 \,||\, C', m \xRightarrow{j} \epsilon, m_q$, from the operational semantics we also have $C_1 \,||\, C_2, m_p \xRightarrow{n} \epsilon, m_q$ and $C_2 \,||\, C_1, m_p \xRightarrow{n} \epsilon, m_q$, as required. □

Lemma A.6. *For all $n, k, \epsilon, m_p, m_r, m_q, C, C_1, C_2$:*

$$\begin{aligned} &C, m_p \xRightarrow{n} \mathit{ok}, m_r \wedge C_1 \,||\, C_2, m_r \xRightarrow{k} \epsilon, m_q \implies \\ &\quad \exists b.\ C_1 \,||\, C; C_2, m_p \xRightarrow{b} \epsilon, m_q \wedge C; C_1 \,||\, C_2, m_p \xRightarrow{b} \epsilon, m_q \end{aligned}$$

Proof. We proceed by natural induction on n.

Base case $n{=}0$
Pick arbitrary $k, \epsilon, m_p, m_r, m_q, C, C_1, C_2$ such that: $C, m_p \xRightarrow{0} \mathit{ok}, m_r$ and $C_1 \,||\, C_2, m_r \xRightarrow{k} \epsilon, m_q$. As $C, m_p \xRightarrow{0} \mathit{ok}, m_r$, from the operational semantics we then know $C{=}\texttt{skip}$ and $m_r{=}m_p$. Consequently, from the control flow transitions we have $C; C_1 \xrightarrow{\text{id}} C_1$ and $C; C_2 \xrightarrow{\text{id}} C_2$. Moreover, from the definition of $[\![.]\!]$ ans since $m_p{=}m_r$ we have $(m_p, m_r) \in [\![\text{id}]\!]\mathit{ok}$. As such, since $C; C_i \xrightarrow{\text{id}} C_i$ for $i \in \{1, 2\}$, $(m_p, m_r) \in [\![\text{id}]\!]\mathit{ok}$ and $C_1 \,||\, C_2, m_r \xRightarrow{k} \epsilon, m_q$, from the operational semantics we have $C_1 \,||\, C; C_2, m_p \xRightarrow{k+1} \epsilon, m_q$ and $C; C_1 \,||\, C_2, m_p \xRightarrow{k+1} \epsilon, m_q$, as required.

Inductive case $n{=}j{+}1$

$$\begin{aligned} &\forall k, \epsilon, m_p, m_r, m_q, C, C_1, C_2. \\ &\quad C, m_p \xRightarrow{j} \mathit{ok}, m_r \wedge C_1 \,||\, C_2, m_r \xRightarrow{k} \epsilon, m_q \implies \\ &\qquad \exists b.\ C_1 \,||\, C; C_2, m_p \xRightarrow{b} \epsilon, m_q \wedge C; C_1 \,||\, C_2, m_p \xRightarrow{b} \epsilon, m_q \end{aligned} \tag{I.H}$$

Pick arbitrary $k, \epsilon, m_p, m_q, m_r, C, C_1, C_2$ such that: $C, m_p \xRightarrow{n} \mathit{ok}, m_r$ and $C_1 \,||\, C_2, m_r \xRightarrow{k} \epsilon, m_q$. As $n > 0$, from the operational semantics we know there exist l, C', m such that, $C \xrightarrow{l} C'$, $(m_p, m) \in [\![l]\!]\mathit{ok}$, and $C', m \xRightarrow{j} \epsilon, m_r$. Consequently, from the control flow transitions we have $C; C_i \xrightarrow{l} C'; C_i$ for $i \in \{1, 2\}$. As $C', m \xRightarrow{j} \epsilon, m_r$ and $C_1 \,||\, C_2, m_r \xRightarrow{k} \epsilon, m_q$, from (I.H) we know there exists b such that $C_1 \,||\, C'; C_2, m \xRightarrow{b} \epsilon, m_q$ and $C'; C_1 \,||\, C_2, m \xRightarrow{b} \epsilon, m_q$. As such, since $C; C_i \xrightarrow{l} C'; C_i$ for $i \in \{1, 2\}$,

$(m_p, m) \in [\![l]\!]ok$, $C_1 \mid\mid C'; C_2, m \overset{b}{\Rightarrow} \epsilon, m_q$ and $C'; C_1 \mid\mid C_2, m \overset{b}{\Rightarrow} \epsilon, m_q$, from the operational semantics we have $C_1 \mid\mid C; C_2, m_p \overset{b+1}{\Longrightarrow} \epsilon, m_q$ and $C; C_1 \mid\mid C_2, m_p \overset{b+1}{\Longrightarrow} \epsilon, m_q$, as required. □

Lemma A.7. *For all* p, C, q, ϵ, *if* $\vdash [p]\ C\ [\epsilon : q]$ *holds, then:*

$$\forall s \in \text{State}, m_q \in \lfloor q * \{s\} \rfloor.\ \exists m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor, n.\ C, m_p \overset{n}{\Rightarrow} \epsilon, m_q$$

Proof. We proceed by induction on the structure of incorrectness triples.

Case Skip
Pick an arbitrary $s \in \text{State}$ and $m_p \in \lfloor p * \{s\} \rfloor$. We then know there exists $s_p \in p$ such that $m_p \in \lfloor s_p \circ s \rfloor$. As $\mathcal{I}$ is reflexive and thus $s \in \mathcal{I}^{-1}(s)$, it then suffices to show that $C, m_p \overset{0}{\Rightarrow} ok, m_p$, which follows immediately from our operational semantics as C=`skip`.

Case Atom
Pick an arbitrary $s \in \text{State}$ and $m_q \in \lfloor q * \{s\} \rfloor$. We then know that C = a for some a. From axiom soundness (Par. 8) we then know there exists $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$ such that $(m_p, m_q) \in [\![a]\!]\epsilon$. There are now two cases to consider: 1) $\epsilon \in \text{ErExit}$; or 2) $\epsilon = ok$.

In case (1) since $(m_p, m_q) \in [\![a]\!]\epsilon$ and from our control flow transitions (Fig. 6) we have $a \xrightarrow{a}$ `skip`, from our operational semantics we have $C, m_p \overset{1}{\Rightarrow} \epsilon, m_q$, as required. In case (2) since $(m_p, m_q) \in [\![a]\!]ok$, from our control flow transitions (Fig. 6) we have $a \xrightarrow{a}$ `skip`, and `skip`, $m_q \overset{0}{\Rightarrow} ok, m_q$, from our operational semantics we have $C, m_p \overset{1}{\Rightarrow} ok, m_q$, as required.

Case SeqEr
We then know $C = C_1; C_2$ for some C_1, C_2. Pick an arbitrary $s \in \text{State}$ and $m_q \in \lfloor q * \{s\} \rfloor$. Since from the premise of SeqEr we have $[p]\ C_1\ [\epsilon : q]$ with $\epsilon \in \text{ErExit}$, from the inductive hypothesis we know there exist $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$, $n \in \mathbb{N}$ such that $C_1, m_p \overset{n}{\Rightarrow} \epsilon, m_q$. Since $\epsilon \in \text{ErExit}$ and thus $\epsilon \neq ok$, from our operational semantics we know that $n > 0$. As such, since $C = C_1; C_2$, $C_1, m_p \overset{n}{\Rightarrow} \epsilon, m_q$, $n > 0$ and $\epsilon \in \text{ErExit}$, from Lemma A.1 $C, m_p \overset{n}{\Rightarrow}, \epsilon, m_q$. That is, there exist n, $m_p, \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$ such that $C, m_p \overset{n}{\Rightarrow} \epsilon, m_q$, as required.

Case Seq
We then know $C = C_1; C_2$ for some C_1, C_2. Pick an arbitrary $s \in \text{State}$ and $m_q \in \lfloor q * \{s\} \rfloor$. Since from the premise of Seq we have $[r]\ C_2\ [\epsilon : q]$, from the inductive hypothesis we know there exist $m_r \in \lfloor r * \mathcal{I}^{-1}(s) \rfloor$, $k \in \mathbb{N}$ such that $C_2, m_r \overset{k}{\Rightarrow} \epsilon, m_q$. That is, there exist $s_r \in r$ and s_1 such that $(s_1, s) \in \mathcal{I}$ and $m_r \in \lfloor s_r \circ s_1 \rfloor$. On the other hand, since $s_r \in r$ and from the premise of Seq we have $[p]\ C_1\ [ok : r]$, from the inductive hypothesis we know there exist $m_p \in \lfloor p * \mathcal{I}^{-1}(s_1) \rfloor$, $n \in \mathbb{N}$ such that $C_1, m_p \overset{n}{\Rightarrow} ok, m_r$. That is, there exist $s_p \in p$ and s_2 such that $(s_2, s_1) \in \mathcal{I}$ and $m_p \in \lfloor s_p \circ s_2 \rfloor$. As such, since $(s_1, s) \in \mathcal{I}$, $(s_2, s_1) \in \mathcal{I}$ and $\mathcal{I}$ is transitive, we have $(s_2, s) \in \mathcal{I}$ and thus $s_2 \in \mathcal{I}^{-1}(s)$; i.e. $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$. Moreover, since $C = C_1; C_2$, $C_1, m_p \overset{n}{\Rightarrow} ok, m_r$, and $C_2, m_r \overset{k}{\Rightarrow} \epsilon, m_q$, from Lemma A.2 we know there exists j such that $C, m_p \overset{j}{\Rightarrow}, \epsilon, m_q$. That is, there exist $j \in \mathbb{N}$, $m_p, \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$ such that $C, m_p \overset{j}{\Rightarrow} \epsilon, m_q$, as required.

Case Loop1
We know there exists C_1 such that $C = C_1^\star$. Pick an arbitrary $s \in$ State and $m_p \in \lfloor p * \{s\} \rfloor$. As $\mathcal{I}$ is reflexive and thus $s \in \mathcal{I}^{-1}(s)$, we also have $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$. From the control flow transitions we have $C_1^\star \xrightarrow{\text{id}}$ `skip`. Moreover, from the definition of $[\![.]\!]$ we have $(m_p, m_p) \in [\![\text{id}]\!]ok$. On the other hand, from the operational semantics we have $\texttt{skip}, m_p \stackrel{0}{\Rightarrow} ok, m_p$. As such, as $C_1^\star \xrightarrow{\text{id}} \texttt{skip}$, $(m_p, m_p) \in [\![\text{id}]\!]ok$, $\texttt{skip}, m_p \stackrel{0}{\Rightarrow} ok, m_p$, from the operational semantics we have $C, m_p \stackrel{1}{\Rightarrow} ok, m_p$. That is, there exist $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$ and n=1 such that $C, m_p \stackrel{n}{\Rightarrow} ok, m_p$, as required.

Case Loop2
We know there exists C_1 such that $C = C_1^\star$. Pick arbitrary $s \in$ State and $m_q \in \lfloor q * \{s\} \rfloor$. From the premise of Loop2 we have $[p]\ C_1^\star; C_1\ [\epsilon : q]$ and thus from the inductive hypothesis we know there exists $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$ and n such that $C_1^\star; C_1, m_p \stackrel{n}{\Rightarrow} \epsilon, m_q$. From the control flow transitions we have $C_1^\star \xrightarrow{\text{id}} C_1^\star; C_1$. Moreover, from the $[\![.]\!]$ definition we have $(m_p, m_p) \in [\![\text{id}]\!]ok$. As such, as $C_1^\star \xrightarrow{\text{id}} C_1^\star; C_1$, $(m_p, m_p) \in [\![\text{id}]\!]ok$, $C_1^\star; C_1, m_p \stackrel{n}{\Rightarrow} \epsilon, m_q$, from the operational semantics we have $C, m_p \stackrel{n+1}{\Longrightarrow} \epsilon, m_q$. That is, there exist $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$, i such that $C, m_p \stackrel{i}{\Rightarrow} \epsilon, m_q$, as required.

Case Choice
We know there exist C_1, C_2 such that $C = C_1 + C_2$. Pick an arbitrary $s \in$ State and $m_q \in \lfloor q * \{s\} \rfloor$. From the premise of Choice we know there exists $i \in \{1, 2\}$ such that $[p]\ C_i\ [\epsilon : q]$, and thus from the inductive hypothesis we know there exists $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$ and n such that $C_i, m_p \stackrel{n}{\Rightarrow} \epsilon, m_q$. From the control flow transitions we have $C_1 + C_2 \xrightarrow{\text{id}} C_i$. Moreover, from the definition of $[\![.]\!]$ we have $(m_p, m_p) \in [\![\text{id}]\!]ok$. As such, as $C_1 + C_2 \xrightarrow{\text{id}} C_i$, $(m_p, m_p) \in [\![\text{id}]\!]ok$, $C_i, m_p \stackrel{n}{\Rightarrow} \epsilon, m_q$, from the operational semantics we have $C, m_p \stackrel{n+1}{\Longrightarrow} \epsilon, m_q$. That is, there exist $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$ and i=n+1 such that $C, m_p \stackrel{i}{\Rightarrow} \epsilon, m_q$, as required.

Case Cons
Pick an arbitrary $s \in$ State and $m_q \in \lfloor q * \{s\} \rfloor$. As form the premise of Cons we have $q \subseteq q'$, we also know that $m_q \in \lfloor q' * \{s\} \rfloor$. On the other hand, from the premise of Cons we have $[p']\ C\ [\epsilon : q']$ and thus from the inductive hypothesis we know there exist $m_p \in \lfloor p' * \mathcal{I}^{-1}(s) \rfloor$ and n such that $C, m_p \stackrel{n}{\Rightarrow} \epsilon, m_q$. Moreover, as $p' \subseteq p$ and $m_p \in \lfloor p' * \mathcal{I}^{-1}(s) \rfloor$ we also have $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$. That is, there exist $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$ and n such that $C, m_p \stackrel{n}{\Rightarrow} \epsilon, m_q$, as required.

Case GCons
Pick an arbitrary $s \in$ State and $m_q \in \lfloor q * \{s\} \rfloor$. As form the premise of Cons we have $q \preceq q'$, we also know that $m_q \in \lfloor q' * \{s\} \rfloor$. On the other hand, from the premise of Cons we have $[p']\ C\ [\epsilon : q']$ and thus from the inductive hypothesis we know there exist $m_p \in \lfloor p' * \mathcal{I}^{-1}(s) \rfloor$ and n such that $C, m_p \stackrel{n}{\Rightarrow} \epsilon, m_q$. Moreover, as $p' \preceq p$ and $m_p \in \lfloor p' * \mathcal{I}^{-1}(s) \rfloor$ we also have $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$. That is, there exist $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$ and n such that $C, m_p \stackrel{n}{\Rightarrow} \epsilon, m_q$, as required.

Case Frame
Note that Frame is used for PCMs with no interference, i.e. $\mathcal{I} \triangleq \text{ID}$. Pick an arbitrary $s \in$ State and $m_q \in \lfloor q * r * \{s\} \rfloor$. That is, there exists $s_q \in q$ and $s_r \in r$ such that $m_1 \in \lfloor s_q \circ s_r \circ s \rfloor$.

As from the premise of Frame we have $[p]$ C $[\epsilon : q]$, from the inductive hypothesis we know there exist $m_p \in \lfloor p * \{s_r \circ s\} \rfloor$ and n such that C, $m_p \overset{n}{\Rightarrow} \epsilon, m_q$. As such, since $s_r \in r$, we have $m_p \in \lfloor p * r * \mathcal{I}^{-1}(s) \rfloor$. That is, there exist $m_p \in \lfloor p * r * \{s\} \rfloor$ and n such that C, $m_p \overset{n}{\Rightarrow} \epsilon, m_q$, as required.

Case FrameInter
Pick an arbitrary $s \in$ State and $m_q \in \lfloor q * r * \{s\} \rfloor$. That is, there exists $s_q \in q$ and $s_r \in r$ such that $m_1 \in \lfloor s_q \circ s_r \circ s \rfloor$. As from the premise of Frame we have $[p]$ C $[\epsilon : q]$, from the inductive hypothesis we know there exist $m_p \in \lfloor p * \mathcal{I}^{-1}(s_r \circ s) \rfloor$ and n such that C, $m_p \overset{n}{\Rightarrow} \epsilon, m_q$. Given the properties on $\mathcal{I}$ (Par. 9) and the definition of $\mathcal{I}^{-1}$ we then know there exist s', s'_r, s'' such that $s''{=}s'_r \circ s'$, $s'' \in \mathcal{I}^{-1}(s_r \circ s)$, i.e. $(s'', s_r \circ s) \in \mathcal{I}$, $m_p \in \lfloor p * \{s'_r\} * \{s'\} \rfloor$, $(s'_r, s_r) \in \mathcal{I}$, $(s', s) \in \mathcal{I}$ and thus $s' \in \mathcal{I}^{-1}(s)$. Moreover, as stable$(r)$ holds (i.e. $\mathcal{I}^{-1}(r) \subseteq r$), $s_r \in r$ and $(s'_r, s_r) \in \mathcal{I}$ (i.e. $s'_r \in \mathcal{I}^{-1}(s_r)$), we also have $s'_r \in r$. As such, we have $m_p \in \lfloor p * r * \mathcal{I}^{-1}(s) \rfloor$. That is, there exist $m_p \in \lfloor p * r * \mathcal{I}^{-1}(s) \rfloor$ and n such that C, $m_p \overset{n}{\Rightarrow} \epsilon, m_q$, as required.

Case Disj
Pick an arbitrary $s \in$ State and $m_q \in \lfloor (q_1 \vee q_2) * \{s\} \rfloor$. We then know there exists $i \in \{1,2\}$ such that $m_q \in \lfloor (q_i) * \{s\} \rfloor$. From the premise of Disj we have $[p_i]$ C $[\epsilon : q_i]$ and thus from the inductive hypothesis we know there exists $m_p \in \lfloor p_i * \mathcal{I}^{-1}(s) \rfloor$ and n_i such that C, $m_p \overset{n_i}{\Rightarrow} \epsilon, m_q$. Moreover, since $p_i \subseteq p_1 \vee p_2$ and $m_p \in \lfloor p_i * \mathcal{I}^{-1}(s) \rfloor$, we also have $m_p \in \lfloor (p_1 \vee p_2) * \mathcal{I}^{-1}(s) \rfloor$. That is, there exist $m_p \in \lfloor (p_1 \vee p_2) * \mathcal{I}^{-1}(s) \rfloor$ and n such that C, $m_p \overset{n}{\Rightarrow} \epsilon, m_q$, as required.

Case Par
Note that Frame is used for PCMs with no interference, i.e. $\mathcal{I} \triangleq \mathsf{ID}$. It thus suffices to show:

$$\forall s \in \text{State}.\ \forall m_q \in \lfloor q_1 * q_2 * \{s\} \rfloor.\ \exists k \in \mathbb{N}, m_p \in \lfloor p_1 * p_2 * \{s\} \rfloor.\ \mathrm{C}_1 \,||\, \mathrm{C}_2, m_p \overset{k}{\Rightarrow} ok, m_q$$

Let $P_1 \triangleq p_1 * p_2$, $Q_1 \triangleq q_1 * p_2$, $P_2 \triangleq Q_1$ and $Q_2 \triangleq q_1 * q_2$. As from the premise of Par we have $[p_i]$ C_i $[ok\colon q_i]$ for all $i \in \{1,2\}$, from the Frame rule (whose soundness we established above) we also have $[P_i]$ C_i $[ok\colon Q_i]$ for all $i \in \{1,2\}$. Consequently, from the inductive hypotheses we know that for all $i \in \{1,2\}$:

$$\forall s \in \text{State}.\ \forall m_q \in \lfloor Q_i * \{s\} \rfloor.\ \exists k \in \mathbb{N}, m_p \in \lfloor P_i * \{s\} \rfloor.\ \mathrm{C}_i, m_p \overset{k}{\Rightarrow} ok, m_q \qquad \text{(ok-i)}$$

Pick arbitrary $s \in$ State and $m_q \in \lfloor (q_1 * q_2) * \{s\} \rfloor$. That is, $m_q \in \lfloor Q_2 * \{s\} \rfloor$. From (ok-i) we then know there exist m_p^2, k^2 such that $m_p^2 \in \lfloor P_2 * \{s\} \rfloor$ and $\mathrm{C}_2, m_p^2 \overset{k^2}{\Rightarrow} ok, m_p^2$. Similarly, as $m_p^2 \in \lfloor P_2 * \{s_2\} \rfloor$ and $Q_1 = P_2$, from (ok-i) we know there exist m_p^1, k^1 such that: $m_p^1 \in \lfloor P_1 * \{s\} \rfloor$ and $\mathrm{C}_1, m_p^1 \overset{k^1}{\Rightarrow} ok, m_p^2$. Let $s_3 = s$ and $m_p^3 = m_q$. As such, since $\mathrm{C}_1, m_p^1 \overset{k^1}{\Rightarrow} ok, m_p^2$ and $\mathrm{C}_2, m_p^2 \overset{k^2}{\Rightarrow} ok, m_p^2$, from Lemma A.4 we know there exist j such that $\mathrm{C}_1 \,||\, \mathrm{C}_2, m_p^1 \overset{j}{\Rightarrow} ok, m_q$. Consequently, from the definition of P_1 we know there exist $j \in \mathbb{N}$ and $m_p^1 \in \lfloor p_1 * p_2 * \{s\} \rfloor$ such that $\mathrm{C}_1 \,||\, \mathrm{C}_2, m_p^1 \overset{j}{\Rightarrow} ok, m_q$, as required.

Case ParInter
We then have $\mathrm{C} = \mathrm{C}_1 \,||\, \mathrm{C}_2$ for some $\mathrm{C}_1, \mathrm{C}_2$, stable$(p_1, q_2) \vee$ stable(p_2, q_1), and $\vdash [p_i]$ C_i $[ok\colon q_i]$ for all $i \in \{1,2\}$. There are two cases two consider: 1) stable(p_2, q_1); or 2) stable(p_1, q_2). In case (1) we

can then derive:

$$\dfrac{\dfrac{\dfrac{[p_1]\ \mathsf{C}_1\ [ok\colon q_1] \quad \text{stable}(p_2)}{[p_1 * p_2]\ \mathsf{C}_1\ [ok\colon q_1 * p_2]}\ \textsc{FrameInter} \qquad \dfrac{[p_2]\ \mathsf{C}_2\ [ok\colon q_2] \quad \text{stable}(q_1)}{[q_1 * p_2]\ \mathsf{C}_1\ [ok\colon q_1 * q_2]}\ \textsc{FrameInter}}{[p_1 * p_2]\ \mathsf{C}_1; \mathsf{C}_2\ [ok\colon q_1 * q_2]}\ \textsc{Seq}}{[p_1 * p_2]\ \mathsf{C}_1 \,||\, \mathsf{C}_2\ [ok\colon q_1 * q_2]}\ \textsc{ParSeq}$$

In case (2) we can then derive:

$$\dfrac{\dfrac{\dfrac{[p_2]\ \mathsf{C}_1\ [ok\colon q_2] \quad \text{stable}(p_1)}{[p_1 * p_2]\ \mathsf{C}_1\ [ok\colon p_1 * q_2]}\ \textsc{FrameInter} \qquad \dfrac{[p_1]\ \mathsf{C}_2\ [ok\colon q_1] \quad \text{stable}(q_2)}{[p_1 * q_2]\ \mathsf{C}_1\ [ok\colon q_1 * q_2]}\ \textsc{FrameInter}}{[p_1 * p_2]\ \mathsf{C}_2; \mathsf{C}_1\ [ok\colon q_1 * q_2]}\ \textsc{Seq}}{[p_1 * p_2]\ \mathsf{C}_1 \,||\, \mathsf{C}_2\ [ok\colon q_1 * q_2]}\ \textsc{ParSeq}$$

Case ParEr

We then have $\mathsf{C} = \mathsf{C}_1 \,||\, \mathsf{C}_2$ for some $\mathsf{C}_1, \mathsf{C}_2$. Pick an arbitrary $s \in \textsc{State}$ and $m_q \in \lfloor q * \{s\} \rfloor$. From the premise of ParEr we know that $\epsilon \in \textsc{ErExit}$ and $[p]\ \mathsf{C}_i\ [\epsilon : q]$ for some $i \in \{1 \cdots n\}$. As such, from the inductive hypothesis we know there exists $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$ and k such that $\mathsf{C}_i, m_p \overset{k}{\Rightarrow} \epsilon, m_q$. Consequently, as $\epsilon \in \textsc{ErExit}$, from Lemma A.5 we have $\mathsf{C}_1 \,||\, \mathsf{C}_2, m_p \overset{k}{\Rightarrow} \epsilon, m_q$, as required.

Case ParL

We then have $\mathsf{C} = \mathsf{C}_1 \,||\, \mathsf{C}_2$ for some $\mathsf{C}_1, \mathsf{C}_2$. Pick an arbitrary $s \in \textsc{State}$ and $m_q \in \lfloor q * \{s\} \rfloor$. From the premise of ParL we know there exist $\mathsf{C}_3, \mathsf{C}_4$ such that $\mathsf{C}_1 {=} \mathsf{C}_3; \mathsf{C}_4$ and $[r]\ \mathsf{C}_4 \,||\, \mathsf{C}_2\ [\epsilon : q]$. As such, from the inductive hypothesis we know there exist $m_r \in \lfloor r * \mathcal{I}^{-1}(s) \rfloor$, $k \in \mathbb{N}$ such that $\mathsf{C}_4 \,||\, \mathsf{C}_2, m_r \overset{k}{\Rightarrow} \epsilon, m_q$. That is, there exist $s_r \in r$ and s_1 such that $(s_1, s) \in \mathcal{I}$ and $m_r \in \lfloor s_r \circ s_1 \rfloor$. On the other hand, since $s_r \in r$ and from the premise of ParL we have $[p]\ \mathsf{C}_3\ [ok\colon r]$, from the inductive hypothesis we know there exist $m_p \in \lfloor p * \mathcal{I}^{-1}(s_1) \rfloor$, $j \in \mathbb{N}$ such that $\mathsf{C}_3, m_p \overset{j}{\Rightarrow} ok, m_r$. That is, there exist $s_p \in p$ and s_2 such that $(s_2, s_1) \in \mathcal{I}$ and $m_p \in \lfloor s_p \circ s_2 \rfloor$. As such, since $(s_1, s) \in \mathcal{I}$, $(s_2, s_1) \in \mathcal{I}$ and $\mathcal{I}$ is transitive, we have $(s_2, s) \in \mathcal{I}$ and thus $s_2 \in \mathcal{I}^{-1}(s)$; i.e. $m_p \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$. Moreover, since $\mathsf{C}_3, m_p \overset{j}{\Rightarrow} ok, m_r$, $\mathsf{C}_4 \,||\, \mathsf{C}_2, m_r \overset{k}{\Rightarrow} \epsilon, m_q$ and $\mathsf{C}_1 = \mathsf{C}_3; \mathsf{C}_4$ from Lemma A.6 we know there exists b such that $\mathsf{C}_1 \,||\, \mathsf{C}_2, m_p \overset{b}{\Rightarrow}, \epsilon, m_q$. That is, there exist $b \in \mathbb{N}$, $m_p, \in \lfloor p * \mathcal{I}^{-1}(s) \rfloor$ such that $\mathsf{C}, m_p \overset{j}{\Rightarrow} \epsilon, m_q$, as required.

The proof of ParR is analogous to that of ParL and is omitted here. □

Theorem A.8 (Soundness). *For all $p, \mathsf{C}, q, \epsilon$, if $\vdash [p]\ \mathsf{C}\ [\epsilon : q]$ holds, then $\models [p]\ \mathsf{C}\ [\epsilon : q]$ also holds.*

Proof. Pick arbitrary $p, \mathsf{C}, q, \epsilon$ such that $\vdash [p]\ \mathsf{C}\ [\epsilon : q]$ holds. Pick an arbitrary $m_q \in \lfloor q \rfloor$. That is, there exists $s_q \in q$ such that $m_q \in \lfloor s_q \rfloor$. From the definition of $\circ$ we then know there exists $s_0 \in \textsc{State}^0$ such that $s_q {=} s_q \circ s_0$. As such, from Lemma A.7 we know there exists $m_p \in \lfloor p * \mathcal{I}^{-1}(s_0) \rfloor$ and $n \in \mathbb{N}$ such that $\mathsf{C}, m_p \overset{n}{\Rightarrow} \epsilon, m_q$. Moreover, from the properties of $\mathcal{I}$ (Par. 9) and since $s_0 \in \textsc{State}^0$ we know that $\mathcal{I}^{-1}(s_0) \subseteq \textsc{State}^0$. Consequently, from the definition of $*$ and the properties of $\textsc{State}^0$ (Par. 2) we know $p * \mathcal{I}^{-1}(s_0) \subseteq p$ and thus $\lfloor p * \mathcal{I}^{-1}(s_0) \rfloor \subseteq \lfloor p \rfloor$. That is, we know there exists $m_p \in \lfloor p \rfloor$ and $n \in \mathbb{N}$ such that $\mathsf{C}, m_p \overset{n}{\Rightarrow} \epsilon, m_q$, as required. □

B CISL_{DC} AXIOM SOUNDNESS

CISL_{DC} Machine States. We assume a Boolean interpretation function, $[\![.]\!]_{(.)} : \text{BAST}\times\text{STATE}_{\text{DC}} \to \text{VAL}$, evaluating Boolean assertions against a machine state. We lift this function to machine states, and given $m \in \text{MSTATE}_{\text{DC}}$, we write $[\![.]\!]_m$ for $[\![.]\!]_s$, where $s \triangleq \bigcup_{x\in dom(m)} [x \mapsto (m(x), 1)]$.

$$
\begin{aligned}
&[\![\text{L}\colon \texttt{error}]\!]_{\text{A}}\,ok \triangleq \emptyset \qquad\qquad [\![\texttt{assume}(B)]\!]_{\text{A}}\,ok \triangleq \{m \mid [\![B]\!]_m \neq 0\}\\
&[\![x := v]\!]_{\text{A}}\,ok \triangleq \big\{(m, m[x \mapsto v]) \,\big|\, x \in dom(m)\big\}\\
&[\![x := \texttt{alloc()}]\!]_{\text{A}}\,ok \triangleq \big\{(m, m[x \mapsto l] \uplus [l \mapsto v]) \,\big|\, v \in \text{VAL} \land x \in dom(m) \land l \notin dom(m)\big\}\\
&[\![x := v]\!]_{\text{A}}\,mse(.) = [\![x := \texttt{alloc()}]\!]_{\text{A}}\,mse(.) = [\![\texttt{assume}(B)]\!]_{\text{A}}\,mse(.) = [\![\texttt{error}]\!]_{\text{A}}\,mse(.) \triangleq \emptyset\\
&[\![\text{L}\colon \texttt{free}(x)]\!]_{\text{A}}\,ok \triangleq \big\{(m, m[l \mapsto \bot]) \,\big|\, \exists l.\ m(x) = l \land m(l) \in \text{VAL}\big\}\\
&[\![\text{L}\colon \texttt{free}(x)]\!]_{\text{A}}\,mse(\text{L}') \triangleq \big\{(m, m) \,\big|\, \text{L} = \text{L}' \land \exists l.\ m(x) = l \land m(l) = \bot\big\}\\
&[\![\text{L}\colon x := [y]]\!]_{\text{A}}\,ok \triangleq \big\{(m, m[x \mapsto v]) \,\big|\, x \in dom(m) \land \exists l.\ m(y) = l \land m(l) = v \in \text{VAL}\big\}\\
&[\![\text{L}\colon x := [y]]\!]_{\text{A}}\,mse(\text{L}') \triangleq \big\{(m, m) \,\big|\, \text{L} = \text{L}' \land x \in dom(m) \land \exists l.\ m(y) = l \land m(l) = \bot\big\}\\
&[\![\text{L}\colon [x] := y]\!]_{\text{A}}\,ok \triangleq \big\{(m, m[l \mapsto m(y)]) \,\big|\, y \in dom(m) \land \exists l.\ m(x)=l \land m(l) \in \text{VAL}\big\}\\
&[\![\text{L}\colon [x] := y]\!]_{\text{A}}\,mse(\text{L}') \triangleq \big\{(m, m) \,\big|\, \text{L} = \text{L}' \land y \in dom(m) \land \exists l.\ m(x)=l \land m(l) = \bot\big\}\\
&[\![\text{a}]\!]_{\text{A}}\,er(\text{L}) \triangleq \begin{cases} \{(m, m) \mid m \in \text{MSTATE}_{\text{DC}}\} & \text{if } \text{a} = \text{L}\colon \texttt{error}\\ \emptyset & \text{otherwise}\end{cases}
\end{aligned}
$$

B.1 CISL_{DC} Axiom Soundness

THEOREM B.1 (CISL_{DC} AXIOMS SOUNDNESS). *For all $(p, l, \epsilon, q) \in \text{ATOM}_{DC}$ the following holds:*

$$\forall s \in \text{STATE}_{DC}, m_q \in \lfloor q * \{s\}\rfloor_{DC}.\ \exists m_p \in \lfloor p * \mathcal{I}_{DC}^{-1}(s)\rfloor_{DC}.\ (m_p, m_q) \in [\![l]\!]_{\text{A}}\epsilon$$

PROOF. Pick an arbitrary $(p, l, \epsilon, q) \in \text{ATOM}_{\text{DC}}$. Note that as the CISL_{DC} interference is simply defined as the identity relation, it suffices to show that the following holds:

$$\forall s \in \text{STATE}_{\text{DC}}, m_q \in \lfloor q * \{s\}\rfloor_{\text{DC}}.\ \exists m_p \in \lfloor p * \{s\}\rfloor_{\text{DC}}.\ (m_p, m_q) \in [\![l]\!]_{\text{A}}\epsilon$$

We proceed by induction on the structure of (p, l, ϵ, q).

Case DC-ASSUME
We then have $l = \texttt{assume}(B)$, that $\epsilon = ok$, $q = \mathop{\circledast}_{x_i\in pvars(B)} x_i \overset{\pi_i}{\mapsto} v_i \land B[\overline{v_i/x_i}]$, and $p = \mathop{\circledast}_{x_i\in pvars(B)} x_i \overset{\pi_i}{\mapsto} v_i$. Pick an arbitrary $s \in \text{STATE}_{\text{DC}}$ and $m_q \in \lfloor q * \{s\}\rfloor_{\text{DC}}$. From the definitions of $\lfloor.\rfloor_{\text{DC}}$ and $*$ we then know that there exists $s_q \in q$ such that $m_q \in \lfloor s_q \circ_{\text{DC}} s\rfloor_{\text{DC}}$ and $[\![B]\!]_{s_q} \neq 0$. From the definition of $[\![.]\!]_\sigma$ we then know $[\![B]\!]_{m_q} \neq 0$

Let $s_p = s_q$ and $m_p = m_q$. From the definitions of $\lfloor.\rfloor_{\text{DC}}$ and $*$ we then know that $s_p \in p$ and $m_p \in \lfloor p * \{s\}\rfloor_{\text{DC}}$. On the other hand, since $[\![B]\!]_{m_q} \neq 0$ and $m_p = m_q$, we also have $[\![B]\!]_{m_p} \neq 0$. As such, from the definition of $[\![\texttt{assume}(B)]\!]_{\text{A}}\,ok$ we have $(m_p, m_q) \in [\![\texttt{assume}(B)]\!]_{\text{A}}\,ok$, as required.

Case DC-ERROR
We then have $l = \text{L}\colon \texttt{error}$, that $\epsilon = er(\text{L})$, $q = \text{emp}$, and $p = q$. Pick an arbitrary $s \in \text{STATE}_{\text{DC}}$ and $m_q \in \lfloor q * \{s\}\rfloor_{\text{DC}}$. From the definitions of $\lfloor.\rfloor_{\text{DC}}$ and $*$ we then know that there exists $s_q \in q$ such that $s_q = \emptyset$, and $m_q \in \lfloor s\rfloor_{\text{DC}}$.

Let $s_p = s_q$ and $m_p = m_q$. From the definitions of $\lfloor . \rfloor_{\mathrm{DC}}$ and $*$ we then know that $s_p \in p$ and $m_p \in \lfloor p * \{s\} \rfloor_{\mathrm{DC}}$. Moreover, from the definition of $[\![\textsc{l}\colon \mathtt{error}]\!]_{\mathrm{A}}\, er(\textsc{l})$ we have $(m_p, m_q) \in [\![\textsc{l}\colon \mathtt{error}]\!]_{\mathrm{A}}\, er(\textsc{l})$, as required.

Case DC-Assign
We then have $l = x := v$ for some x, v, that $\epsilon = ok$, $q = x \mapsto v$, and $p = x \mapsto v'$ for some v'. Pick an arbitrary $s \in \textsc{State}_{\mathrm{DC}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\mathrm{DC}}$. From the definitions of $\lfloor . \rfloor_{\mathrm{DC}}$ and $*$ we then know that there exist $s_q \in q$ such that $s_q = [x \mapsto (v, 1)]$, $x \notin dom(s)$, and $m_q \in \lfloor s_q \circ_{\mathrm{DC}} s \rfloor_{\mathrm{DC}}$.

Let $s_p = [x \mapsto v']$ and pick $m_p = m_q[x \mapsto v']$. From the definitions of $\lfloor . \rfloor_{\mathrm{DC}}$ and $*$ we then know that $s_p \in p$ and $m_p \in \lfloor p * \{s\} \rfloor_{\mathrm{DC}}$. Moreover, from the definition of $[\![x := v]\!]_{\mathrm{A}}\, ok$ we have $(m_p, m_q) \in [\![x := v]\!]_{\mathrm{A}}\, ok$, as required.

Case DC-Load
We then have $l = x := [y]$ for some x, y, that $\epsilon = ok$, $q = x \mapsto v * y \overset{\pi_y}{\mapsto} l * l \overset{\pi}{\mapsto} v$ for some v, l, π, and $p = x \mapsto v' * y \overset{\pi_y}{\mapsto} l * l \overset{\pi}{\mapsto} v$ for some v'. Pick an arbitrary $s \in \textsc{State}_{\mathrm{DC}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\mathrm{DC}}$. From the definitions of $\lfloor . \rfloor_{\mathrm{DC}}$ and $*$ we then know that there exist $s_q \in q$ such that $s_q = [x \mapsto (v, 1)] \circ_{\mathrm{DC}} [y \mapsto (l, \pi_y)] \circ_{\mathrm{DC}} [l \mapsto (v, \pi)]$, $x \notin dom(s)$, $(\pi_y{=}1 \land y \notin dom(s)) \lor (\pi_y < 1 \land s(y){=}(l, \pi'_y) \land \pi_y{+}\pi'_y \leq 1)$ for some π'_y, $(\pi{=}1 \land l \notin dom(s)) \lor (\pi < 1 \land s(l){=}(v, \pi') \land \pi{+}\pi' \leq 1)$ for some π', and $m_q = \lfloor s \circ_{\mathrm{DC}} [x \mapsto (v, 1)] \circ_{\mathrm{DC}} [y \mapsto (l, \pi_y)] \circ_{\mathrm{DC}} [l \mapsto (v, \pi)] \rfloor_{\mathrm{DC}}$.

Let $s_p = [x \mapsto (v', 1)] \circ_{\mathrm{DC}} [y \mapsto (l, \pi_y)] \circ_{\mathrm{DC}} [l \mapsto (v, \pi)]$ and $m_p = m_q[x \mapsto v']$. From the definitions of $\lfloor . \rfloor_{\mathrm{DC}}$ and $*$ we then know that $s_p \in p$ and $m_p \in \lfloor p * \{s\} \rfloor_{\mathrm{DC}}$. Moreover, from the definition of $[\![x := [y]]\!]_{\mathrm{A}}\, ok$ we have $(m_p, m_q) \in [\![x := [y]]\!]_{\mathrm{A}}\, ok$, as required.

Case DC-LoadEr
We then have $l = \textsc{l}\colon x := [y]$ for some $x, y, \textsc{l}$, that $\epsilon = mse(\textsc{l})$, $q = y \overset{\pi_y}{\mapsto} l * l \overset{\pi}{\not\mapsto}$ for some v, l, π, and $p = q$. Pick an arbitrary $s \in \textsc{State}_{\mathrm{DC}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\mathrm{DC}}$. From the definitions of $\lfloor . \rfloor_{\mathrm{DC}}$ and $*$ we then know that there exist $s_q \in q$ such that $s_q = [y \mapsto (l, \pi_y)] \circ_{\mathrm{DC}} [l \mapsto (\bot, \pi)]$, $(\pi_y{=}1 \land y \notin dom(s)) \lor (\pi_y < 1 \land s(y){=}(l, \pi'_y) \land \pi_y{+}\pi'_y \leq 1)$ for some π'_y, $(\pi{=}1 \land l \notin dom(s)) \lor (\pi < 1 \land s(l){=}(\bot, \pi') \land \pi{+}\pi' \leq 1)$ for some π', and $m_q = \lfloor s \circ_{\mathrm{DC}} [y \mapsto (l, \pi_y)] \circ_{\mathrm{DC}} [l \mapsto (\bot, \pi)] \rfloor_{\mathrm{DC}}$.

Let $s_p = s_q$ and $m_p = m_q$. We then simply have $m_p \in \lfloor p * \{s\} \rfloor_{\mathrm{DC}}$. Moreover, from the definition of $[\![\textsc{l}\colon x := [y]]\!]_{\mathrm{A}}\, mse(\textsc{l})$ we have $(m_p, m_q) \in [\![\textsc{l}\colon x := [y]]\!]_{\mathrm{A}}\, mse(\textsc{l})$, as required.

The proofs of the DC-Store and DC-StoreEr cases are analogous to those of DC-Load and DC-LoadEr respectively, and are omitted here.

Case DC-Alloc
We then have $l = x := \mathtt{alloc()}$ for some x, that $\epsilon = ok$, $q = x \mapsto l * l \mapsto v$ for some v, l, and $p = x \mapsto v'$ for some v'. Pick an arbitrary $s \in \textsc{State}_{\mathrm{DC}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\mathrm{DC}}$. From the definitions of $\lfloor . \rfloor_{\mathrm{DC}}$ and $*$ we then know that there exist $s_q \in q, \sigma, h, \mathbf{h}$ such that $s_q = [x \mapsto (l, 1)] \circ_{\mathrm{DC}} [l \mapsto (v, 1)]$, $x, l \notin dom(s)$, and $m_q = \lfloor s \circ_{\mathrm{DC}} [x \mapsto (l, 1)] \circ_{\mathrm{DC}} [l \mapsto (v, 1)] \rfloor_{\mathrm{DC}}$.

Let $s_p = [x \mapsto (v', 1)]$ and $m_p = \lfloor s \circ_{\mathrm{DC}} [x \mapsto (v', 1)] \rfloor_{\mathrm{DC}}$ (from the definitions of $\circ_{\mathrm{DC}}$, s and s_p we know this is defined). From the definitions of $\lfloor . \rfloor_{\mathrm{DC}}$ and $*$ we then know that $s_p \in p$ and $m_p \in \lfloor p * \{s\} \rfloor_{\mathrm{DC}}$. Moreover, from the definition of $[\![x := \mathtt{alloc()}]\!]_{\mathrm{A}}\, ok$ we have $(m_p, m_q) \in [\![x := \mathtt{alloc()}]\!]_{\mathrm{A}}\, ok$, as required.

Case DC-Free
We then have $l = \mathtt{free}(x)$ for some x, that $\epsilon = ok$, $q = x \overset{\pi}{\mapsto} l * l \not\mapsto$ for some l, and $p = x \mapsto l\pi * l \mapsto v$

for some v. Pick an arbitrary $s \in \textsc{State}_{\text{DC}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\text{DC}}$. From the definitions of $\lfloor . \rfloor_{\text{DC}}$ and $*$ we then know that there exist $s_q \in q$ such that $s_q = [x \mapsto (l, \pi)] \circ_{\text{DC}} [l \mapsto (\bot, 1)]$, $(\pi{=}1 \land x \notin dom(s)) \lor (\pi < 1 \land s(x){=}(l, \pi') \land \pi{+}\pi' \leq 1)$ for some π', $l \notin dom(s)$, and $m_q = \lfloor s \circ_{\text{DC}} [x \mapsto (l, \pi)] \circ_{\text{DC}} [l \mapsto (\bot, 1)] \rfloor_{\text{DC}}$.

Let $s_p = [x \mapsto (l, \pi)] \circ_{\text{DC}} [l \mapsto (v, 1)]$ and $m_p = m_q[x \mapsto v]$. From the definitions of $\lfloor . \rfloor_{\text{DC}}$ and $*$ we then know that $s_p \in p$ and $m_p \in \lfloor p * \{s\} \rfloor_{\text{DC}}$. Moreover, from the definition of $[\![\texttt{free}(x)]\!]_{\text{A}} ok$ we have $(m_p, m_q) \in [\![\texttt{free}(x)]\!]_{\text{A}} ok$, as required.

Case DC-FreeEr

We then have $l = \text{L}\colon \texttt{free}(x)$ for some x, L, that $\epsilon = mse(\text{L})$, $q = x \overset{\pi_x}{\mapsto} l * l \overset{\pi}{\not\mapsto}$ for some l, π, π_x, and $p = q$. Pick an arbitrary $s \in \textsc{State}_{\text{DC}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\text{DC}}$. From the definitions of $\lfloor . \rfloor_{\text{DC}}$ and $*$ we then know that there exist $s_q \in q$ such that $s_q = [x \mapsto (l, \pi_x)] \circ_{\text{DC}} [l \mapsto (\bot, \pi)]$, $(\pi_x{=}1 \land x \notin dom(s)) \lor (\pi_x < 1 \land s(x){=}(l, \pi') \land \pi_x{+}\pi'_x \leq 1)$ for some π'_x, $(\pi{=}1 \land l \notin dom(s)) \lor (\pi < 1 \land s(l){=}(\bot, \pi') \land \pi{+}\pi' \leq 1)$ for some π', and $m_q = \lfloor s \circ_{\text{DC}} [x \mapsto (l, \pi_x)] \circ_{\text{DC}} [l \mapsto (\bot, \pi)] \rfloor_{\text{DC}}$.

Let $s_p = s_q$ and $m_p = m_q$. We then simply have $m_p \in \lfloor p * \{s\} \rfloor_{\text{DC}}$. Moreover, from the definition of $[\![\text{L}\colon \texttt{free}(x)]\!]_{\text{A}} mse(\text{L})$ we have $(m_p, m_q) \in [\![\text{L}\colon \texttt{free}(x)]\!]_{\text{A}} mse(\text{L})$, as required.

□

C CISL$_{\text{RD}}$ SOUNDNESS

Theorem C.1 (CISL$_{\text{RD}}$ axioms soundness). *For all $(p, l, \epsilon, q) \in \textsc{Atom}_{RD}$ the following holds:*

$$\forall s \in \textsc{State}_{RD}, m_q \in \lfloor q * \{s\} \rfloor_{RD}.\ \exists m_p \in \lfloor p * \mathcal{I}_{RD}^{-1}(s) \rfloor_{RD}.\ (m_p, m_q) \in [\![l]\!]_{\text{A}} \epsilon$$

Proof. Pick an arbitrary $(p, l, \epsilon, q) \in \textsc{Atom}_{\text{RD}}$. Note that as the CISL$_{\text{RD}}$ interference is simply defined as the identity relation, it suffices to show that the following holds:

$$\forall s \in \textsc{State}_{\text{RD}}, m_q \in \lfloor q * \{s\} \rfloor_{\text{RD}}.\ \exists m_p \in \lfloor p * \{s\} \rfloor_{\text{RD}}.\ (m_p, m_q) \in [\![l]\!]_{\text{A}} \epsilon$$

We proceed by induction on the structure of (p, l, ϵ, q).

Case RD-Lock

We then have $l = \texttt{lock}_\tau\ l$ for some τ, l, that $\epsilon = ok$, $q = \tau \mapsto (H +\!\!+ \mathsf{L}(\tau, l), S \uplus \{l\})$ for some H, S such that $l \notin S$, and $p = \tau \mapsto (H, S)$. Let $H' \triangleq H +\!\!+ \mathsf{L}(\tau, l)$. Pick an arbitrary $s \in \textsc{State}_{\text{RD}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\text{RD}}$. From the definitions of $\lfloor . \rfloor_{\text{RD}}$ and $*$ we then know that there exist $s_q \in q, H_q$ such that $s_q = ([\tau \mapsto (H', S \uplus \{l\})], \tau \notin dom(s), m_q = H_q, H' = H_q|_\tau, \forall \tau' \in dom(s).\ s(\tau') = (H'', -) \Rightarrow H'' = H_q|_{\tau'}$ and $\mathsf{wf}(H_q)$. That is, there exists H_1, H_2, H_p such that $H_q = H_1 +\!\!+ \mathsf{L}(\tau, l) +\!\!+ H_2$, $\forall e \in H_2.\ e.\mathsf{tid} \neq \tau$, $H_p = H_1 +\!\!+ H_2$, and $H = H_p|_\tau$, $\forall \tau' \in dom(s).\ s(\tau') = (H'', -) \Rightarrow H'' = H_p|_{\tau'}$.

Let s_p=$[\tau \mapsto (H, S)]$ and m_p=H_p. From the definitions of $\lfloor . \rfloor_{\text{RD}}$, H_p and $*$ we then know that $s_p \in p$, that $p * \{s\}$ is defined (since $\tau \notin dom(s)$), and that $m_p \in \lfloor p * \{s\} \rfloor_{\text{RD}}$. Moreover, as $\mathsf{wf}(H_q)$, $\forall e \in H_2.\ e.\mathsf{tid} \neq \tau$, H_q=$H_1 +\!\!+ \mathsf{L}(\tau, l) +\!\!+ H_2$ and H_p=$H_1 +\!\!+ H_2$, it is straightforward to show that $\mathsf{wf}(H_p)$. Finally, from the definition of $[\![.]\!]_{\text{A}}$ we have $(m_p, m_q) \in [\![\texttt{lock}_\tau\ l]\!]_{\text{A}} ok$, as required.

The proof of the RD-Unlock case is analogous and thus omitted here.

Case RD-Read

We then have $l = \text{L}\colon a :=_\tau x$ for some τ, x, L, that $\epsilon = ok$, $q = \tau \mapsto (H +\!\!+ e, S)$ for some H, e, S such that $e = \mathsf{R}(\text{L}, \tau, x)S$, and that $p = \tau \mapsto (H, S)$. Let $H' \triangleq H +\!\!+ e$. Pick an arbitrary $s \in \textsc{State}_{\text{RD}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\text{RD}}$. From the definitions of $\lfloor . \rfloor_{\text{RD}}$ and $*$ we then know that there exist $s_q \in q, H_q$ such that $s_q = ([\tau \mapsto (H', S)], \tau \notin dom(s), m_q = H_q, H' = H_q|_\tau, \forall \tau' \in dom(s).\ s(\tau') = (H'', -) \Rightarrow H'' = H_q|_{\tau'}$ and $\mathsf{wf}(H_q)$. That is, there exists H_1, H_2, H_p such that $H_q = H_1 +\!\!+ e +\!\!+ H_2$, $\forall e \in H_2.\ e.\mathsf{tid} \neq \tau$, $H_p = H_1 +\!\!+ H_2$, and $H = H_p|_\tau$, $\forall \tau' \in dom(s).\ s(\tau') = (H'', -) \Rightarrow H'' = H_p|_{\tau'}$. Moreover, from the definitions of H_p, H_q we have: $\forall \tau'.\ \mathsf{locks}(H_p, \tau') = \mathsf{locks}(H_q, \tau')$.

Let s_p=$[\tau \mapsto (H, S)]$ and m_p=H_p. From the definitions of $\lfloor . \rfloor_{\text{RD}}$, H_p and $*$ we then know that $s_p \in p$, that $p * \{s\}$ is defined (since $\tau \notin dom(s)$), and that $m_p \in \lfloor p * \{s\} \rfloor_{\text{RD}}$. Moreover, as $\mathsf{wf}(H_q)$ and $\forall \tau'.\ \mathsf{locks}(H_p, \tau') = \mathsf{locks}(H_q, \tau')$, H_q=$H_1 +\!\!+ \mathsf{L}(\tau, l) +\!\!+ H_2$ and H_p=$H_1 +\!\!+ H_2$, it is straightforward to show that $\mathsf{wf}(H_p)$. Finally, from the definition of of $[\![.]\!]_{\text{A}}$ we have $(m_p, m_q) \in [\![\text{L}\colon a :=_\tau x]\!]_{\text{A}} ok$, as required.

The proof of the RD-Write case is analogous and thus omitted here. □

D CISL$_{\mathrm{DD}}$ SOUNDNESS

Theorem D.1 (CISL$_{\mathrm{DD}}$ axioms soundness). *For all* $(p, l, \epsilon, q) \in \text{Atom}_{DD}$ *the following holds:*

$$\forall s \in \text{State}_{DD}, m_q \in \lfloor q * \{s\} \rfloor_{DD}. \exists m_p \in \lfloor p * \mathcal{I}_{DD}^{-1}(s) \rfloor_{DD}. (m_p, m_q) \in [\![l]\!]_{\mathrm{A}}\epsilon$$

Proof. Pick an arbitrary $(p, l, \epsilon, q) \in \text{Atom}_{\mathrm{DD}}$. Note that as the CISL$_{\mathrm{DD}}$ interference is simply defined as the identity relation, it suffices to show that the following holds:

$$\forall s \in \text{State}_{\mathrm{DD}}, m_q \in \lfloor q * \{s\} \rfloor_{\mathrm{DD}}. \exists m_p \in \lfloor p * \{s\} \rfloor_{\mathrm{DD}}. (m_p, m_q) \in [\![l]\!]_{\mathrm{A}}\epsilon$$

We proceed by induction on the structure of (p, l, ϵ, q).

Case DD-Lock

We then have $l = \text{L}\colon \mathtt{lock}_\tau\ l$ for some τ, l, that $\epsilon = ok$, $q = \tau \mapsto (H +\!\!+ \mathsf{L}(\tau, l), S \uplus \{l\})$ for some H, S such that $l \notin S$, and $p = \tau \mapsto (H, S)$. Let $H' \triangleq H +\!\!+ \mathsf{L}(\tau, l)$. Pick an arbitrary $s \in \text{State}_{\mathrm{DD}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\mathrm{DD}}$. From the definitions of $\lfloor . \rfloor_{\mathrm{DD}}$ and $*$ we then know that there exist $s_q \in q, H_q$ such that $s_q = ([\tau \mapsto (H', S \uplus \{l\})], \tau \notin dom(s), m_q = H_q, H' = H_q|_\tau, \forall \tau' \in dom(s). s(\tau') = (H'', -) \Rightarrow H'' = H_q|_{\tau'}$ and $\mathsf{wf}(H_q)$. That is, there exists H_1, H_2, H_p such that $H_q = H_1 +\!\!+ \mathsf{L}(\tau, l) +\!\!+ H_2$, $\forall e \in H_2.\ e.\mathsf{tid} \neq \tau$, $H_p = H_1 +\!\!+ H_2$, and $H = H_p|_\tau, \forall \tau' \in dom(s). s(\tau') = (H'', -) \Rightarrow H'' = H_p|_{\tau'}$.

Let s_p=$[\tau \mapsto (H, S)]$ and m_p=H_p. From the definitions of $\lfloor . \rfloor_{\mathrm{DD}}$, H_p and $*$ we then know that $s_p \in p$, that $p * \{s\}$ is defined (since $\tau \notin dom(s)$), and that $m_p \in \lfloor p * \{s\} \rfloor_{\mathrm{DD}}$. Moreover, as $\mathsf{wf}(H_q)$, $\forall e \in H_2.\ e.\mathsf{tid} \neq \tau$, H_q=$H_1 +\!\!+ \mathsf{L}(\tau, l) +\!\!+ H_2$ and H_p=$H_1 +\!\!+ H_2$, it is straightforward to show that $\mathsf{wf}(H_p)$. Finally, from the definition of $[\![.]\!]_{\mathrm{A}}$ we have $(m_p, m_q) \in [\![\text{L}\colon \mathtt{lock}_\tau\ l]\!]_{\mathrm{A}} ok$, as required.

Case DD-Unlock

We then have $l = \mathtt{unlock}_\tau\ l$ for some τ, l, that $\epsilon = ok$, $q = \tau \mapsto (H +\!\!+ \mathsf{U}(\tau, l), S)$ for some H, S, S' such that $l \notin S$, $S' = S \uplus \{l\}$ and $p = \tau \mapsto (H, S')$. Let $H' \triangleq H +\!\!+ \mathsf{L}(\tau, l)$. Pick an arbitrary $s \in \text{State}_{\mathrm{DD}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\mathrm{DD}}$. From the definitions of $\lfloor . \rfloor_{\mathrm{DD}}$ and $*$ we then know that there exist $s_q \in q, H_q$ such that $s_q = ([\tau \mapsto (H', S)], \tau \notin dom(s), m_q = H_q, H' = H_q|_\tau, \forall \tau' \in dom(s). s(\tau') = (H'', -) \Rightarrow H'' = H_q|_{\tau'}$ and $\mathsf{wf}(H_q)$. That is, there exists H_1, H_2, H_p such that $H_q = H_1 +\!\!+ \mathsf{U}(\tau, l) +\!\!+ H_2$, $\forall e \in H_2.\ e.\mathsf{tid} \neq \tau$, $H_p = H_1 +\!\!+ H_2$, and $H = H_p|_\tau, \forall \tau' \in dom(s). s(\tau') = (H'', -) \Rightarrow H'' = H_p|_{\tau'}$.

Let s_p=$[\tau \mapsto (H, S')]$ and m_p=H_p. From the definitions of $\lfloor . \rfloor_{\mathrm{DD}}$, H_p and $*$ we then know that $s_p \in p$, that $p * \{s\}$ is defined (since $\tau \notin dom(s)$), and that $m_p \in \lfloor p * \{s\} \rfloor_{\mathrm{DD}}$. Moreover, as $\mathsf{wf}(H_q)$, $\forall e \in H_2.\ e.\mathsf{tid} \neq \tau$, H_q=$H_1 +\!\!+ \mathsf{L}(\tau, l) +\!\!+ H_2$ and H_p=$H_1 +\!\!+ H_2$, it is straightforward to show that $\mathsf{wf}(H_p)$. Finally, from the definition of $[\![.]\!]_{\mathrm{A}}$ we have $(m_p, m_q) \in [\![\mathtt{unlock}_\tau\ l]\!]_{\mathrm{A}} ok$, as required.

$\square$

E CISL_{SV} SOUNDNESS

CISL_{SV} Machine States. As the LSTATE PCM is supplied as a parameter to CISL_{SV}, their corresponding machine states, MSTATE_{L}, must similarly be supplied as a parameter to CISL_{SV}. Since here we instantiated LSTATE with STATE_{DC}, we accordingly take $\text{MSTATE}_{\text{L}} \triangleq \text{MSTATE}_{\text{DC}}$. The set of CISL_{SV} machine states is: $\text{MSTATE}_{\text{SV}} \triangleq \text{MSTATE}_{\text{L}} \cup (\text{RID} \xrightharpoonup{\text{fin}} \{\bot\} \uplus \text{TID})$.

CISL_{SV} Atomic Semantics.

$$\llbracket x := v \rrbracket_{\text{A}} ok \triangleq \left\{ (m, m[x \mapsto v]) \,\middle|\, x \in dom(m) \right\}$$
$$\llbracket x := \texttt{alloc()} \rrbracket_{\text{A}} ok \triangleq \left\{ (m, m[x \mapsto l] \uplus [l \mapsto v]) \,\middle|\, v \in \text{VAL} \land x \in dom(m) \land l \notin dom(m) \right\}$$
$$\llbracket x := v \rrbracket_{\text{A}} mse(.) = \llbracket x := \texttt{alloc()} \rrbracket_{\text{A}} mse(.) \triangleq \emptyset$$
$$\llbracket \text{L}\colon \texttt{free}(x) \rrbracket_{\text{A}} ok \triangleq \left\{ (m, m[l \mapsto \bot]) \,\middle|\, \exists l.\ m(x) = l \land m(l) \in \text{VAL} \right\}$$
$$\llbracket \text{L}\colon \texttt{free}(x) \rrbracket_{\text{A}} mse(\text{L}') \triangleq \left\{ (m, m) \,\middle|\, \text{L} = \text{L}' \land \exists l.\ m(x) = l \land m(l) = \bot \right\}$$
$$\llbracket \text{L}\colon x := [y] \rrbracket_{\text{A}} ok \triangleq \left\{ (m, m[x \mapsto v]) \,\middle|\, x \in dom(m) \land \exists l.\ m(y) = l \land m(l) = v \in \text{VAL} \right\}$$
$$\llbracket \text{L}\colon x := [y] \rrbracket_{\text{A}} mse(\text{L}') \triangleq \left\{ (m, m) \,\middle|\, \text{L} = \text{L}' \land x \in dom(m) \land \exists l.\ m(y) = l \land m(l) = \bot \right\}$$
$$\llbracket \text{L}\colon [x] := y \rrbracket_{\text{A}} ok \triangleq \left\{ (m, m[l \mapsto m(y)]) \,\middle|\, y \in dom(m) \land \exists l.\ m(x) = l \land m(l) \in \text{VAL} \right\}$$
$$\llbracket \text{L}\colon [x] := y \rrbracket_{\text{A}} mse(\text{L}') \triangleq \left\{ (m, m) \,\middle|\, \text{L} = \text{L}' \land y \in dom(m) \land \exists l.\ m(x) = l \land m(l) = \bot \right\}$$
$$\llbracket \texttt{acq}_\tau\ \mathbf{r} \rrbracket_{\text{A}} ok \triangleq \left\{ (m, m') \,\middle|\, m(\mathbf{r}) = \bot \land m' = m[\mathbf{r} \mapsto \tau] \right\}$$
$$\llbracket \texttt{rel}_\tau\ \mathbf{r} \rrbracket_{\text{A}} ok \triangleq \left\{ (m, m') \,\middle|\, m(\mathbf{r}) = \tau \land m' = m[\mathbf{r} \mapsto \bot] \right\}$$

CISL_{SV} Erasure. As LSTATE and MSTATE_{L} are supplied as a parameter to CISL_{SV}, the erasure $\lfloor . \rfloor_{\text{L}} : \text{LSTATE} \to \mathcal{P}(\text{MSTATE}_{\text{L}})$ must similarly be supplied as a parameter to CISL_{SV}. Since here we instantiated LSTATE with STATE_{DC} and MSTATE_{L} with $\text{MSTATE}_{\text{DC}}$, we accordingly take $\lfloor . \rfloor_{\text{L}} \triangleq \lfloor . \rfloor_{\text{DC}}$.

Given a resource map ρ and a resource $\mathbf{r}$, since at most one thread may be within $\mathbf{r}$ at any given time and thus claim its associated resource, we write $SV(\rho(\mathbf{r}))$ (resp. $owner(\rho(\mathbf{r}))$) to denote the resource associated with $\mathbf{r}$ (resp. the thread currently accessing $\mathbf{r}$), if such resource (resp. thread) exists; and otherwise to denote the set of empty resource LSTATE^0 (resp. $\bot$). That is, when $\rho(\mathbf{r}) = (o, -, -)$, if $o \in \text{TID}$ then $SV(\rho(\mathbf{r})) = \text{LSTATE}^0$ and $owner(\rho(\mathbf{r})) = o$; and if $o = \bot$ then $SV(\rho(\mathbf{r})) = \mathcal{S}(count(\rho, \mathbf{r}))$ and $owner(\rho(\mathbf{r})) = o = \bot$. The CISL_{SV} erasure function is then defined as follows:

$$\lfloor (\mathbf{l}, \mathbf{p}, \rho) \rfloor_{\text{SV}} \triangleq \left\{ (\mathbf{l} \circ_{\text{l}} \mathbf{l}_1 \circ_{\text{l}} \mathbf{l}_2) \,\middle|\, \mathbf{l}_1 \in \mathop{\ast}_{\mathbf{r} \in dom(\rho)} SV(\rho(\mathbf{r})) \land \mathbf{l}_2 = (\emptyset, \biguplus_{\mathbf{r} \in dom(\rho)} [\mathbf{r} \mapsto owner(\rho(\mathbf{r}))]) \right\}$$

E.1 CISL_{SV} Axiom Soundness

THEOREM E.1 (CISL_{SV} AXIOMS SOUNDNESS). *For all $(p, l, \epsilon, q) \in \text{ATOM}_{SV}$ the following holds:*

$$\forall s \in \text{STATE}_{SV}, m_q \in \lfloor q * \{s\} \rfloor_{SV}.\ \exists m_p \in \lfloor p * \mathcal{I}_{SV}^{-1}(s) \rfloor_{SV}.\ (m_p, m_q) \in \llbracket l \rrbracket_{\text{A}} \epsilon$$

PROOF. Pick an arbitrary $(p, l, \epsilon, q) \in \text{ATOM}_{\text{SV}}$. We proceed by induction on the structure of (p, l, ϵ, q).

Case SV-ACQ

We then have $\epsilon = ok$, $l = \texttt{acq}_\tau\ \mathbf{r}$ for some $\tau, \mathbf{r}$, $q = \bigvee_{m \geq n} (\mathcal{S}(m) * \text{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau\colon n, m))$ for some n, and $p = \text{res}^{\mathbf{r}}_{\mathcal{S}}(\tau\colon n)$. Pick an arbitrary $s \in \text{STATE}_{\text{SV}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\text{SV}}$. From the definitions of $\lfloor . \rfloor_{\text{SV}}$ and $*$ we then know that there exist $\mathbf{l}, \rho, t, k, \mathbf{l}_k, \mathbf{p}, \mathbf{l}_1, \mathbf{l}_2$ such that:

$s = (\mathbf{l}, \mathbf{p}, \rho)$, $(\mathbf{r}, \tau) \notin dom(\mathbf{p})$,

$\rho(\mathbf{r})=(\tau, \mathcal{S}, t)$, $t(\tau)=n$, $k=count\,(t)$, $k \geq n$,
$\mathbf{l}_k \in \mathcal{S}(k)$,
$m_q=\mathbf{l}_k \circ_{\mathrm{l}} \mathbf{l} \circ_{\mathrm{l}} \mathbf{l}_1 \circ_{\mathrm{l}} \mathbf{l}_2$, $\mathbf{l}_1 \in \mathop{\circledast}\limits_{\mathbf{r}' \in dom(\rho)} SV\,(\rho(\mathbf{r}'))$, and $\mathbf{l}_2=(\emptyset, \biguplus\limits_{\mathbf{r}' \in dom(\rho)} [\mathbf{r}' \mapsto owner\,(\rho(\mathbf{r}))])$.

From the definition of m_q we know $m_q(\mathbf{r})=\tau$. Let $s' = (\mathbf{l}, \mathbf{p}, \rho')$ where $\rho' = \rho[\mathbf{r} \mapsto (\perp, \mathcal{S}, t)]$; let $m_p = m_q[\mathbf{r} \mapsto \perp]$. From the definitions of $\lfloor . \rfloor_{\mathsf{SV}}$ and $*$ we have $m_p \in \lfloor \mathrm{res}^{\mathbf{r}}_{\mathcal{S}}(\tau\colon n) * \{s'\} \rfloor_{\mathsf{SV}}$; that is, $m_p \in \lfloor p * \{s'\} \rfloor_{\mathsf{SV}}$. Moreover, from the definition of $\mathcal{I}_a$ we have $(s', s) \in \mathcal{I}_a \subseteq \mathcal{I}$ and thus $s' \in \mathcal{I}^{-1}(s)$. Finally, from the definition of $[\![\mathtt{acq}_\tau\ x]\!]_{\mathsf{A}} ok$ we have $(m_p, m_q) \in [\![\mathtt{acq}_\tau\ x]\!]_{\mathsf{A}} ok$, as required.

Case SV-Rel

We then have $\epsilon = ok$, $l = \mathtt{rel}_\tau\ \mathbf{r}$ for some $\tau, \mathbf{r}$, $q = \mathrm{res}^{\mathbf{r}}_{\mathcal{S}}(\tau\colon n{+}1)$ and $p = \bigvee\limits_{m \geq n} (\mathcal{S}(m{+}1) * \mathrm{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau\colon n, m))$ for some n. Pick an arbitrary $s \in \textsc{State}_{\mathsf{SV}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\mathsf{SV}}$. From the definitions of $\lfloor . \rfloor_{\mathsf{SV}}$ and $*$ we then know that there exist $\mathbf{l}, \rho, t, k, \mathbf{l}_k, \mathbf{p}, \mathbf{l}_1, \mathbf{l}_2$ such that:

$s=(\mathbf{l}, \mathbf{p}, \rho)$, $(\mathbf{r}, \tau) \notin dom(\mathbf{p})$,
$\rho(\mathbf{r})=(\perp, \mathcal{S}, t)$, $t(\tau)=n{+}1$, $k=count\,(t)$, $k \geq n{+}1$, $\mathbf{l}_k \in \mathcal{S}(k)$,
$m_q=\mathbf{l} \circ_{\mathrm{l}} \mathbf{l}_k \circ_{\mathrm{l}} \mathbf{l}_1 \circ_{\mathrm{l}} \mathbf{l}_2$, $\mathbf{l}_1= \mathop{\circledast}\limits_{\mathbf{r}' \in dom(\rho) \setminus \{\mathbf{r}\}} SV\,(\rho(\mathbf{r}'))$, and $\mathbf{l}_2=(\emptyset, \biguplus\limits_{\mathbf{r}' \in dom(\rho)} [\mathbf{r}' \mapsto owner\,(\rho(\mathbf{r}))])$.

From the definition of m_q we know $m_q(\mathbf{r})=\perp$. Let $s'=(\mathbf{l}, \mathbf{p}, \rho')$ where $\rho' = \rho[\mathbf{r} \mapsto (\tau, \mathcal{S}, t')]$ and $t'=t[\tau \mapsto n]$; and let $m_p=m_q[\mathbf{r} \mapsto \tau]$. From the definitions of s, s', ρ, ρ', $\lfloor . \rfloor_{\mathsf{SV}}$ and $*$ we then have $m_p \in \lfloor \{\mathbf{l}_k\} * \mathrm{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau\colon n, k{-}1) * \{s'\} \rfloor_{\mathsf{SV}}$, i.e. $m_p \in \lfloor \mathcal{S}(k) * \mathrm{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau\colon n, k{-}1) * \{s'\} \rfloor_{\mathsf{SV}}$. As $k \geq n{+}1$ we also have $k{-}1 \geq n$. As such, we also have $m_p \in \lfloor \bigvee\limits_{m \geq n} \mathcal{S}(m{+}1) * \mathrm{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau\colon n, m) * \{s'\} \rfloor_{\mathsf{SV}}$; that is, $m_p \in \lfloor p * \{s'\} \rfloor_{\mathsf{SV}}$. Moreover, from the definition of $\mathcal{I}_r$ we have $(s', s) \in \mathcal{I}_r \subseteq \mathcal{I}$ and thus $s' \in \mathcal{I}^{-1}(s)$. Finally, from the definition of $[\![\mathtt{rel}_\tau\ x]\!]_{\mathsf{A}} ok$ we have $(m_p, m_q) \in [\![\mathtt{rel}_\tau\ x]\!]_{\mathsf{A}} ok$, as required.

Case SV-Acq-G

We then have $\epsilon = ok$, $l = \mathtt{acq}_\tau\ \mathbf{r}$ for some $\tau, \mathbf{r}$, $q = \mathcal{S}(m) * \mathrm{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau, m)$ for some m, and $p = \mathrm{res}^{\mathbf{r}}_{\mathcal{S}}(m)$. Pick an arbitrary $s \in \textsc{State}_{\mathsf{SV}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\mathsf{SV}}$. From the definitions of $\lfloor . \rfloor_{\mathsf{SV}}$ and $*$ we then know that there exist $\mathbf{l}, \rho, t, k, \mathbf{l}_k, n, \mathbf{p}, \mathbf{l}_1, \mathbf{l}_2$ such that:

$s=(\mathbf{l}, \mathbf{p}, \rho)$, $\forall \tau.\ (\mathbf{r}, \tau) \notin dom(\mathbf{p})$,
$\rho(\mathbf{r})=(\tau, \mathcal{S}, t)$, $t(\tau)=n$, $m=count\,(t)$, $m \geq n$,
$\mathbf{l}_m \in \mathcal{S}(m)$,
$m_q=\mathbf{l}_m \circ_{\mathrm{l}} \mathbf{l} \circ_{\mathrm{l}} \mathbf{l}_1 \circ_{\mathrm{l}} \mathbf{l}_2$, $\mathbf{l}_1 \in \mathop{\circledast}\limits_{\mathbf{r}' \in dom(\rho)} SV\,(\rho(\mathbf{r}'))$, and $\mathbf{l}_2=(\emptyset, \biguplus\limits_{\mathbf{r}' \in dom(\rho)} [\mathbf{r}' \mapsto owner\,(\rho(\mathbf{r}))])$.

From the definition of m_q we know $m_q(\mathbf{r})=\tau$. Let $s' = (\mathbf{l}, \mathbf{p}, \rho')$ where $\rho' = \rho[\mathbf{r} \mapsto (\perp, \mathcal{S}, t)]$; let $m_p = m_q[\mathbf{r} \mapsto \perp]$. From the definitions of $\lfloor . \rfloor_{\mathsf{SV}}$ and $*$ we have $m_p \in \lfloor \mathrm{res}^{\mathbf{r}}_{\mathcal{S}}(m) * \{s'\} \rfloor_{\mathsf{SV}}$; that is, $m_p \in \lfloor p * \{s'\} \rfloor_{\mathsf{SV}}$. Moreover, from the definition of $\mathcal{I}_a$ we have $(s', s) \in \mathcal{I}_a \subseteq \mathcal{I}$ and thus $s' \in \mathcal{I}^{-1}(s)$. Finally, from the definition of $[\![\mathtt{acq}_\tau\ x]\!]_{\mathsf{A}} ok$ we have $(m_p, m_q) \in [\![\mathtt{acq}_\tau\ x]\!]_{\mathsf{A}} ok$, as required.

Case SV-Rel-G

We then have $\epsilon = ok$, $l = \mathtt{rel}_\tau\ \mathbf{r}$ for some $\tau, \mathbf{r}$, $q = \mathrm{res}^{\mathbf{r}}_{\mathcal{S}}(m{+}1)$ for some m and $p = \mathcal{S}(m{+}1) * \mathrm{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau, m)$. Pick an arbitrary $s \in \textsc{State}_{\mathsf{SV}}$ and $m_q \in \lfloor q * \{s\} \rfloor_{\mathsf{SV}}$. From the definitions of $\lfloor . \rfloor_{\mathsf{SV}}$ and $*$ we then know that there exist $\mathbf{l}, \rho, t, n, \mathbf{l}_{m+1}, \mathbf{p}, \mathbf{l}_1, \mathbf{l}_2$ such that:

$s=(\mathbf{l}, \mathbf{p}, \rho)$, $\forall \tau.\ (\mathbf{r}, \tau) \notin dom(\mathbf{p})$,
$\rho(\mathbf{r})=(\perp, \mathcal{S}, t)$, $t(\tau)=n{+}1$, $m{+}1=count\,(t)$, $m{+}1 \geq n{+}1$ and thus $m \geq n$, $\mathbf{l}_{m+1} \in \mathcal{S}(m{+}1)$,
$m_q=\mathbf{l} \circ_{\mathrm{l}} \mathbf{l}_{m+1} \circ_{\mathrm{l}} \mathbf{l}_1 \circ_{\mathrm{l}} \mathbf{l}_2$, $\mathbf{l}_1= \mathop{\circledast}\limits_{\mathbf{r}' \in dom(\rho) \setminus \{\mathbf{r}\}} SV\,(\rho(\mathbf{r}'))$, and $\mathbf{l}_2=(\emptyset, \biguplus\limits_{\mathbf{r}' \in dom(\rho)} [\mathbf{r}' \mapsto owner\,(\rho(\mathbf{r}))])$.

From the definition of m_q we know $m_q(\mathbf{r})=\perp$. Let $s'=(\mathbf{l}, \mathbf{p}, \rho')$ where $\rho' = \rho[\mathbf{r} \mapsto (\tau, \mathcal{S}, t')]$ and $t'=t[\tau \mapsto n]$; and let $m_p=m_q[\mathbf{r} \mapsto \tau]$. From the definitions of s, s', ρ, ρ', $\lfloor . \rfloor_{\mathsf{SV}}$ and $*$ we then have $m_p \in \lfloor \{\mathbf{l}_{m+1}\} * \mathsf{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau, m) * \{s'\} \rfloor_{\mathsf{SV}}$, i.e. $m_p \in \lfloor \mathcal{S}(m{+}1) * \mathsf{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau, m) * \{s'\} \rfloor_{\mathsf{SV}}$ and thus $m_p \in \lfloor p * \{s'\} \rfloor_{\mathsf{SV}}$. Moreover, from the definition of $\mathcal{I}_r$ we have $(s', s) \in \mathcal{I}_r \subseteq \mathcal{I}$ and thus $s' \in \mathcal{I}^{-1}(s)$. Finally, from the definition of $[\![\mathtt{rel}_\tau\ x]\!]_{\mathsf{A}}\, ok$ we have $(m_p, m_q) \in [\![\mathtt{rel}_\tau\ x]\!]_{\mathsf{A}}\, ok$, as required.

Case SV-CS
This rule can be derived as follows, where Asm denotes an assumption given by the premise:

$$
\dfrac{
(1) \qquad
\dfrac{(2) \qquad (3)}{\left[p * \bigvee_{m \geq n} (\mathcal{S}(m) * \mathsf{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n, m))\right] \mathtt{C}; \mathtt{rel}_\tau\ \mathbf{r} \left[ok{:}\ q * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n{+}1)\right]}\ \textsc{Seq}
}{
\dfrac{\left[p * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n)\right] \mathtt{acq}_\tau\ \mathbf{r}; \mathtt{C}; \mathtt{rel}_\tau\ \mathbf{r} \left[ok{:}\ q * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n{+}1)\right]}{\left[p * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n)\right] \mathtt{with}_\tau\ \mathbf{r}\ \mathtt{do}\ \mathtt{C} \left[ok{:}\ q * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n{+}1)\right]}
}\ \textsc{Seq}
$$

$$
\dfrac{
\dfrac{}{\left[* \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n)\right] \mathtt{acq}_\tau\ \mathbf{r} \left[ok{:}\ \bigvee_{m \geq n} (\mathcal{S}(m) * \mathsf{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n, m))\right]}\ \textsc{SV-Acq}
\qquad
\dfrac{}{\mathsf{stable}(p)}
}{
\dfrac{\left[p * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n)\right] \mathtt{acq}_\tau\ \mathbf{r} \left[ok{:}\ p * \bigvee_{m \geq n} (\mathcal{S}(m) * \mathsf{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n, m))\right]}{(1)}
}\ \textsc{FrameInter}
$$

$$
\dfrac{
\dfrac{
\dfrac{}{\forall m \geq n.\ [p * \mathcal{S}(m)]\ \mathtt{C}\ [ok{:}\ q * \mathcal{S}(m{+}1)]}\ \textsc{Asm}
\qquad
\dfrac{}{\mathsf{stable}\left(\mathsf{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n, m)\right)}
}{
\forall m \geq n.\ \left[p * \mathcal{S}(m) * \mathsf{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n, m)\right] \mathtt{C} \left[ok{:}\ q * \mathcal{S}(m{+}1) * \mathsf{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n, m)\right]
}\ \textsc{FrameInter}
}{
\dfrac{\left[p * \bigvee_{m \geq n} (\mathcal{S}(m) * \mathsf{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n, m))\right] \mathtt{C} \left[ok{:}\ q * \bigvee_{m \geq n} (\mathcal{S}(m{+}1) * \mathsf{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n, m))\right]}{(2)}
}\ \textsc{Disj, Cons}
$$

$$
\dfrac{
\dfrac{}{\left[\bigvee_{m \geq n} (\mathcal{S}(m{+}1) * \mathsf{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n, m))\right] \mathtt{rel}_\tau\ \mathbf{r} \left[ok{:}\ \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n{+}1)\right]}\ \textsc{SV-Rel}
\qquad
\dfrac{}{\mathsf{stable}(q)}
}{
\dfrac{\left[q * \bigvee_{m \geq n} (\mathcal{S}(m{+}1) * \mathsf{cs}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n, m))\right] \mathtt{rel}_\tau\ \mathbf{r} \left[ok{:}\ q * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\, n{+}1)\right]}{(3)}
}\ \textsc{FrameInter}
$$

Case SV-CS-G

This rule can be derived as follows, where $r \triangleq n{=}k{+}\sum k_i * \mathop{\circledast}_{\tau_i \in \text{TID}\setminus\{\tau\}} \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau_i{:}\, k_i)$:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{\left[p * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\,k)\right] \mathtt{with}_\tau\, \mathbf{r}\ \mathtt{do}\ \mathtt{C} \left[ok{:}\ q * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\,k{+}1)\right]}\ \text{SV-CS} \qquad \dfrac{}{\mathsf{stable}(r)}}{\left[p * n{=}k{+}\sum k_i * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\,k) * \mathop{\circledast}_{\tau_i \in \text{TID}\setminus\{\tau\}} \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau_i{:}\,k_i)\right] \mathtt{with}_\tau\, \mathbf{r}\ \mathtt{do}\ \mathtt{C} \left[ok{:}\ q * n{=}k{+}\sum k_i * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\,k{+}1) * \mathop{\circledast}_{\tau_i \in \text{TID}\setminus\{\tau\}} \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau_i{:}\,k_i)\right]}\ \textsc{FrameInter}}{\left[p * n{=}k{+}\sum k_i * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\,k) * \mathop{\circledast}_{\tau_i \in \text{TID}\setminus\{\tau\}} \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau_i{:}\,k_i)\right] \mathtt{with}_\tau\, \mathbf{r}\ \mathtt{do}\ \mathtt{C} \left[ok{:}\ q * n{+}1{=}k{+}1{+}\sum k_i * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\,k{+}1) * \mathop{\circledast}_{\tau_i \in \text{TID}\setminus\{\tau\}} \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau_i{:}\,k_i)\right]}\ \textsc{Cons}}{\left[\exists \overline{k_i}, k.\ p * n{=}k{+}\sum k_i * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\,k) * \mathop{\circledast}_{\tau_i \in \text{TID}\setminus\{\tau\}} \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau_i{:}\,k_i)\right] \mathtt{with}_\tau\, \mathbf{r}\ \mathtt{do}\ \mathtt{C} \left[ok{:}\ \exists \overline{k_i}, k.\ q * n{+}1{=}k{+}1{+}\sum k_i * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau{:}\,k{+}1) * \mathop{\circledast}_{\tau_i \in \text{TID}\setminus\{\tau\}} \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(\tau_i{:}\,k_i)\right]}\ \textsc{Disj}}{\left[p * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(n)\right] \mathtt{with}_\tau\, \mathbf{r}\ \mathtt{do}\ \mathtt{C} \left[ok{:}\ q * \mathsf{res}^{\mathbf{r}}_{\mathcal{S}}(n{+}1)\right]}\ \textsc{Cons}, \textsc{Subv-Split}$$

□