Mathematical proofs
in complement of the book

Principles of Abstract Interpretation

(MIT Press, 2021)

Patrick Cousot

New York University

June 17, 2020

1 Mathematical proofs of chapter 4

Proof of Lemma 4.17 The lemma trivially holds if $\mathsf{escape}[\![\mathtt{S}]\!] = \mathrm{ff}$. Otherwise $\mathsf{escape}[\![\mathtt{S}]\!] = \mathrm{tt}$ and the proof is by induction on the distance $\delta(\mathtt{S})$ of $\mathtt{S}$ to the root of the abstract syntax tree of $\mathtt{P}$ (where $\delta(\mathtt{P}) = 0$).

- For $\mathtt{Sl} ::= \mathtt{Sl}'\ \mathtt{S}$, $\delta(\mathtt{Sl}') = \delta(\mathtt{S}) = \delta(\mathtt{Sl})+1$. So, in case $\mathsf{escape}[\![\mathtt{Sl}]\!] = \mathrm{tt}$, we have $\mathsf{break\text{-}to}[\![\mathtt{Sl}]\!] \neq \mathsf{after}[\![\mathtt{Sl}]\!]$ by induction hypothesis. By def. $\mathsf{escape}[\![\mathtt{Sl}]\!] \triangleq \mathsf{escape}[\![\mathtt{Sl}']\!] \vee \mathsf{escape}[\![\mathtt{S}]\!]$, there are two subcases.
  - If $\mathsf{escape}[\![\mathtt{Sl}']\!] = \mathrm{tt}$ then, on one hand, $\mathtt{Sl} \neq \mathtt{\{\ \ldots\{\ \epsilon\ \}\ldots\ \}}$, $\mathsf{after}[\![\mathtt{Sl}']\!] = \mathsf{at}[\![\mathtt{S}]\!]$, $\mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \triangleq \mathsf{break\text{-}to}[\![\mathtt{Sl}]\!]$, $\mathsf{at}[\![\mathtt{S}]\!] \in \mathsf{in}[\![\mathtt{S}]\!]$ by Lemma 4.14, so $\mathsf{after}[\![\mathtt{Sl}']\!] \in \mathsf{in}[\![\mathtt{S}]\!]$.
    On the other hand $\mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \notin \mathsf{in}[\![\mathtt{S}]\!]$ since otherwise $\mathsf{break\text{-}to}[\![\mathtt{Sl}]\!] = \mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \in \mathsf{in}[\![\mathtt{S}]\!] \subseteq \mathsf{in}[\![\mathtt{Sl}]\!]$ in contradiction with Lemma 4.16, proving $\mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \neq \mathsf{after}[\![\mathtt{Sl}']\!]$;
  - If $\mathsf{escape}[\![\mathtt{S}]\!] = \mathrm{tt}$ then $\mathtt{S} \neq \mathtt{\{\ \ldots\{\ \epsilon\ \}\ldots\ \}}$, $\mathsf{after}[\![\mathtt{S}]\!] = \mathsf{after}[\![\mathtt{Sl}]\!]$, $\mathsf{break\text{-}to}[\![\mathtt{S}]\!] \triangleq \mathsf{break\text{-}to}[\![\mathtt{Sl}]\!]$, $\mathsf{break\text{-}to}[\![\mathtt{Sl}]\!] \neq \mathsf{after}[\![\mathtt{Sl}]\!]$ by induction hypothesis, so $\mathsf{break\text{-}to}[\![\mathtt{S}]\!] \neq \mathsf{after}[\![\mathtt{S}]\!]$. □
- If $\mathtt{S} ::= \mathtt{if}\ \ell\ \mathtt{(B)}\ \mathtt{S}_t$ then $\mathsf{escape}[\![\mathtt{S}_t]\!] = \mathsf{escape}[\![\mathtt{S}]\!] = \mathrm{tt}$, $\mathsf{after}[\![\mathtt{S}_t]\!] = \mathsf{after}[\![\mathtt{S}]\!]$, $\mathsf{break\text{-}to}[\![\mathtt{S}_t]\!] = \mathsf{break\text{-}to}[\![\mathtt{S}]\!]$, and $\mathsf{break\text{-}to}[\![\mathtt{S}]\!] \neq \mathsf{after}[\![\mathtt{S}]\!]$ by induction hypothesis since $\delta(\mathtt{S}_t) = \delta(\mathtt{S}) + 1$, so $\mathsf{break\text{-}to}[\![\mathtt{S}_t]\!] \neq \mathsf{after}[\![\mathtt{S}_t]\!]$.
- The proof is similar for $\mathtt{S} ::= \mathtt{if}\ \ell\ \mathtt{(B)}\ \mathtt{S}_t\ \mathtt{else}\ \mathtt{S}_f$ and $\mathtt{S} ::= \mathtt{\{\ Sl\ \}}$. □

2 Mathematical proofs of chapter 41

Proof of Theorem 41.24 • For the ***statement list*** $\texttt{Sl} ::= \texttt{Sl}'\ \texttt{S}$, by (17.3) (following (6.13), and (6.14)), we have $\mathcal{S}^*[\![\texttt{Sl}]\!] = \mathcal{S}^*[\![\texttt{Sl}']\!] \cup \{\langle\pi_1,\ \pi_2 \frown \pi_3\rangle \mid \langle\pi_1,\ \pi_2\rangle \in \mathcal{S}^*[\![\texttt{Sl}']\!] \wedge \langle\pi_1 \frown \pi_2,\ \pi_3\rangle \in \mathcal{S}^*[\![\texttt{S}]\!]\}$.

- A first case is when $\texttt{Sl}' = \epsilon$ is empty. Then, □

$$
\begin{aligned}
&\alpha^{\exists l}_{\text{use,mod}}[\![\texttt{Sl}]\!](\mathcal{S}^*[\![\texttt{Sl}]\!])\, L_b, L_e\\
=\ &\bigcup\{\alpha^{l}_{\text{use,mod}}[\![\ \epsilon\ \texttt{S}]\!]\, L_b, L_e\, \langle\pi_0,\ \pi_1\rangle \mid \langle\pi_0,\ \pi_1\rangle \in \mathcal{S}^*[\![\ \epsilon\ \texttt{S}]\!]\}\\
&\qquad \text{\textit{def. (41.3) of} } \alpha^{\exists l}_{\text{use,mod}}[\![\texttt{S}]\!] \text{ for } \texttt{Sl} ::= \epsilon\ \texttt{S}\\
=\ &\bigcup\{\alpha^{l}_{\text{use,mod}}\ L_b, L_e\, \langle\pi_0\ell,\ \pi_1\rangle \mid \langle\pi_0\ell,\ \pi_1\rangle \in \mathcal{S}^*[\![\ \epsilon\ ]\!] \cup \{\langle\pi_0\ell,\ \pi_2 \frown \pi_3\rangle \mid \langle\pi_0\ell,\ \pi_2\rangle \in \\
&\mathcal{S}^+[\![\ \epsilon\ ]\!] \wedge \langle\pi_0\ell \frown \pi_2,\ \pi_3\rangle \in \mathcal{S}^*[\![\texttt{S}]\!]\}\} \qquad \text{def. } \mathcal{S}^*[\![\ \epsilon\ \texttt{S}]\!]\\
=\ &\bigcup\{\alpha^{l}_{\text{use,mod}}\ L_b, L_e\, \langle\pi_0,\ \pi_1\rangle \mid \langle\pi_0,\ \pi_1\rangle \in \mathcal{S}^*[\![\texttt{S}]\!]\}\}\\
&\qquad \text{(6.15) so that } \mathcal{S}^*[\![\ \epsilon\ ]\!] = \{\langle\pi_0\mathsf{at}[\![\texttt{S}]\!],\ \mathsf{at}[\![\texttt{S}]\!]\rangle \mid \pi_0\mathsf{at}[\![\texttt{S}]\!] \in \mathbb{T}^+\} \text{ and } \langle\pi_0\mathsf{at}[\![\texttt{S}]\!],\ \mathsf{at}[\![\texttt{S}]\!]\rangle \in\\
&\qquad \mathcal{S}^*[\![\texttt{S}]\!] \text{ by (6.11)}\\
=\ &\alpha^{\exists l}_{\text{use,mod}}[\![\texttt{Sl}]\!]\ (\mathcal{S}^*[\![\texttt{S}]\!])\, L_b, L_e \qquad \text{def. (41.3) of } \alpha^{\exists l}_{\text{use,mod}}[\![\texttt{S}]\!]\\
=\ &\alpha^{\exists l}_{\text{use,mod}}[\![\texttt{S}]\!]\ (\mathcal{S}^*[\![\texttt{S}]\!])\, L_b, L_e\\
&\qquad \text{(41.3) since } \mathsf{after}[\![\texttt{Sl}]\!] = \mathsf{after}[\![\texttt{S}]\!],\ \mathsf{escape}[\![\texttt{Sl}]\!] = \mathsf{escape}[\![\texttt{S}]\!], \text{ and } \mathsf{break\text{-}to}[\![\texttt{Sl}]\!] =\\
&\qquad \mathsf{break\text{-}to}[\![\texttt{S}]\!] \text{ when } \texttt{Sl}' = \epsilon\\
\subseteq\ &\widehat{\mathcal{S}}^{\exists l}[\![\texttt{S}]\!]\, L_b, L_e \qquad \text{ind. hyp. for Theorem 41.24}\\
=\ &\widehat{\mathcal{S}}^{\exists l}[\![\texttt{S}]\!]\, L_b, (\widehat{\mathcal{S}}^{\exists l}[\![\ \epsilon\ ]\!]\, L_b, L_e) \qquad \text{since } \widehat{\mathcal{S}}^{\exists l}[\![\ \epsilon\ ]\!]\, L_b, L_e \triangleq L_e \text{ by (41.22)}
\end{aligned}
$$

proving (41.22) when $\texttt{Sl}' = \epsilon$.

- A second case is when $\texttt{S} = \texttt{\{ ...\{ } \epsilon \texttt{ \}... \}}$ is empty. Then, as required by (41.22), we have, by induction hypothesis, $\alpha^{\exists l}_{\text{use,mod}}[\![\texttt{Sl}]\!]\, L_b, L_e = \alpha^{\exists l}_{\text{use,mod}}[\![\texttt{Sl}']\!]\, L_b, L_e \subseteq \widehat{\mathcal{S}}^{\exists l}[\![\texttt{Sl}']\!]\ L_b, (\widehat{\mathcal{S}}^{\exists l}[\![\texttt{S}]\!]\ L_b, L_e) \triangleq \widehat{\mathcal{S}}^{\exists l}[\![\texttt{Sl}]\!]\ L_b, L_e$ since $\widehat{\mathcal{S}}^{\exists l}[\![\texttt{S}]\!]\ L_b, L_e = L_e$ when $\texttt{S}$ is empty. □

- Otherwise, $\texttt{Sl}' \neq \epsilon$ and $\texttt{S} \neq \texttt{\{ ...\{ } \epsilon \texttt{ \}... \}}$ so, by Lemma 4.15, $\mathsf{after}[\![\texttt{S}]\!] \notin \mathsf{in}[\![\texttt{S}]\!]$. In that case, let us calculate

$$
\begin{aligned}
&\alpha^{\exists l}_{\text{use,mod}}[\![\texttt{Sl}]\!]\, L_b, L_e\\
=\ &\bigcup\{\alpha^{l}_{\text{use,mod}}[\![\texttt{Sl}]\!]\, L_b, L_e\, \langle\pi_0,\ \pi_1\rangle \mid \langle\pi_0,\ \pi_1\rangle \in \mathcal{S}^*[\![\texttt{Sl}]\!]\} \qquad \text{def. (41.3) of } \alpha^{\exists l}_{\text{use,mod}}[\![\texttt{S}]\!]
\end{aligned}
$$

$= \bigcup\{\{\mathsf{x} \in \mathbb{V} \mid \exists i \in [1, n-1] \,.\, \forall j \in [1, i-1] \,.\, \mathsf{x} \notin \mathsf{mod}[\![\mathsf{a}_j]\!] \wedge \mathsf{x} \in \mathsf{use}[\![\mathsf{a}_i]\!]\} \cup (\!| \ell_n = \mathsf{after}[\![\mathsf{Sl}]\!] \mathrel{?} L_e \mathrel{:} \varnothing |\!) \cup (\!| \mathsf{escape}[\![\mathsf{Sl}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathsf{Sl}]\!] \mathrel{?} L_b \mathrel{:} \varnothing |\!) \mid \langle \pi_0, \pi_1 \rangle \in \mathcal{S}^*[\![\mathsf{Sl}]\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathsf{a}_1} \ell_2 \xrightarrow{\mathsf{a}_2} \ldots \xrightarrow{\mathsf{a}_{n-1}} \ell_n\}$ ⟅By Lemma 41.8, omitting the useless parameters of use and mod⟆

$= \bigcup\{\{\mathsf{x} \in \mathbb{V} \mid \exists i \in [1, n-1] \,.\, \forall j \in [1, i-1] \,.\, \mathsf{x} \notin \mathsf{mod}[\![\mathsf{a}_j]\!] \wedge \mathsf{x} \in \mathsf{use}[\![\mathsf{a}_i]\!]\} \cup (\!| \ell_n = \mathsf{after}[\![\mathsf{S}]\!] \mathrel{?} L_e \mathrel{:} \varnothing |\!) \cup (\!| \mathsf{escape}[\![\mathsf{Sl}']\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathsf{Sl}']\!] \mathrel{?} L_b \mathrel{:} \varnothing |\!) \cup (\!| \mathsf{escape}[\![\mathsf{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathsf{S}]\!] \mathrel{?} L_b \mathrel{:} \varnothing |\!) \mid \langle \pi_0, \pi_1 \rangle \in \mathcal{S}^*[\![\mathsf{Sl}']\!] \cup \{\langle \pi_0 \frown \pi_2, \pi_2 \frown \pi_3 \rangle \mid \langle \pi_0, \pi_2 \rangle \in \mathcal{S}^+[\![\mathsf{Sl}']\!] \wedge \langle \pi_0 \frown \pi_2, \pi_3 \rangle \in \mathcal{S}^*[\![\mathsf{S}]\!]\} \wedge \pi_1 = \ell_1 \xrightarrow{\mathsf{a}_1} \ell_2 \xrightarrow{\mathsf{a}_2} \ldots \xrightarrow{\mathsf{a}_{n-1}} \ell_n\}$

⟅def. $\mathcal{S}^*[\![\mathsf{Sl}]\!]$, $\mathsf{after}[\![\mathsf{Sl}]\!] = \mathsf{after}[\![\mathsf{S}]\!]$ in Section 4.2.2, $\mathsf{escape}[\![\mathsf{Sl}]\!] \triangleq \mathsf{escape}[\![\mathsf{Sl}']\!] \vee \mathsf{escape}[\![\mathsf{S}]\!]$, and $\mathsf{break\text{-}to}[\![\mathsf{Sl}']\!] \triangleq \mathsf{break\text{-}to}[\![\mathsf{S}]\!] \triangleq \mathsf{break\text{-}to}[\![\mathsf{Sl}]\!]$ in Section 4.2.4 ⟆

$= \bigcup\{\{\mathsf{x} \in \mathbb{V} \mid \exists i \in [1, n-1] \,.\, \forall j \in [1, i-1] \,.\, \mathsf{x} \notin \mathsf{mod}[\![\mathsf{a}_j]\!] \wedge \mathsf{x} \in \mathsf{use}[\![\mathsf{a}_i]\!]\} \cup (\!| \ell_n = \mathsf{after}[\![\mathsf{S}]\!] \mathrel{?} L_e \mathrel{:} \varnothing |\!) \cup (\!| \mathsf{escape}[\![\mathsf{Sl}']\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathsf{Sl}']\!] \mathrel{?} L_b \mathrel{:} \varnothing |\!) \cup (\!| \mathsf{escape}[\![\mathsf{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathsf{S}]\!] \mathrel{?} L_b \mathrel{:} \varnothing |\!) \mid \langle \pi_0, \pi_1 \rangle \in \mathcal{S}^*[\![\mathsf{Sl}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathsf{a}_1} \ell_2 \xrightarrow{\mathsf{a}_2} \ldots \xrightarrow{\mathsf{a}_{n-1}} \ell_n\} \cup$
$\bigcup\{\{\mathsf{x} \in \mathbb{V} \mid \exists i \in [1, n-1] \,.\, \forall j \in [1, i-1] \,.\, \mathsf{x} \notin \mathsf{mod}[\![\mathsf{a}_j]\!] \wedge \mathsf{x} \in \mathsf{use}[\![\mathsf{a}_i]\!]\} \cup (\!| \ell_n = \mathsf{after}[\![\mathsf{S}]\!] \mathrel{?} L_e \mathrel{:} \varnothing |\!) \cup (\!| \mathsf{escape}[\![\mathsf{Sl}']\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathsf{Sl}']\!] \mathrel{?} L_b \mathrel{:} \varnothing |\!) \cup (\!| \mathsf{escape}[\![\mathsf{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathsf{S}]\!] \mathrel{?} L_b \mathrel{:} \varnothing |\!) \mid \langle \pi_0, \pi_2 \rangle \in \mathcal{S}^+[\![\mathsf{Sl}']\!] \wedge \langle \pi_0 \frown \pi_2, \pi_3 \rangle \in \mathcal{S}^*[\![\mathsf{S}]\!] \wedge \pi_2 \frown \pi_3 = \ell_1 \xrightarrow{\mathsf{a}_1} \ell_2 \xrightarrow{\mathsf{a}_2} \ldots \xrightarrow{\mathsf{a}_{n-1}} \ell_n\}$

⟅def. $\cup$ and def. $\in$ so $\langle \pi_0, \pi_1 \rangle = \langle \pi_0 \frown \pi_2, \pi_2 \frown \pi_3 \rangle$⟆

$\subseteq \bigcup\{\{\mathsf{x} \in \mathbb{V} \mid \exists i \in [1, m-1] \,.\, \forall j \in [1, i-1] \,.\, \mathsf{x} \notin \mathsf{mod}[\![\mathsf{a}_j]\!] \wedge \mathsf{x} \in \mathsf{use}[\![\mathsf{a}_i]\!]\} \cup (\!| \mathsf{escape}[\![\mathsf{Sl}']\!] \wedge \ell_m = \mathsf{break\text{-}to}[\![\mathsf{Sl}']\!] \mathrel{?} L_b \mathrel{:} \varnothing |\!) \mid \langle \pi_0, \pi_1 \rangle \in \mathcal{S}^*[\![\mathsf{Sl}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathsf{a}_1} \ell_2 \xrightarrow{\mathsf{a}_2} \ldots \xrightarrow{\mathsf{a}_{m-1}} \ell_m\} \cup$
$\bigcup\{\{\mathsf{x} \in \mathbb{V} \mid \exists i \in [1, n-1] \,.\, \forall j \in [1, i-1] \,.\, \mathsf{x} \notin \mathsf{mod}[\![\mathsf{a}_j]\!] \wedge \mathsf{x} \in \mathsf{use}[\![\mathsf{a}_i]\!]\} \cup (\!| \ell_n = \mathsf{after}[\![\mathsf{S}]\!] \mathrel{?} L_e \mathrel{:} \varnothing |\!) \cup (\!| \mathsf{escape}[\![\mathsf{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathsf{S}]\!] \mathrel{?} L_b \mathrel{:} \varnothing |\!) \mid \langle \pi_0, \pi_1 \rangle \in \mathcal{S}^+[\![\mathsf{Sl}']\!] \wedge \langle \pi'_0, \pi_3 \rangle \in \mathcal{S}^*[\![\mathsf{S}]\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathsf{a}_1} \ell_2 \xrightarrow{\mathsf{a}_2} \ldots \xrightarrow{\mathsf{a}_{m-1}} \ell_m \wedge \ell_m = \mathsf{after}[\![\mathsf{Sl}']\!] \wedge \pi_3 = \ell_m \xrightarrow{\mathsf{a}_m} \ell_{m+1} \xrightarrow{\mathsf{a}_{m+1}} \ldots \xrightarrow{\mathsf{a}_{n-1}} \ell_n\}$

⟅— For the first term, $\langle \pi_0, \pi_1 \rangle \in \mathcal{S}^*[\![\mathsf{Sl}']\!]$, π_1 ends in ℓ_n, and $\ell_n = \mathsf{after}[\![\mathsf{S}]\!]$ is impossible since Sl' and S are not empty. Moreover, if $\ell_n = \mathsf{break\text{-}to}[\![\mathsf{S}]\!] = \mathsf{break\text{-}to}[\![\mathsf{Sl}']\!]$ then a_{n-1} is a break, so $\mathsf{escape}[\![\mathsf{Sl}']\!]$ holds. L_b is included in $(\!| \mathsf{escape}[\![\mathsf{Sl}']\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathsf{Sl}']\!] \mathrel{?} L_b \mathrel{:} \varnothing |\!)$ and so $(\!| \mathsf{escape}[\![\mathsf{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathsf{S}]\!] \mathrel{?} L_b \mathrel{:} \varnothing |\!)$ is redundant. Finally, renaming $n \leftarrow m$.⟆

$\wr$— For the second term, if $\ell_n = \text{break-to}[\![\text{Sl}']\!] = \text{break-to}[\![\text{S}]\!]$ then a_{n-1} is a break, so $\text{escape}[\![\text{S}]\!]$ holds. L_b is included in $(\!|\text{escape}[\![\text{S}]\!] \wedge \ell_n = \text{break-to}[\![\text{S}]\!] \,?\, L_b \,\mathbin{⨾}\, \varnothing|\!)$ and so $(\!|\text{escape}[\![\text{Sl}']\!] \wedge \ell_n = \text{break-to}[\![\text{Sl}']\!] \,?\, L_b \,\mathbin{⨾}\, \varnothing|\!)$ is redundant. Moreover, $\pi_2 \frown \pi_3 = \ell_1 \xrightarrow{\text{a}_1} \ell_2 \xrightarrow{\text{a}_2} \dots \xrightarrow{\text{a}_{n-1}} \ell_n$ is decomposed into $\pi_2 = \ell_1 \xrightarrow{\text{a}_1} \ell_2 \xrightarrow{\text{a}_2} \dots \xrightarrow{\text{a}_{m-1}} \ell_m$ and $\pi_3 = \ell_m \xrightarrow{\text{a}_m} \ell_{m+1} \xrightarrow{\text{a}_{m+1}} \dots \xrightarrow{\text{a}_{n-1}} \ell_n$ where, by $\langle \pi_0, \pi_2 \rangle \in \mathcal{S}^+[\![\text{Sl}']\!]$ and $\langle \pi_0 \frown \pi_2, \pi_3 \rangle \in \mathcal{S}^*[\![\text{S}]\!]$, $\ell_m = \text{after}[\![\text{Sl}']\!] = \text{at}[\![\text{S}]\!]$. Moreover, $\pi_0 \frown \pi_2$ is generalized to π'_0 (whence inclusion) and π_2 is renamed into π_1. $\wr$

$$= \bigcup\{\{\text{x} \in \mathbb{V} \mid \exists i \in [1, m-1] \,.\, \forall j \in [1, i-1] \,.\, \text{x} \notin \text{mod}[\![\text{a}_j]\!] \wedge \text{x} \in \text{use}[\![\text{a}_i]\!]\} \cup (\!|\text{escape}[\![\text{Sl}']\!] \wedge \ell_m = \text{break-to}[\![\text{Sl}']\!] \,?\, L_b \,⨾\, \varnothing|\!) \mid \langle \pi_0, \pi_1 \rangle \in \mathcal{S}^*[\![\text{Sl}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\text{a}_1} \ell_2 \xrightarrow{\text{a}_2} \dots \xrightarrow{\text{a}_{m-1}} \ell_m\} \cup \bigcup\{\{\text{x} \in \mathbb{V} \mid \exists i \in [m, n-1] \,.\, \forall j \in [1, i-1] \,.\, \text{x} \notin \text{mod}[\![\text{a}_j]\!] \wedge \text{x} \in \text{use}[\![\text{a}_i]\!]\} \cup (\!|\ell_n = \text{after}[\![\text{S}]\!] \,?\, L_e \,⨾\, \varnothing|\!) \cup (\!|\text{escape}[\![\text{S}]\!] \wedge \ell_n = \text{break-to}[\![\text{S}]\!] \,?\, L_b \,⨾\, \varnothing|\!) \mid \langle \pi_0, \pi_1 \rangle \in \mathcal{S}^+[\![\text{Sl}']\!] \wedge \langle \pi'_0, \pi_3 \rangle \in \mathcal{S}^*[\![\text{S}]\!] \wedge \pi_1 = \ell_1 \xrightarrow{\text{a}_1} \ell_2 \xrightarrow{\text{a}_2} \dots \xrightarrow{\text{a}_{m-1}} \ell_m \wedge \ell_m = \text{after}[\![\text{Sl}']\!] \wedge \pi_3 = \ell_m \xrightarrow{\text{a}_m} \ell_{m+1} \xrightarrow{\text{a}_{m+1}} \dots \xrightarrow{\text{a}_{n-1}} \ell_n\}$$

$\wr$since the case $i \in [1, m-1]$ of the second term is already incorporated in the first term$\wr$

$$= \bigcup\{\{\text{x} \in \mathbb{V} \mid \exists i \in [1, m-1] \,.\, \forall j \in [1, i-1] \,.\, \text{x} \notin \text{mod}[\![\text{a}_j]\!] \wedge \text{x} \in \text{use}[\![\text{a}_i]\!]\} \cup (\!|\ell_m = \text{after}[\![\text{Sl}']\!] \,?\, \Big(\bigcup\{\{\text{x} \in \mathbb{V} \mid \exists i \in [m, n-1] \,.\, \forall j \in [1, i-1] \,.\, \text{x} \notin \text{mod}[\![\text{a}_j]\!] \wedge \text{x} \in \text{use}[\![\text{a}_i]\!]\} \cup (\!|\ell_n = \text{after}[\![\text{S}]\!] \,?\, L_e \,⨾\, \varnothing|\!) \cup (\!|\text{escape}[\![\text{S}]\!] \wedge \ell_n = \text{break-to}[\![\text{S}]\!] \,?\, L_b \,⨾\, \varnothing|\!) \mid \langle \pi'_0, \pi_3 \rangle \in \mathcal{S}^*[\![\text{S}]\!] \wedge \pi_3 = \ell_m \xrightarrow{\text{a}_m} \ell_{m+1} \xrightarrow{\text{a}_{m+1}} \dots \xrightarrow{\text{a}_{n-1}} \ell_n\}\Big) \,⨾\, \varnothing|\!) \cup (\!|\text{escape}[\![\text{Sl}']\!] \wedge \ell_m = \text{break-to}[\![\text{Sl}']\!] \,?\, L_b \,⨾\, \varnothing|\!) \mid \langle \pi_0, \pi_1 \rangle \in \mathcal{S}^*[\![\text{Sl}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\text{a}_1} \ell_2 \xrightarrow{\text{a}_2} \dots \xrightarrow{\text{a}_{m-1}} \ell_m\}$$

$\wr$incorporating the second term in the first term, in case $\ell_m = \text{after}[\![\text{Sl}']\!]$$\wr$

$$\subseteq \bigcup\{\{\text{x} \in \mathbb{V} \mid \exists i \in [1, m-1] \,.\, \forall j \in [1, i-1] \,.\, \text{x} \notin \text{mod}[\![\text{a}_j]\!] \wedge \text{x} \in \text{use}[\![\text{a}_i]\!]\} \cup (\!|\ell_m = \text{after}[\![\text{Sl}']\!] \,?\, (\bigcup\{\{\text{x} \in \mathbb{V} \mid \exists i \in [m, n-1] \,.\, \forall j \in [m, i-1] \,.\, \text{x} \notin \text{mod}[\![\text{a}_j]\!] \wedge \text{x} \in \text{use}[\![\text{a}_i]\!]\} \cup (\!|\ell_n = \text{after}[\![\text{S}]\!] \,?\, L_e \,⨾\, \varnothing|\!) \cup (\!|\text{escape}[\![\text{S}]\!] \wedge \ell_n = \text{break-to}[\![\text{S}]\!] \,?\, L_b \,⨾\, \varnothing|\!) \mid \langle \pi'_0, \pi_3 \rangle \in \mathcal{S}^*[\![\text{S}]\!] \wedge \pi_3 = \ell_m \xrightarrow{\text{a}_m} \ell_{m+1} \xrightarrow{\text{a}_{m+1}} \dots \xrightarrow{\text{a}_{n-1}} \ell_n\}) \,⨾\, \varnothing|\!) \cup (\!|\text{escape}[\![\text{Sl}']\!] \wedge \ell_m = \text{break-to}[\![\text{Sl}']\!] \,?\, L_b \,⨾\, \varnothing|\!) \mid \langle \pi_0, \pi_1 \rangle \in \mathcal{S}^*[\![\text{Sl}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\text{a}_1} \ell_2 \xrightarrow{\text{a}_2} \dots \xrightarrow{\text{a}_{m-1}} \ell_m\}$$

$\wr$dropping the test $\forall j \in [1, m-1] \,.\, \text{x} \notin \text{mod}[\![\text{a}_j]\!]$$\wr$

$$= \bigcup\{\{\text{x} \in \mathbb{V} \mid \exists i \in [1, m-1] \,.\, \forall j \in [1, i-1] \,.\, \text{x} \notin \text{mod}[\![\text{a}_j]\!] \wedge \text{x} \in \text{use}[\![\text{a}_i]\!]\} \cup (\!|\ell_m = \text{after}[\![\text{Sl}']\!] \,?\, (\bigcup\{\alpha^l_{\text{use},\text{mod}}[\![\text{S}]\!]\ L_b, L_e\ \langle \pi'_0, \pi_3 \rangle \mid \langle \pi'_0, \pi_3 \rangle \in \mathcal{S}^*[\![\text{S}]\!]\}) \,⨾\, \varnothing|\!) \cup (\!|\text{escape}[\![\text{Sl}']\!] \wedge \ell_m = \text{break-to}[\![\text{Sl}']\!] \,?\, L_b \,⨾\, \varnothing|\!) \mid \langle \pi_0, \pi_1 \rangle \in \mathcal{S}^*[\![\text{Sl}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\text{a}_1} \ell_2 \xrightarrow{\text{a}_2} \dots \xrightarrow{\text{a}_{m-1}} \ell_m\}$$

$\wr$Lemma 41.8$\wr$

$$
\begin{aligned}
&\subseteq \bigcup\{\alpha^{l}_{\texttt{use,mod}}\llbracket \texttt{sl}'\rrbracket\ L_b, (\mathcal{S}^{\exists \mathrm{l}}\llbracket \texttt{s}\rrbracket\ L_b, L_e)\ \langle\pi_0,\ \pi_1\rangle \mid \langle\pi_0,\ \pi_1\rangle\ \in\ \widehat{\mathcal{S}}^{*}\llbracket \texttt{sl}'\rrbracket\} \\
&\hfill \wr\text{Lemma 41.8 and (41.3)}\int \\
&= \alpha^{\exists l}_{\texttt{use,mod}}\llbracket \texttt{sl}'\rrbracket(\mathcal{S}^{*}\llbracket \texttt{sl}'\rrbracket)\ L_b, (\widehat{\mathcal{S}}^{\exists \mathrm{l}}\llbracket \texttt{s}\rrbracket\ L_b, L_e) \qquad \wr\text{def. (41.3) of } \alpha^{\exists l}_{\texttt{use,mod}}\int \\
&\subseteq \widehat{\mathcal{S}}^{\exists \mathrm{l}}\llbracket \texttt{sl}'\rrbracket\ L_b, (\widehat{\mathcal{S}}^{\exists \mathrm{l}}\llbracket \texttt{s}\rrbracket\ L_b, L_e) \\
&\qquad \wr\text{ind. hyp. of Theorem 41.24: } \alpha^{\exists l}_{\texttt{use,mod}}\llbracket \texttt{sl}'\rrbracket(\widehat{\mathcal{S}}^{*}\llbracket \texttt{sl}'\rrbracket)\ L_b, (\widehat{\mathcal{S}}^{\exists \mathrm{l}}\llbracket \texttt{s}\rrbracket\ L_b, L_e) \subseteq \\
&\qquad \widehat{\mathcal{S}}^{\exists \mathrm{l}}\llbracket \texttt{sl}'\rrbracket\ L_b, (\widehat{\mathcal{S}}^{\exists \mathrm{l}}\llbracket \texttt{s}\rrbracket\ L_b, L_e)\text{ , Q.E.D.}\int
\end{aligned}
$$

- For the ***empty statement list*** $\texttt{sl} ::= \epsilon$, we have $\mathcal{S}^{*}\llbracket \texttt{sl}\rrbracket = \{\langle\pi_0\ell,\ \ell\rangle\}$ by (6.15), where $\ell = \texttt{at}\llbracket \texttt{sl}\rrbracket$ and so

$$
\begin{aligned}
&\alpha^{\exists l}_{\texttt{use,mod}}\llbracket \texttt{sl}\rrbracket\ (\mathcal{S}^{*}\llbracket \texttt{sl}\rrbracket)\ L_b, L_e \\
&= \bigcup\{\alpha^{l}_{\texttt{use,mod}}\llbracket \texttt{sl}\rrbracket\ L_b, L_e\ \langle\pi_0,\ \pi_1\rangle \mid \langle\pi_0,\ \pi_1\rangle\ \in\ \mathcal{S}^{*}\llbracket \texttt{sl}\rrbracket\} && \wr(41.3)\int \\
&= \bigcup\{\alpha^{l}_{\texttt{use,mod}}\llbracket \texttt{sl}\rrbracket\ L_b, L_e\ \langle\pi_0,\ \pi_1\rangle \mid \langle\pi_0,\ \pi_1\rangle\ \in\ \{\langle\pi_0\ell,\ \ell\rangle\}\} && \wr\text{def. } \mathcal{S}^{*}\llbracket \texttt{sl}\rrbracket\int \\
&= \alpha^{\exists l}_{\texttt{use,mod}}\llbracket \texttt{sl}\rrbracket\ L_b, L_e\ \langle\pi_0\ell,\ \ell\rangle && \wr\text{def. } \in \text{ and } \cup\int \\
&= \{\texttt{x} \in \mathbb{V} \mid (\ell = \texttt{after}\llbracket \texttt{sl}\rrbracket \wedge \texttt{x} \in L_e) \vee (\texttt{escape}\llbracket \texttt{sl}\rrbracket \wedge \ell = \texttt{break-to}\llbracket \texttt{sl}\rrbracket \wedge \texttt{x} \in L_b)\} && \wr(41.3)\int \\
&= L_e \quad \wr\ell = \texttt{at}\llbracket \texttt{sl}\rrbracket = \texttt{after}\llbracket \texttt{sl}\rrbracket \text{ in Appendix 4.2.1 and } \texttt{escape}\llbracket \texttt{sl}\rrbracket = \mathit{ff} \text{ in 4.2.4 when } \texttt{sl} = \epsilon\int
\end{aligned}
$$

Proof of Theorem 41.27 The proof is by structural induction and essentially consists in applying De Morgan laws for complement. For example,

$$
\begin{aligned}
&\widehat{\mathcal{S}}^{\forall \mathrm{d}}\llbracket \texttt{if (B) S}_t\rrbracket\ D_b, D_e \\
&= \neg\widehat{\mathcal{S}}^{\exists \mathrm{l}}\llbracket \texttt{if (B) S}_t\rrbracket\ \neg D_b, \neg D_e && \wr\text{definition of } \widehat{\mathcal{S}}^{\forall \mathrm{d}}\llbracket \texttt{s}\rrbracket \text{ as dual of } \widehat{\mathcal{S}}^{\exists \mathrm{l}}\llbracket \texttt{s}\rrbracket\int \\
&= \neg(\texttt{use}\llbracket \texttt{B}\rrbracket \cup \neg D_e \cup \widehat{\mathcal{S}}^{\exists \mathrm{l}}\llbracket \texttt{S}_t\rrbracket\ \neg D_b, \neg D_e) && \wr(41.22)\int \\
&= \neg\,\texttt{use}\llbracket \texttt{B}\rrbracket \cap \neg\neg D_e \cap \neg\widehat{\mathcal{S}}^{\exists \mathrm{l}}\llbracket \texttt{S}_t\rrbracket\ \neg D_b, \neg D_e) && \wr\text{De Morgan laws}\int \\
&= \neg\,\texttt{use}\llbracket \texttt{B}\rrbracket \cap D_e \cap \widehat{\mathcal{S}}^{\forall \mathrm{d}}\llbracket \texttt{S}_t\rrbracket\ D_b, D_e && \wr\text{structural induction hypothesis}\int
\end{aligned}
$$

All other cases are similar. □

3 Mathematical proofs of chapter 44

Proof of Theorem 44.38 • In case (44.41) of an empty temporal specification ε, we have

$$
\begin{aligned}
&\mathcal{M}^{\dagger}\llbracket \texttt{S}\rrbracket\langle\underline{\varrho},\ \varepsilon\rangle \\
&\triangleq \mathcal{M}^{\dagger}\langle\underline{\varrho},\ \varepsilon\rangle(\widehat{\mathcal{S}}^{*}_{\mathbb{s}}\llbracket \texttt{S}\rrbracket) && \wr(44.26)\int \\
&= \{\langle\pi,\ \texttt{R}'\rangle \mid \pi \in \widehat{\mathcal{S}}^{*}_{\mathbb{s}}\llbracket \texttt{S}\rrbracket \wedge \langle\mathit{tt},\ \texttt{R}'\rangle = \mathcal{M}^{t}\langle\rho,\ \varepsilon\rangle\pi\} && \wr(44.25)\int
\end{aligned}
$$

$$= \{\langle \pi,\ \varepsilon\rangle \mid \pi \in \widehat{\mathcal{S}}^{\,*}_{\mathbb{S}}[\![\mathtt{S}]\!]\} \qquad \wr\text{since } \mathcal{M}^{t}\langle \underline{\varrho},\ \varepsilon\rangle\pi \triangleq \langle \mathtt{tt},\ \varepsilon\rangle \text{ by (44.24)}\wr$$

$$\triangleq \widehat{\mathcal{M}}^{+}[\![\mathtt{S}]\!]\langle \underline{\varrho},\ \varepsilon\rangle \qquad \wr(44.41)\wr$$

- In case (44.43) of an empty statement list $\mathtt{Sl} ::= \epsilon$

$$\mathcal{M}^{+}[\![\mathtt{Sl}]\!]\ \langle \underline{\varrho},\ \mathtt{R}\rangle$$

$$= \mathcal{M}^{+}\langle \underline{\varrho},\ \mathtt{R}\rangle(\widehat{\mathcal{S}}^{\,*}_{\mathbb{S}}[\![\mathtt{Sl}]\!]) \qquad \wr(44.26)\wr$$

$$= \{\langle \pi,\ \mathtt{R}'\rangle \mid \pi \in \widehat{\mathcal{S}}^{\,*}_{\mathbb{S}}[\![\mathtt{Sl}]\!] \wedge \langle \mathtt{tt},\ \mathtt{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R}\rangle\pi\} \qquad \wr(44.25)\wr$$

$$= \{\langle \pi,\ \mathtt{R}'\rangle \mid \pi \in \{\langle \mathsf{at}[\![\mathtt{Sl}]\!],\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \wedge \langle \mathtt{tt},\ \mathtt{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R}\rangle\pi\} \qquad \wr(42.10)\wr$$

$$= \{\langle\langle \mathsf{at}[\![\mathtt{Sl}]\!],\ \rho\rangle,\ \mathtt{R}'\rangle \mid \rho \in \mathbb{E}\mathbb{v} \wedge \langle \mathtt{tt},\ \mathtt{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R}\rangle(\langle \mathsf{at}[\![\mathtt{Sl}]\!],\ \rho\rangle)\} \qquad \wr\text{def. } \in\wr$$

$$= \{\langle\langle \mathsf{at}[\![\mathtt{Sl}]\!],\ \rho\rangle,\ \mathtt{R}'\rangle \mid \rho \in \mathbb{E}\mathbb{v} \wedge \langle \mathtt{L : B},\ \mathtt{R}'\rangle = \mathsf{fstnxt}(\mathtt{R}) \wedge \langle \underline{\varrho},\ \langle \mathsf{at}[\![\mathtt{Sl}]\!],\ \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathtt{L : B}]\!]\}$$

$$\wr(44.24) \text{ with } \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R}'\rangle\ni = \langle \mathtt{tt},\ \mathtt{R}'\rangle\wr$$

$$= \widehat{\mathcal{M}}^{+}[\![\mathtt{Sl}]\!]\langle \underline{\varrho},\ \mathtt{R}\rangle \qquad \wr(44.43)\wr$$

- In case (44.44) of a skip statement $\mathtt{S} ::= \mathtt{;}$

$$\mathcal{M}^{+}[\![\mathtt{S}]\!]\ \langle \underline{\varrho},\ \mathtt{R}\rangle$$

$$= \{\langle \pi,\ \mathtt{R}'\rangle \mid \pi \in \widehat{\mathcal{S}}^{\,*}_{\mathbb{S}}[\![\mathtt{S}]\!] \wedge \langle \mathtt{tt},\ \mathtt{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R}\rangle\pi\} \qquad \wr(44.26) \text{ and } (44.25)\wr$$

$$= \{\langle \pi,\ \mathtt{R}'\rangle \mid \pi \in \{\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \wedge \langle \mathtt{tt},\ \mathtt{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R}\rangle\pi\} \qquad \wr(42.11)\wr$$

$$= \{\langle\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle,\ \mathtt{R}'\rangle \mid \rho \in \mathbb{E}\mathbb{v} \wedge \langle \mathtt{tt},\ \mathtt{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R}\rangle(\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle)\} \qquad \wr\text{def. } \in\wr$$

$$= \{\langle\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle,\ \mathtt{R}'\rangle \mid \rho \in \mathbb{E}\mathbb{v} \wedge \langle \mathtt{L : B},\ \mathtt{R}'\rangle = \mathsf{fstnxt}(\mathtt{R}) \wedge \langle \underline{\varrho},\ \langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathtt{L : B}]\!]\}$$

$$\wr(44.24) \text{ with } \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R}'\rangle\ni = \langle \mathtt{tt},\ \mathtt{R}'\rangle\wr$$

$$= \widehat{\mathcal{M}}^{+}[\![\mathtt{S}]\!]\langle \underline{\varrho},\ \mathtt{R}\rangle \qquad \wr(44.44)\wr$$

- In case (44.49) of an iteration statement $\mathtt{S} ::= \mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b$, we apply Corollary 18.29 so we have to calculate the abstract transformer that satisfies the commutation property for an iterate X of the concrete transformer $\mathcal{F}^{*}_{\mathbb{S}}[\![\mathtt{S}]\!]$ (which traces must be of the form $\pi\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle$).

$$\mathcal{M}^{+}\langle \underline{\varrho},\ \mathtt{R}\rangle(\mathcal{F}^{*}_{\mathbb{S}}[\![\mathtt{S}]\!]\ X)$$

$$= \mathcal{M}^{+}\langle \underline{\varrho},\ \mathtt{R}\rangle(\{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \cup \{\pi_2\langle \ell',\ \rho\rangle\langle \mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle \mid \pi_2\langle \ell',\ \rho\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\,\rho = \mathtt{ff} \wedge \ell' = \ell\} \cup \{\pi_2\langle \ell',\rho\rangle\langle \mathsf{at}[\![\mathtt{S}_b]\!],\rho\rangle\cdot\pi_3 \mid \pi_2\langle \ell',\rho\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\rho = \mathtt{tt} \wedge \langle \mathsf{at}[\![\mathtt{S}_b]\!],\rho\rangle\cdot\pi_3 \in \widehat{\mathcal{S}}^{\,*}_{\mathbb{S}}[\![\mathtt{S}_b]\!] \wedge \ell' = \ell\})$$

$$\wr(42.6)\wr$$

$$= \mathcal{M}^{+}\langle \underline{\varrho},\ \mathtt{R}\rangle(\{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\}) \cup \mathcal{M}^{+}\langle \underline{\varrho},\ \mathtt{R}\rangle(\{\pi_2\langle \ell',\ \rho\rangle\langle \mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle \mid \pi_2\langle \ell',\ \rho\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\,\rho = \mathtt{ff} \wedge \ell' = \ell\}) \cup \mathcal{M}^{+}\langle \underline{\varrho},\ \mathtt{R}\rangle(\{\pi_2\langle \ell',\ \rho\rangle\langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho\rangle\cdot\pi_3 \mid \pi_2\langle \ell',\ \rho\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\,\rho = \mathtt{tt} \wedge \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho\rangle\cdot\pi_3 \in \widehat{\mathcal{S}}^{\,*}_{\mathbb{S}}[\![\mathtt{S}_b]\!] \wedge \ell' = \ell\})$$

$$\wr\text{Galois connection (44.30), so that, by Lemma 11.34, } \mathcal{M}^{+}\langle \underline{\varrho},\ \mathtt{R}\rangle \text{ preserves joins}\wr$$

To avoid repeating (44.41), we assume that $\mathsf{R} \notin \mathbb{R}_\varepsilon$ so we can let $\langle \mathsf{L}' : \mathsf{B}', \mathsf{R}' \rangle = \mathsf{fstnxt}(\mathsf{R})$. There are three subcases.

— The first case is that of an observation of the execution that stops at loop entry $\ell = \mathsf{at}[\![\mathsf{S}]\!]$. This is similar to the above proof *e.g.* of (44.44) for a skip statement, and we get

$$\begin{aligned}
&\mathcal{M}^{+}\langle \underline{\varrho}, \mathsf{R}\rangle(\{\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\}\\
= &\{\langle\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}'\rangle \mid \rho \in \mathbb{E}\mathbb{v} \wedge \langle \mathsf{L}' : \mathsf{B}', \mathsf{R}'\rangle = \mathsf{fstnxt}(\mathsf{R}) \wedge \langle \underline{\varrho}, \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\rangle \in \mathcal{S}^{\mathfrak{r}}[\![\mathsf{L}' : \mathsf{B}']\!]\}
\end{aligned}$$

— The second case is that of the loop exit

$$\begin{aligned}
&\mathcal{M}^{+}\langle \underline{\varrho}, \mathsf{R}\rangle(\{\pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!], \rho\rangle \mid \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\,\rho = \mathrm{ff}\})\\
= &\{\langle \pi, \mathsf{R}'\rangle \mid \pi \in \{\pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!], \rho\rangle \mid \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\,\rho = \mathrm{ff}\} \wedge \langle \mathrm{tt}, \mathsf{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}\rangle\pi\} && \text{(44.25)}\\
= &\{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}'\rangle \mid \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\,\rho = \mathrm{ff} \wedge \langle \mathrm{tt}, \mathsf{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}\rangle(\pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!], \rho\rangle)\} && \text{def. } \in\\
= &\{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}'\rangle \mid \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\,\rho = \mathrm{ff} \wedge \exists \mathsf{R}'' \in \mathbb{R}\,.\, \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}\rangle(\pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle) = \langle \mathrm{tt}, \mathsf{R}''\rangle \wedge \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!], \rho\rangle) = \langle \mathrm{tt}, \mathsf{R}'\rangle\} && \text{Lemma 44.37}\\
= &\{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \in \{\langle \pi, \mathsf{R}''\rangle \mid \pi \in X \wedge \langle \mathrm{tt}, \mathsf{R}''\rangle = \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}\rangle\pi\} \wedge \mathcal{B}[\![\mathsf{B}]\!]\,\rho = \mathrm{ff} \wedge \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!], \rho\rangle) = \langle \mathrm{tt}, \mathsf{R}'\rangle\}\\
& && \text{X is an iterate of the concrete transformer $\mathcal{F}_{\mathbb{S}}^{*}[\![\mathsf{S}]\!]$ so its traces must be of the form $\pi\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle$}\\
= &\{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \in \mathcal{M}^{+}\langle \underline{\varrho}, \mathsf{R}\rangle X \wedge \mathcal{B}[\![\mathsf{B}]\!]\,\rho = \mathrm{ff} \wedge \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!], \rho\rangle) = \langle \mathrm{tt}, \mathsf{R}'\rangle\} && \text{(44.25)}\\
= &\{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!], \rho\rangle, \varepsilon\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \varepsilon\rangle \in \mathcal{M}^{+}\langle \underline{\varrho}, \mathsf{R}\rangle X \wedge \mathcal{B}[\![\mathsf{B}]\!]\,\rho = \mathrm{ff}\} \cup{}\\
&\{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \in \mathcal{M}^{+}\langle \underline{\varrho}, \mathsf{R}\rangle X \wedge \mathcal{B}[\![\mathsf{B}]\!]\,\rho = \mathrm{ff} \wedge \mathsf{R}'' \notin \mathbb{R}_\varepsilon \wedge \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!], \rho\rangle) = \langle \mathrm{tt}, \mathsf{R}'\rangle\}\\
& && \text{case analysis and } \mathcal{M}^{t}\langle \underline{\varrho}, \varepsilon\rangle\pi \triangleq \langle \mathrm{tt}, \varepsilon\rangle \text{ in (44.24)}
\end{aligned}$$

$= \{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho\rangle,\ \varepsilon\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle,\ \varepsilon\rangle \in \mathcal{M}^{\dagger}\langle \underline{\varrho},\ \mathsf{R}\rangle X \wedge \mathcal{B}[\![\mathsf{B}]\!]\ \rho = \mathrm{ff}\} \cup$
$\{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho\rangle,\ \varepsilon\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle,\ \mathsf{R}''\rangle \in \mathcal{M}^{\dagger}\langle \underline{\varrho},\ \mathsf{R}\rangle X \wedge \mathcal{B}[\![\mathsf{B}]\!]\ \rho = \mathrm{ff} \wedge \mathsf{R}'' \notin \mathbb{R}_{\varepsilon} \wedge \langle \mathsf{L}'\ \mathsf{:}\ \mathsf{B}',\ \mathsf{R}'\rangle = \mathsf{fstnxt}(\mathsf{R}'') \wedge \mathsf{R}' \in \mathbb{R}_{\varepsilon} \wedge \langle \underline{\varrho},\ \langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L}'\ \mathsf{:}\ \mathsf{B}']\!]\} \cup$
$\{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho\rangle,\ \mathsf{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle,\ \mathsf{R}''\rangle \in \mathcal{M}^{\dagger}\langle \underline{\varrho},\ \mathsf{R}\rangle X \wedge \mathcal{B}[\![\mathsf{B}]\!]\ \rho = \mathrm{ff} \wedge \mathsf{R}'' \notin \mathbb{R}_{\varepsilon} \wedge \langle \mathsf{L}'\ \mathsf{:}\ \mathsf{B}',\ \mathsf{R}'''\rangle = \mathsf{fstnxt}(\mathsf{R}'') \wedge \langle \underline{\varrho},\ \langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L}'\ \mathsf{:}\ \mathsf{B}']\!] \wedge \mathsf{R}''' \notin \mathbb{R}_{\varepsilon} \wedge \langle \mathsf{L}''\ \mathsf{:}\ \mathsf{B}'',\ \mathsf{R}'\rangle = \mathsf{fstnxt}(\mathsf{R}''') \wedge \langle \underline{\varrho},\ \langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L}''\ \mathsf{:}\ \mathsf{B}'']\!]\}$

(since $(\langle \mathrm{tt},\ \mathsf{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho\rangle)) \Leftrightarrow ((\langle \mathsf{L}'\ \mathsf{:}\ \mathsf{B}',\ \mathsf{R}'\rangle = \mathsf{fstnxt}(\mathsf{R}'') \wedge \mathsf{R}' \in \mathbb{R}_{\varepsilon} \wedge \langle \underline{\varrho},\ \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L}'\ \mathsf{:}\ \mathsf{B}']\!]) \vee (\langle \mathsf{L}'\ \mathsf{:}\ \mathsf{B}', \mathsf{R}'''\rangle = \mathsf{fstnxt}(\mathsf{R}'') \wedge \langle \underline{\varrho},\ \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L}'\ \mathsf{:}\ \mathsf{B}']\!] \wedge \mathsf{R}''' \notin \mathbb{R}_{\varepsilon} \wedge \langle \mathsf{L}''\ \mathsf{:}\ \mathsf{B}'', \mathsf{R}'\rangle = \mathsf{fstnxt}(\mathsf{R}''') \wedge \langle \underline{\varrho},\ \langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L}''\ \mathsf{:}\ \mathsf{B}'']\!])$ as shown above while proving the second term in case (44.46) of a conditional statement $\mathsf{S} ::= \mathtt{if}\ \ell\ \mathtt{(B)}\ \mathsf{S}_t$)

— The third and last case is that of an iteration executing the loop body.

$\mathcal{M}^{\dagger}\langle \underline{\varrho},\ \mathsf{R}\rangle(\{\pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle \cdot \pi_3 \mid \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\ \rho = \mathrm{tt} \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle\pi_3 \in \widehat{\mathcal{S}}^{*}_{\mathbb{S}}[\![\mathsf{S}_b]\!]\})$

$= \{\langle \pi,\ \mathsf{R}'\rangle \mid \pi \in \{\pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle\pi_3 \mid \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\ \rho = \mathrm{tt} \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle\pi_3 \in \widehat{\mathcal{S}}^{*}_{\mathbb{S}}[\![\mathsf{S}_b]\!]\} \wedge \langle \mathrm{tt},\ \mathsf{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathsf{R}\rangle\pi\}$ (44.25)

$= \{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle\pi_3,\ \mathsf{R}'\rangle \mid \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\ \rho = \mathrm{tt} \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle\pi_3 \in \widehat{\mathcal{S}}^{*}_{\mathbb{S}}[\![\mathsf{S}_b]\!] \wedge \langle \mathrm{tt},\ \mathsf{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathsf{R}\rangle(\pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle\pi_3)\}$ (def. $\in$)

$= \{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle\pi_3,\ \mathsf{R}'\rangle \mid \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\ \rho = \mathrm{tt} \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle\pi_3 \in \widehat{\mathcal{S}}^{*}_{\mathbb{S}}[\![\mathsf{S}_b]\!] \wedge \exists \mathsf{R}'' \in \mathbb{R}\ .\ \mathcal{M}^{t}\langle \underline{\varrho},\ \mathsf{R}\rangle(\pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle) = \langle \mathrm{tt},\ \mathsf{R}''\rangle \wedge \mathcal{M}^{t}\langle \underline{\varrho},\ \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle\pi_3) = \langle \mathrm{tt},\ \mathsf{R}'\rangle\}$ (Lemma 44.37)

$= \{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \mathsf{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \in \{\langle \pi, \mathsf{R}''\rangle \mid \pi \in X \wedge \langle \mathrm{tt}, \mathsf{R}''\rangle = \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}\rangle\pi\} \wedge \mathcal{B}[\![\mathsf{B}]\!]\ \rho = \mathrm{tt} \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \in \widehat{\mathcal{S}}^{*}_{\mathbb{S}}[\![\mathsf{S}_b]\!] \wedge \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3) = \langle \mathrm{tt}, \mathsf{R}'\rangle\}$

(def. $\in$ and X is an iterate of the concrete transformer $\mathcal{F}^{*}_{\mathbb{S}}[\![\mathsf{S}]\!]$ so its traces must be of the form $\pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle$)

$= \{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \mathsf{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \in \mathcal{M}^{\dagger}\langle \underline{\varrho}, \mathsf{R}\rangle X \wedge \mathcal{B}[\![\mathsf{B}]\!]\rho = \mathrm{tt} \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \in \widehat{\mathcal{S}}^{*}_{\mathbb{S}}[\![\mathsf{S}_b]\!] \wedge \mathcal{M}^{t}\langle \underline{\varrho},\ \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle\pi_3) = \langle \mathrm{tt},\ \mathsf{R}'\rangle\}$ (44.25)

$= \{\langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \mathsf{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \in \mathcal{M}^{\dagger}\langle \underline{\varrho}, \mathsf{R}\rangle X \wedge \mathcal{B}[\![\mathsf{B}]\!]\rho = \mathrm{tt} \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \in \widehat{\mathcal{S}}^{*}_{\mathbb{S}}[\![\mathsf{S}_b]\!] \wedge (\exists \mathsf{R}''' \in \mathbb{R}\ .\ \mathcal{M}^{t}\langle \underline{\varrho},\ \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle) = \langle \mathrm{tt},\ \mathsf{R}'''\rangle \wedge \mathcal{M}^{t}\langle \underline{\varrho},\ \mathsf{R}'''\rangle(\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle\pi_3) = \langle \mathrm{tt},\ \mathsf{R}'\rangle)\}$ (Lemma 44.37)

$= \{\langle \pi_2 \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \mathsf{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \in \mathscr{M}^{+}\langle \underline{\varrho}, \mathsf{R}\rangle X \wedge \mathscr{B}[\![\mathsf{B}]\!]\rho = \mathsf{tt} \wedge \exists \mathsf{R}''' \in \mathbb{R} \;.\; \langle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \mathsf{R}'\rangle \in \{\langle \pi, \mathsf{R}'\rangle \mid \pi \in \widehat{\mathcal{S}}^{\,*}_{\mathbb{s}}[\![\mathsf{S}_b]\!] \wedge \langle \mathsf{tt}, \mathsf{R}'\rangle = \mathscr{M}^{t}\langle \underline{\varrho}, \mathsf{R}'''\rangle\pi\} \wedge \mathscr{M}^{t}\langle \underline{\varrho}, \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle) = \langle \mathsf{tt}, \mathsf{R}'''\rangle\}$

$\wr$ def. $\in$ and def. $\widehat{\mathcal{S}}^{\,*}_{\mathbb{s}}[\![\mathsf{S}_b]\!]$ in Chapter 42 so that its traces must be of the form $\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3$ $\wr$

$= \{\langle \pi_2 \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \mathsf{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \in \mathscr{M}^{+}\langle \underline{\varrho}, \mathsf{R}\rangle X \wedge \mathscr{B}[\![\mathsf{B}]\!]\rho = \mathsf{tt} \wedge \mathscr{M}^{t}\langle \underline{\varrho}, \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle) = \langle \mathsf{tt}, \mathsf{R}'''\rangle \wedge \langle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \mathsf{R}'\rangle \in \mathscr{M}^{+}[\![\mathsf{S}_b]\!]\langle \underline{\varrho}, \mathsf{R}'''\rangle\}$

$\wr$(44.26) and (44.25), $\wedge$ commutative$\wr$

There are two subcases depending on whether $\mathsf{R}'' \in \mathbb{R}_\varepsilon$ or not.

— If $\mathsf{R}'' \in \mathbb{R}_\varepsilon$, then

$= \{\langle \pi_2 \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \varepsilon\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \varepsilon\rangle \in \mathscr{M}^{+}\langle \underline{\varrho}, \mathsf{R}\rangle X \wedge \mathscr{B}[\![\mathsf{B}]\!]\rho = \mathsf{tt} \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \in \widehat{\mathcal{S}}^{\,*}_{\mathbb{s}}[\![\mathsf{S}_b]\!]\}$

$\wr$since $\mathsf{R}'' \in \mathbb{R}_\varepsilon$ and $\mathscr{M}^{t}\langle \underline{\varrho}, \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle) = \langle \mathsf{tt}, \mathsf{R}'''\rangle$ imply that $\mathsf{R}''' = \varepsilon$ by (44.24) and so $\langle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \mathsf{R}'\rangle \in \mathscr{M}^{+}[\![\mathsf{S}_b]\!]\langle \underline{\varrho}, \mathsf{R}'''\rangle = \{\langle \pi, \varepsilon\rangle \mid \pi \in \widehat{\mathcal{S}}^{\,*}_{\mathbb{s}}[\![\mathsf{S}_b]\!]\}$ by (44.26) and (44.25) implies $\mathsf{R}' = \varepsilon$ and $\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \in \widehat{\mathcal{S}}^{\,*}_{\mathbb{s}}[\![\mathsf{S}_b]\!]$$\wr$

— Otherwise $\mathsf{R}'' \notin \mathbb{R}_\varepsilon$

$= \{\langle \pi_2 \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \mathsf{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \in \mathscr{M}^{+}\langle \underline{\varrho}, \mathsf{R}\rangle X \wedge \mathscr{B}[\![\mathsf{B}]\!]\rho = \mathsf{tt} \wedge \mathsf{R}'' \notin \mathbb{R}_\varepsilon \wedge \langle \mathsf{L} : \mathsf{B}, \mathsf{R}''''\rangle = \mathsf{fstnxt}(\mathsf{R}'') \wedge \langle \underline{\varrho}, \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L} : \mathsf{B}]\!] \wedge \mathscr{M}^{t}\langle \underline{\varrho}, \mathsf{R}''''\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle = \langle \mathsf{tt}, \mathsf{R}'''\rangle \wedge \langle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \mathsf{R}'\rangle \in \mathscr{M}^{+}[\![\mathsf{S}_b]\!]\langle \underline{\varrho}, \mathsf{R}'''\rangle\}$ $\wr$(44.24)$\wr$

There are two subsubcases, depending on whether R'''' is empty or not.

– If $\mathsf{R}'''' \in \mathbb{R}_\varepsilon$ then, as shown before, $\mathscr{M}^{t}\langle \underline{\varrho}, \mathsf{R}''''\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle = \langle \mathsf{tt}, \mathsf{R}'''\rangle$ implies that $\mathsf{R}''' \in \mathbb{R}_\varepsilon$ and so $\langle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \mathsf{R}'\rangle \in \mathscr{M}^{+}[\![\mathsf{S}_b]\!]\langle \underline{\varrho}, \mathsf{R}'''\rangle$ if and only if $\mathsf{R}' \in \mathbb{R}_\varepsilon$ and $\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \in \widehat{\mathcal{S}}^{\,*}_{\mathbb{s}}[\![\mathsf{S}_b]\!]$. We get

$= \{\langle \pi_2 \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \varepsilon\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \in \mathscr{M}^{+}\langle \underline{\varrho}, \mathsf{R}\rangle X \wedge \mathscr{B}[\![\mathsf{B}]\!]\rho = \mathsf{tt} \wedge \mathsf{R}'' \notin \mathbb{R}_\varepsilon \wedge \langle \mathsf{L} : \mathsf{B}, \varepsilon\rangle = \mathsf{fstnxt}(\mathsf{R}'') \wedge \langle \underline{\varrho}, \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L} : \mathsf{B}]\!] \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3 \in \widehat{\mathcal{S}}^{\,*}_{\mathbb{s}}[\![\mathsf{S}_b]\!]\}$

$\wr$(44.24)$\wr$

– Otherwise $\mathsf{R}'''' \notin \mathbb{R}_\varepsilon$.

$= \{\langle \pi_2 \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \mathsf{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \in \mathscr{M}^{+}\langle \underline{\varrho}, \mathsf{R}\rangle X \wedge \mathscr{B}[\![\mathsf{B}]\!]\rho = \mathsf{tt} \wedge \mathsf{R}'' \notin \mathbb{R}_\varepsilon \wedge \langle \mathsf{L} : \mathsf{B}, \mathsf{R}''''\rangle = \mathsf{fstnxt}(\mathsf{R}'') \wedge \langle \underline{\varrho}, \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L} : \mathsf{B}]\!] \wedge \mathsf{R}'''' \notin \mathbb{R}_\varepsilon \wedge \mathscr{M}^{t}\langle \underline{\varrho}, \mathsf{R}''''\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle = \langle \mathsf{tt}, \mathsf{R}'''\rangle \wedge \langle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\pi_3, \mathsf{R}'\rangle \in \mathscr{M}^{+}[\![\mathsf{S}_b]\!]\langle \underline{\varrho}, \mathsf{R}'''\rangle\}$

$= \{\langle \pi_2 \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle \langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle \pi_3, \mathsf{R}'\rangle \mid \langle \pi_2 \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \in \mathcal{M}^{\dagger}\langle \underline{\varrho}, \mathsf{R}\rangle X \wedge \mathcal{B}[\![\mathsf{B}]\!]\rho = \mathsf{tt} \wedge \mathsf{R}'' \notin \mathbb{R}_\varepsilon \wedge \langle \mathsf{L} : \mathsf{B}, \mathsf{R}''''\rangle = \mathsf{fstnxt}(\mathsf{R}'') \wedge \langle \underline{\varrho}, \langle \mathsf{at}[\![\mathsf{S}]\!], \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L} : \mathsf{B}]\!] \wedge \mathsf{R}'''' \notin \mathbb{R}_\varepsilon \wedge \langle \mathsf{L}' : \mathsf{B}', \mathsf{R}'''\rangle = \mathsf{fstnxt}(\mathsf{R}'''') \wedge \langle \underline{\varrho}, \langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L}' : \mathsf{B}']\!] \wedge \langle\langle \mathsf{at}[\![\mathsf{S}_b]\!], \rho\rangle \pi_3, \mathsf{R}'\rangle \in \mathcal{M}^{\dagger}[\![\mathsf{S}_b]\!]\langle \underline{\varrho}, \mathsf{R}'''\rangle\}$

$\wr$(44.24)$\wr$

— Grouping all cases together we get the term (44.50) defining $\widehat{\mathcal{F}}^{\dagger}[\![\mathsf{S}]\!]\langle \underline{\varrho}, \mathsf{R}\rangle$ $(\mathcal{M}^{\dagger}\langle \underline{\varrho}, \mathsf{R}\rangle X)$ and so Corollary 18.29 and the commutation condition $\mathcal{M}^{\dagger}\langle \underline{\varrho}, \mathsf{R}\rangle(\mathcal{F}^{*}_{\mathbb{S}}[\![\mathsf{S}]\!](X)) = \widehat{\mathcal{F}}^{\dagger}[\![\mathsf{S}]\!]\langle \underline{\varrho}, \mathsf{R}\rangle$ $(\mathcal{M}^{\dagger}\langle \underline{\varrho}, \mathsf{R}\rangle(X))$ for the iterates X of $\mathcal{F}^{*}_{\mathbb{S}}[\![\mathsf{S}]\!]$ yield $\widehat{\mathcal{M}}^{\dagger}[\![\mathsf{S}]\!]\langle \underline{\varrho}, \mathsf{R}\rangle \triangleq \mathsf{lfp}^{\subseteq}(\widehat{\mathcal{F}}^{\dagger}[\![\mathsf{S}]\!]\langle \underline{\varrho}, \mathsf{R}\rangle)$ that is (44.49).

- In case (44.48) of a break statement $\mathsf{S} ::= \ell$ **break ;**

$\mathcal{M}^{\dagger}[\![\mathsf{S}]\!]\ \langle \underline{\varrho}, \mathsf{R}\rangle$

$= \{\langle \pi, \mathsf{R}'\rangle \mid \pi \in \widehat{\mathcal{S}}^{*}_{\mathbb{S}}[\![\mathsf{S}]\!] \wedge \langle \mathsf{tt}, \mathsf{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}\rangle \pi\}$ $\wr$(44.26) and (44.25)$\wr$

$= \{\langle \pi, \mathsf{R}'\rangle \mid \pi \in \{\langle \ell, \rho\rangle \mid \rho \in \mathbb{E}\mathsf{v}\} \cup \{\langle \ell, \rho\rangle \langle \mathsf{break\text{-}to}[\![\mathsf{S}]\!], \rho\rangle \mid \rho \in \mathbb{E}\mathsf{v}\} \wedge \langle \mathsf{tt}, \mathsf{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}\rangle \pi\}$

$\wr$(42.14)$\wr$

$= \{\langle \langle \ell, \rho\rangle, \mathsf{R}''\rangle \mid \langle \mathsf{tt}, \mathsf{R}''\rangle = \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}\rangle \langle \ell, \rho\rangle\} \cup \{\langle \langle \ell, \rho\rangle \langle \mathsf{break\text{-}to}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \mid \langle \mathsf{tt}, \mathsf{R}''\rangle = \mathcal{M}^{t}\langle \underline{\varrho}, \mathsf{R}\rangle(\langle \ell, \rho\rangle \langle \mathsf{break\text{-}to}[\![\mathsf{S}]\!], \rho\rangle)\}$ $\wr$def. $\cup$ and $\in$$\wr$

$= \mathsf{let}\ \langle \mathsf{L} : \mathsf{B}, \mathsf{R}'\rangle = \mathsf{fstnxt}(\mathsf{R})\ \mathsf{in}\ \{\langle \langle \ell, \rho\rangle, \mathsf{R}'\rangle \mid \langle \underline{\varrho}, \langle \ell, \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L} : \mathsf{B}]\!]\} \cup \{\langle \langle \ell, \rho\rangle \langle \mathsf{break\text{-}to}[\![\mathsf{S}]\!], \rho\rangle, \varepsilon\rangle \mid \mathsf{R}' \in \mathbb{R}_\varepsilon \wedge \langle \underline{\varrho}, \langle \ell, \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L} : \mathsf{B}]\!]\} \cup \{\langle \langle \ell, \rho\rangle \langle \mathsf{break\text{-}to}[\![\mathsf{S}]\!], \rho\rangle, \mathsf{R}''\rangle \mid \mathsf{R}' \notin \mathbb{R}_\varepsilon \wedge \langle \underline{\varrho}, \langle \ell, \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L} : \mathsf{B}]\!] \wedge \langle \mathsf{L}' : \mathsf{B}', \mathsf{R}''\rangle = \mathsf{fstnxt}(\mathsf{R}') \wedge \langle \underline{\varrho}, \langle \mathsf{break\text{-}to}[\![\mathsf{S}]\!], \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L}' : \mathsf{B}']\!]\}$

$\wr$$\mathsf{R} \notin \mathbb{R}_\varepsilon$, case analysis on $\mathsf{R}' \in \mathbb{R}_\varepsilon$, and(44.24)$\wr$ □

4 Mathematical proofs of chapter 47

Proof (47.47) There are three cases depending on whether the program label ℓ is at or after statement S, or in the true branch S_t.

— (1) — The cases $\ell = \mathsf{at}[\![\mathsf{S}]\!]$ was handled in (47.41) and $\ell \notin \mathsf{labx}[\![\mathsf{S}]\!]$ in (47.42).
— (2) — Assume $\ell = \mathsf{after}[\![\mathsf{S}]\!]$.

$\alpha^{\mathsf{d}}(\{\mathcal{S}^{+\infty}[\![\mathsf{S}]\!]\})\ \mathsf{after}[\![\mathsf{S}]\!]$

$= \alpha^{\mathsf{d}}(\{\mathcal{S}^{*}[\![\mathsf{S}]\!]\})\ \mathsf{after}[\![\mathsf{S}]\!]$ $\wr$Lemma 47.23$\wr$

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \mathcal{S}^{*}[\![\mathsf{S}]\!] \in \mathcal{D}(\mathsf{after}[\![\mathsf{S}]\!])\langle \mathsf{x}', \mathsf{y}\rangle\}$ $\wr$def. (47.25) of $\alpha^{\mathsf{d}}$$\wr$

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists \langle \pi_0, \pi_1\rangle, \langle \pi'_0, \pi'_1\rangle \in \mathcal{S}^{*}[\![\mathsf{S}]\!]\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\}\ .\ \boldsymbol{\varrho}(\pi_0)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0, \pi_1), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0, \pi'_1))\}$ $\wr$def. (47.19) of $\mathcal{D}^{\ell}\langle \mathsf{x}', \mathsf{y}\rangle$$\wr$

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists\langle \pi_0, \pi_1\rangle, \langle \pi'_0, \pi'_1\rangle \in \{\langle \pi\mathsf{at}[\![\mathsf{S}]\!], \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathit{ff}\} \cup \{\langle \pi\mathsf{at}[\![\mathsf{S}]\!], \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathit{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathsf{S}_t]\!](\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\} \,.\, (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \,.\, \varrho(\pi_0)\mathsf{z} = \varrho(\pi'_0)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0, \pi_1), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0, \pi'_1))\}$

(def. $\mathcal{S}^*[\![\mathsf{S}]\!]$ in (6.9), (6.19), and (6.18) so that $\mathsf{after}[\![\mathsf{S}]\!] = \mathsf{after}[\![\mathsf{S}_t]\!]$)

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists\langle \pi_0, \pi_1\mathsf{after}[\![\mathsf{S}]\!]\rangle, \langle \pi'_0, \pi'_1\mathsf{after}[\![\mathsf{S}]\!]\rangle \in \{\langle \pi\mathsf{at}[\![\mathsf{S}]\!], \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathit{ff}\} \cup \{\langle \pi\mathsf{at}[\![\mathsf{S}]\!], \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathit{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathsf{S}_t]\!](\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \,.\, \varrho(\pi_0)\mathsf{z} = \varrho(\pi'_0)\mathsf{z}) \wedge \mathsf{diff}(\varrho(\pi_0 \frown \pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y}, \varrho(\pi'_0 \frown \pi'_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\}$

(def. $\in$ so that π_1 and π'_1 must end with $\mathsf{after}[\![\mathsf{S}]\!]$ and def. (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]$)

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists\pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!], \pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!] \in \{\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathit{ff}\} \cup \{\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathit{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathsf{S}_t]\!](\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \,.\, \varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z}) \wedge \mathsf{diff}(\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y}, \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\}$

(def. $\in$ and trace concatenation $\frown$)

$$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists\pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!], \pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!] \in \{\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathit{ff}\} \cup \{\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathit{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathsf{S}_t]\!](\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \,.\, \varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z}) \wedge (\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\} \tag{1}$$

(def. (47.18) of diff)

There are four subcases, depending upon which branch of the conditional is taken by the two executions $\pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!]$ and $\pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!]$.

— (2.a) — If both executions $\pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!]$ and $\pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!]$ are through the false branch, we have,

(1)

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!], \pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \,.\, \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathit{ff} \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathit{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \,.\, \varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z}) \wedge (\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\}$

(case $\mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathit{ff}$ and $\mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathit{ff}$)

$= \{\langle \mathtt{x}', \mathtt{y}\rangle \mid \exists \pi_0\mathsf{at}[\![\mathtt{S}]\!], \pi'_0\mathsf{at}[\![\mathtt{S}]\!] \mathrel{.} \mathscr{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathtt{S}]\!]) = \mathrm{ff} \wedge \mathscr{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathtt{S}]\!]) = \mathrm{ff} \wedge (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}'\} \mathrel{.} \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathtt{S}]\!])\mathtt{z} = \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathtt{S}]\!])\mathtt{z}) \wedge (\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathtt{S}]\!])\mathtt{y} \neq \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathtt{S}]\!]))\mathtt{y}\}$

$\wr$def. (6.6) of $\boldsymbol{\varrho}$ so that $\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathtt{S}]\!] \xrightarrow{\neg(\mathtt{B})} \mathsf{after}[\![\mathtt{S}]\!])\mathtt{y} = \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathtt{S}]\!]\mathtt{y})$$\wr$

$= \{\langle \mathtt{x}', \mathtt{y}\rangle \mid \exists \rho, \nu \mathrel{.} \mathscr{B}[\![\mathtt{B}]\!]\rho = \mathrm{ff} \wedge \mathscr{B}[\![\mathtt{B}]\!]\rho[\mathtt{x}' \leftarrow \nu] = \mathrm{ff} \wedge \rho(\mathtt{y}) \neq \rho[\mathtt{x}' \leftarrow \nu]\mathtt{y}\}$

$\wr$letting $\rho = \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathtt{S}]\!])$, $\nu = \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathtt{S}]\!])\mathtt{x}'$ so that $\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}'\} \mathrel{.} \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathtt{S}]\!])\mathtt{z} = \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathtt{S}]\!])\mathtt{z}$ implies $\boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathtt{S}]\!]) = \rho[\mathtt{x}' \leftarrow \nu]$ and, conversely Exercise 6.8, so that any environment ρ can be computed as the result $\boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathtt{S}]\!])$ of an appropriate initialization trace ${}'_0\mathsf{at}[\![\mathtt{S}]\!]$ (otherwise, this is $\subseteq$)$\wr$

$= \{\langle \mathtt{x}', \mathtt{x}'\rangle \mid \exists \rho, \nu \mathrel{.} \rho(\mathtt{x}') \neq \nu \wedge \mathscr{B}[\![\mathtt{B}]\!]\rho = \mathrm{ff} \wedge \mathscr{B}[\![\mathtt{B}]\!]\rho[\mathtt{x}' \leftarrow \nu] = \mathrm{ff}\}$

$\wr$since $\rho[\mathtt{x}' \leftarrow \nu](\mathtt{y}) = \rho(\mathtt{y})$ when $\mathtt{y} \neq \mathtt{x}'$$\wr$

$= \{\langle \mathtt{x}', \mathtt{x}'\rangle \mid \mathtt{x}' \in \mathsf{nondet}(\neg\mathtt{B}, \neg\mathtt{B})\}$ $\wr$def. (47.48) of $\mathsf{nondet}$$\wr$

$= \mathbb{1}_{\mathbb{V}} \rceil \mathsf{nondet}(\neg\mathtt{B}, \neg\mathtt{B})$ $\wr$def. left restriction $\rceil$$\wr$

$\subseteq \mathbb{1}_{\mathbb{V}}$

In words for that first case, the initial value of $\mathtt{x}'$ flows to the value of $\mathtt{x}'$ by the false branch of the conditional `if (B) S`$_t$ when there are at least two different values of $\mathtt{x}'$ for which $\mathtt{B}$ is false. (If there is only one, $\mathtt{x}'$ is constant on the false branch. This can be disproved by a constancy analysis [3, 4, 6, 7, 9, 10] or a determinacy analysis [5, 8].) A classical coarser over-approximation is to ignore values *i.e.* that variables may have only one value making the test false.

— (2.b) — Else, if both executions $\pi_0\mathsf{at}[\![\mathtt{S}]\!]\pi_1\mathsf{after}[\![\mathtt{S}]\!]$ and $\pi'_0\mathsf{at}[\![\mathtt{S}]\!]\pi'_1\mathsf{after}[\![\mathtt{S}]\!]$ are through the true branch, we have,

(1)

$= \{\langle \mathtt{x}', \mathtt{y}\rangle \mid \exists \pi_0\mathsf{at}[\![\mathtt{S}]\!]\pi_1\mathsf{after}[\![\mathtt{S}]\!], \pi'_0\mathsf{at}[\![\mathtt{S}]\!]\pi'_1\mathsf{after}[\![\mathtt{S}]\!] \in \{\pi\mathsf{at}[\![\mathtt{S}]\!] \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_t]\!]\pi'\mathsf{after}[\![\mathtt{S}]\!] \mid \mathscr{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi\mathsf{at}[\![\mathtt{S}]\!]) = \mathrm{tt} \wedge \mathsf{at}[\![\mathtt{S}_t]\!]\pi'\mathsf{after}[\![\mathtt{S}]\!] \in \widehat{\mathscr{S}}^{+\infty}[\![\mathtt{S}_t]\!](\pi\mathsf{at}[\![\mathtt{S}]\!] \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_t]\!])\} \wedge (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}'\} \mathrel{.} \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathtt{S}]\!])\mathtt{z} = \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathtt{S}]\!])\mathtt{z}) \wedge (\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathtt{S}]\!]\pi_1\mathsf{after}[\![\mathtt{S}]\!])\mathtt{y} \neq \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathtt{S}]\!]\pi'_1\mathsf{after}[\![\mathtt{S}]\!])\mathtt{y})\}$

$\wr$case $\mathscr{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathtt{S}]\!]) = \mathrm{tt}$ and $\mathscr{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathtt{S}]\!]) = \mathrm{ff}$$\wr$

$= \{\langle \mathtt{x}', \mathtt{y}\rangle \mid \exists \pi_0, \pi_1, \pi'_0, \pi'_1 \mathrel{.} \mathscr{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathtt{S}]\!]) = \mathrm{tt} \wedge \mathsf{at}[\![\mathtt{S}_t]\!]\pi_1\mathsf{after}[\![\mathtt{S}]\!] \in \widehat{\mathscr{S}}^{+\infty}[\![\mathtt{S}_t]\!](\pi_0\mathsf{at}[\![\mathtt{S}]\!] \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_t]\!]) \wedge \mathscr{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathtt{S}]\!]) = \mathrm{tt} \wedge \mathsf{at}[\![\mathtt{S}_t]\!]\pi'_1\mathsf{after}[\![\mathtt{S}]\!] \in \widehat{\mathscr{S}}^{+\infty}[\![\mathtt{S}_t]\!](\pi'_0\mathsf{at}[\![\mathtt{S}]\!] \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_t]\!]) \wedge (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}'\} \mathrel{.} \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathtt{S}]\!])\mathtt{z} = \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathtt{S}]\!])\mathtt{z}) \wedge (\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathtt{S}]\!] \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_t]\!]\pi_1\mathsf{after}[\![\mathtt{S}]\!])\mathtt{y} \neq \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathtt{S}]\!] \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_t]\!]\pi'_1\mathsf{after}[\![\mathtt{S}]\!])\mathtt{y})\}$ $\wr$def. $\in$$\wr$

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists \langle \pi_0 \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!], \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}_t]\!]\pi_2\rangle, \langle \pi'_0 \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!], \mathsf{at}[\![\mathsf{S}_t]\!]\pi'_1\mathsf{after}[\![\mathsf{S}_t]\!]\pi'_2\rangle \in \mathcal{S}^{+\infty}[\![\mathsf{S}_t]\!] \,.\, \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]) = \mathsf{tt} \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]) = \mathsf{tt} \wedge (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}'\} \,.\, \varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z}) \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \pi_1 \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \pi'_1 \wedge (\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\}$ ⦃$\mathsf{after}[\![\mathsf{S}]\!] = \mathsf{after}[\![\mathsf{S}_t]\!], \pi_2 = \pi'_2 = \ni$, def. (6.6) of ϱ⦄

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists \langle \pi_0 \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!], \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}_t]\!]\pi_2\rangle, \langle \pi'_0 \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!], \mathsf{at}[\![\mathsf{S}_t]\!]\pi'_1\mathsf{after}[\![\mathsf{S}_t]\!]\pi'_2\rangle \in \mathcal{S}^{+\infty}[\![\mathsf{S}_t]\!] \,.\, \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]) = \mathsf{tt} \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]) = \mathsf{tt} \wedge (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}'\} \,.\, \varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z}) \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \pi_1 \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \pi'_1 \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}_t]\!])(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!] \frown \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}_t]\!], \mathsf{after}[\![\mathsf{S}_t]\!]\pi_2), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}_t]\!])(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!] \frown \mathsf{at}[\![\mathsf{S}_t]\!]\pi'_1\mathsf{after}[\![\mathsf{S}_t]\!], \mathsf{after}[\![\mathsf{S}_t]\!]\pi'_2))\}$ ⦃def. (47.18) of diff and (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]$⦄

$\subseteq \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists \langle \bar\pi_0, \bar\pi_1\mathsf{after}[\![\mathsf{S}_t]\!]\pi_2\rangle, \langle \bar\pi_0{}', \bar\pi_1{}'\mathsf{after}[\![\mathsf{S}_t]\!]\pi'_2\rangle \in \mathcal{S}^{+\infty}[\![\mathsf{S}_t]\!] \,.\, \mathcal{B}[\![\mathsf{B}]\!]\varrho(\bar\pi_0) = \mathsf{tt} \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\bar\pi_0{}') = \mathsf{tt} \wedge (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}'\} \,.\, \varrho(\bar\pi_0)\mathsf{z} = \varrho(\bar\pi_0{}')\mathsf{z}) \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \bar\pi_1 \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \bar\pi_1{}' \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}_t]\!])(\bar\pi_0 \frown \bar\pi_1\mathsf{after}[\![\mathsf{S}_t]\!], \mathsf{after}[\![\mathsf{S}_t]\!]\pi_2), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}_t]\!])(\bar\pi_0{}' \frown \bar\pi_1{}'\mathsf{after}[\![\mathsf{S}_t]\!], \mathsf{after}[\![\mathsf{S}_t]\!]\pi'_2))\}$

⦃letting $\bar\pi_0 = \pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]$, $\bar\pi_1 = \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1$, $\bar\pi_0{}' = \pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]$, and $\bar\pi_1{}' = \mathsf{at}[\![\mathsf{S}_t]\!]\pi'_1$⦄

$\subseteq \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists \rho, \nu \,.\, \rho(\mathsf{x}') \neq \nu \wedge \mathcal{B}[\![\mathsf{B}]\!]\rho = \mathsf{tt} \wedge \mathcal{B}[\![\mathsf{B}]\!]\rho[\mathsf{x}' \leftarrow \nu] = \mathsf{tt}\} \cap \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists \langle \bar\pi_0, \bar\pi_1\mathsf{after}[\![\mathsf{S}_t]\!]\pi_2\rangle, \langle \bar\pi_0{}', \bar\pi_1{}'\mathsf{after}[\![\mathsf{S}_t]\!]\pi'_2\rangle \in \mathcal{S}^{+\infty}[\![\mathsf{S}_t]\!] \,.\, (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}'\} \,.\, \varrho(\bar\pi_0)\mathsf{z} = \varrho(\bar\pi_0{}')\mathsf{z}) \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \bar\pi_1 \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \bar\pi_1{}' \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}_t]\!])(\bar\pi_0 \frown \bar\pi_1\mathsf{after}[\![\mathsf{S}_t]\!], \mathsf{after}[\![\mathsf{S}_t]\!]\pi_2), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}_t]\!])(\bar\pi_0{}' \frown \bar\pi_1{}'\mathsf{after}[\![\mathsf{S}_t]\!], \mathsf{after}[\![\mathsf{S}_t]\!]\pi'_2))\}$

⦃letting $\rho = \varrho(\bar\pi_0)$ and $\nu = \varrho(\bar\pi_0{}')(\mathsf{x}')$⦄

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists \rho, \nu \,.\, \rho(\mathsf{x}') \neq \nu \wedge \mathcal{B}[\![\mathsf{B}]\!]\rho = \mathsf{tt} \wedge \mathcal{B}[\![\mathsf{B}]\!]\rho[\mathsf{x}' \leftarrow \nu] = \mathsf{tt}\} \cap \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \mathcal{S}^{+\infty}[\![\mathsf{S}_t]\!] \in \mathcal{D}(\mathsf{after}[\![\mathsf{S}_t]\!])\langle \mathsf{x}', \mathsf{y}\rangle\}$ ⦃def. (47.19) of $\mathcal{D}^{\ell}\langle \mathsf{x}', \mathsf{y}\rangle$⦄

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists \rho, \nu \,.\, \rho(\mathsf{x}') \neq \nu \wedge \mathcal{B}[\![\mathsf{B}]\!]\rho = \mathsf{tt} \wedge \mathcal{B}[\![\mathsf{B}]\!]\rho[\mathsf{x}' \leftarrow \nu] = \mathsf{tt}\} \cap \alpha^{\mathsf{d}}(\{\mathcal{S}^{+\infty}[\![\mathsf{S}_t]\!]\})\ \mathsf{after}[\![\mathsf{S}_t]\!]$

⦃def. $\subseteq$ and def. (47.25) of α^{d}⦄

In words for that second case, the initial value of x' flows to the value of y by the true branch of the conditional `if (B)` S_t when there are at least two different values of x' for which B is true and x' flows to the value of y in S_t.

$\subseteq \widehat{\mathcal{S}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_t]\!]\ \mathsf{after}[\![\mathsf{S}_t]\!] \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})$

⦃by structural ind. hyp. , def. (47.48) of nondet, and def. of the left restriction $\rceil$ of a relation in Section 2.2.2⦄

$\subseteq \widehat{\mathcal{S}}^{\exists}_{\text{diff}}[\![\mathsf{S}_t]\!]\ \mathsf{after}[\![\mathsf{S}_t]\!]$ $\quad\wr$A coarse over-approximation ignoring values$\wr$

— (2.c–d) — Otherwise, one execution is through the true branch (say $\pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!]$) and the other is through the false branch (say $\pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!]$), we have (the other case is symmetric),

(1)

$= \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!] \in \{\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathtt{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathsf{S}_t]\!](\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\} \mathrel{.} \exists \pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!] \in \{\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathtt{ff}\} \mathrel{.} (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \mathrel{.} \varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z}) \wedge (\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\}$

$\wr$case $\mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathtt{tt}$ and $\mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathtt{ff}\wr$

$= \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \pi_0, \pi_1, \pi'_0 \mathrel{.} \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathtt{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathsf{S}_t]\!](\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]) \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathtt{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \mathrel{.} \varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z}) \wedge (\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\}$ $\quad\wr$def. $\in\wr$

$= \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \bar{\pi}_0, \pi_1, \pi'_0 \mathrel{.} \mathcal{B}[\![\mathsf{B}]\!]\varrho(\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!]) = \mathtt{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathsf{S}_t]\!](\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!]) \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathtt{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \mathrel{.} \varrho(\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z}) \wedge (\varrho(\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{y}\}$

$\wr$letting $\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!] = \pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]$ so that by def. (6.6) of ϱ, $\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!]) = \varrho(\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!])$ so $\mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathcal{B}[\![\mathsf{B}]\!]\varrho(\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!])$ and $\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{y}\wr$

$= \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \bar{\pi}_0, \pi_1, \pi'_0 \mathrel{.} \mathcal{B}[\![\mathsf{B}]\!]\varrho(\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!]) = \mathtt{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathsf{S}_t]\!](\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!]) \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]) = \mathtt{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \mathrel{.} \varrho(\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z}) \wedge (\varrho(\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{y}\}$

$\wr$by def. (6.6) of ϱ so that $\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]) = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\wr$

$= \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \pi_0, \pi_1, \pi'_0 \mathrel{.} (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \mathrel{.} \varrho(\pi_0\mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z}) \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\mathsf{at}[\![\mathsf{S}_t]\!]) = \mathtt{tt} \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}_t]\!]) = \mathtt{ff} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathsf{S}_t]\!](\pi_0\mathsf{at}[\![\mathsf{S}_t]\!]) \wedge (\varrho(\pi_0\mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{y}\}$

$\wr$letting $\pi'_0\mathsf{at}[\![\mathsf{S}_t]\!] = \pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]$, commutativity of $\wedge\wr$

$= \{\langle \mathtt{x'},\ \mathtt{x'}\rangle \mid \exists \pi_0, \pi_1, \pi'_0 \ .\ (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x'}\} \ .\ \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{z} = \varrho(\pi'_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{z}) \wedge \mathscr{B}[\![\mathtt{B}]\!]\varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!]) = \mathsf{tt} \wedge \mathscr{B}[\![\mathtt{B}]\!]\varrho(\pi'_0 \mathsf{at}[\![\mathtt{S}_t]\!]) = \mathsf{ff} \wedge \mathsf{at}[\![\mathtt{S}_t]\!]\pi_1 \mathsf{after}[\![\mathtt{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathtt{S}_t]\!](\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!]) \wedge (\varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!]\pi_1 \mathsf{after}[\![\mathtt{S}]\!])\mathtt{x'} \neq \varrho(\pi'_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{x'}\}$
$\cup \{\langle \mathtt{x'},\ \mathtt{y}\rangle \mid \mathtt{x'} \neq \mathtt{y} \wedge \exists \pi_0, \pi_1, \pi'_0 \ .\ (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x'}\} \ .\ \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{z} = \varrho(\pi'_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{z}) \wedge \mathscr{B}[\![\mathtt{B}]\!]\varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!]) = \mathsf{tt} \wedge \mathscr{B}[\![\mathtt{B}]\!]\varrho(\pi'_0 \mathsf{at}[\![\mathtt{S}_t]\!]) = \mathsf{ff} \wedge \mathsf{at}[\![\mathtt{S}_t]\!]\pi_1 \mathsf{after}[\![\mathtt{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathtt{S}_t]\!](\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!]) \wedge (\varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!]\pi_1 \mathsf{after}[\![\mathtt{S}]\!])\mathtt{y} \neq \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{y}\}$

$\wr$since when $\mathtt{x'} \neq \mathtt{y}$, $\varrho(\pi'_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{y} = \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{y}$$\int$

In words for that third case, $\mathtt{x'}$ flows to $\mathtt{x'}$ if and only if changing $\mathtt{x'}$ changes the boolean expression $\mathtt{B}$ and when $\mathtt{B}$ is true, $\mathtt{S}_t$ changes $\mathtt{x'}$ to a value different from that when $\mathtt{B}$ is false. A counter-example is `if (x' != 1) x' = 1 ;`.

Moreover, $\mathtt{x'}$ flows to $\mathtt{y} \neq \mathtt{x'}$ if and only if changing $\mathtt{x'}$ changes the boolean expression $\mathtt{B}$ and when $\mathtt{B}$ is true, $\mathtt{S}_t$ changes $\mathtt{y}$.

$= \{\langle \mathtt{x'},\ \mathtt{y}\rangle \mid \exists \pi_0, \pi_1, \pi'_0 \ .\ (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x'}\} \ .\ \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{z} = \varrho(\pi'_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{z}) \wedge \mathscr{B}[\![\mathtt{B}]\!]\varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!]) = \mathsf{tt} \wedge \mathscr{B}[\![\mathtt{B}]\!]\varrho(\pi'_0 \mathsf{at}[\![\mathtt{S}_t]\!]) = \mathsf{ff} \wedge \mathsf{at}[\![\mathtt{S}_t]\!]\pi_1 \mathsf{after}[\![\mathtt{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathtt{S}_t]\!](\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!]) \wedge (\varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!]\pi_1 \mathsf{after}[\![\mathtt{S}]\!])\mathtt{y} \neq \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{y}\}$ $\wr$grouping cases together$\int$

$= \{\langle \mathtt{x'},\ \mathtt{y}\rangle \mid \exists \pi_0, \pi_1, \pi'_0 \ .\ (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x'}\} \ .\ \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{z} = \varrho(\pi'_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{z}) \wedge \mathscr{B}[\![\mathtt{B}]\!]\varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!]) = \mathsf{tt} \wedge \mathscr{B}[\![\mathtt{B}]\!]\varrho(\pi'_0 \mathsf{at}[\![\mathtt{S}_t]\!]) = \mathsf{ff} \wedge \mathsf{at}[\![\mathtt{S}_t]\!]\pi_1 \mathsf{after}[\![\mathtt{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathtt{S}_t]\!](\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!]) \wedge (\varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!]\pi_1 \mathsf{after}[\![\mathtt{S}]\!])\mathtt{y} \neq \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}_t]\!])\mathtt{y}\} \rceil \mathsf{nondet}(\mathtt{B}, \neg\mathtt{B})$

$\wr$letting $\rho = \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}]\!])$, $\nu = \varrho(\pi'_0 \mathsf{at}[\![\mathtt{S}]\!])\mathtt{x'}$ so that $\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x'}\} \ .\ \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}]\!])\mathtt{z} = \varrho(\pi'_0 \mathsf{at}[\![\mathtt{S}]\!])\mathtt{z}$ implies $\varrho(\pi'_0 \mathsf{at}[\![\mathtt{S}]\!]) = \rho[\mathtt{x'} \leftarrow \nu]$. It follows that $\exists \rho, \nu \ .\ \rho(\mathtt{x'}) \neq \nu \wedge \mathscr{B}[\![\mathtt{B}]\!]\rho = \mathsf{tt} \wedge \mathscr{B}[\![\mathtt{B}]\!]\rho[\mathtt{x'} \leftarrow \nu] = \mathsf{ff}$. Therefore, by def. (47.48) of nondet, $\mathtt{x'} \in \mathsf{nondet}(\mathtt{B}, \neg\mathtt{B})$$\int$

$\subseteq \{\langle \mathtt{x'},\ \mathtt{y}\rangle \mid \mathtt{x'} \in \mathsf{nondet}(\mathtt{B}, \neg\mathtt{B}) \wedge \mathtt{y} \in \mathsf{mod}[\![\mathtt{S}_t]\!]\}$

$\wr$Since $\{\mathtt{x} \mid \exists \pi_0, \pi_1 \ .\ \mathsf{at}[\![\mathtt{S}]\!]\pi_1 \mathsf{after}[\![\mathtt{S}]\!] \in \widehat{\mathcal{S}}^{*}[\![\mathtt{S}]\!](\pi_0 \mathsf{at}[\![\mathtt{S}]\!]) \wedge \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}]\!]\pi_1 \mathsf{after}[\![\mathtt{S}]\!])\mathtt{x} \neq \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}]\!])\mathtt{x}\} \subseteq \mathsf{mod}[\![\mathtt{S}]\!]$, a simple coarse approximation is to consider the variables $\mathtt{y}$ appearing to the left of an assignment in $\mathtt{S}_t$, a necessary condition for $\mathtt{y}$ to be modified by the execution of $\mathtt{S}_t$ where the set $\mathsf{mod}[\![\mathtt{S}]\!]$ of variables that may be modified by the execution of $\mathtt{S}$ is syntactically defined as in (47.50). $\int$

$= \mathsf{nondet}(\mathtt{B}, \neg\mathtt{B}) \times \mathsf{mod}[\![\mathtt{S}_t]\!]$ $\wr$def. cartesian product$\int$

$\subseteq \{\langle \mathtt{x'},\ \mathtt{y}\rangle \mid \mathtt{x'} \in \mathbb{vars}[\![\mathtt{B}]\!] \wedge \mathtt{y} \in \mathsf{mod}[\![\mathtt{S}_t]\!]\}$

$\wr$$\mathsf{nondet}(\mathtt{B}, \neg\mathtt{B})$ can be over-approximated by the set of variables $\mathtt{x'}$ occurring in the boolean expression $\mathtt{B}$ as defined in Exercise 3.3$\int$

Exercise 2 Prove that for all program components $\mathtt{S} \in \mathbb{P}\mathbb{c}$,

$$\{\mathtt{x} \mid \exists \pi_0, \pi_1 \ .\ \mathsf{at}[\![\mathtt{S}]\!]\pi_1 \mathsf{after}[\![\mathtt{S}]\!] \in \widehat{\mathcal{S}}^{+\infty}[\![\mathtt{S}]\!](\pi_0 \mathsf{at}[\![\mathtt{S}]\!]) \wedge \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}]\!]\pi_1 \mathsf{after}[\![\mathtt{S}]\!])\mathtt{x} \neq \varrho(\pi_0 \mathsf{at}[\![\mathtt{S}]\!])\mathtt{x}\} \subseteq \mathsf{mod}[\![\mathtt{S}]\!]. \qquad \square$$

— (3) — Finally, assume $\ell \in \mathsf{in}[\![\mathsf{S}_t]\!]$.

$\alpha^{\mathrm{d}}(\{\mathcal{S}^*[\![\mathsf{S}]\!]\})\,\ell$

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \mathcal{S}^*[\![\mathsf{S}]\!] \in \mathcal{D}^\ell\langle \mathsf{x}', \mathsf{y}\rangle\}$ $\wr$def. (47.25) of $\alpha^{\mathrm{d}}\wr$

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists\langle\pi_0, \pi_1\rangle, \langle\pi'_0, \pi'_1\rangle \in \mathcal{S}^*[\![\mathsf{S}]\!] \;.\; (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}'\} \;.\; \varrho(\pi_0)\mathsf{z} = \varrho(\pi'_0)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\pi_0, \pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\pi'_0, \pi'_1))\}$ $\wr$def. (47.19) of $\mathcal{D}^\ell\langle \mathsf{x}', \mathsf{y}\rangle\wr$

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists\langle\pi_0, \pi_1\rangle, \langle\pi'_0, \pi'_1\rangle \in \{\langle\pi\mathsf{at}[\![\mathsf{S}]\!], \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\ell\pi''\rangle \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\ell\pi'' \in \widehat{\mathcal{S}}^*[\![\mathsf{S}_t]\!](\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\} \;.\; (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}'\} \;.\; \varrho(\pi_0)\mathsf{z} = \varrho(\pi'_0)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\pi_0, \pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\pi'_0, \pi'_1))\}$ $\wr$def. (6.19) of $\mathcal{S}^*[\![\mathsf{S}]\!]\wr$

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists\langle\pi_0, \pi_1\rangle, \langle\pi'_0, \pi'_1\rangle \in \{\langle\pi\mathsf{at}[\![\mathsf{S}]\!], \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\ell\pi''\rangle \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\ell\pi'' \in \widehat{\mathcal{S}}^*[\![\mathsf{S}_t]\!](\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\} \;.\; (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}'\} \;.\; \varrho(\pi_0)\mathsf{z} = \varrho(\pi'_0)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\pi_0, \pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\pi'_0, \pi'_1))\}$

$\wr$since if $\langle\pi_0, \pi_1\rangle$ (or $\langle\pi'_0, \pi'_1\rangle$) has the form $\langle\pi\mathsf{at}[\![\mathsf{S}]\!], \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle$ then ℓ does not appear in π_1 (resp. π'_1) so that, by (47.16), $\mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\pi_0, \pi_1) = \ni$ (resp. $\mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\pi'_0, \pi'_1) = \ni$ and therefore, by (47.18), $\mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\ell)(\pi_0, \pi_1), \mathsf{seqval}[\![\mathsf{y}]\!](\ell)(\pi'_0, \pi'_1))$ is false$\wr$

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists\pi_0, \pi_1, \pi_2, \pi'_0, \pi'_1, \pi'_2 \;.\; \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\ell\pi_2 \in \widehat{\mathcal{S}}^*[\![\mathsf{S}_t]\!](\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\} \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'_1\ell\pi'_2 \in \widehat{\mathcal{S}}^*[\![\mathsf{S}_t]\!](\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]) \wedge (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}'\} \;.\; \varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z}) \wedge \ell \notin \pi_1 \wedge \ell \notin \pi'_1 \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\ell, \ell\pi_2), \mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'_1\ell, \ell\pi'_2))\}$

$\wr$def. $\in$ and if ℓ has multiple occurrences in $\pi'_1\ell\pi'_2$, we choose the first one, same for $\pi'_1\ell\pi'_2\wr$

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists\bar{\pi}_0, \pi_1, \pi_2, \bar{\pi}_0', \pi'_1, \pi'_2 \;.\; \mathcal{B}[\![\mathsf{B}]\!]\varrho(\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!]) = \mathsf{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\ell\pi_2 \in \widehat{\mathcal{S}}^*[\![\mathsf{S}_t]\!](\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!])\} \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\bar{\pi}_0'\mathsf{at}[\![\mathsf{S}_t]\!]) = \mathsf{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'_1\ell\pi'_2 \in \widehat{\mathcal{S}}^*[\![\mathsf{S}_t]\!](\bar{\pi}_0'\mathsf{at}[\![\mathsf{S}_t]\!]) \wedge (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}'\} \;.\; \varrho(\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z} = \varrho(\bar{\pi}_0'\mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z}) \wedge \ell \notin \pi_1 \wedge \ell \notin \pi'_1 \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\ell, \ell\pi_2), \mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\bar{\pi}_0'\mathsf{at}[\![\mathsf{S}_t]\!]\pi'_1\ell, \ell\pi'_2))\}$

$\wr$letting $\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!] = \pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]$, $\bar{\pi}_0'\mathsf{at}[\![\mathsf{S}_t]\!] = \pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]$ so that by def. (6.6) of ϱ, $\varrho(\bar{\pi}_0\mathsf{at}[\![\mathsf{S}_t]\!]) = \varrho(\pi_0\mathsf{at}[\![\mathsf{S}]\!])$ and $\varrho(\bar{\pi}_0'\mathsf{at}[\![\mathsf{S}_t]\!]) = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\wr$

$\subseteq \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists\pi_0, \pi'_0 \;.\; \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\mathsf{at}[\![\mathsf{S}_t]\!]) = \mathsf{tt} \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}_t]\!]) = \mathsf{tt} \wedge (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}'\} \;.\; \varrho(\pi_0\mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z} = \varrho(\pi_0'\mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z})\} \cap \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists\pi_0, \pi_1, \pi_2, \pi'_0, \pi'_1, \pi'_2 \;.\; \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\ell\pi_2 \in \widehat{\mathcal{S}}^*[\![\mathsf{S}_t]\!](\pi_0\mathsf{at}[\![\mathsf{S}_t]\!]) \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'_1\ell\pi'_2 \in \widehat{\mathcal{S}}^*[\![\mathsf{S}_t]\!](\pi'_0\mathsf{at}[\![\mathsf{S}_t]\!]) \wedge (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}'\} \;.\; \varrho(\pi_0\mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z} = \varrho(\pi_0'\mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z}) \wedge \ell \notin \pi_1 \wedge \ell \notin \pi'_1 \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\pi_0\mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\ell, \ell\pi_2), \mathsf{seqval}[\![\mathsf{y}]\!]^\ell(\pi_0'\mathsf{at}[\![\mathsf{S}_t]\!]\pi'_1\ell, \ell\pi'_2))\}$ $\wr$def. $\exists$ and $\subseteq\wr$

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists\rho, \nu \;.\; \rho(\mathsf{x}') \neq \nu \wedge \mathcal{B}[\![\mathsf{B}]\!]\rho = \mathsf{tt} \wedge \mathcal{B}[\![\mathsf{B}]\!]\rho[\mathsf{x}' \leftarrow \nu] = \mathsf{tt}\} \cap \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \mathcal{S}^*[\![\mathsf{S}_t]\!] \in \mathcal{D}(\ell)\langle \mathsf{x}', \mathsf{y}\rangle\}$ $\wr$letting $\rho = \varrho(\bar{\pi}_0)$, $\nu = \varrho(\bar{\pi}_0')(\mathsf{x}')$ and def. (47.19) of $\mathcal{D}^\ell\langle \mathsf{x}', \mathsf{y}\rangle\wr$

$= \{\langle \mathtt{x}', \mathtt{y}\rangle \mid \exists \rho, \nu \,.\, \rho(\mathtt{x}') \neq \nu \wedge \mathscr{B}[\![\mathtt{B}]\!]\rho = \mathrm{tt} \wedge \mathscr{B}[\![\mathtt{B}]\!]\rho[\mathtt{x}' \leftarrow \nu] = \mathrm{tt}\} \cap \{\langle \mathtt{x}', \mathtt{y}\rangle \mid \{\mathcal{S}^*[\![\mathtt{S}_t]\!]\} \subseteq \mathcal{D}(\ell)\langle \mathtt{x}', \mathtt{y}\rangle\}$ $\wr$def. $\subseteq\int$

$= \{\langle \mathtt{x}', \mathtt{y}\rangle \mid \exists \rho, \nu \,.\, \rho(\mathtt{x}') \neq \nu \wedge \mathscr{B}[\![\mathtt{B}]\!]\rho = \mathrm{tt} \wedge \mathscr{B}[\![\mathtt{B}]\!]\rho[\mathtt{x}' \leftarrow \nu] = \mathrm{tt}\} \cap \alpha^{\mathrm{d}}(\{\mathcal{S}^*[\![\mathtt{S}_t]\!]\})\,\ell$

$\wr$def. (47.25) of $\alpha^{\mathrm{d}}\int$

$\subseteq \{\langle \mathtt{x}', \mathtt{y}\rangle \mid \exists \rho, \nu \,.\, \rho(\mathtt{x}') \neq \nu \wedge \mathscr{B}[\![\mathtt{B}]\!]\rho = \mathrm{tt} \wedge \mathscr{B}[\![\mathtt{B}]\!]\rho[\mathtt{x}' \leftarrow \nu] = \mathrm{tt}\} \cap \mathcal{S}^{\mathrm{d}}[\![\mathtt{S}_t]\!]\,\ell$

$\wr$structural induction hypothesis$\int$

$= \mathcal{S}^{\mathrm{d}}[\![\mathtt{S}_t]\!]\,\ell \rceil \mathsf{nondet}(\mathtt{B}, \mathtt{B})$ $\wr$def. (47.48) of $\mathsf{nondet}\int$

In words, the initial value of $\mathtt{x}'$ flows to the value of $\mathtt{y}$ at ℓ in the true branch $\mathtt{S}_t$ of the conditional $\mathtt{if}$ $\mathtt{(B)}$ $\mathtt{S}_t$ when there are at least two different values of $\mathtt{x}'$ for which $\mathtt{B}$ is true and $\mathtt{x}'$ flows to the value of $\mathtt{y}$ at ℓ in $\mathtt{S}_t$.

$\subseteq \mathcal{S}^{\mathrm{d}}[\![\mathtt{S}_t]\!]\,\ell$

$\wr$A coarse over-approximation ignoring values *i.e.* that the conditional holds for only one value of $\mathtt{x}'\int$ □

Proof of (47.65) By Lemma 47.23, the Definition 47.28 of value dependency using the maximal traces semantics is equivalent to the definition of value dependency for finite prefix traces, as defined by (17.4). So the soundness of (47.65) follows from the following (3):

$$\left[\begin{array}{lcll} & \alpha^{\mathrm{d}}(\mathcal{S}^*[\![\mathtt{S}]\!]) & = & \alpha^{\mathrm{d}}(\mathsf{lfp}^{\subseteq}\, \mathcal{F}^*[\![\mathtt{while}\,\ell\,\mathtt{(B)}\,\mathtt{S}_b]\!]) \\ \dot{\subseteq} & \mathsf{lfp}^{\dot{\subseteq}}\, \mathcal{F}^{\mathrm{diff}}[\![\mathtt{while}\,\ell\,\mathtt{(B)}\,\mathtt{S}_b]\!] & = & \widehat{\mathcal{S}}^{\exists}_{\mathrm{diff}}[\![\mathtt{S}]\!] \end{array}\right. \tag{3}$$

The proof of (3) is an application of Exercise 18.15. $\langle C, \sqsubseteq, \bot, \sqcup\rangle$ is the complete lattice $\langle \wp(\wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})), \subseteq, \emptyset, \cup\rangle$. $\langle \mathcal{A}, \preccurlyeq, 0, \curlyvee\rangle$ is the complete lattice $\langle \mathbb{P}^{\mathrm{d}}, \subseteq^{\mathrm{d}}, \bot^{\mathrm{d}}, \cup^{\mathrm{d}}\rangle$. The Galois connection $\langle C, \sqsubseteq\rangle \xleftarrow[\alpha]{\gamma} \langle \mathcal{A}, \preccurlyeq\rangle$ is given by Lemma 47.26. The transformer f is (17.4). It preserves arbitrary non-empty unions so it is continuous. The transformer g is (47.65). It preserves arbitrary non-empty unions pointwise so it is pointwise continuous (*i.e.* for $\subseteq^{\mathrm{d}}$ and $\cup^{\mathrm{d}}$ defined pointwise). The main point of the proof is to check the semi-commutation condition

$$\alpha^{\mathrm{d}} \circ \mathcal{F}^*[\![\mathtt{while}\,\ell\,\mathtt{(B)}\,\mathtt{S}_b]\!] \quad \dot{\subseteq} \quad \mathcal{F}^{\mathrm{diff}}[\![\mathtt{while}\,\ell\,\mathtt{(B)}\,\mathtt{S}_b]\!] \circ \alpha^{\mathrm{d}}\,. \tag{4}$$

By Exercise 18.15, we need to make the proof only for elements $X \in \mathcal{X}$ where $\mathcal{X}$ is chosen to be exactly the iterates of the transformer $\mathcal{F}^*[\![\mathtt{while}\,\ell\,\mathtt{(B)}\,\mathtt{S}_b]\!]$ from $\emptyset$.

In practice, we have discovered $\mathcal{F}^{\mathrm{diff}}[\![\mathtt{while}\,\ell\,\mathtt{(B)}\,\mathtt{S}_b]\!]$ knowing $\mathcal{F}^*[\![\mathtt{while}\,\ell\,\mathtt{(B)}\,\mathtt{S}_b]\!]$ and α^{d} by rewriting until getting a formula of the form $\mathcal{F}^{\mathrm{diff}}[\![\mathtt{while}\,\ell\,\mathtt{(B)}\,\mathtt{S}_b]\!] \circ \alpha^{\mathrm{d}}$ and using $\dot{\subseteq}$-over-approximations to ignore values in the static analysis. By Exercise 18.15, we conclude that

$$\alpha^{\mathrm{d}}(\mathsf{lfp}^{\subseteq}\, \mathcal{F}^*[\![\mathtt{while}\,\ell\,\mathtt{(B)}\,\mathtt{S}_b]\!]) \mathrel{\dot{\subseteq}} \mathsf{lfp}^{\dot{\subseteq}}\, \mathcal{F}^{\mathrm{diff}}[\![\mathtt{while}\,\ell\,\mathtt{(B)}\,\mathtt{S}_b]\!]\,.$$

The proof of semi-commutation (4) is by calculational design as follows. By def. (47.18) of diff, we do not have to compare futures of prefix traces where one is a prefix of the other.

$$\begin{aligned}
&\alpha^{\mathrm{d}}(\{\mathcal{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\ X\})\,\ell' \\
=\ &\{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \mathcal{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\ X \in \mathcal{D}(\ell')\langle \mathtt{x},\ \mathtt{y}\rangle\} && \text{(def. (47.25) of } \alpha^{\mathrm{d}}\text{)} \\
=\ &\{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \exists\langle \pi_0,\ \pi_1\rangle, \langle \pi'_0,\ \pi'_1\rangle \in \mathcal{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\ X\ .\ (\forall \mathtt{z} \in \mathbb{V}\setminus\{\mathtt{x}\}\ .\ \varrho(\pi_0)\mathtt{z} = \varrho(\pi'_0)\mathtt{z}) \wedge \\
&\mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0,\pi_1), \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi'_0,\pi'_1))\} && \text{(def. (47.19) of } \mathcal{D}\ell\langle \mathtt{x},\ \mathtt{y}\rangle\text{)} \\
=\ &\{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_1\rangle, \langle \pi'_0\ell,\ \ell\pi'_1\rangle \in \mathcal{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\ X\ .\ (\forall \mathtt{z} \in \mathbb{V}\setminus\{\mathtt{x}\}\ . && (5) \\
&\varrho(\pi_0\ell)\mathtt{z} = \varrho(\pi'_0\ell)\mathtt{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell,\ell\pi_1), \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi'_0\ell,\ell\pi'_1))\} \\
&\qquad \text{(since } \langle \pi_0\ell',\ \ell''\pi_1\rangle \notin \mathcal{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!](X) \text{ when } \ell' \neq \ell \text{ or } \ell'' \neq \ell\text{)}
\end{aligned}$$

There are three main cases depending on whether the dependency observation point ℓ' is **(1)** at the iteration (so $\ell' = \ell = \mathsf{at}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]$), **(2)** is in the loop body (so $\ell' \in \mathsf{in}[\![\texttt{S}_b]\!]$), or **(3)** is after the iteration (so $\ell' = \mathsf{after}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]$).

For each of these case, we have to consider all possible ways the traces $\ell\pi_1$ and $\ell\pi'_1$ in (5) can go through the dependency observation program point ℓ'. The definition of $\mathcal{F}^*$ below shows all possible choices **(A)**, **(B)**, or **(C)** of $\ell\pi_1$ and $\ell\pi'_1$ in (5). Notice that diff in (47.16) is commutative so $\langle \pi_0\ell,\ \ell\pi_1\rangle$ and $\langle \pi'_0\ell,\ \ell\pi'_1\rangle$ play symmetric rôles in (5) which reduces the number of cases to be considered.

$$\begin{aligned}
\mathcal{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!](X) \ \triangleq\ &\{\langle \pi_0\ell,\ \ell\rangle\} && \textbf{(A)} \qquad (17.4) \\
\cup\, \{\langle \pi_0\ell,\ &\ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\texttt{S}_b]\!]\pi_3\ell''\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{tt} && \textbf{(B)} \\
&\wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\texttt{S}_b]\!],\ \mathsf{at}[\![\texttt{S}_b]\!]\pi_3\ell''\rangle \in \mathcal{S}^*[\![\texttt{S}_b]\!]\} \\
\cup\, \{\langle \pi_0\ell,\ &\ell\pi_2\ell \xrightarrow{\neg(\mathtt{B})} \mathsf{after}[\![\texttt{S}]\!]\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{ff}\} && \textbf{(C)}
\end{aligned}$$

The case **(B)** covers essentially 3 subcases depending of where is ℓ'' that is where the prefix observation $\mathsf{at}[\![\texttt{S}_b]\!]\pi_3\ell''$ of the execution of the body $\texttt{S}_b$ has terminated:

(Ba) within the loop body $\ell'' \in \mathsf{in}[\![\texttt{S}_b]\!]$;

(Bb) after the loop body $\ell'' = \mathsf{after}[\![\texttt{S}_b]\!] = \mathsf{at}[\![\texttt{S}]\!] = \ell$, because of the normal termination of the loop body, and thus at ℓ, just before the next iteration or the loop exit;

(Bc) after the loop $\ell'' = \mathsf{after}[\![\texttt{S}]\!]$ because of a **`break ;`** statement in the loop body $\texttt{S}_b$;

—— **(1)** If the dependency observation point ℓ' is at loop entry then $\ell' = \ell = \mathsf{at}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]$. There are three subcases, depending on how $\ell' = \ell$ is reached $\ell\pi_1$ by **(A)**, **(B)**, or **(C)** of $\ell\pi_1$ and $\ell\pi'_1$ in (5).

— **(1–A)** In the first case $\ell\pi_1 = \ell$ so $\pi_1 = \ni$ in **(A)**. We have $\mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell,\ell) = \varrho(\pi_0\ell)\mathtt{y}$ by (47.16). Whether $\ell\pi'_1$ is determined by **(A)**, **(B)**, or **(C)** we have in all cases that $\mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi'_0\ell,\ell\pi'_1) = \varrho(\pi'_0\ell) \mathbin{\hat{\cdot}} \sigma$ where σ is a possibly empty sequence of values of $\mathtt{y}$ at $\ell' = \ell$. By def. (47.18) of diff, we don't care about σ since $\mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_1))$ is true if and only if $\varrho(\pi_0\ell)\mathtt{y} \neq \varrho(\pi'_0\ell)$. In that case, we have

$$
\begin{aligned}
& (5) \\
= \;& \{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \exists\langle\pi_0\ell,\ \ell\pi_1\rangle, \langle\pi'_0\ell,\ \ell\pi'_1\rangle \in \mathcal{F}^*[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b]\!]\, X \;.\; (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}\} \;.\; \varrho(\pi_0\ell)\mathtt{z} = \varrho(\pi'_0\ell)\mathtt{z}) \wedge \varrho(\pi_0\ell)\mathtt{y} \neq \varrho(\pi_0\ell)\mathtt{y}\} \\
\subseteq \;& \{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \exists\pi_0\ell, \pi'_0\ell \;.\; (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}\} \;.\; \varrho(\pi_0\ell)\mathtt{z} = \varrho(\pi'_0\ell)\mathtt{z}) \wedge (\varrho(\pi_0\ell)\mathtt{y} \neq \varrho(\pi'_0\ell)\mathtt{y})\} && \text{(def. } \subseteq\text{)} \\
= \;& \{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \exists\rho, \nu \;.\; \rho(\mathtt{y}) \neq \rho[\mathtt{x} \leftarrow \nu](\mathtt{y})\} \\
& && \text{(letting } \rho = \varrho(\pi_0\ell), \rho[\mathtt{x} \leftarrow \nu] = \varrho(\pi'_0\ell) \text{ and Exercise 6.8)} \\
= \;& \{\langle \mathtt{x},\ \mathtt{x}\rangle \mid \mathtt{x} \in \mathbb{V}\} && \text{(def. (19.10) of the environment assignment)} \\
= \;& \mathbb{1}_{\mathbb{V}} && \text{(def. identity relation on the set } \mathbb{V} \text{ of variables in Section 2.2.2)}
\end{aligned}
$$

— **(1–Ba/Bc/C)** In this second case the trace $\ell\pi_1$ corresponds to one or more iterations of the loop followed by an execution of the loop body or a loop exit.

– In case **(Ba)**, we have

$$
\begin{aligned}
& \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_1) \\
= \;& \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell'') \text{ where } \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathtt{tt} \wedge \\
& \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!],\ \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell''\rangle \in \mathcal{S}^*[\![\mathtt{S}_b]\!] && \text{((B) with } \ell'' \in \mathsf{in}[\![\mathtt{S}_b]\!]\text{)} \\
= \;& \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell) \text{ where } \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathtt{tt}
\end{aligned}
$$

(def. (47.16) of $\mathsf{seqval}[\![\mathtt{y}]\!]$ since $\langle\pi_0\ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!],\ \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell''\rangle \in \mathcal{S}^*[\![\mathtt{S}_b]\!]$ with $\ell'' \in \mathsf{in}[\![\mathtt{S}_b]\!]$ so that ℓ cannot appear in the trace $\mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell''$)

– In case **(Bc)**, we have

$$
\begin{aligned}
& \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_1) \\
= \;& \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{break\text{-}to}[\![\mathtt{S}]\!]) \text{ where } \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in \\
& X \wedge \mathcal{B}[\![\mathtt{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathtt{tt} \wedge \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!],\ \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{break\text{-}to}[\![\mathtt{S}]\!]\rangle \in \mathcal{S}^*[\![\mathtt{S}_b]\!] \\
& && \text{((B) with } \ell'' \in \mathsf{breaks\text{-}of}[\![\mathtt{S}]\!] \text{ and } \mathsf{break\text{-}to}[\![\mathtt{S}]\!] = \mathsf{after}[\![\mathtt{S}]\!]\text{)} \\
= \;& \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell) \text{ where } \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathtt{tt}
\end{aligned}
$$

(def. (47.16) of $\mathsf{seqval}[\![\mathtt{y}]\!]$ since $\langle\pi_0\ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!],\ \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{break\text{-}to}[\![\mathtt{S}]\!]\rangle \in \mathcal{S}^*[\![\mathtt{S}_b]\!]$ so that ℓ cannot appear in the trace $\mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{break\text{-}to}[\![\mathtt{S}]\!]$)

– In case **(C)**, we have

$$\mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_1)$$

$= \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])$ where $\langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathsf{ff}$ $\quad$ $\wr$(C)$\wr$

$= \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell)$ where $\langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathsf{ff}$ $\quad$ $\wr$def. (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]$$\wr$

In all of these cases, the future observation $\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_1)$ is the same so we can handle all cases (1–Ba/Bc/C) as follows:

(5)

$= \{\langle\mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle\pi_0\ell,\ \ell\pi_1\rangle, \langle\pi'_0\ell,\ \ell\pi'_1\rangle \in \mathscr{F}^*[\![\mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b]\!]\ X\ .\ (\forall\mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_1))\}$

$\subseteq \{\langle\mathsf{x}, \mathsf{y}\rangle \mid \exists\langle\pi_0\ell, \ell\pi_2\ell\rangle \in X\ .\ \exists\langle\pi'_0\ell,\ \ell\pi'_1\rangle \in \mathscr{F}^*[\![\mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b]\!]X\ .\ (\forall\mathsf{z} \in \mathbb{V}\setminus\{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_1))\}$ (6)

$\wr$abstracting away the value of the conditions$\wr$

The possible choices for $\langle\pi'_0\ell,\ \ell\pi'_1\rangle \in \mathscr{F}^*[\![\mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b]\!]\ X$ are given by **(A)**, **(B)**, and **(C)** and are considered below.

– **(1–Ba/Bc/C–A)** This case is the symmetric of **(1–A)**, and so has already bean considered.

– **(1–Ba/Bc/C–Ba/Bc/C)** In this case the above reasoning that we have done in **(1–Ba/Bc/C)** for the first trace $\ell\pi_1$ is also valid for the second trace $\ell\pi'_1$, and so we get

(6)

$= \{\langle\mathsf{x}, \mathsf{y}\rangle \mid \exists\langle\pi_0\ell, \ell\pi_2\ell\rangle \in X\ .\ \exists\langle\pi'_0\ell,\ \ell\pi'_1\rangle \in \mathscr{F}^*[\![\mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b]\!]X\ .\ (\forall\mathsf{z} \in \mathbb{V}\setminus\{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_1))\}$

$\subseteq \{\langle\mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X\ .\ \exists\langle\pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X\ .\ (\forall\mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_2\ell))\}$

$\wr$abstracting away the value of the conditions$\wr$

$\subseteq \{\langle\mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle\pi_0,\ \pi_1\rangle, \langle\pi'_0,\ \pi'_1\rangle \in X\ .\ (\forall\mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0)\mathsf{z} = \varrho(\pi'_0)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0, \pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0, \pi'_1))\}$

$\wr$letting $\pi_0 \leftarrow \pi_0\ell, \pi_1 \leftarrow \ell\pi_2\ell, \pi'_0 \leftarrow \pi'_0\ell, \pi'_1 \leftarrow \ell\pi'_2\ell$, and $\ell' = \ell$ in case **(1)**$\wr$

$= \{\langle\mathsf{x},\ \mathsf{y}\rangle \mid X \in \{\Pi \in \wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty}) \mid \exists\langle\pi_0,\ \pi_1\rangle, \langle\pi'_0,\ \pi'_1\rangle \in \Pi\ .\ (\forall\mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0)\mathsf{z} = \varrho(\pi'_0)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0, \pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0, \pi'_1))\}\}$ $\quad$ $\wr$def. $\in$$\wr$

$= \{\langle\mathsf{x},\ \mathsf{y}\rangle \mid X \in \mathcal{D}^\ell\langle\mathsf{x},\ \mathsf{y}\rangle\}$ $\quad$ $\wr$def. (47.19) of $\mathcal{D}^\ell\langle\mathsf{x}',\ \mathsf{y}\rangle$$\wr$

$= \alpha^{\mathrm{d}}(\{X\})\ell$ $\quad$ $\wr$def. (47.25) of α^{d} $\wr$

– **(1–Ba/Bc/C–Bb)** In this case we are in case **(1–Ba/Bc/C)** for the first prefix observation trace $\ell\pi_1$ corresponding to one or more iterations of the loop followed by an execution of the loop body or a loop exit and in case **Bb** for the second trace $\ell\pi'_1$ so that, after zero or more executions, the loop body has terminated normally at $\ell'' = \mathsf{after}[\![\mathsf{S}_b]\!] = \mathsf{at}[\![\mathsf{S}]\!] = \ell$ and the prefix observation stops there, just before the next iteration or the loop exit. We have

$$
\begin{aligned}
&(6)\\
= \;& \{\langle \mathsf{x},\, \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\, \ell\pi_2\ell\rangle \in X \,.\, \exists\langle \pi'_0\ell,\, \ell\pi'_1\rangle \in \mathcal{F}^*[\![\texttt{while}\,\ell\,\texttt{(B)}\;\texttt{S}_b]\!]X \,.\, (\forall \mathsf{z} \in \mathbb{V}\setminus\{\mathsf{x}\} \,.\, \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \\
& \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_1))\}\\
& \hfill \text{\textlbrackdbl case (1) so } \ell' = \ell = \mathsf{at}[\![\texttt{while}\,\ell\,\texttt{(B)}\;\texttt{S}_b]\!] \text{\textrbrackdbl}\\
= \;& \{\langle \mathsf{x},\, \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\, \ell\pi_2\ell\rangle \in X \,.\, \exists\langle \pi'_0\ell,\, \ell\pi'_1\rangle \in \{\langle \pi'_0\ell,\, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \mid \langle \pi'_0\ell,\, \ell\pi'_2\ell\rangle \in X \wedge \\
& \mathcal{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi'_0\ell\pi'_2\ell) = \mathsf{tt} \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge \ell'' = \mathsf{after}[\![\mathsf{S}_b]\!] = \mathsf{at}[\![\mathsf{S}]\!] = \\
& \ell\} \,.\, (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \,.\, \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_1))\}\\
& \hfill \text{\textlbrackdbl case (Bb) for } \ell\pi'_1 \text{\textrbrackdbl}\\
= \;& \{\langle \mathsf{x},\, \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\, \ell\pi_2\ell\rangle \in X \,.\, \exists\langle \pi'_0\ell,\, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \,.\, \langle \pi'_0\ell,\, \ell\pi'_2\ell\rangle \in X \wedge \\
& \mathcal{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi'_0\ell\pi'_2\ell) = \mathsf{tt} \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \,.\\
& \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell))\}\\
& \hfill \text{\textlbrackdbl def. } \in \text{ and } \ell'' = \ell \text{\textrbrackdbl}\\
= \;& \{\langle \mathsf{x},\, \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\, \ell\pi_2\ell\rangle \in X \,.\, \exists\langle \pi'_0\ell,\, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \,.\, \langle \pi'_0\ell,\, \ell\pi'_2\ell\rangle \in X \wedge \\
& \mathcal{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi'_0\ell\pi'_2\ell) = \mathsf{tt} \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \,.\\
& \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_2\ell))\}\\
& \cup\\
& \{\langle \mathsf{x},\, \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\, \ell\pi_2\ell\rangle \in X \,.\, \exists\langle \pi'_0\ell,\, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \,.\, \langle \pi'_0\ell,\, \ell\pi'_2\ell\rangle \in X \wedge \\
& \mathcal{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi'_0\ell\pi'_2\ell) = \mathsf{tt} \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \,.\\
& \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell))\}
\end{aligned}
$$

(By def. (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]$ and (47.18) of diff, there is an instant of ℓ in $\ell\pi_2\ell$ and one in $\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell$ where the values of y while being the same before. So there are two possible cases whether this ℓ is in $\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]$ or in $\mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell$. So we have $\mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell)) = \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_2\ell)) \vee \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell))$)

$$
\begin{aligned}
\subseteq \;& \{\langle \mathsf{x},\, \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\, \ell\pi_2\ell\rangle \in X \,.\, \exists\langle \pi'_0\ell,\, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \,.\, \langle \pi'_0\ell,\, \ell\pi'_2\ell\rangle \in X \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \,.\\
& \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_2\ell))\}\\
& \cup
\end{aligned}
$$

$$\{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle\ .\ \langle \pi_0\ell,\ \ell\pi''_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi''_2\ell) = \mathtt{tt} \wedge \langle \pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge \exists \langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle\ .\ \langle \pi'_0\ell, \ell\pi'_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell\pi'_2\ell) = \mathtt{tt} \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi''_3\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell))\}$$

≀for the second term, we are in the case $\langle \pi_0\ell, \ell\pi_2\ell\rangle \in X$ with $\ell\pi_2\ell = \ell\pi_1$ corresponding to one or more iterations of the loop (so $\ell\pi_2\ell \neq \ell$ since otherwise we would be in case (**1–A**)), X is an iterate of $\mathcal{F}^*[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathsf{S}_b]\!]$, and so, by (17.4), can be written in the form $\ell\pi_2\ell = \ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi''_3\ell$ (where $\ell\pi''_2\ell$ may be reduced to ℓ for the first iteration) with $\ell\pi''_2\ell \in X$, $\mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi''_2\ell) = \mathtt{tt}$ and $\langle \pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]$. Moreover if the difference on y is in $\ell\pi''_2\ell$, the case is covered by the first term.≀ (7)

$$\subseteq \alpha^{\mathrm{d}}(\{X\})\ell \cup \{\langle \mathsf{x}, \mathsf{y}\rangle \mid \exists \langle \pi_0\ell, \ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle\ .\ \langle \pi_0\ell, \ell\pi''_2\ell\rangle \in X \wedge \langle \pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \{\langle \pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi)\} \wedge \exists \langle \pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle\ .\ \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \{\langle \pi, \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi)\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi''_3\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell))\}$$

≀since $\varrho(\pi) = \varrho(\pi \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!])$≀

$$= \alpha^{\mathrm{d}}(\{X\})\ell \cup \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle\ .\ \langle \pi_0\ell,\ \ell\pi''_2\ell\rangle \in X \wedge \langle \pi_0\ell\pi''_2\ell, \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \{\langle \pi_0\ell,\ \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi\rangle \mid \langle \pi_0\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi\rangle \in \{\langle \pi, \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi)\}\} \wedge \exists \langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle\ .\ \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \langle \pi'_0\ell\pi'_2\ell, \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \{\langle \pi_0\ell,\ \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi\rangle \mid \langle \pi_0\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi\rangle \in \{\langle \pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi)\}\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell\pi''_2\ell, \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi''_3\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell\pi'_2\ell, \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell))\}$$

≀def. $\in$, def. (47.18) of diff, and def. (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]$ with $\ell \neq \mathsf{at}[\![\mathsf{S}_b]\!]$ ≀

$$\subseteq \alpha^{\mathrm{d}}(\{X\})\ell \cup \{\langle \mathsf{x}, \mathsf{y}\rangle \mid \exists \pi_0\ell_0\pi_1\ell'\pi_2\ell\pi_3, \pi'_0\ell_0\pi'_1\ell'\pi'_2\ell\pi'_3\ .\ \langle \pi_0\ell_0, \ell_0\pi_1\ell'\rangle \in X \wedge \langle \pi_0\ell_0\pi_1\ell', \ell'\pi_2\ell\pi_3\rangle \in \{\langle \pi_0\ell,\ \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi\rangle \mid \langle \pi_0\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi\rangle \in \{\langle \pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi)\}\} \wedge \langle \pi'_0\ell_0,\ \ell_0\pi'_1\ell'\rangle \in X \wedge \langle \pi'_0\ell_0\pi'_1\ell',\ \ell'\pi'_2\ell\pi'_3\rangle \in \{\langle \pi_0\ell,\ \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi\rangle \mid \langle \pi_0\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi\rangle \in \{\langle \pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi)\}\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell_0)\mathsf{z} = \varrho(\pi'_0\ell_0)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell_0\pi_1\ell'\pi_2\ell,\ \ell\pi_3), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell_0\pi'_1\ell'\pi'_2\ell,\ \ell\pi'_3))\})$$

$\wr$by letting $\pi_0\ell_0 \leftarrow \pi_0\ell$, $\ell_0\pi_1\ell' \leftarrow \ell\pi''_2\ell$, $\ell'\pi_2\ell \leftarrow \ell$, $\ell\pi_3 \leftarrow \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi''_3\ell$, and similarly for the second trace $\wr$

$\subseteq \alpha^{\mathsf{d}}(\{X\})\ell \cup (\alpha^{\mathsf{d}}(\{X\})\ell \mathbin{;} \alpha^{\mathsf{d}}(\{\{\langle\pi_0\ell,\ \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi\rangle \mid \langle\pi_0\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi\rangle \in \{\langle\pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi)\}\}\})\ell)$

$\wr$Lemma 47.61 with $\mathcal{S} \leftarrow X$ and $\mathcal{S}' \leftarrow \{\langle\pi_0\ell,\ \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi\rangle \mid \langle\pi_0\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi\rangle \in \{\langle\pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi)\}\}\wr$

$= \alpha^{\mathsf{d}}(\{X\})\ell \cup (\alpha^{\mathsf{d}}(\{X\})\ell \mathbin{;} \alpha^{\mathsf{d}}(\{\{\langle\pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi)\}\}\})\ell)$

$\wr$def. (47.25) of α^{d}, (47.18) of diff, and (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]$ with $\ell \neq \ell\wr$

$= \alpha^{\mathsf{d}}(\{X\})\ell \cup (\alpha^{\mathsf{d}}(\{X\})\ell \mathbin{;} (\alpha^{\mathsf{d}}(\{\mathcal{S}^*[\![\mathsf{S}_b]\!]\})\ell \rceil \mathsf{nondet}(\mathsf{B},\mathsf{B})))$ $\wr$Lemma 47.64$\wr$

$= \alpha^{\mathsf{d}}(\{X\})\ell \cup (\alpha^{\mathsf{d}}(\{X\})\ell \mathbin{;} (\alpha^{\mathsf{d}}(\{\mathcal{S}^{+\infty}[\![\mathsf{S}_b]\!]\})\ell) \rceil \mathsf{nondet}(\mathsf{B},\mathsf{B}))$ $\wr$Lemma 47.23$\wr$

$\subseteq \alpha^{\mathsf{d}}(\{X\})\ell \cup (\alpha^{\mathsf{d}}(\{X\})\ell \mathbin{;} (\widehat{\mathcal{S}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell \rceil \mathsf{nondet}(\mathsf{B},\mathsf{B})))$ $\wr$ind. hyp. (47.32), $;$ and $\rceil$ are $\subseteq$-increasing$\wr$

— **(1–Bb)** In this third and last case for (1), we have $\ell\pi_1 = \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell$ so the prefix observation ends after the normal termination of the loop body at $\mathsf{after}[\![\mathsf{S}_b]\!] = \mathsf{at}[\![\mathsf{S}]\!] = \ell$ (just before the next iteration or the loop exit).

The possible choices for $\langle\pi'_0\ell,\ \ell\pi'_1\rangle \in \mathcal{F}^*[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b]\!]\ X$ are given by (A), (B), and (C) and are considered below.

– **(1–Bb–A)** This case is the symmetric of **(1–A)**, and so has already been considered.

– **(1–Bb–Ba/Bc/C)** This case is the symmetric of **(1–Ba/Bc/C–Bb)**, and so has already been considered.

– **(1–Bb–Bb)** This is the case when the prefix observation traces $\langle\pi_0\ell,\ \ell\pi_1\rangle$ and $\langle\pi'_0\ell,\ \ell\pi'_1\rangle$ in (5) both end after the normal termination of the loop body at $\mathsf{after}[\![\mathsf{S}_b]\!] = \mathsf{at}[\![\mathsf{S}]\!] = \ell$ and so belong to $\{\langle\pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \mid \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]\}$. In that case, we have

(5)

$= \{\langle\mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle\pi_0\ell,\ \ell\pi_1\rangle, \langle\pi'_0\ell,\ \ell\pi'_1\rangle \in \{\langle\pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \mid \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]\}\ .\ (\forall\mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_1))\}$ $\wr$case **(1–Bb–Bb)**$\wr$

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle\ .\ \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge \exists\langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle\ .\ \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell\pi'_2\ell) = \mathsf{tt} \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi'_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell))\}$
≀def. ∈∫

$\subseteq \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle\ .\ \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \{\langle \pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi)\} \wedge \exists\langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle\ .\ \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \{\langle \pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi)\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi'_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell))\}$ ≀def. ∈∫

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle\ .\ \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \{\langle \pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi)\} \wedge \exists\langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle\ .\ \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \{\langle \pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi)\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi'_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_2\ell))\}$

≀by def. (47.18) of diff, and def. (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]$ since in case (1), $\ell' = \ell$ does not appear in $\xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3$ and the value of y is the same at ℓ after $\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell$ and at ℓ after $\pi_0\ell\pi_2\ell$. Same for $\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell$. ∫

$\subseteq \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X, \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi'_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_2\ell))\}$ ≀def. ⊆∫

$\subseteq \alpha^{\mathsf{d}}(\{X\})\ell$ ≀def. (47.25) of α^{d} ∫

— Summing up for case (1) we get $(5) \subseteq \mathbb{1}_{\mathbb{V}} \cup \alpha^{\mathsf{d}}(\{X\})\ell \cup (\alpha^{\mathsf{d}}(\{X\})\ell \,⨾\, \widehat{\widehat{\mathcal{S}}}{}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell)\ \rceil\ \mathsf{nondet}(\mathsf{B}, \mathsf{B})$ which yields (47.65.a) of the form

$$(\!|\ \ell' = \ell\ ?\ \mathbb{1}_{\mathbb{V}} \cup X(\ell) \cup \big(X(\ell) \,⨾\, ((\widehat{\widehat{\mathcal{S}}}{}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell)\ \rceil\ \mathsf{nondet}(\mathsf{B}, \mathsf{B}))\big) \,\text{\textasciicircum}\, \varnothing\ |\!)\ .$$

However, the term $X(\ell)$ does not appear in (47.65.a) since it can be simplified thanks to Exercise 15.7.

—— **(2)** Else, if the dependency observation point ℓ' on prefix traces is in the loop body S_b after zero or more loop iterations. So the two traces $\ell\pi_1$ and $\ell\pi'_1$ in (5) cannot be generated by (17.4.**A**). The case $\ell' = \ell = \mathsf{after}[\![\mathsf{S}_b]\!] = \mathsf{at}[\![\mathsf{S}]\!]$ has already been considered in case **(1)** (for subcases involving **(B)** and **(C)**). By def. (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]$ the case $\ell' = \mathsf{at}[\![\mathsf{S}_b]\!]$ is equivalent to $\ell' = \mathsf{at}[\![\mathsf{S}]\!]$ already considered in **(1)** since the evaluation of boolean expressions has no side effect so the value of variables y at $\mathsf{at}[\![\mathsf{S}_b]\!]$ and $\mathsf{at}[\![\mathsf{S}]\!]$ are the same. Similarly, the value of variables y before a `break ;`

statement at labels in $\mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]$ that can escape the loop body S_b is the same as the value at $\mathsf{break\text{-}to}[\![\mathsf{S}_b]\!] = \mathsf{after}[\![\mathsf{S}]\!]$ and will be handled with case **(3)**.

It follows that in this case **(2)** we only have to consider the case $\ell' \in \mathsf{in}[\![\mathsf{S}_b]\!] \setminus (\{\mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{after}[\![\mathsf{S}_b]\!]\} \cup \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!])$ and the two traces $\ell\pi_1$ and $\ell\pi'_1$ in(5) are generated by **(B)** or **(C)**. There are three cases to consider.

— **(2–B–B)** The dependency observation point ℓ' on the two prefix observation traces $\ell\pi_1$ and $\ell\pi'_1$ in (5) is in the loop body S_b after zero or more loop iterations and the observation along these two traces stops in the loop body.

$$
\begin{aligned}
&(5)\\
= {} & \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_1\rangle, \langle \pi'_0\ell,\ \ell\pi'_1\rangle \in \{\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge{} \\
& \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathtt{tt} \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]\} \ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ . \\
& \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_1))\} \qquad \text{⦃case } \mathbf{2\text{–}B\text{–}B}\text{⦄}\\
= {} & \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle\ .\ \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathtt{tt} \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \\
& \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge \exists \langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''\rangle\ .\ \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge{} \\
& \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi'_0\ell\pi'_2\ell) = \mathtt{tt} \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ . \\
& \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \\
& \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''))\} \qquad \text{⦃def. } \in\text{⦄}\\
\subseteq {} & \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle\ .\ \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \in{} \\
& \{\langle \pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi)\} \wedge \exists \langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''\rangle\ .\ \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge{} \\
& \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''\rangle \in \{\langle \pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi)\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ . \\
& \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \\
& \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''))\} \qquad \text{⦃def. } \in\text{⦄}\\
\subseteq {} & \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X\ .\ \exists \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge{} \\
& \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_2\ell))\}\\
& \cup\\
& \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X\ .\ \exists \langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''\rangle\ .\ \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \\
& \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''\rangle \in \{\langle \pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi)\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = {} \\
& \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''))\}\\
& \cup\\
& \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle\ .\ \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \in{} \\
& \{\langle \pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi)\} \wedge \exists \langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''\rangle\ .\ \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge{} \\
& \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''\rangle \in \{\langle \pi,\ \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi)\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ . \\
& \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \\
& \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''))\}
\end{aligned}
$$

$\wr$by def. (47.18) of diff and (47.16) of seqval$[\![\mathsf{y}]\!]\ell'$, there is an instance of ℓ' in both $\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''$ and $\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''$ before which the values of y at ℓ' and at which they differ. There are four cases (indeed 3 by symmetry), depending on whether the occurrence of ℓ'' is before or after the transition $\xrightarrow{\mathsf{B}}$. $\wr$

$$\subseteq \alpha^{\mathrm{d}}(\{X\})\ell' \cup \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \ .\ \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \in \{\langle \pi,\ \pi'\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!] \mid \boldsymbol{\mathcal{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi)\} \wedge \exists \langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''\rangle \ .\ \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''\rangle \in \{\langle \pi,\ \pi'\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!] \mid \boldsymbol{\mathcal{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi)\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \ .\ \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''))\}$$

$\wr$For the second term where ℓ' occurs in $\ell\pi_2\ell$, the trace $\ell\pi_2\ell$ must have reached the loop body, and so, by the reasoning of (7), this second term is an instance of the third one.$\wr$

$$\subseteq \alpha^{\mathrm{d}}(\{X\})\ell' \cup \big(\alpha^{\mathrm{d}}(\{X\})\ell \,\mathbin{;}\, ((\widehat{\boldsymbol{\mathcal{S}}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell') \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B}))\big)$$

$\wr$by a reasoning similar to the one we did in case **(1–Ba/Bc/C–Bb)** from (7) on.$\wr$

— **(2–B–C/2–C–B)** The dependency observation point ℓ' on the two prefix observation traces $\ell\pi_1$ and $\ell\pi'_1$ in (5) is in the loop body S_b after zero or more loop iterations and the observation along these two traces stops in the loop body for one and at the loop exit for the other.

(5)

$$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_1\rangle \in \{\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \boldsymbol{\mathcal{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!]\} \ .\ \exists \langle \pi'_0\ell,\ \ell\pi'_1\rangle \in \{\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \boldsymbol{\mathcal{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathsf{ff}\} \ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \ .\ \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_1))\}$$

$\wr$case **2–B–C**$\wr$

$$\subseteq \alpha^{\mathrm{d}}(\{X\})\ell' \cup \big(\alpha^{\mathrm{d}}(\{X\})\ell \,\mathbin{;}\, ((\widehat{\boldsymbol{\mathcal{S}}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell') \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B}))\big)$$

$\wr$This case is handled exactly as the previous one since the program point ℓ' where the change of value of variable y is observed is within the loop body so the loop must be entered in part $\ell\pi_2\ell$ of $\ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]$ and the loop exit $\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]$ does not affect the variable y.$\wr$

— **(2–C–C)** The dependency observation point ℓ' on the two prefix observation traces $\ell\pi_1$ and $\ell\pi'_1$ in (5) is in the loop body S_b after zero or more loop iterations and the observation along these two traces stops at the loop exit.

(5)

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_1\rangle, \langle \pi'_0\ell,\ \ell\pi'_1\rangle \in \{\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{ff}\} \ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_1))\}$ ⟅case **2–C–C**⟆

$\subseteq \alpha^{\mathrm{d}}(\{X\})\ell' \cup \big(\alpha^{\mathrm{d}}(\{X\})\ell \,\mathbin{⨾}\, ((\widehat{\mathcal{S}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell') \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})\big)\big)$

⟅This case is handled exactly as the two previous ones since, again, the program point ℓ' where the change of value of variable y is observed is within the loop body so the loop must be entered in part $\ell\pi_2\ell$ of $\ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]$ and the loop exit $\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]$ does not affect the variable y. Similarly for the second trace $\ell\pi'_1$.⟆

— Summing up for case (2), we get (5) $\subseteq \alpha^{\mathrm{d}}(\{X\})\ell' \cup \big(\alpha^{\mathrm{d}}(\{X\})\ell \,⨾\, ((\widehat{\mathcal{S}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell') \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B}))\big)$ which yields (47.65.b) of the form

$$(\!|\ \ell' \in \mathsf{in}[\![\mathsf{S}_b]\!]\ ?\ \big(X(\ell) \,⨾\, ((\widehat{\mathcal{S}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell') \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B}))\big) \,⨾\, \varnothing\ |\!).$$

where the term $X(\ell')$ does not appear in (47.65.b) by the simplification following from Exercise 15.7.

—— (3) Otherwise, the dependency observation point $\ell' = \mathsf{after}[\![\mathsf{S}]\!]$ on prefix traces is after the loop statement $\mathsf{S} = \texttt{while}\ \ell\ \texttt{(B)}\ \mathsf{S}_b$.

(5)

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_1\rangle, \langle \pi'_0\ell,\ \ell\pi'_1\rangle \in \mathcal{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathsf{S}_b]\!]\ X\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0\ell, \ell\pi'_1))\}$ ⟅$\ell' = \mathsf{after}[\![\mathsf{S}]\!]$⟆

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_1\rangle, \langle \pi'_0\ell,\ \ell\pi'_1\rangle \in \big\{\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{ff}\big\} \cup \big\{\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]\big\}\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0\ell, \ell\pi'_1))\}$ (8)

⟅The only cases in (17.4) where $\ell' = \mathsf{after}[\![\mathsf{S}]\!]$ is reachable is either via (C) for normal termination after zero or more iterations or via (B) through a `break ;` in the loop body S_b during the first or later iteration⟆

There are now three subcases, depending on whether the observation prefix traces $\ell\pi_1$ and $\ell\pi'_1$ are both from a normal exit, a both from a break, or one is from a break and the other from a normal exit.

— (3–C–C) This is the case when the observation prefix traces $\ell\pi_1$ and $\ell\pi'_1$ are both from a normal exit.

(8)

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle\ .\ \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{ff} \wedge \exists\langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle\ .\ \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell\pi'_2\ell) = \mathrm{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]))\}$ ⦇def. $\in$ and $\ell' = \mathsf{after}[\![\mathsf{S}]\!]$⦈

$\subseteq \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_2\ell\rangle, \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{ff} \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell\pi'_2\ell) = \mathrm{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \varrho(\pi_0\ell\pi_2\ell)\mathsf{y} \neq \varrho(\pi'_0\ell\pi'_2\ell)\mathsf{y}\}$ (9)

⦇X is an iterate of $\mathcal{F}^*[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!]$ so $\ell\pi_2\ell$ and $\ell\pi'_2\ell$ are iterates of the loop body. By definition of the labelling in Section 4.2, $\mathsf{after}[\![\mathsf{S}]\!]$ appears neither in $\ell\pi_2\ell$ nor in $\ell\pi'_2\ell$. It follows by def. (47.18) of diff and (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]\mathsf{after}[\![\mathsf{S}]\!]$ that $\mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])) = \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!]), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0\ell\pi'_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!])) = \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\ell)(\pi_0\ell\pi_2\ell, \ell), \mathsf{seqval}[\![\mathsf{y}]\!](\ell)(\pi'_0\ell\pi'_2\ell, \ell)) = \varrho(\pi_0\ell\pi_2\ell)\mathsf{y} \neq \varrho(\pi'_0\ell\pi'_2\ell)\mathsf{y}$⦈

From there on, the development is very similar to the cases (2.a), (2.b), and (2.c–d) of the conditional with execution traces that may go through the true branch (here entering the loop) or the false branch (here not entering the iteration). There are four subcases (three by symmetry).

– **(3–C–C.a)** If none of the executions $\pi_0\ell\pi_2\ell$ and $\pi'_0\ell\pi'_2\ell$ enter the loop body since in both cases the condition B is false, we have $\ell\pi_2\ell = \ell$ and $\ell\pi'_2\ell = \ell$.

(9)

$\subseteq \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\rangle, \langle \pi'_0\ell,\ \ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell) = \mathrm{ff} \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell) = \mathrm{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \varrho(\pi_0\ell)\mathsf{y} \neq \varrho(\pi'_0\ell)\mathsf{y}\} \rceil \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B})$ ⦇case (3–C–C.a)⦈

$\subseteq \mathbb{1}_{\mathbb{V}} \rceil \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B})$

⦇since if $\mathsf{x} \notin \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B})$ then $\mathsf{x} \in \mathsf{det}(\neg\mathsf{B}, \neg\mathsf{B})$ so $\mathcal{B}[\![\neg\mathsf{B}]\!]\varrho(\pi_0\ell)$ and $\mathcal{B}[\![\neg\mathsf{B}]\!]\varrho(\pi'_0\ell)$ would imply $\varrho(\pi_0\ell)\mathsf{x} = \varrho(\pi'_0\ell)\mathsf{x}$. Therefore $\varrho(\pi_0\ell) = \varrho(\pi'_0\ell)$ in contradiction with $\varrho(\pi_0\ell)\mathsf{y} \neq \varrho(\pi'_0\ell)\mathsf{y}$.⦈

– **(3–C–C.b)** Else, if both executions $\pi_0\ell\pi_2\ell$ and $\pi'_0\ell\pi'_2\ell$ enter the loop body since in both cases the condition B is true, we have $\ell\pi_2\ell \neq \ell$ and $\ell\pi'_2\ell \neq \ell$

(9)

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_2\ell\rangle, \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{ff} \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell\pi'_2\ell) = \mathrm{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \varrho(\pi_0\ell\pi_2\ell)\mathsf{y} \neq \varrho(\pi'_0\ell\pi'_2\ell)\mathsf{y}\} \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})$

$\wr$case (**3–C–C.b**) and X belongs to the iterates of $\mathcal{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]$ so this is possible only when $\mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0{}^\ell) = \texttt{tt}$ and $\mathcal{B}[\![\texttt{B}]\!]\varrho(\pi'_0{}^\ell) = \texttt{tt}$ and def. (47.48) of $\texttt{nondet}\,\wr$

$\subseteq \{\langle \texttt{x},\ \texttt{y}\rangle \mid \exists\langle \pi_0{}^\ell,\ {}^\ell\pi_2{}^\ell\rangle \in X\ .\ \exists\langle \pi'_0{}^\ell,\ {}^\ell\pi'_2{}^\ell \xrightarrow{\texttt{B}} \texttt{at}[\![\texttt{S}_b]\!]\pi_3{}^\ell\rangle\ .\ \langle \pi'_0{}^\ell,\ {}^\ell\pi'_2{}^\ell\rangle \in X \wedge (\forall \texttt{z} \in \mathbb{V} \setminus \{\texttt{x}\}\ .$ $\varrho(\pi_0{}^\ell)\texttt{z} = \varrho(\pi'_0{}^\ell)\texttt{z}) \wedge \texttt{diff}(\texttt{seqval}[\![\texttt{y}]\!]^\ell(\pi_0{}^\ell, {}^\ell\pi_2{}^\ell), \texttt{seqval}[\![\texttt{y}]\!]^\ell(\pi'_0{}^\ell, {}^\ell\pi'_2{}^\ell))\}$

$\wr$since $\varrho(\pi_0{}^\ell\pi_2{}^\ell)\texttt{y} \neq \varrho(\pi'_0{}^\ell\pi'_2{}^\ell)\texttt{y}$ implies $\texttt{diff}(\texttt{seqval}[\![\texttt{y}]\!]^\ell(\pi_0{}^\ell, {}^\ell\pi_2{}^\ell), \texttt{seqval}[\![\texttt{y}]\!]^\ell(\pi'_0{}^\ell, {}^\ell\pi'_2{}^\ell))\,\wr$

$\subseteq \alpha^{\mathrm{d}}(\{X\})^\ell$ $\qquad\wr$def. (47.25) of $\alpha^{\mathrm{d}}\,\wr$

– **(3–C–C.c)** Otherwise, one execution enters the loop body (say $\pi_0{}^\ell\pi_2{}^\ell$) and the other does not (say $\pi'_0{}^\ell\pi'_2{}^\ell$), we have (the other case is symmetric) ${}^\ell\pi_2{}^\ell \neq \ell$ and ${}^\ell\pi'_2{}^\ell = \ell$. The calculation is similar to **(2.c–d)** for the simple conditional.

(9)

$= \{\langle \texttt{x},\ \texttt{y}\rangle \mid \exists\langle \pi_0{}^\ell,\ {}^\ell\pi_2{}^\ell\rangle, \langle \pi'_0{}^\ell,\ \ell\rangle \in X \wedge \mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0{}^\ell) = \texttt{tt} \wedge \mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0{}^\ell\pi_2{}^\ell) = \texttt{ff} \wedge \mathcal{B}[\![\texttt{B}]\!]\varrho(\pi'_0{}^\ell) =$ $\texttt{ff} \wedge (\forall \texttt{z} \in \mathbb{V} \setminus \{\texttt{x}\}\ .\ \varrho(\pi_0{}^\ell)\texttt{z} = \varrho(\pi'_0{}^\ell)\texttt{z}) \wedge \varrho(\pi_0{}^\ell\pi_2{}^\ell)\texttt{y} \neq \varrho(\pi'_0{}^\ell)\texttt{y}\}$

$\wr$case (**3–C–C.c**) and X is included in the iterates of $\mathcal{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]$ so this is possible only when $\mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0{}^\ell) = \texttt{tt}$, $\mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0{}^\ell\pi_2{}^\ell) = \texttt{ff}$, and $\mathcal{B}[\![\texttt{B}]\!]\varrho(\pi'_0{}^\ell) = \texttt{ff}\,\wr$

$= \{\langle \texttt{x},\ \texttt{y}\rangle \mid \exists\langle \pi_0{}^\ell,\ {}^\ell\pi_2{}^\ell\rangle, \langle \pi'_0{}^\ell,\ \ell\rangle \in X \wedge \mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0{}^\ell) = \texttt{tt} \wedge \mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0{}^\ell\pi_2{}^\ell) = \texttt{ff} \wedge \mathcal{B}[\![\texttt{B}]\!]\varrho(\pi'_0{}^\ell) =$ $\texttt{ff} \wedge (\forall \texttt{z} \in \mathbb{V} \setminus \{\texttt{x}\}\ .\ \varrho(\pi_0{}^\ell)\texttt{z} = \varrho(\pi'_0{}^\ell)\texttt{z}) \wedge \varrho(\pi_0{}^\ell\pi_2{}^\ell)\texttt{y} \neq \varrho(\pi'_0{}^\ell)\texttt{y}\} \rceil \texttt{nondet}(\texttt{B}, \neg\texttt{B})$

$\wr$since, by def. (47.48) of $\texttt{nondet}$, if $\texttt{x} \notin \texttt{nondet}(\texttt{B}, \neg\texttt{B})$ then $\texttt{x} \in \texttt{det}(\texttt{B}, \neg\texttt{B})$ so by (47.48), $\mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0{}^\ell)$ and $\mathcal{B}[\![\neg\texttt{B}]\!]\varrho(\pi'_0{}^\ell)$ would imply $\varrho(\pi_0{}^\ell)\texttt{x} = \varrho(\pi'_0{}^\ell)\texttt{x}$ and therefore $\varrho(\pi_0{}^\ell) = \varrho(\pi'_0{}^\ell)$. X being included in the iterates of $\mathcal{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]$ and, by Exercises 17.13 and 17.21, the language being deterministic, this would imply that ${}^\ell\pi_2{}^\ell = \ell$, in contradiction with $\mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0{}^\ell) = \texttt{tt}$ and $\mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0{}^\ell\pi_2{}^\ell) = \texttt{ff}\,\wr$

$= \{\langle \texttt{x},\ \texttt{y}\rangle \mid \exists\langle \pi_0{}^\ell,\ {}^\ell\pi''_2{}^\ell \xrightarrow{\texttt{B}} \texttt{at}[\![\texttt{S}_b]\!]\pi'_3{}^\ell\rangle\ .\ \langle \pi_0{}^\ell,\ {}^\ell\pi''_2{}^\ell \xrightarrow{\texttt{B}} \texttt{at}[\![\texttt{S}_b]\!]\pi'_3{}^\ell\rangle \in X \wedge \mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0{}^\ell) = \texttt{tt} \wedge$ $\mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0{}^\ell\pi''_2{}^\ell \xrightarrow{\texttt{B}} \texttt{at}[\![\texttt{S}_b]\!]\pi'_3{}^\ell) = \texttt{ff} \wedge \langle \pi_0{}^\ell\pi''_2{}^\ell \xrightarrow{\texttt{B}} \texttt{at}[\![\texttt{S}_b]\!],\ \texttt{at}[\![\texttt{S}_b]\!]\pi'_3{}^\ell\rangle \in \mathcal{S}^*[\![\texttt{S}_b]\!] \wedge \exists\langle \pi'_0{}^\ell,$ $\ell\rangle \in X \wedge \mathcal{B}[\![\texttt{B}]\!]\varrho(\pi'_0{}^\ell) = \texttt{ff} \wedge (\forall \texttt{z} \in \mathbb{V} \setminus \{\texttt{x}\}\ .\ \varrho(\pi_0{}^\ell)\texttt{z} = \varrho(\pi'_0{}^\ell)\texttt{z}) \wedge \varrho(\pi_0{}^\ell\pi''_2{}^\ell \xrightarrow{\texttt{B}} \texttt{at}[\![\texttt{S}_b]\!]\pi'_3{}^\ell)\texttt{y} \neq$ $\varrho(\pi'_0{}^\ell)\texttt{y}\} \rceil \texttt{nondet}(\texttt{B}, \neg\texttt{B})$

$\wr$by the argument (7) that if $\langle \pi_0{}^\ell,\ {}^\ell\pi_2{}^\ell\rangle \in X$ corresponds to one or more iterations of the loop then it can be written in the form ${}^\ell\pi_2{}^\ell = {}^\ell\pi''_2{}^\ell \xrightarrow{\texttt{B}} \texttt{at}[\![\texttt{S}_b]\!]\pi'_3{}^\ell$ (where ${}^\ell\pi''_2{}^\ell$ may be reduced to ℓ for the first iteration) with ${}^\ell\pi''_2{}^\ell \in X$, $\mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0{}^\ell\pi''_2{}^\ell) = \texttt{tt}$ and $\langle \pi_0{}^\ell\pi''_2{}^\ell \xrightarrow{\texttt{B}} \texttt{at}[\![\texttt{S}_b]\!],\ \texttt{at}[\![\texttt{S}_b]\!]\pi'_3{}^\ell\rangle \in \mathcal{S}^*[\![\texttt{S}_b]\!]\,\wr$

$$\subseteq \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell, \pi'_0\ell \;.\; \langle \pi_0\ell,\ \ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell\rangle \in X \wedge \langle \pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket,\ \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell\rangle \in \boldsymbol{\mathcal{S}}^*\llbracket \mathsf{S}_b\rrbracket \wedge \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\boldsymbol{\varrho}(\pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell) = \mathsf{ff} \wedge \langle \pi'_0\ell,\ \ell\rangle \in X \wedge \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\boldsymbol{\varrho}(\pi_0\ell\pi''_2\ell) = \mathsf{tt} \wedge \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\boldsymbol{\varrho}(\pi'_0\ell) = \mathsf{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \;.\; \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}\llbracket \mathsf{y}\rrbracket\mathsf{after}\llbracket \mathsf{S}\rrbracket(\pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket, \mathsf{after}\llbracket \mathsf{S}\rrbracket), \mathsf{seqval}\llbracket \mathsf{y}\rrbracket\mathsf{after}\llbracket \mathsf{S}\rrbracket(\pi'_0\ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket, \mathsf{after}\llbracket \mathsf{S}\rrbracket))\} \rceil \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$$

≀def. (6.6) of $\boldsymbol{\varrho}$, def. (47.16) of $\mathsf{seqval}\llbracket \mathsf{y}\rrbracket$ and program labelling so that $\mathsf{after}\llbracket \mathsf{S}\rrbracket$ does not appear in the trace (in particular $\ell \neq \mathsf{after}\llbracket \mathsf{S}\rrbracket$), and def. (47.18) of diff≀

$$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket, \pi'_0\ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket \;.\; \langle \pi_0\ell,\ \ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell\rangle \in X \wedge \langle \pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell,\ \ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket\rangle \in \boldsymbol{\mathcal{S}}' \wedge \langle \pi'_0\ell,\ \ell\rangle \in X \wedge \langle \pi'_0\ell,\ \ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket\rangle \in \boldsymbol{\mathcal{S}}' \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \;.\; \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}\llbracket \mathsf{y}\rrbracket\mathsf{after}\llbracket \mathsf{S}\rrbracket(\pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket, \mathsf{after}\llbracket \mathsf{S}\rrbracket), \mathsf{seqval}\llbracket \mathsf{y}\rrbracket\mathsf{after}\llbracket \mathsf{S}\rrbracket(\pi'_0\ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket, \mathsf{after}\llbracket \mathsf{S}\rrbracket))\} \rceil \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$$

≀where $\boldsymbol{\mathcal{S}}' = \{\langle \pi'_1\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell,\ \ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket\rangle \mid \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\boldsymbol{\varrho}(\pi'_1\ell) = \mathsf{tt} \wedge \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\boldsymbol{\varrho}(\pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell) = \mathsf{ff} \wedge \langle \pi'_1\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket, \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell\rangle \in \boldsymbol{\mathcal{S}}^*\llbracket \mathsf{S}_b\rrbracket\} \cup \{\langle \pi'_0\ell,\ \ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket\rangle \mid \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\boldsymbol{\varrho}(\pi'_0\ell) = \mathsf{ff}\}$≀

$$\subseteq (\alpha^{\mathrm{d}}(\{X\})\,\ell \,\mathbin{;}\, \alpha^{\mathrm{d}}(\{\boldsymbol{\mathcal{S}}'\})\ \mathsf{after}\llbracket \mathsf{S}\rrbracket) \rceil \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$$

≀Lemma 47.61 with $\ell_0 \leftarrow \ell$, $\ell' \leftarrow \ell$, and $\ell \leftarrow \mathsf{after}\llbracket \mathsf{S}\rrbracket$≀

We have to calculate the second term

$$\alpha^{\mathrm{d}}(\{\boldsymbol{\mathcal{S}}'\})\ \mathsf{after}\llbracket \mathsf{S}\rrbracket \tag{10}$$

$$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \boldsymbol{\mathcal{S}}' \in \mathcal{D}(\mathsf{after}\llbracket \mathsf{S}\rrbracket)\langle \mathsf{x},\ \mathsf{y}\rangle\}$$

≀def. (47.25) of α^{d}≀

$$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0,\ \pi_1\rangle, \langle \pi'_0,\ \pi'_1\rangle \in \boldsymbol{\mathcal{S}}' \;.\; (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \;.\; \boldsymbol{\varrho}(\pi_0)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}\llbracket \mathsf{y}\rrbracket\mathsf{after}\llbracket \mathsf{S}\rrbracket(\pi_0, \pi_1), \mathsf{seqval}\llbracket \mathsf{y}\rrbracket\mathsf{after}\llbracket \mathsf{S}\rrbracket(\pi'_0, \pi'_1))\}$$

≀def. (47.19) of $\mathcal{D}^{\ell}\langle \mathsf{x},\ \mathsf{y}\rangle$≀

$$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket \;.\; \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\boldsymbol{\varrho}(\pi'_2\ell) = \mathsf{tt} \wedge \langle \pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket,\ \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell\rangle \in \boldsymbol{\mathcal{S}}^*\llbracket \mathsf{S}_b\rrbracket\}, \exists \pi'_0\ell \;.\; \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\boldsymbol{\varrho}(\pi'_0\ell) = \mathsf{ff}\} \;.\; (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \;.\; \boldsymbol{\varrho}(\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}\llbracket \mathsf{y}\rrbracket\mathsf{after}\llbracket \mathsf{S}\rrbracket(\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell, \ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket), \mathsf{seqval}\llbracket \mathsf{y}\rrbracket\mathsf{after}\llbracket \mathsf{S}\rrbracket(\pi'_0\ell, \ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket))\}$$

≀def. $\boldsymbol{\mathcal{S}}'$ and the other two combinations have already been considered in (**3–C–C.a**) and (**3–C–C.b**)≀

$$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}\llbracket \mathsf{S}\rrbracket \;.\; \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\boldsymbol{\varrho}(\pi'_2\ell) = \mathsf{tt} \wedge \langle \pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket,\ \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell\rangle \in \boldsymbol{\mathcal{S}}^*\llbracket \mathsf{S}_b\rrbracket \wedge \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\boldsymbol{\varrho}(\pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell) = \mathsf{ff} \wedge \exists \pi'_0\ell \;.\; \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\boldsymbol{\varrho}(\pi'_0\ell) = \mathsf{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \;.\; \boldsymbol{\varrho}(\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \boldsymbol{\varrho}(\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket \mathsf{S}_b\rrbracket\pi'_3\ell)\mathsf{y} \neq \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{y})\}$$

$\wr$def. (6.6) of ϱ, def. (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]$ and program labelling so that $\mathsf{after}[\![\mathsf{S}]\!]$ does not appear in the trace (in particular $\ell \neq \mathsf{after}[\![\mathsf{S}]\!]$), and def. (47.18) of $\mathsf{diff}$$\wr$

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}[\![\mathsf{S}]\!] \ .\ \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi'_2\ell) = \mathsf{tt} \wedge \langle \pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell) = \mathsf{ff} \wedge \exists \pi'_0\ell\ .\ \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell) = \mathsf{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \varrho(\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell)\mathsf{y} \neq \varrho(\pi'_0\ell)\mathsf{y})\} \rceil \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B})$

$\wr$since if $\mathsf{x} \notin \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B})$ then $\mathsf{x} \in \mathsf{det}(\neg\mathsf{B}, \neg\mathsf{B})$ so by (47.48), $\mathscr{B}[\![\neg\mathsf{B}]\!]\varrho(\pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell)$, and $\mathscr{B}[\![\neg\mathsf{B}]\!]\varrho(\pi'_0\ell)$, we would have $\varrho(\pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell) = \varrho(\pi'_0\ell)$, which, with $\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}$, would imply $\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell) = \varrho(\pi'_0\ell)$, in contradiction with $\varrho(\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell)\mathsf{y} \neq \varrho(\pi'_0\ell)\mathsf{y})$$\wr$

$\subseteq \{\langle \mathsf{x}, \mathsf{y}\rangle \mid \exists \pi_0, \pi_1, \pi'_0\ .\ (\forall \mathsf{z} \in \mathbb{V}\setminus\{\mathsf{x}\}\ .\ \varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{z}) \wedge \langle \pi_0\mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_1\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!]\pi_1\ell)\mathsf{y} \neq \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{y}\} \rceil \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B})$

$\wr$letting $\pi_0\mathsf{at}[\![\mathsf{S}_b]\!] \leftarrow \pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]$ with $\varrho(\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]) = \varrho(\pi'_2\ell)$, $\pi_0\mathsf{at}[\![\mathsf{S}_b]\!] \leftarrow \pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell$, and $\pi_1\ell \leftarrow \pi'_3\ell$ $\wr$

$= (\{\langle \mathsf{x},\ \mathsf{x}\rangle \mid \exists \pi_0, \pi_1, \pi'_0\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{z}) \wedge \langle \pi_0\mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_1\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!]\pi_1\ell)\mathsf{x} \neq \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{x}\}$
$\cup \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \mathsf{x} \neq \mathsf{y} \wedge \exists \pi_0, \pi_1, \pi'_0\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{z}) \wedge \langle \pi_0\mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_1\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!]\pi_1\ell)\mathsf{y} \neq \varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{y}\}) \rceil \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B})$

$\wr$since when $\mathsf{x} \neq \mathsf{y}$, $\varrho(\pi'_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{y} = \varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{y}$$\wr$

$= \{\langle \mathsf{x}, \mathsf{y}\rangle \mid \exists \pi_0, \pi_1, \pi'_0\ .\ (\forall \mathsf{z} \in \mathbb{V}\setminus\{\mathsf{x}\}\ .\ \varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{z}) \wedge \langle \pi_0\mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_1\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!]\pi_1\ell)\mathsf{y} \neq \varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{y}\} \rceil \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B})$ $\wr$grouping cases together$\wr$

$= \{\langle \mathsf{x}, \mathsf{y}\rangle \mid \exists \pi_0, \pi_1, \pi'_0\ .\ (\forall \mathsf{z} \in \mathbb{V}\setminus\{\mathsf{x}\}\ .\ \varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{z} = \varrho(\pi'_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{z}) \wedge \langle \pi_0\mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_1\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!]\pi_1\ell)\mathsf{y} \neq \varrho(\pi_0\mathsf{at}[\![\mathsf{S}_b]\!])\mathsf{y}\} \rceil \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B})$

$\wr$letting $\rho = \varrho(\pi_0\ell)$, $\nu = \varrho(\pi'_0\ell)\mathsf{x}$ so that $\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}$ implies $\varrho(\pi'_0\ell) = \rho[\mathsf{x} \leftarrow \nu]$.$\wr$

$\subseteq (\{\langle \mathsf{x},\ \mathsf{x}\rangle \mid \mathsf{x} \in \mathbb{V}\} \cup \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \mathsf{x} \in \mathbb{V} \wedge \mathsf{y} \in \mathsf{mod}[\![\mathsf{S}_b]\!]\}) \rceil \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B})$

$\wr$A coarse approximation is to consider the variables $\mathsf{y} \neq \mathsf{x}$ appearing to the left of an assignment in S_b, a necessary condition for y to be modified by the execution of S_b where the set $\mathsf{mod}[\![\mathsf{S}]\!]$ of variables that may be modified by the execution of S is syntactically defined as in (47.50). $\wr$

$= \mathbb{1}_{\mathsf{nondet}(\neg\mathsf{B},\neg\mathsf{B})} \cup \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B}) \times \mathsf{mod}[\![\mathsf{S}_b]\!]$ $\wr$def. $\rceil$$\wr$

– Summing up for all subcases of (3–C–C), we get $(5) \subseteq \mathbb{1}_{\mathsf{nondet}(\neg\mathsf{B},\neg\mathsf{B})} \cup \alpha^{\mathrm{d}}(\{X\})\ell \cup (\alpha^{\mathrm{d}}(\{X\})\ \ell\ ⨾\ (\mathbb{1}_{\mathsf{nondet}(\neg\mathsf{B},\neg\mathsf{B})} \cup \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B}) \times \mathsf{mod}[\![\mathsf{S}_b]\!])) \rceil \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$.

— **(3–B–B)** This is the case when the observation prefix traces $\ell\pi_1$ and $\ell\pi'_1$ are both from a $\texttt{break ;}$ in the iteration body S_b.

$$
\begin{aligned}
&(8)\\
&= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle\pi_0\ell,\ \ell\pi_1\rangle, \langle\pi'_0\ell,\ \ell\pi'_1\rangle \in \{\langle\pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \\
&\quad \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \\
&\quad \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]\} \ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \\
&\quad \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0\ell, \ell\pi'_1))\} \qquad \text{(case (3–B–B))}\\
&= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\ .\ \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \ell'' \in \\
&\quad \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge \exists\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \\
&\quad \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''\ .\ \langle\pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell\pi'_2\ell) = \mathsf{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \\
&\quad \langle\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\\
&\quad \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \\
&\quad \mathsf{after}[\![\mathsf{S}]\!]), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]))\} \qquad \text{(def. } \in)\\
&= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\ .\ \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \ell'' \in \\
&\quad \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge \exists\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \\
&\quad \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''\ .\ \langle\pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell\pi'_2\ell) = \mathsf{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \\
&\quad \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \\
&\quad \varrho(\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'') \neq \varrho(\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell'')\}
\end{aligned}
$$

(\langle $\langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X$ and X contains only iterates of $\mathcal{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathsf{S}_b]\!]$ so $\mathsf{after}[\![\mathsf{S}]\!] \neq \ell$ cannot appear in $\ell\pi_2\ell$. Moreover, $\langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]$ so, by def. Section **4.2** of program labelling, $\mathsf{after}[\![\mathsf{S}]\!] \neq \mathsf{at}[\![\mathsf{S}_b]\!]$ cannot appear in $\mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''$. Therefore, by def. (6.6) of ϱ and (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]\ell$, $\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]) = \varrho(\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'')$. We conclude by def. (47.18) of diff)

$$
\begin{aligned}
&= \bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\ .\ \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \\
&\quad \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge \exists\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell''\ .\\
&\quad \langle\pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell\pi'_2\ell) = \mathsf{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \\
&\quad \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \varrho(\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \\
&\quad \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'') \neq \varrho(\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell'')\}
\end{aligned}
$$

$$\subseteq \bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \alpha^{\mathrm{d}}(\{X\})\ell \mathbin{⨟} (\widehat{\mathcal{S}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\,\ell'' \rceil \mathsf{nondet}(\mathsf{B},\mathsf{B}))$$

≀by a reasoning similar to the one we did in case **(1–Ba/Bc/C–Bb)** from (7) on.≀

$$= \alpha^{\mathrm{d}}(\{X\})\ell \mathbin{⨟} \Big(\Big(\bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\mathcal{S}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\,\ell''\Big) \rceil \mathsf{nondet}(\mathsf{B},\mathsf{B})\Big) \qquad \text{≀⨟ and } \rceil \text{ preserve arbitrary joins≀}$$

— **(3–B–C)** This is the case when the observation prefix trace $\ell\pi_1$ is from a normal exit of the iteration and $\ell\pi'_1$ is from a **break ;** in the iteration body S_b. By symmetry of diff this also covers the inverse case.

(8)

$$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_1\rangle \in \{\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]\}\ .\ \exists \langle \pi'_0\ell,\ \ell\pi'_1\rangle \in \{\langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell\pi'_2\ell) = \mathrm{ff}\}\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0\ell, \ell\pi'_1))\} \qquad \text{≀case (3–B–C)≀}$$

$$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\pi'_0\ell\pi'_2\ell\ .\ \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell\pi'_2\ell) = \mathrm{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{after}[\![\mathsf{S}]\!]), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]))\} \qquad \text{≀def. }\in\text{≀}$$

$$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{after}[\![\mathsf{S}]\!], \pi'_0\ell\pi'_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\ .\ \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]\langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{tt} \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell\pi'_2\ell) = \mathrm{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{after}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!]), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0\ell\pi'_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!]))\}$$

$\wr\langle\pi_0\ell,\ \ell\pi_2\ell\rangle, \langle\pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X$ and X contains only iterates of $\mathscr{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]$ so $\mathsf{after}[\![\mathsf{S}]\!] \neq \ell$ can appear neither in $\ell\pi_2\ell$ nor in $\ell\pi'_2\ell$. Moreover, $\langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]$, $\mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]$ so, by def. Section 4.2 of program labelling, $\mathsf{after}[\![\mathsf{S}]\!] \neq \mathsf{at}[\![\mathsf{S}_b]\!]$ cannot appear in $\mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''$. Therefore, by def. (6.6) of ϱ and (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]\ell$, $\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!])$ $= \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!])$ and $\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]) = \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0\ell\pi'_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!])$.$\wr$

$= \{\langle\mathsf{x},\ \mathsf{y}\rangle \mid \exists\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!], \pi'_0\ell\pi'_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\ .\ \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \langle\pi_0\ell\pi_2\ell,\ \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \{\langle\pi\ell,\ \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi\ell) = \mathsf{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle\pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]\} \wedge \langle\pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \langle\pi'_0\ell\pi'_2\ell,\ \ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \{\langle\pi\ell,\ \ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi\ell) = \mathsf{ff}\} \wedge (\forall\mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!]), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0\ell\pi'_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!]))\}$ $\qquad\wr$def. $\in\wr$

$\subseteq \alpha^{\mathrm{d}}(\{X\})\ \ell\ \mathbin{;}\ \alpha^{\mathrm{d}}(\{\mathcal{S}'\})\ \mathsf{after}[\![\mathsf{S}]\!]$

$\wr$by Lemma 47.61 where $\mathcal{S}' = \{\langle\pi\ell,\ \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi\ell) = \mathsf{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle\pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]\} \cup \{\langle\pi\ell,\ \ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi\ell) = \mathsf{ff}\}$ with $\pi_0\ell_0 \leftarrow \pi_0\ell$, $\ell_0\pi_1\ell' \leftarrow \ell\pi_2\ell$, $\ell \leftarrow \mathsf{after}[\![\mathsf{S}]\!]$, $\ell'\pi_2\ell \leftarrow \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathsf{S}]\!]$, $\ell\pi_3 \leftarrow \mathsf{after}[\![\mathsf{S}]\!]$ so $\pi_3 = \ni$, and $\pi'_0\ell_0 \leftarrow \pi'_0\ell$, $\ell_0\pi'_1\ell' \leftarrow \ell_0\pi'_2\ell$, $\ell'\pi'_2\ell \leftarrow \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]$, $\ell\pi'_3 \leftarrow \mathsf{after}[\![\mathsf{S}]\!]$ so $\pi'_3 = \ni\ \wr$

Similar to the calculation starting at (10), we have to calculate the second term

$\alpha^{\mathrm{d}}(\{\mathcal{S}'\})\ \mathsf{after}[\![\mathsf{S}]\!]$

$= \{\langle\mathsf{x},\ \mathsf{y}\rangle \mid \mathcal{S}' \in \mathcal{D}(\mathsf{after}[\![\mathsf{S}]\!])\langle\mathsf{x},\ \mathsf{y}\rangle\}$ $\qquad\wr$def. (47.25) of $\alpha^{\mathrm{d}}\wr$

$= \{\langle\mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle\pi_0,\ \pi_1\rangle, \langle\pi'_0,\ \pi'_1\rangle \in \mathcal{S}'\ .\ (\forall\mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0)\mathsf{z} = \varrho(\pi'_0)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\mathsf{after}[\![\mathsf{S}]\!](\pi_0, \pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]\mathsf{after}[\![\mathsf{S}]\!](\pi'_0, \pi'_1))\}$ $\qquad\wr$def. (47.19) of $\mathcal{D}\ell\langle\mathsf{x},\ \mathsf{y}\rangle\wr$

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!], \pi'\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \;.\; \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\ell) = \mathsf{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle \pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'\ell) = \mathsf{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \;.\; \varrho(\pi\ell)\mathsf{z} = \varrho(\pi'\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\mathsf{after}[\![\mathsf{S}]\!](\pi\ell, \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]), \mathsf{seqval}[\![\mathsf{y}]\!]\mathsf{after}[\![\mathsf{S}]\!](\pi'\ell, \ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]))\}$

≀def. $\mathcal{S}'$ and the other two combinations have already been considered in (**3–B–B**) and (**2–C–C**)∫

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!], \pi'\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \;.\; \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\ell) = \mathsf{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle \pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'\ell) = \mathsf{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \;.\; \varrho(\pi\ell)\mathsf{z} = \varrho(\pi'\ell)\mathsf{z}) \wedge \varrho(\pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \varrho(\pi'\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\}$

≀$\langle \pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]$ so, by def. Section **4.2** of program labelling, $\mathsf{after}[\![\mathsf{S}]\!] \neq \mathsf{at}[\![\mathsf{S}_b]\!]$ cannot appear in $\mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''$. Therefore, by def. (6.6) of ϱ and (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]\ell$, $\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]) = \varrho(\pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'')$ and $\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'\ell, \ell\pi'_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]) = \varrho(\pi'\ell\pi'_2\ell)$. We conclude by def. (47.18) of diff∫

$\subseteq \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!], \pi'\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \;.\; \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle \pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\forall \mathsf{z} \in \mathbb{V}\setminus\{\mathsf{x}\} \;.\; \varrho(\pi\ell)\mathsf{z} = \varrho(\pi'\ell)\mathsf{z}) \wedge \varrho(\pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \varrho(\pi'\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\} \urcorner \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$

≀since if $\mathsf{x} \notin \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$ then $\mathsf{x} \in \mathsf{det}(\mathsf{B}, \neg\mathsf{B})$ so by (47.48), $\mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\ell) = \mathsf{tt}$ and $\mathcal{B}[\![\neg\mathsf{B}]\!]\varrho(\pi'\ell) = \mathsf{tt}$ imply $\varrho(\pi\ell)\mathsf{x} = \varrho(\pi'\ell)\mathsf{x}$ which, together with $\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \;.\; \varrho(\pi\ell)\mathsf{z} = \varrho(\pi'\ell)\mathsf{z}$, implies that $\varrho(\pi\ell) = \varrho(\pi'\ell)$, in contradiction with $\mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi\ell) = \mathsf{tt}$ and $\mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi'\ell) = \mathsf{ff}$∫

$= \bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!], \pi'\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \;.\; \langle \pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\} \;.\; \varrho(\pi\ell)\mathsf{z} = \varrho(\pi'\ell)\mathsf{z}) \wedge \varrho(\pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \varrho(\pi'\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\} \urcorner \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$

≀def. ∪∫

$\subseteq \bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} (\{\langle \mathsf{x},\ \mathsf{x}\rangle \mid \mathsf{x} \in \mathbb{V}\} \cup \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \mathsf{x} \in \mathbb{V} \wedge \mathsf{y} \in \mathsf{mod}[\![\mathsf{S}_b]\!]\}) \urcorner \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$

$\wr$since if $\mathsf{y} \neq \mathsf{x}$ then $\varrho(\pi\ell)\mathsf{y} = \varrho(\pi'\ell)\mathsf{y} = \varrho(\pi'\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y}$ so for the value of y to be different in $\varrho(\pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]) = \varrho(\pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'') = \varrho(\pi'\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'')$, y must be modified during the execution $\mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''$ of S_b. A coarse approximation is to consider that variable y appears to the left of an assignment in S_b, a necessary condition for y to be modified by the execution of S_b where the set $\mathsf{mod}[\![\mathsf{S}]\!]$ of variables that may be modified by the execution of S is syntactically defined as in (47.50). $\wr$

$(\mathbb{1}_{\mathbb{V}} \cup \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \mathsf{x} \in \mathbb{V} \wedge \mathsf{y} \in \mathsf{mod}[\![\mathsf{S}_b]\!]\})\ \rceil\ \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$ $\wr$def. identity relation $\mathbb{1}$ and $\cup\wr$

$= \mathbb{1}_{\mathsf{nondet}(\mathsf{B},\neg\mathsf{B})} \cup (\mathsf{nondet}(\mathsf{B}, \neg\mathsf{B}) \times \mathsf{mod}[\![\mathsf{S}_b]\!])$ $\wr$def. $\rceil\wr$

– Summing up for cases (3–B–B) and (3–B–C), we get
$(5) \subseteq \alpha^{\mathrm{d}}(\{X\})\ell \,;\Big(\Big(\bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\boldsymbol{\mathcal{S}}}^{\exists}_{\mathrm{diff}}[\![\mathsf{S}_b]\!]\ell''\Big)\rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})\Big) \cup \mathbb{1}_{\mathsf{nondet}(\mathsf{B},\neg\mathsf{B})} \cup (\mathsf{nondet}(\mathsf{B}, \neg\mathsf{B}) \times \mathsf{mod}[\![\mathsf{S}_b]\!])$.

— Summing up for all subcases of (3) for a dependency observation point $\ell' = \mathsf{after}[\![\mathsf{S}]\!]$, we would get a term (47.65.c) of the form

$$\begin{aligned}
&(\!|\ \ell' = \mathsf{after}[\![\mathsf{S}]\!] \ ?\ (\mathbb{1}_{\mathsf{nondet}(\neg\mathsf{B},\neg\mathsf{B})} \cup X(\ell) \cup \\
&\quad (X(\ell) \,; (\mathbb{1}_{\mathsf{nondet}(\neg\mathsf{B},\neg\mathsf{B})} \cup \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B}) \times \mathsf{mod}[\![\mathsf{S}_b]\!]))\ \rceil\ \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B}) \cup \\
&\qquad X(\ell) \,; \Big(\Big(\bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\boldsymbol{\mathcal{S}}}^{\exists}_{\mathrm{diff}}[\![\mathsf{S}_b]\!]\ \ell''\Big)\ \rceil\ \mathsf{nondet}(\mathsf{B}, \mathsf{B})\Big) \cup \\
&\qquad\quad \mathbb{1}_{\mathsf{nondet}(\mathsf{B},\neg\mathsf{B})} \cup (\mathsf{nondet}(\mathsf{B}, \neg\mathsf{B}) \times \mathsf{mod}[\![\mathsf{S}_b]\!]))\ :\ \varnothing\ |\!).
\end{aligned} \tag{47.65.c$'$}$$

that can be simplified as follows (while loosing precision)

(5)

$\subseteq \mathbb{1}_{\mathsf{nondet}(\neg\mathsf{B},\neg\mathsf{B})} \cup \alpha^{\mathrm{d}}(\{X\})\ell \cup (\alpha^{\mathrm{d}}(\{X\})\ \ell \,; (\mathbb{1}_{\mathsf{nondet}(\neg\mathsf{B},\neg\mathsf{B})} \cup \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B}) \times \mathsf{mod}[\![\mathsf{S}_b]\!]))\ \rceil\ \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B}) \cup \alpha^{\mathrm{d}}(\{X\})\ell \,; \Big(\Big(\bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\boldsymbol{\mathcal{S}}}^{\exists}_{\mathrm{diff}}[\![\mathsf{S}_b]\!]\ \ell''\Big)\ \rceil\ \mathsf{nondet}(\mathsf{B}, \mathsf{B})\Big) \cup \mathbb{1}_{\mathsf{nondet}(\mathsf{B},\neg\mathsf{B})} \cup (\mathsf{nondet}(\mathsf{B}, \neg\mathsf{B}) \times \mathsf{mod}[\![\mathsf{S}_b]\!])$

$\subseteq \mathbb{1}_{\mathbb{V}} \cup \alpha^{\mathrm{d}}(\{X\})\ell \cup (\alpha^{\mathrm{d}}(\{X\})\ \ell \,; (\mathbb{1}_{\mathbb{V}} \cup \mathbb{V} \times \mathsf{mod}[\![\mathsf{S}_b]\!])) \cup \alpha^{\mathrm{d}}(\{X\})\ell \,; \Big(\Big(\bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\boldsymbol{\mathcal{S}}}^{\exists}_{\mathrm{diff}}[\![\mathsf{S}_b]\!]\ \ell''\Big)\ \rceil\ \mathsf{nondet}(\mathsf{B}, \mathsf{B})\Big) \cup \mathbb{1}_{\mathbb{V}} \cup (\mathbb{V} \times \mathsf{mod}[\![\mathsf{S}_b]\!])$

$\wr$since $\mathsf{nondet}(\mathsf{B}_1, \mathsf{B}_2) \subseteq \mathbb{V}$ so $\mathbb{1}_{\mathsf{nondet}(\mathsf{B}_1,\mathsf{B}_2)} \subseteq \mathbb{1}_{\mathbb{V}}$ and def. $\rceil\wr$

$$\subseteq \mathbb{1}_{\mathbb{V}} \cup \alpha^{\mathsf{d}}(\{X\})\ell \cup (\alpha^{\mathsf{d}}(\{X\})\ \ell \fatsemi \mathbb{1}_{\mathbb{V}}) \cup (\alpha^{\mathsf{d}}(\{X\})\ \ell \fatsemi \mathbb{V} \times \mathsf{mod}[\![\mathsf{S}_b]\!]) \cup \alpha^{\mathsf{d}}(\{X\})\ell \fatsemi \Big(\Big(\bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\widehat{\mathcal{S}}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell''\Big) \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})\Big) \cup \mathbb{1}_{\mathbb{V}} \cup (\mathbb{V} \times \mathsf{mod}[\![\mathsf{S}_b]\!])$$

$$\wr \text{since } \fatsemi \text{ distributes over } \cup \wr$$

$$= \mathbb{1}_{\mathbb{V}} \cup \alpha^{\mathsf{d}}(\{X\})\ell \cup \big((\mathbb{1}_{\mathbb{V}} \cup \alpha^{\mathsf{d}}(\{X\})\ell) \fatsemi (\mathbb{V} \times \mathsf{mod}[\![\mathsf{S}_b]\!])\big) \cup \alpha^{\mathsf{d}}(\{X\})\ell \fatsemi \Big(\Big(\bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\widehat{\mathcal{S}}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell''\Big) \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})\Big)$$

$$\wr \text{idempotency law for } \cup \text{ and } \fatsemi \text{ distributes over } \cup \wr$$

After simplification, we get a term (47.65.c) of the form

$$(\!|\ \ell' = \mathsf{after}[\![\mathsf{S}]\!]\ ?\ \mathbb{1}_{\mathbb{V}} \cup X(\ell) \cup \big((\mathbb{1}_{\mathbb{V}} \cup X(\ell)) \fatsemi (\mathbb{V} \times \mathsf{mod}[\![\mathsf{S}_b]\!])\big) \cup X(\ell) \fatsemi \Big(\Big(\bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\widehat{\mathcal{S}}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell''\Big) \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})\Big) \,\text{:}\, \varnothing\ |\!).$$

For fixpoints X of $\mathscr{F}^{\mathsf{diff}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]$, we have $\mathbb{1}_{\mathbb{V}} \subseteq X(\ell)$ by (47.65.a) so that, by the chaotic iteration theorem [1, 2], $\mathbb{1}_{\mathbb{V}} \cup X(\ell)$ can be replaced by $X(\ell)$. We get a term (47.65.c) of the form

$$(\!|\ \ell' = \mathsf{after}[\![\mathsf{S}]\!]\ ?\ X(\ell) \cup \big(X(\ell \fatsemi (\mathbb{V} \times \mathsf{mod}[\![\mathsf{S}_b]\!])\big) \cup X(\ell) \fatsemi \Big(\Big(\bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!]} \widehat{\widehat{\mathcal{S}}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell''\Big) \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})\Big) \,\text{:}\, \varnothing\ |\!).$$

— Summing up for all cases (1), (2), and (3) for all dependency observation points, we conclude that

$$\forall \ell' \in \mathsf{labx}[\![\mathsf{S}]\!]\ .\ \alpha^{\mathsf{d}}(\{\mathscr{F}^{*}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!](X)\})\ \ell' \subseteq \mathscr{F}^{\mathsf{diff}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \texttt{S}_b]\!]\ \alpha^{\mathsf{d}}(\{X\})\ \ell'$$

proving pointwise semi-commutation. □

5 Mathematical proofs of chapter 48

Proof of Lemma 48.62 By induction on the sequence of calls to unify. We proceed by by calculational design and case analysis on the structure of $\boldsymbol{\tau}_1$ and $\boldsymbol{\tau}_2$ which can be a variable or a structured term and may belong to the domain of ϑ_0, or not.

- If $\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0) = \Omega^{\mathsf{r}}_{\mathsf{s}}$ in case (48.47.8) of an occur-check, we have $\gamma^{\mathsf{r}}_{\mathsf{s}}(\Omega^{\mathsf{r}}_{\mathsf{s}}) = \varnothing$ by (48.46). By the test (48.47.8), $\alpha \in \mathbb{vars}[\![\boldsymbol{\tau}_2]\!]$. If $\boldsymbol{\tau}_2 = \beta \in \mathbb{V}_{\mathfrak{t}}$ were a variable then the test $\alpha \in \mathbb{vars}[\![\boldsymbol{\tau}_2]\!]$ at (48.47.8) would be true only if $\alpha = \beta$ but this case is prevented by the test (48.47.7). By contradiction, $\boldsymbol{\tau}_2 \notin \mathbb{V}_{\mathfrak{t}}$ in case (48.47.8). It follows, by def. (48.50) of γ_{e} that $\gamma_{\mathsf{e}}(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) = \gamma_{\mathsf{e}}(\alpha \doteq \boldsymbol{\tau}_2) = \varnothing$ since otherwise, there would be some $\boldsymbol{\varrho}$ such that $\boldsymbol{\varrho}(\boldsymbol{\tau}_1) = \boldsymbol{\varrho}(f(\ldots\alpha\ldots))$ which would be an infinite object not in $\mathbf{P}^{\mathsf{v}}$, as shown in Lemma 48.9.

- By Lemma 48.57, unify does terminate so that, in case (48.47.6) with $\vartheta_n = \Omega^{\mathsf{r}}_{\mathsf{s}}$ there must be a series of recursive calls ending up in (48.47.8). So $\boldsymbol{\tau}_1$ or $\boldsymbol{\tau}_2$ has a recursive subterm which, again by Lemma 48.9, implies $\gamma^{\mathsf{r}}_{\mathsf{s}}(\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0)) = \gamma^{\mathsf{r}}_{\mathsf{s}}(\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0)) = \gamma^{\mathsf{r}}_{\mathsf{s}}(\Omega^{\mathsf{r}}_{\mathsf{s}}) = \varnothing$;

- In case (48.47.6) with $\vartheta_n \neq \Omega^{\mathsf{r}}_{\mathsf{s}}$, we have,

$$
\begin{aligned}
& \gamma_{\mathsf{e}}(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0) \\
= {} & \gamma_{\mathsf{e}}(f(\boldsymbol{\tau}^1_1, \ldots, \boldsymbol{\tau}^n_1) \doteq g(\boldsymbol{\tau}^1_2, \ldots, \boldsymbol{\tau}^m_2)) \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0) && \text{≀test (48.47.1) is } \mathsf{tt} \text{≀} \\
= {} & \gamma_{\mathsf{e}}(f(\boldsymbol{\tau}^1_1, \ldots, \boldsymbol{\tau}^n_1) \doteq f(\boldsymbol{\tau}^1_2, \ldots, \boldsymbol{\tau}^n_2)) \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0) && \text{≀test (48.47.2) is } \mathsf{ff} \text{≀} \\
= {} & \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(f(\boldsymbol{\tau}^1_1, \ldots, \boldsymbol{\tau}^n_1)) = \boldsymbol{\varrho}(f(\boldsymbol{\tau}^1_2, \ldots, \boldsymbol{\tau}^n_2))\} \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0) && \text{≀def. (48.50) of } \gamma_{\mathsf{e}} \text{≀} \\
= {} & \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \bigwedge_{i=1}^{n} \boldsymbol{\varrho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\varrho}(\boldsymbol{\tau}^i_2)\} && \text{≀def. (48.7) of assignment application≀} \\
= {} & \bigcap_{i=1}^{n} \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\varrho}(\boldsymbol{\tau}^i_2)\} \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0) && \text{≀def.} \textstyle\bigcap \text{≀} \\
= {} & (\{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\varrho}(\boldsymbol{\tau}^1_2)\} \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0)) \cap \bigcap_{2=1}^{n} \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\varrho}(\boldsymbol{\tau}^i_2)\} \\
& && \text{≀} \textstyle\bigcap \text{ is associative and commutative≀} \\
= {} & (\gamma_{\mathsf{e}}(\boldsymbol{\tau}^1_i) \doteq \boldsymbol{\tau}^1_2) \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0)) \cap \bigcap_{2=1}^{n} \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\boldsymbol{\tau}^1_i = \boldsymbol{\varrho}(\boldsymbol{\tau}^i_2)\} && \text{≀def. (48.50)x of } \gamma_{\mathsf{e}} \text{≀} \\
= {} & \mathsf{let}\ \vartheta_1 = \mathsf{unify}(\boldsymbol{\tau}^1_i, \boldsymbol{\tau}^1_2, \vartheta_0)\ \mathsf{in} \\
& \quad \bigcap_{2=1}^{n} \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\varrho}(\boldsymbol{\tau}^i_2)\} \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_1) && \text{≀ind. hyp. and} \textstyle\bigcap \text{ commutative≀} \\
= {} & \mathsf{let}\ \vartheta_1 = \mathsf{unify}((\boldsymbol{\tau}^1_i, \boldsymbol{\tau}^1_2, \vartheta_0)\ \mathsf{in} \\
& \quad \ldots \\
& \qquad \mathsf{let}\ \vartheta_j = \mathsf{unify}(\boldsymbol{\tau}^j_i, \boldsymbol{\tau}^j_2, \vartheta_{j-1})\ \mathsf{in} \\
& \qquad \quad \bigcap_{i=j+1}^{n} \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\varrho}(\boldsymbol{\tau}^i_2)\} \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_j) && \text{≀recurrence hyp., } j < n \text{≀} \\
= {} & \mathsf{let}\ \vartheta_1 = \mathsf{unify}(\boldsymbol{\tau}^1_i, \boldsymbol{\tau}^1_2, \vartheta_0)\ \mathsf{in} \\
& \quad \ldots \\
& \qquad \mathsf{let}\ \vartheta_j = \mathsf{unify}(\boldsymbol{\tau}^j_i, \boldsymbol{\tau}^j_2, \vartheta_{j-1})\ \mathsf{in} \\
& \qquad \quad \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\boldsymbol{\tau}^{j+1}_i) = \boldsymbol{\varrho}(\boldsymbol{\tau}^{j+1}_2)\} \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_j) \cap \\
& \qquad \qquad \bigcap_{i=j+2}^{n} \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\varrho}(\boldsymbol{\tau}^i_2)\} && \text{≀} \textstyle\bigcap \text{ is associative and commutative≀}
\end{aligned}
$$

$$
\begin{aligned}
= \;& \mathsf{let}\ \vartheta_1 = \mathsf{unify}(\boldsymbol{\tau}_i^1, \boldsymbol{\tau}_2^1, \vartheta_0)\ \mathsf{in} \\
& \quad \ldots \\
& \quad\ \mathsf{let}\ \vartheta_j = \mathsf{unify}(\boldsymbol{\tau}_i^j, \boldsymbol{\tau}_2^j, \vartheta_{j-1})\ \mathsf{in} \\
& \quad\quad \mathsf{let}\ \vartheta_{j+1} = \mathsf{unify}(\boldsymbol{\tau}_i^{j+1}, \boldsymbol{\tau}_2^{j+1}, \vartheta_j)\ \mathsf{in} \\
& \quad\quad\quad \bigcap_{i=j+2}^{n} \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\boldsymbol{\tau}_i^1) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2^i)\} \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_{j+1}) && \text{(ind. hyp. and } \textstyle\bigcap \text{ commutative)} \\
= \;& \mathsf{let}\ \vartheta_1 = \mathsf{unify}(\boldsymbol{\tau}_i^1, \boldsymbol{\tau}_2^1, \vartheta_0)\ \mathsf{in} \\
& \quad \ldots \\
& \quad\ \mathsf{let}\ \vartheta_j = \mathsf{unify}(\boldsymbol{\tau}_i^n, \boldsymbol{\tau}_2^n, \vartheta_{n-1})\ \mathsf{in} \\
& \quad\quad \bigcap_{i=n+2}^{n} \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\boldsymbol{\tau}_i^1) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2^i)\} \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_n) && \text{(by recurrence when } j+1=n\text{)} \\
= \;& \mathsf{let}\ \vartheta_1 = \mathsf{unify}(\boldsymbol{\tau}_i^1, \boldsymbol{\tau}_2^1, \vartheta_0)\ \mathsf{in} \\
& \quad \ldots \\
& \quad\ \mathsf{let}\ \vartheta_j = \mathsf{unify}(\boldsymbol{\tau}_i^n, \boldsymbol{\tau}_2^n, \vartheta_{n-1})\ \mathsf{in} \\
& \quad\quad \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_n) \\
& && \text{(since } \textstyle\bigcap_{i=n+2}^{n}\{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\boldsymbol{\tau}_i^1) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2^i)\} = \bigcap\varnothing = \mathbf{P}^\nu \text{ is the identity for } \cap\text{)}
\end{aligned}
$$

- In case (48.47.7), we have

$$
\begin{aligned}
& \gamma_{\mathsf{e}}(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) \\
= \;& \gamma_{\mathsf{e}}(\alpha \doteq \alpha) \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) && \text{(}\alpha \in \mathbb{V}_{\mathfrak{t}} \text{ by test (48.47.7))} \\
= \;& \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\alpha)\} \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) && \text{(def. (48.50) of } \gamma_{\mathsf{e}}\text{)} \\
= \;& \mathbf{P}^\nu \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) && \text{(since } \boldsymbol{\varrho} \in \mathbf{P}^\nu \triangleq \mathbb{V}_{\mathfrak{t}} \to \mathbf{T} \text{ by (48.6))} \\
= \;& \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) && \text{(}\mathbf{P}^\nu \text{ is the identity for } \cap\text{)} \\
= \;& \gamma_{\mathsf{s}}^{\mathsf{r}}(\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0)) && \text{(def. } \mathsf{unify} \text{ in case (48.47.7))}
\end{aligned}
$$

- In case (48.47.11), we have

$$
\begin{aligned}
& \gamma_{\mathsf{e}}(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) \\
= \;& \gamma_{\mathsf{e}}(\alpha \doteq \boldsymbol{\tau}_2) \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) \\
& \text{(where } \alpha \in \mathbb{V}_{\mathfrak{t}} \text{ by test (48.47.9), } \alpha \notin \mathbb{vars}[\![\boldsymbol{\tau}_2]\!] \text{ since test (48.47.8) is ff, } \alpha \notin \mathsf{dom}(\vartheta_0) \text{ by} \\
& \text{test (48.47.10), and } \boldsymbol{\tau}_2 \notin \mathbb{V}_{\mathfrak{t}} \text{ since test (48.47.1) is ff)} \\
= \;& \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2)\} \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) && \text{(def. (48.50) of } \gamma_{\mathsf{e}}\text{)} \\
= \;& \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2)\} \cap \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\vartheta_0(\beta))\} && \text{(def. (48.51) of } \gamma_{\mathsf{s}}^{\mathsf{r}}\text{)} \\
= \;& \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2) \wedge \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\vartheta_0(\beta))\} && \text{(def. } \cap\text{)} \\
= \;& \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = (\!|\, \beta = \alpha \;?\; \boldsymbol{\varrho}(\vartheta_0(\beta)[\beta \in \mathbb{vars}[\![\boldsymbol{\tau}_2]\!] \leftarrow \boldsymbol{\tau}_2]) \;:\; \boldsymbol{\varrho}(\boldsymbol{\tau}_2[\alpha \leftarrow \vartheta_0(\beta)]) \,|\!)\}
\end{aligned}
$$

$\wr$def. (48.7) of assignment application where $\boldsymbol{\varrho}(\alpha)$ is replaced by its equal $\boldsymbol{\varrho}(\boldsymbol{\tau}_2)$ and for $\beta \in \mathbb{V}_{\mathfrak{t}} \setminus \{\alpha\}$, $\boldsymbol{\varrho}(\beta)$ is replaced by its equal $\boldsymbol{\varrho}(\vartheta_0(\beta))\wr$

$$
\begin{aligned}
&= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = (\!\!| \beta = \alpha \mathbin{?} \boldsymbol{\varrho}(\vartheta_0(\beta)[\beta \in \mathsf{vars}[\![\boldsymbol{\tau}_2]\!] \leftarrow \boldsymbol{\tau}_2]) \mathbin{⸽} \boldsymbol{\varrho}(\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\}(\vartheta_0(\beta))) |\!\!)\} \\
&\hspace{20em} \wr\text{by Exercise 48.59 where } \boldsymbol{\tau}' = \vartheta_0(\beta)\wr \\
&= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = (\!\!| \beta = \alpha \mathbin{?} \boldsymbol{\varrho}(\vartheta_0(\boldsymbol{\tau}_2)) \mathbin{⸽} \boldsymbol{\varrho}(\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\}(\vartheta_0(\beta))) |\!\!)\} \quad \wr\text{by Exercise 48.61}\wr \\
&= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}((\!\!| \beta = \alpha \mathbin{?} \vartheta_0(\boldsymbol{\tau}_2) \mathbin{⸽} (\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\} \circ \vartheta_0)(\beta) |\!\!))\} \\
&\hspace{16em} \wr\text{def. conditional and function composition } \circ\wr \\
&= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}((\!\!| \beta = \alpha \mathbin{?} (\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\} \circ \vartheta_0)(\alpha) \mathbin{⸽} (\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\} \circ \vartheta_0)(\beta) |\!\!))\} \\
&\hspace{4em} \wr\text{since } X \notin \mathsf{dom}(\vartheta_0) \text{ so } (\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\} \circ \vartheta_0)(\alpha) = \{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\}(\vartheta_0(\alpha)) = \{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\}(\alpha) = \boldsymbol{\tau}_2\wr \\
&= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\} \circ \vartheta_0)(\beta) \qquad \wr\text{def. conditional}\wr \\
&= \gamma^{\mathsf{r}}_{\mathsf{s}}\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\} \circ \vartheta_0 \qquad \wr\text{def. (48.51) of } \gamma^{\mathsf{r}}_{\mathsf{s}}\wr \\
&= \gamma^{\mathsf{r}}_{\mathsf{s}}(\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0)) \qquad \wr(48.47.11)\wr
\end{aligned}
$$

- In case (48.47.12), we have $\boldsymbol{\tau}_1 = \alpha \in \mathsf{dom}(\vartheta_0)$ by tests (48.47.9) and (48.47.10) and $\boldsymbol{\tau}_2 \notin \mathbb{V}_{\mathfrak{t}}$ since test (48.47.1) is ff.

$$
\begin{aligned}
&\gamma_{\mathsf{e}}(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0) \\
&= \gamma_{\mathsf{e}}(\alpha \doteq \boldsymbol{\tau}_2) \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0) \qquad \wr\boldsymbol{\tau}_1 = \alpha\wr \\
&= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2) \wedge \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\vartheta_0(\beta))\} \\
&\hspace{16em} \wr\text{def. (48.50) of } \gamma_{\mathsf{e}}\text{, (48.51) of } \gamma^{\mathsf{r}}_{\mathsf{s}}\text{, and def. } \cap\wr \\
&= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\vartheta_0(\alpha)) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2) \wedge \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\vartheta_0(\beta))\} \\
&\hspace{16em} \wr\alpha \in \mathsf{dom}(\vartheta_0) \text{ so } \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\vartheta_0(\beta)) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2)\wr \\
&= \gamma_{\mathsf{e}}(\vartheta_0(\alpha) \doteq \boldsymbol{\tau}_2) \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0) \qquad \wr\text{def. (48.50) of } \gamma_{\mathsf{e}}\text{, (48.51) of } \gamma^{\mathsf{r}}_{\mathsf{s}}\text{, and def. } \cap\wr \\
&= \gamma^{\mathsf{r}}_{\mathsf{s}}(\mathsf{unify}(\vartheta_0(\alpha), \boldsymbol{\tau}_2, \vartheta_0)) \qquad \wr\text{ind. hyp. of Lemma 48.62}\wr \\
&= \gamma^{\mathsf{r}}_{\mathsf{s}}(\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0)) \qquad \wr(48.47.12)\wr
\end{aligned}
$$

- In case (48.47.13) we are back to (48.47.11) or (48.47.12) by the symmetry argument of Remark 48.48. □

The following Lemma 11 shows that new entries are successively added to the table T_0.

Lemma 11 For all $\boldsymbol{\tau}^0_1, \boldsymbol{\tau}^0_2 \in \mathbf{T}^{\nu}$, if $\mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0)$ is (recursively) called from the main call $\mathsf{lcg}(\boldsymbol{\tau}^0_1, \boldsymbol{\tau}^0_2)$ and returns $\langle\boldsymbol{\tau},\ T'\rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0)$, then

$$\begin{array}{ll}\text{preinvariant:} & \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \in \mathbf{T}^\nu \wedge T_0 \in \mathbb{V} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu \\ \text{postinvariant:} & \boldsymbol{\tau} \in \mathbf{T}^\nu \wedge T' \in \mathbb{V} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu \wedge \mathsf{vars}[\![\boldsymbol{\tau}]\!] \subseteq \mathsf{dom}(T') \wedge \\ & \quad \forall \alpha \in \mathsf{dom}(T_0) \,.\, T_0(\alpha) = T'(\alpha)\end{array} \tag{12}$$

□

Proof of Lemma 11 By induction on the sequence of calls to lub and, for any given call, by recurrence to handle the recursive calls at (48.67.2), …, (48.67.4), and by case analysis on the conditional.

The first call at (48.67.12) satisfies the preinvariant of (48.39) since $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0 \in \mathbf{T}^\nu$ by hypothesis and $T_0 = \varnothing \in \mathbb{V} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu$;

Assuming that an intermediate call to $\mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0)$ satisfies the preinvariant (48.39), the proof that it satisfies the postinvariant (48.39) is by case analysis.

- In case (48.67.5), $\boldsymbol{\tau}_j \in \mathbf{T}^\nu$ by hypothesis on the intermediate call, so $\boldsymbol{\tau}_j^i \in \mathbf{T}^\nu$, $i = 1, \dots, n$, $j = 1, 2$, by the test (48.67.1). Then we proceed by recurrence on the recursive calls.
  - For the basis $i = 0$, T_0 satisfies (48.39) by hypothesis on the intermediate call;
  - Assume, by recurrence hypothesis for $i \in [0, n[$, that $T_i \in \mathbb{V} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu \wedge \forall \alpha \in \mathsf{dom}(T_0) \,.\, T_0(\alpha) = T_i(\alpha)$. Then, by induction on the sequence of calls to lub, $\boldsymbol{\tau}^{i+1} \in \mathbf{T}^\nu$ and $T_{i+1} \in \mathbb{V} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu \wedge \mathsf{vars}[\![\boldsymbol{\tau}^{i+1}]\!] \subseteq \mathsf{dom}(T_{i+1}) \wedge \forall \alpha \in \mathsf{dom}(T_i) \,.\, T_i(\alpha) = T_{i+1}(\alpha)$. By transitivity, $\forall \alpha \in \mathsf{dom}(T_0) \,.\, T_0(\alpha) = T_{i+1}(\alpha)$.≤□

  By recurrence for $i = n$, $T' = T_n$ at (48.67.5) satisfies (48.39) since $\boldsymbol{\tau}^i \in \mathbf{T}^\nu$, $i = 1, \dots, n$, implies $f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n) \in \mathbf{T}^\nu$ and $\mathsf{vars}[\![f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)]\!] = \bigcup_{i=1}^n \mathsf{vars}[\![\boldsymbol{\tau}^i]\!]$;
- The case (48.67.7) is trivial since $\beta \in \mathbf{T}^\nu$, $T' = T_0$, and $\beta \in \mathsf{dom}(T_0)$;
- In case (48.67.9), $T_0 \in \mathbb{V} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu$ by hypothesis, $\beta \in \mathbf{T}^\nu$, and $\beta \in \mathbb{V} \setminus \mathsf{dom}(T_0)$ by the test (48.67.8) so $T' = \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0] \in \mathbb{V} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu$ and for all $\alpha \in \mathsf{dom}(T_0)$, $\alpha \neq \beta$ so $T'(\alpha) = \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0](\alpha) = T_0(\alpha)$. Moreover $\beta \in \mathsf{vars}[\![\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0]]\!] = \mathsf{vars}[\![T']\!]$. □

Remark Lemma 11 shows that T_0 can be declared as a variable local to lcg and global to lub, which would be unitialized to $\varnothing$ and updated by an assignment at (48.67.9).

For $T \in \mathbb{V} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu$, let us define, when $\alpha \in \mathsf{dom}(T)$,

$$\begin{array}{lcl}\bar{\varsigma}_1(T)\alpha & \triangleq & \mathsf{let}\ \langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle = T(\alpha)\ \mathsf{in}\ \boldsymbol{\tau}_1 \\ \bar{\varsigma}_2(T)\alpha & \triangleq & \mathsf{let}\ \langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle = T(\alpha)\ \mathsf{in}\ \boldsymbol{\tau}_2\end{array} \tag{13}$$

(which is undefined when $\alpha \notin \mathsf{dom}(T)$ in which case (48.30) applies, in particular when $T = \varnothing$).

The following Lemma 14 shows that table T_0 maintains two substitutions $\bar{\varsigma}_1(T)$ and $\bar{\varsigma}_1(T)$ which can be used to instantiate the term resulting from the call to the parameters.

Lemma 14 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \in \mathbf{T}^\nu$ and $T_0 \in \wp(\mathbb{V} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, if $\mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0)$ is (recursively) called from the main call $\mathsf{lcg}(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0)$ and returns $\langle \boldsymbol{\tau},\ T' \rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0)$, then

$$\bar{\varsigma}_1(T')\boldsymbol{\tau} \quad = \quad \boldsymbol{\tau}_1 \quad \text{and} \quad \bar{\varsigma}_2(T')\boldsymbol{\tau} \quad = \quad \boldsymbol{\tau}_2 \tag{15}$$ □

Proof of Lemma 14 The preinvariant is tt. By induction on the sequence of calls to lub and, for any given call, by recurrence to handle the recursive calls at (48.67.2), …, (48.67.4), and by case analysis for the conditional.

- In case (48.67.5), by recurrence and induction on the sequence of recursive calls to leq, we have $\bar{\varsigma}_1(T_i)\boldsymbol{\tau}^i \ = \ \boldsymbol{\tau}_1^i$ and $\bar{\varsigma}_2(T_i)\boldsymbol{\tau}^i \ = \ \boldsymbol{\tau}_2^i$ for all $i \in [1, n]$. By the postinvariant of (48.39), we have $\forall \alpha \in \mathsf{dom}(T_i)\ .\ T_0(\alpha) = T_{i+1}(\alpha)$. It follows, by (13) that $\forall \alpha \in \mathbb{vars}[\![\boldsymbol{\tau}^i]\!] \subseteq \mathsf{dom}(T_i)\ .\ T_i(\alpha) = T_{i+1}(\alpha)$. Therefore, by (13), $\forall \alpha \in \mathbb{vars}[\![\boldsymbol{\tau}^i]\!]\ .\ \vartheta_j(T_{i+1})(\boldsymbol{\tau}^i) = \vartheta_j(T_i)(\boldsymbol{\tau}^i)$. It follows by (48.30) that $\vartheta_j(T_n)(f(\boldsymbol{\tau}^1, \boldsymbol{\tau}^2, \ldots, \boldsymbol{\tau}^n)) = f(\vartheta_j(T_n)(\boldsymbol{\tau}^1), \vartheta_j(T_n)(\boldsymbol{\tau}^2), \ldots, \vartheta_j(T_n)(\boldsymbol{\tau}^n)) = f(\vartheta_j(T_1)(\boldsymbol{\tau}^1), \vartheta_j(T_2)(\boldsymbol{\tau}^2), \ldots, \vartheta_j(T_n)(\boldsymbol{\tau}^n)) = f(\boldsymbol{\tau}_j^1, \ldots, \boldsymbol{\tau}_j^n) = \boldsymbol{\tau}_j$, $j = 1, 2$;
- In case (48.67.7), (15) directly follows from $\boldsymbol{\tau} = \beta$, $T' = T_0$, $\beta \in \mathsf{dom}(T_0)$, $T_0(\beta) = \langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle$, and (13);
- In case (48.67.9), $\bar{\varsigma}_j(T')\boldsymbol{\tau} = \vartheta_j(\langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])\beta = \mathsf{if}\ \beta \in \mathsf{dom}(T)\ \mathsf{then\ let}\ \langle \boldsymbol{\tau}_1',\ \boldsymbol{\tau}_2' \rangle = \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0](\beta)\ \mathsf{in}\ \boldsymbol{\tau}_j'\ \mathsf{else}\ \alpha = \boldsymbol{\tau}_j$, $j = 1, 2$. □

$\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)$ computes an upper-bound of $\boldsymbol{\tau}_1$ and $\boldsymbol{\tau}_2$.

Lemma 16 For all $\boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \in \mathbf{T}^\nu$, the lgc algorithm terminates with $[\boldsymbol{\tau}_1]_{\simeq^\nu} \preceq_{\simeq^\nu} [\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)]_{\simeq^\nu}$ and $[\boldsymbol{\tau}_2]_{\simeq^\nu} \preceq_{\simeq^\nu} [\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)]_{\simeq^\nu}$. □

Proof of Lemma 16 The termination proof of $\mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0)$ is by structural induction on $\boldsymbol{\tau}_1$ (or $\boldsymbol{\tau}_2$). So the main call $\mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \varnothing)$ at (48.67.12) does terminate.

Lemma 16 follows by def. of the infimum $\overline{\varnothing}^\nu$ in cases (48.67.11).

Otherwise, at (48.67.12), $\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2) = \boldsymbol{\tau}$ where $\langle \boldsymbol{\tau},\ T \rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \varnothing)$. By (48.42), $\bar{\varsigma}_j(T)\boldsymbol{\tau} = \boldsymbol{\tau}_j$, $j = 1, 2$. So by Exercise 48.16, $[\boldsymbol{\tau}_j]_{\simeq^\nu} \preceq_{\simeq^\nu} [\boldsymbol{\tau}]_{\simeq^\nu} = [\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)]_{\simeq^\nu}$. □

Let $[\boldsymbol{\tau}']_{\simeq^\nu}$ be an upper bound of $[\boldsymbol{\tau}_1]_{\simeq^\nu}$ and $[\boldsymbol{\tau}_2]_{\simeq^\nu}$ i.e. $\boldsymbol{\tau}_1 \preceq_{\simeq^\nu} \boldsymbol{\tau}'$ and $\boldsymbol{\tau}_2 \preceq_{\simeq^\nu} \boldsymbol{\tau}'$ so that, by Exercise 48.16, there exists substitutions ϑ_1 and ϑ_2 such that $\vartheta_1(\boldsymbol{\tau}') = \boldsymbol{\tau}_1$ and $\vartheta_2(\boldsymbol{\tau}') = \boldsymbol{\tau}_2$. We must prove that $[\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)]_{\simeq^\nu} \preceq_{\simeq^\nu} [\boldsymbol{\tau}']_{\simeq^\nu}$ that is, by Exercise 48.16, that there exist a substitution ϑ' such that $\vartheta'(\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)) = \boldsymbol{\tau}'$.

We modify the lub algorithm into lub' (which calls lub) as follows to construct this substitution ϑ' given any upper bound $\boldsymbol{\tau}'$.

$$
\begin{array}{ll}
\text{let rec lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0) = & (17)\\
\quad \text{if } \boldsymbol{\tau}_1 = f(\boldsymbol{\tau}_1^1, \dots, \boldsymbol{\tau}_1^n) \wedge \boldsymbol{\tau}_2 = f(\boldsymbol{\tau}_2^1, \dots, \boldsymbol{\tau}_2^n) \text{ then} & (1)\\
\quad\quad \text{if } \boldsymbol{\tau}' = \gamma \in \mathbb{V} \text{ then} & (a)\\
\quad\quad\quad \text{let } \langle \boldsymbol{\tau}^1,\ T_1 \rangle = \text{lub}(\boldsymbol{\tau}_1^1, \boldsymbol{\tau}_2^1, T_0) \text{ in} & (2a)\\
\quad\quad\quad\quad \text{let } \langle \boldsymbol{\tau}^2,\ T_2 \rangle = \text{lub}(\boldsymbol{\tau}_1^2, \boldsymbol{\tau}_2^2, T_1) \text{ in} & (3a)\\
\quad\quad\quad\quad\quad \dots & \dots\\
\quad\quad\quad\quad\quad\quad \text{let } \langle \boldsymbol{\tau}^n,\ T_n \rangle = \text{lub}(\boldsymbol{\tau}_1^n, \boldsymbol{\tau}_2^n, T_{n-1}) \text{ in} & (4a)\\
\quad\quad\quad\quad\quad\quad\quad \langle f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n),\ T_n,\ f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0] \rangle & (5a)\\
\quad\quad \text{else /* } \boldsymbol{\tau}' = f(\boldsymbol{\tau}_1', \dots, \boldsymbol{\tau}_n') \text{ */} & (b)\\
\quad\quad\quad \text{let } \langle \boldsymbol{\tau}^1,\ T_1,\ \vartheta_1 \rangle = \text{lub}'(\boldsymbol{\tau}_1^1, \boldsymbol{\tau}_2^1, T_0, \boldsymbol{\tau}_1', \vartheta_0) \text{ in} & (2b)\\
\quad\quad\quad\quad \text{let } \langle \boldsymbol{\tau}^2,\ T_2,\ \vartheta_2 \rangle = \text{lub}'(\boldsymbol{\tau}_1^2, \boldsymbol{\tau}_2^2, T_1, \boldsymbol{\tau}_2', \vartheta_1) \text{ in} & (3b)\\
\quad\quad\quad\quad\quad \dots & \dots\\
\quad\quad\quad\quad\quad\quad \text{let } \langle \boldsymbol{\tau}^n,\ T_n,\ \vartheta_n \rangle = \text{lub}'(\boldsymbol{\tau}_1^n, \boldsymbol{\tau}_2^n, T_{n-1}, \boldsymbol{\tau}_n', \vartheta_{n-1}) \text{ in} & (4b)\\
\quad\quad\quad\quad\quad\quad\quad \langle f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n),\ T_n,\ \vartheta_n \rangle & (5b)\\
\quad \text{elsif } \exists \beta \in \text{dom}(T_0) \;.\; T_0(\beta) = \langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle \text{ then} \quad \text{/* } \boldsymbol{\tau}' = \gamma \in \mathbb{V} \text{ */} & (6)\\
\quad\quad \langle \beta,\ T_0,\ \vartheta_0 \rangle & (7)\\
\quad \text{else let } \beta \in \mathbb{V} \setminus \text{dom}(T_0) \text{ in} \quad \text{/* } \boldsymbol{\tau}' = \gamma \in \mathbb{V} \text{ */} & (8)\\
\quad\quad \langle \beta,\ \langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle [\beta \leftarrow T_0],\ \beta[\gamma \leftarrow \vartheta_0] \rangle & (9)\\
\text{let lcg}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2) = & (10)\\
\quad \text{if } \boldsymbol{\tau}_1 = \overline{\varnothing}^{\mathcal{V}} \text{ then } \boldsymbol{\tau}_2 & (11)\\
\quad \text{elsif } \boldsymbol{\tau}_2 = \overline{\varnothing}^{\mathcal{V}} \text{ then } \boldsymbol{\tau}_1 & (12)\\
\quad \text{else} \quad \text{/* assume } \exists \vartheta_1, \vartheta_2 \;.\; \vartheta_1(\boldsymbol{\tau}') = \boldsymbol{\tau}_1 \wedge \vartheta_2(\boldsymbol{\tau}') = \boldsymbol{\tau}_2 \text{ */} & (13)\\
\quad\quad\quad \text{let } \langle \boldsymbol{\tau},\ T,\ \vartheta' \rangle = \text{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \varnothing, \boldsymbol{\tau}', \varepsilon, \varnothing) \text{ in } \boldsymbol{\tau} \quad \text{/* } \vartheta'(\boldsymbol{\tau}') = \boldsymbol{\tau} \text{ */} & (14)
\end{array}
$$

Example 18 The assumption (17.13) prevents a call like $\text{lub}'(f(a,b), f(b,a), \varnothing, f(\alpha,\alpha), \varepsilon, \varnothing)$ where $f(\alpha,\alpha)$ is not an upper bound of $\{f(a,b), f(b,a)\}$. □

Example 19 For $\boldsymbol{\tau}_1 = f(g(a), g(g(a)), g(a), b, b)$, $\boldsymbol{\tau}_2 = f(g(b), g(h(b)), g(b), a, a)$ and $\boldsymbol{\tau}' = f(g(\alpha), \beta, g(\alpha), \gamma, U)$, we have

$$
\begin{array}{ll}
\text{lub}'(f(g(a), g(g(a)), g(a), b, b), f(g(b), g(h(b)), g(b), a, a), \varnothing, f(g(\alpha), \beta, g(\alpha), \gamma, U), \varepsilon) & \\
\quad \text{lub}'(g(a), g(b), \varnothing, g(\alpha), \varepsilon) & (17.2b)\\
\quad\quad \text{lub}'(a, b, \varnothing, \alpha, \varepsilon) & (17.2b)\\
\quad\quad = \langle \beta,\ \{\langle \beta,\ \langle a,\ b \rangle \rangle\},\ \{\langle \alpha,\ \beta \rangle\} \rangle & (17.9)\\
\quad = \langle g(\beta),\ \{\langle \beta,\ \langle a,\ b \rangle \rangle\},\ \{\langle \alpha,\ \beta \rangle\} \rangle & (17.5b)\\
\quad \text{lub}'(g(g(a)), g(h(b)), \{\langle \beta,\ \langle a,\ b \rangle \rangle\}, \beta, \{\langle \alpha,\ \beta \rangle\}) & (17.3b)\\
\quad\quad \text{lub}(g(a), h(b), \{\langle \beta,\ \langle a,\ b \rangle \rangle\}) & (17.2a)
\end{array}
$$

$= \langle \gamma,\ \{\langle \beta,\ \langle a,\ b\rangle\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle\}\rangle$

$= \langle g(\gamma),\ \{\langle \beta,\ \langle a,\ b\rangle\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle\},\ \{\langle \alpha,\ \beta\rangle, \langle \beta,\ g(\gamma)\rangle\}\rangle$ (17.5a)

$\mathsf{lub}'(g(a), g(b), \{\langle \beta,\ \langle a,\ b\rangle\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle\}, g(\alpha), \{\langle \alpha,\ \beta\rangle, \langle \beta,\ g(\gamma)\rangle\})$ (17.4b)

$\mathsf{lub}'(a, b, \{\langle \beta,\ \langle a,\ b\rangle\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle\}, \alpha, \{\langle \alpha,\ \beta\rangle, \langle \beta,\ g(\gamma)\rangle\})$ (17.6)

$= \langle \beta,\ \{\langle \beta,\ \langle a,\ b\rangle\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle\},\ \{\langle \alpha,\ \beta\rangle, \langle \beta,\ g(\gamma)\rangle\}\rangle$ (17.7)

$= \langle g(\beta),\ \{\langle \beta,\ \langle a,\ b\rangle\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle\},\ \{\langle \alpha,\ \beta\rangle, \langle \beta,\ g(\gamma)\rangle\}\rangle$ (17.5b)

$\mathsf{lub}'(b, a, \{\langle \beta,\ \langle a,\ b\rangle\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle\}, \gamma, \{\langle \alpha,\ \beta\rangle, \langle \beta,\ g(\gamma)\rangle\})$ (17.8)

$=\langle \alpha,\ \{\langle \alpha,\ \langle b,\ a\rangle\rangle, \langle \beta,\ \langle a,\ b\rangle\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle\},\ \{\langle \alpha,\ \beta\rangle, \langle \beta,\ g(\gamma)\rangle, \langle \gamma,\ \alpha\rangle\}\rangle$ (17.9)

$\mathsf{lub}'(b, a, \{\{\langle \alpha,\ \langle b,\ a\rangle\rangle, \langle \beta,\ \langle a,\ b\rangle\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle\}, U, \{\langle \alpha,\ \beta\rangle, \langle \beta,\ g(\gamma)\rangle, \langle \gamma,\ \alpha\rangle\})$ (17.8)

$= \langle \alpha,\ \{\{\langle \alpha,\ \langle b,\ a\rangle\rangle, \langle \beta,\ \langle a,\ b\rangle\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle\},\ \{\langle \alpha,\ \beta\rangle, \langle \beta,\ g(\gamma)\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle, \langle U,\ \alpha\rangle\}\rangle$

$= \langle f(g(\beta), g(\gamma), g(\beta), \alpha, \alpha),\ \{\langle \alpha,\ \langle b,\ a\rangle\rangle, \langle \beta,\ \langle a,\ b\rangle\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle\},\ \{\langle \alpha,\ \beta\rangle, \langle \beta,\ g(\gamma)\rangle, \langle \gamma,\ \alpha\rangle, \langle U,\ \alpha\rangle\}\rangle$ (17.5b)

so that $\boldsymbol{\tau} = f(g(\beta), g(\gamma), g(\beta), \alpha, \alpha), T = \{\langle \alpha, \langle b, a\rangle\rangle, \langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}$, and $\vartheta' = \{\langle \alpha, \beta\rangle, \langle \beta,\ g(\gamma)\rangle, \langle \gamma,\ \alpha\rangle, \langle U,\ \alpha\rangle\}$. Let us check that

1. $\vartheta'(\boldsymbol{\tau}') = \{\langle \alpha,\ \beta\rangle, \langle \beta,\ g(\gamma)\rangle, \langle \gamma,\ \alpha\rangle, \langle U,\ \alpha\rangle\}(f(g(\alpha), \beta, g(\alpha), \gamma, U)) = f(g(\beta), g(\gamma), g(\beta), \alpha, \alpha) = \boldsymbol{\tau}$;
2. $\bar{\varsigma}_1(T) = \bar{\varsigma}_1(\{\langle \alpha,\ \langle b,\ a\rangle\rangle, \langle \beta,\ \langle a,\ b\rangle\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle\}) = \{\langle \alpha,\ b\rangle, \langle \beta,\ a\rangle, \langle \gamma,\ g(a)\rangle\}$;
3. $\bar{\varsigma}_1(T)(\boldsymbol{\tau}) = \{\langle \alpha,\ b\rangle, \langle \beta,\ a\rangle, \langle \gamma,\ g(a)\rangle\}(f(g(\beta), g(\gamma), g(\beta), \alpha, \alpha)) = f(g(a), g(g(a)), g(a), b, b) = \boldsymbol{\tau}_1$;
4. $\bar{\varsigma}_2(T) = \bar{\varsigma}_2(\{\langle \alpha,\ \langle b,\ a\rangle\rangle, \langle \beta,\ \langle a,\ b\rangle\rangle, \langle \gamma,\ \langle g(a),\ h(b)\rangle\rangle\}) = \{\langle \alpha,\ a\rangle, \langle \beta,\ b\rangle, \langle \gamma,\ h(b)\rangle\}$;
5. $\bar{\varsigma}_2(T)(\boldsymbol{\tau}) = \{\langle \alpha,\ a\rangle, \langle \beta,\ b\rangle, \langle \gamma,\ h(b)\rangle\}(f(g(\beta), g(\gamma), g(\beta), \alpha, \alpha)) = f(g(b), g(h(b)), g(b), a, a) = \boldsymbol{\tau}_2$. □

We must show that lub' and lub compute the same result $\boldsymbol{\tau}$.

Lemma 20 For all $\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}, \boldsymbol{\tau}', \boldsymbol{\tau}'' \in \mathbf{T}^{\mathcal{V}}, T_0, T, T'' \in \wp(\mathcal{V} \times \mathbf{T}^{\mathcal{V}} \times \mathbf{T}^{\mathcal{V}})$, and $\vartheta_0, \vartheta' \in \mathcal{V} \nrightarrow \mathbf{T}^{\mathcal{V}}$, if $\langle \boldsymbol{\tau},\ T,\ \vartheta'\rangle = \mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ and $\langle \boldsymbol{\tau}'',\ T''\rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0)$ then $\boldsymbol{\tau} = \boldsymbol{\tau}''$ and $T = T''$. □

Proof of Lemma 20 Any execution trace of $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ can be abstracted into an execution trace of $\mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0)$ simply by ignoring the input ϑ_0, the resulting substitution ϑ', ignoring the program point (17.a) and mapping (17.2a), …, (17.5a) and (17.2b), …, (17.5b) to the program point (48.67.2), …, (48.67.5). The proof is by induction on the calls to lub and lub' which are synchronous in the two traces. The point is that the result $\langle \boldsymbol{\tau},\ T\rangle$ of a call $\langle \boldsymbol{\tau},\ T,$

$\vartheta'\rangle = \mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ does not depend during its computation on the parameters $\boldsymbol{\tau}'$, and ϑ_0. An exception is the test (17.a) but the two alternative yield the same result. (17.2a), …, (17.4a) is identical to (48.67.2), …, (48.67.4) while, by induction on the sequence of calls to lub' (17.2b), …, (17.4b) is abstracted to that of (48.67.2), …, (48.67.4). It follows that $\langle\boldsymbol{\tau},\ T\rangle$ at (48.67.12) is equal to $\langle\boldsymbol{\tau},\ T\rangle$ at (17.14). □

The following Lemma 21 proves the well-typing of algorithm lub'.

Lemma 21 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}'_0, \boldsymbol{\tau}' \in \mathbf{T}^{\mathbb{V}}$, $T_0 \in \wp(\mathbb{V} \times \mathbf{T}^{\mathbb{V}} \times \mathbf{T}^{\mathbb{V}})$, and $\vartheta_0, \vartheta_1, \vartheta_2 \in \mathbb{V} \nrightarrow \mathbf{T}^{\mathbb{V}}$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}'_0, \varepsilon)$ with hypothesis $\vartheta_1(\boldsymbol{\tau}'_0) = \boldsymbol{\tau}_1^0 \wedge \vartheta_2(\boldsymbol{\tau}'_0) = \boldsymbol{\tau}_2^0$, then the case analysis in the definition of lub' is complete (i.e., there is no missing case) and $\exists \gamma \in \mathbb{V}\ .\ \boldsymbol{\tau}' = \gamma$ at (17.6) and (17.8). □

Proof of Lemma 21 Notice that Lemma 11, 14, and 16 are valid for lub' since they do not involve the extra parameters $\boldsymbol{\tau}', \vartheta_0$ or result ϑ'. The proof is by case analysis.

- For (17.1), the only possible cases for $\boldsymbol{\tau}'$ are (17.a) and (17.b), by definition (48.2) of terms with variables.
- For (17.6) and (17.8), the test (17.1) is false so, by the preinvariant of Lemma 11 and def. (48.2) of terms with variables, at least one $\boldsymbol{\tau}_j$, $j = 1, 2$ of $\boldsymbol{\tau}_1$ or $\boldsymbol{\tau}_2$ is a variable. Then $\boldsymbol{\tau}'$ must be a variable since otherwise $\boldsymbol{\tau}' = g(\boldsymbol{\tau}'_1, \ldots, \boldsymbol{\tau}'_m)$ so that it is impossible that $\vartheta_j(\boldsymbol{\tau}') = \boldsymbol{\tau}_j$ be a variable. □

The following Lemma 22 shows that variables recorded in T_0 are for non-matching subterms only.

Lemma 22 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \in \mathbf{T}^{\mathbb{V}}$ and $T_0 \in \wp(\mathbb{V}\times\mathbf{T}^{\mathbb{V}}\times\mathbf{T}^{\mathbb{V}})$, if $\mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0)$ is (recursively) called from the main call $\mathsf{lub}(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing)$, then for all $\boldsymbol{\tau}'_1, {\boldsymbol{\tau}'_1}^1, \ldots, {\boldsymbol{\tau}'_1}^n, \boldsymbol{\tau}'_2, {\boldsymbol{\tau}'_2}^1, \ldots, {\boldsymbol{\tau}'_2}^n \in \mathbf{T}^{\mathbb{V}}$,

$$\text{if } \exists f \in \mathbf{F}_n\ .\ \boldsymbol{\tau}'_1 = f({\boldsymbol{\tau}'_1}^1, \ldots, {\boldsymbol{\tau}'_1}^n) \wedge \boldsymbol{\tau}'_2 = f({\boldsymbol{\tau}'_2}^1, \ldots, {\boldsymbol{\tau}'_2}^n) \text{ then } \forall \beta \in \mathsf{dom}(T_0)\ .\ T_0(\beta) \neq \langle\boldsymbol{\tau}'_2,\ \boldsymbol{\tau}'_1\rangle.$$

□

Proof of Lemma 22 Let us prove the contraposition, that is "if $\exists \beta \in \mathsf{dom}(T_0)\ .\ T_0(\beta) = \langle\boldsymbol{\tau}'_2,\ \boldsymbol{\tau}'_1\rangle$ then $\forall f \in \mathbf{F}_n\ .\ \boldsymbol{\tau}'_1 \neq f({\boldsymbol{\tau}'_1}^1, \ldots, {\boldsymbol{\tau}'_1}^n) \vee \boldsymbol{\tau}'_2 \neq f({\boldsymbol{\tau}'_2}^1, \ldots, {\boldsymbol{\tau}'_2}^n)$".

The proof is by induction on the sequence of calls to lub and Lemma 22 is obviously true for the initial value of $T_0 = \varnothing$. Then observe that the only modification to the parameter T_0 in calls to lub is (48.67.9) for which (48.67.1) is false so that the returned T' is $\langle\boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2\rangle[\beta \leftarrow T_0]$ with $\neg(\boldsymbol{\tau}_1 = f(\boldsymbol{\tau}_1^1, \ldots, \boldsymbol{\tau}_1^n) \wedge \boldsymbol{\tau}_2 = f(\boldsymbol{\tau}_2^1, \ldots, \boldsymbol{\tau}_2^n))$. This property is preserved by the recursive calls (17.2a) to (17.4a) for T_n returned at (17.5a) as well as for the unmodified T_0 returned at (17.7). By induction, Lemma 22 holds for all calls from the main call (17.14). □

Lemma 23 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}, \boldsymbol{\tau}' \in \mathbf{T}^\nu$, $T_0, T \in \mathbb{V} \nrightarrow (\mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \varepsilon)$ with hypothesis $\vartheta_1(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_1^0 \wedge \vartheta_2(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_2^0$ and returns $\langle \boldsymbol{\tau},\ T,\ \vartheta' \rangle$, then

$$(\exists \beta \in \mathsf{dom}(T_0) \;.\; T_0(\beta) = \langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle \wedge \boldsymbol{\tau}' = \gamma) \Rightarrow (\gamma \in \mathsf{dom}(\vartheta_0) \wedge \vartheta_0(\gamma) = \beta) \qquad \square$$

Proof of Lemma 23 We prove the stronger property that the following preinvariant and postinvariant do hold for any call $\langle \boldsymbol{\tau},\ T,\ \vartheta' \rangle = \mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$.

$$\begin{array}{ll} \text{preinvariant} & (\exists \beta \in \mathsf{dom}(T_0) \;.\; T_0(\beta) = \langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle \wedge \boldsymbol{\tau}' = \gamma) \Rightarrow (\gamma \in \mathsf{dom}(\vartheta_0) \wedge \vartheta_0(\gamma) = \beta) \\ \text{postinvariant} & (\exists \beta \in \mathsf{dom}(T) \;.\; T(\beta) = \langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle \wedge \boldsymbol{\tau}' = \gamma) \Rightarrow (\gamma \in \mathsf{dom}(\vartheta') \wedge \vartheta'(\gamma) = \beta) \end{array} \qquad (24)$$

The proof is by induction on the sequence of calls to lub' and, for any given call, by recurrence to handle the recursive calls at (17.2b), (17.3b),…, (17.4b), and by case analysis for the conditional.

- For the basis, the preinvariant of (24) holds vacuously at the first call (17.14) since $T_0 = \varnothing$;
- For the induction step, we proceed by case analysis.
  - In case (17.5a), there is no recursive call to lub' and, by Lemma 22, the premiss of the postinvariant of (24) is ff so it does hold vacuously.
  - In case (17.5b), the first recursive call at (17.2a) satisfies the preinvariant because this preinvariant is assumed to hold for the intermediate call at (17).

    In case $n = 0$, this is also the postinvariant.

    Otherwise $n > 0$. Assume, by recurrence hypothesis, that the preinvariant holds before the call $\langle \boldsymbol{\tau}^i,\ T_i,\ \vartheta_i \rangle = \mathsf{lub}'(\boldsymbol{\tau}_1^i, \boldsymbol{\tau}_2^n, T_{i-1}, \boldsymbol{\tau}_i', \vartheta_{i-1})$. Then, by induction hypothesis on the sequence of calls to lub', the postinvariant (24) holds for T_i and ϑ_i, which is the preinvariant of the next recursive call, if any.

    It follows, by recurrence, that the postinvariant of (24) holds at (17.5b) for T_n and ϑ_n.
  - In case (17.7), we know by the test (17.6) and Lemma 21 that $\exists \beta \in \mathsf{dom}(T_0) \;.\; T_0(\beta) = \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle \wedge \boldsymbol{\tau}' = \gamma$ so by the preinvariant $\gamma \in \mathsf{dom}(\vartheta_0)$ and $\vartheta_0(\gamma) = \beta$. Since $T = T_0$ and $\vartheta' = \vartheta_0$, we have $\gamma \in \mathsf{dom}(\vartheta') \wedge \vartheta'(\gamma) = \beta$;
  - In case (17.9), $\vartheta' = \beta[\gamma \leftarrow \vartheta_0]$, which implies the postinvariant (24). $\square$

Let us prove the converse of Lemma 23.

Lemma 25 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu$, $T_0, T \in \wp(\mathbb{V} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \varepsilon)$ with hypothesis $\vartheta_1(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_1^0 \wedge \vartheta_2(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_2^0$ and returns $\langle \boldsymbol{\tau},\ T,\ \vartheta' \rangle$, then

$$\forall \beta, \gamma \in \mathbb{V} \;.\; (\gamma \in \mathsf{dom}(\vartheta_0) \wedge \vartheta_0(\gamma) = \beta) \Rightarrow (\beta \in \mathsf{dom}(T_0)). \qquad \square$$

–

Proof of Lemma 25 We prove the stronger property that the following preinvariant and postinvariant do hold for any call $\langle \boldsymbol{\tau}, T, \vartheta' \rangle = \mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$.

$$\begin{array}{ll} \text{preinvariant} & \forall \beta, \gamma \in \mathbb{V} \,.\, (\gamma \in \mathsf{dom}(\vartheta_0) \wedge \vartheta_0(\gamma) = \beta) \Rightarrow (\beta \in \mathsf{dom}(T_0)) \\ \text{postinvariant} & \forall \beta, \gamma \in \mathbb{V} \,.\, (\gamma \in \mathsf{dom}(\vartheta') \wedge \vartheta'(\gamma) = \beta) \Rightarrow (\beta \in \mathsf{dom}(T)) \end{array} \tag{26}$$

The proof is by induction on the sequence of calls to lub' and, for any given call, by recurrence to handle the recursive calls at (17.2b), (17.3b),…, (17.4b), and by case analysis for the conditional.

- For the basis, $\vartheta_0 = \varepsilon$ so $\mathsf{dom}(\vartheta_0) = \varnothing$ so the preinvariant (26) holds vacuously;
- The induction step is by case analysis.
  - In case (17.5a), there is no recursive call to lub' and $\vartheta' = f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0]$. So if $\alpha \in \mathsf{dom}(\vartheta') \setminus \{\gamma\}$ then the postinvariant follows from the preinvariant. For $\gamma \in \mathsf{dom}(\vartheta')$, we have $\vartheta'(\gamma) = f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n) \notin \mathbb{V}$ so that the postondition holds vacuously;
  - In case (17.5b), the preinvariant of the first recursive call (17.2a) holds by the preinvariant of (26) on the main call (17). Assuming the preinvariant holds for a following recursive call, the postinvariant holds by induction on the sequence of calls to lub', which is also the preinvariant of the next call. By recurrence the postinvariant of (26) holds for $\vartheta' = \vartheta_n$ and $T = T_n$ after the last call at (17.5b);
  - In case (17.7), we have $\gamma \in \mathsf{dom}(\vartheta') \wedge \vartheta'(\gamma) = \beta$ so the preinvariant (26) on the intermediate call trivially implies the postinvariant;
  - In case (17.9), $T = \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle [\beta \leftarrow T_0]$ and $\vartheta' = \beta[\gamma \leftarrow \vartheta_0]$.
    If $\alpha \in \mathsf{dom}(\vartheta') \setminus \{\gamma\}$ and $\vartheta'(\alpha) = \beta'$ then $\alpha \in \mathsf{dom}(\vartheta_0)$ and $\vartheta_0(\alpha) = \beta'$ then, by the preinvariant on the intermediate call, $\beta' \in \mathsf{dom}(T_0) = \mathsf{dom}(T)$.
    Otherwise, for $\gamma \in \mathsf{dom}(\vartheta')$, we have $\vartheta'(\gamma) = \beta[\gamma \leftarrow \vartheta_0](\gamma) = \beta$ with $\beta \in \mathsf{dom}(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle [\beta \leftarrow T_0]) = \mathsf{dom}(T)$. □

The next Lemma 27 shows how the term variables are used.

Lemma 27 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu$, $T_0, T \in \wp(\mathbb{V} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1^0, \vartheta_2^0, \vartheta' \in \mathbb{V} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \varepsilon)$ with hypothesis $\vartheta_1^0(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_1^0 \wedge \vartheta_2^0(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_2^0$ and returns $\langle \boldsymbol{\tau}, T, \vartheta' \rangle$, then

$$\begin{array}{ll} \text{preinvariant} & \mathsf{vars}[\![\vartheta_0(\mathbb{V})]\!] \subseteq \mathsf{dom}(T_0) \\ \text{postinvariant} & \mathsf{vars}[\![\vartheta'(\mathbb{V})]\!] \subseteq \mathsf{dom}(T) \end{array} \tag{28}$$

(where $\vartheta_0(S) = \{\vartheta_0(\alpha) \mid \alpha \in S\}$ and $\mathsf{vars}[\![S]\!] = \bigcup\{\mathsf{vars}[\![\boldsymbol{\tau}]\!] \mid \boldsymbol{\tau} \in S\}$.) □

Proof of Lemma 27 The proof is by induction on the sequence of calls to lub' and, for any given call, by recurrence to handle the recursive calls at (17.2b), (17.3b),…, (17.4b), and by case analysis for the conditional.

- For the first call at (17.14), $\vartheta_0 = \varepsilon$ so $\mathsf{vars}[\![\vartheta_0(\mathcal{V})]\!] = \mathsf{vars}[\![\varnothing]\!] = \varnothing \subseteq \mathsf{dom}(T_0)$;
- Otherwise the preinvariant of (28) holds for T_0 and ϑ_0 at the first recursive call (17.2b). Assume, by induction hypothesis, that $\mathsf{vars}[\![\vartheta_{i-1}(\mathcal{V})]\!] \subseteq \mathsf{dom}(T_{i-1})$ before the i^{th} call (17.2b),…, (17.4b), $i \in [1, n]$. By induction hypothesis on the sequence of calls to lub', we have $\mathsf{vars}[\![\vartheta_i(\mathcal{V})]\!] \subseteq \mathsf{dom}(T_i)$ after that call, which is also the preinvariant of the next call, if any. By recurrence, $\mathsf{vars}[\![\vartheta'(\mathcal{V})]\!] = \mathsf{vars}[\![\vartheta_n(\mathcal{V})]\!] \subseteq \mathsf{dom}(T_n) = \mathsf{dom}(T)$ in case the call (17)to lub' terminates at (17.5b);
- If lub' terminates at (17.5a), there are two cases.
  - $\mathsf{vars}[\![\vartheta'(\{\gamma\})]\!] = \mathsf{vars}[\![f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\{\gamma\})]\!] = \mathsf{vars}[\![f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)]\!] = \bigcup_{i=1}^n \mathsf{vars}[\![\boldsymbol{\tau}^i]\!]$. By Lemma 11 and 20, we have $\mathsf{vars}[\![\boldsymbol{\tau}^i]\!] \subseteq \mathsf{dom}(T_i)$, $i = 1, \dots, n$ and $\mathsf{dom}(T_i) \subseteq \mathsf{dom}(T_n)$ so that $\bigcup_{i=1}^n \mathsf{vars}[\![\boldsymbol{\tau}^i]\!] \subseteq \bigcup_{i-1}^n \mathsf{dom}(T_i) \subseteq \mathsf{dom}(T_n) = \mathsf{dom}(T)$;
  - $\mathsf{vars}[\![\vartheta'(\mathcal{V} \setminus \{\gamma\})]\!] = \mathsf{vars}[\![f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\mathcal{V} \setminus \{\gamma\})]\!] = \mathsf{vars}[\![\vartheta_0(\mathcal{V} \setminus \{\gamma\})]\!] \subseteq \mathsf{vars}[\![\vartheta_0(\mathcal{V})]\!]$ which, by the preinvariant (28), is included in $\mathsf{dom}(T_0)$. By Lemma 11 and 20, $\mathsf{dom}(T_{i=1}) \subseteq \mathsf{dom}(T_i)$, $i = 1, \dots, n$ so that, by transitivity, $\mathsf{dom}(T_0) \subseteq \mathsf{dom}(T_n) = \mathsf{dom}(T)$. Therefore $\mathsf{vars}[\![\vartheta'(\mathcal{V} \setminus \{\gamma\})]\!] \subseteq \mathsf{dom}(T)$;
  - Since $\vartheta'(\mathcal{V}) = \vartheta'(\{\gamma\}) \cup \vartheta'(\mathcal{V} \setminus \{\gamma\})$, we conclude that $\mathsf{vars}[\![\vartheta'(\mathcal{V})]\!] = \mathsf{vars}[\![\vartheta'(\{\gamma\}) \cup \vartheta'(\mathcal{V} \setminus \{\gamma\})]\!] = \mathsf{vars}[\![\vartheta'(\{\gamma\})]\!] \cup \mathsf{vars}[\![\vartheta'(\mathcal{V} \setminus \{\gamma\})]\!] \subseteq \mathsf{dom}(\vartheta') \cup \mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta')$; □
- If lub' terminates at (17.7) then the postinvariant directly follows from the preinvariant of (28) since $T = T_0$ and $\vartheta' = \vartheta_0$;
- Finally, if lub' terminates at (17.9), there are two subcases.
  - We have $\mathsf{vars}[\![\vartheta'(\{\gamma\})]\!] = \mathsf{vars}[\![\beta[\gamma \leftarrow \vartheta_0](\{\gamma\})]\!] = \mathsf{vars}[\![\{\beta\}]\!] = \{\beta\} \subseteq \mathsf{dom}(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0]) = \mathsf{dom}(T)$;
  - Moreover $\mathsf{vars}[\![\vartheta'(\mathcal{V} \setminus \{\gamma\})]\!] = \mathsf{vars}[\![\beta[\gamma \leftarrow \vartheta_0](\mathcal{V} \setminus \{\gamma\})]\!] = \mathsf{vars}[\![\vartheta_0(\mathcal{V} \setminus \{\gamma\})]\!] \subseteq \mathsf{vars}[\![\vartheta_0(\mathcal{V})]\!] \subseteq \mathsf{dom}(T_0)$, by the preinvariant of (28). But $\mathsf{dom}(T_0) \subseteq \mathsf{dom}(T_0) \cup \{\beta\} = \mathsf{dom}(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0]) = \mathsf{dom}(T)$, proving the postinvariant of vars-codom-substitution0 by transitivity;
  - We conclude since vars preserves joins. □

The following series of lemmata aims at proving that the substitution built by lub' is the one allowing us to prove that lub returns the least common generalization.

Lemma 29 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}' \in \mathbf{T}^\nu$, $T_0, T \in \wp(\mathbb{V} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1^0, \vartheta_2^0, \vartheta' \in \mathbb{V} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \varepsilon)$ with hypothesis $\vartheta_1^0(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_1^0 \wedge \vartheta_2^0(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_2^0$ and returns $\langle \boldsymbol{\tau}, T, \vartheta' \rangle$, then

$$\vartheta_1^0(\boldsymbol{\tau}') = \boldsymbol{\tau}_1 \wedge \vartheta_2^0(\boldsymbol{\tau}') = \boldsymbol{\tau}_2. \tag{30}$$ □

Proof of Lemma 29 For the first call at (17.14), (30) holds by the hypothesis $\vartheta_1^0(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_1^0 \wedge \vartheta_2^0(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_2^0$ on the actual parameters. Assume that $\vartheta_j^0(\boldsymbol{\tau}') = \boldsymbol{\tau}_j$, $j = 1, 2$ before an intermediate call (17). Then (30) holds before the recursive calls (17.2b), …, (17.4b) since the induction hypothesis $\vartheta_j^0(\boldsymbol{\tau}') = \boldsymbol{\tau}_j$, $\boldsymbol{\tau}' = f(\boldsymbol{\tau}_1', \ldots, \boldsymbol{\tau}_n')$ by the test (17.a) which is false, $\boldsymbol{\tau}_j = f(\boldsymbol{\tau}_j^1, \ldots, \boldsymbol{\tau}_j^n)$ by the test (17.1) which is true, and (48.30) imply that $\vartheta_j^0(\boldsymbol{\tau}') = \vartheta_j^0(f(\boldsymbol{\tau}_1', \ldots, \boldsymbol{\tau}_n')) = f(\vartheta_j^0(\boldsymbol{\tau}_1'), \ldots, \vartheta_j^0(\boldsymbol{\tau}_n')) = f(\boldsymbol{\tau}_j^1, \ldots, \boldsymbol{\tau}_j^n) = \boldsymbol{\tau}_j$ and therefore $\vartheta_j^0(\boldsymbol{\tau}_i') = \boldsymbol{\tau}_j^i$, $j = 1, \ldots, n$. We conclude by induction on the sequence of calls to lub'. □

Lemma 31 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu$, $T_0, T \in \wp(\mathbb{V} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1^0, \vartheta_2^0, \vartheta' \in \mathbb{V} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \varepsilon)$ with hypothesis $\vartheta_1^0(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_1^0 \wedge \vartheta_2^0(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_2^0$ and returns $\langle \boldsymbol{\tau}, T, \vartheta' \rangle$, then

$$\begin{array}{ll} \text{preinvariant} & \forall j = 1, 2 \,.\, \forall \alpha \in \mathsf{dom}(\vartheta_0) \,.\, \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_0)(\vartheta_0(\alpha)) \\ \text{postinvariant} & \forall j = 1, 2 \,.\, \forall \alpha \in \mathsf{dom}(\vartheta') \,.\, \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T)(\vartheta'(\alpha)) \wedge \bar{\varsigma}_j(T)(\boldsymbol{\tau}) = \boldsymbol{\tau}_j \end{array} \tag{32}$$ □

Proof of Lemma 31 Notice again that Lemma 11, 14, and 16 are valid for lub' since they do not involve the extra parameters $\boldsymbol{\tau}', \vartheta_0$, or result ϑ'. It follows, by Lemma 14, that the postinvariant of (32) satisfies $\bar{\varsigma}_j(T)(\boldsymbol{\tau}) = \boldsymbol{\tau}_j$, $j = 1, 2$. The proof of (32) is by induction on the sequence of calls to lub' and, for any given call, by recurrence to handle the recursive calls at (17.2b), (17.3b),…, (17.4b), and by case analysis for the conditional.

- For the basis, the preinvariant (32) holds vacuously for the main call (17.14) since $\vartheta_0 = \varepsilon$ so $\mathsf{dom}(\vartheta_0) = \varnothing$;
- Assume that the preinvariant (32) holds before any intermediate call (17)of lub'. We must show that it holds before all recursive calls (17.2b), …, (17.4b).

  By hypothesis on the intermediate call, we have $\forall j = 1, 2 \,.\, \forall \alpha \in \mathsf{dom}(\vartheta') \,.\, \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_0)(\vartheta'(\alpha))$ at the first recursive call (17.2b).

  Assume that $\forall j = 1, 2 \,.\, \forall \alpha \in \mathsf{dom}(\vartheta_{i-1}) \,.\, \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_{i-1})(\vartheta_{i-1}(\alpha))$ before the i^{th} recursive call. By induction on the sequence of calls to lub', the postinvariant of (32) holds. Therefore we have $\forall j = 1, 2 \,.\, \forall \alpha \in \mathsf{dom}(\vartheta_i) \,.\, \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_i)(\vartheta_i(\alpha))$ before the $i + 1^{\text{th}}$ call. By recurrence, all recursive calls do satisfy (32).

We must also show that the intermediate call satisfies the postinvariant of (32). We proceed by cases.

- In case (17.5b), we have $T = T_n$ and ϑ_n which satisfy the postinvariant of (32), as shown above.
- In case (17.5a), the postinvariant is $\forall j = 1, 2 \,.\, \forall \alpha \in \mathsf{dom}(f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0]) \,.\, \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_n)(f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\alpha))$.
  - If $\alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\}$, we must show that $\vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_n)(\vartheta_0(\alpha))$.
    By Lemma 11, $\forall \alpha \in \mathsf{dom}(T_{i-1}) \,.\, T_{i-1}(\alpha) = T_i(\alpha)$, $i = 1, \dots, n$ so that, by transitivity, $\forall \alpha \in \mathsf{dom}(T_0) \,.\, T_0(\alpha) = T_n(\alpha)$. Therefore, by (13), for all $\beta \in \mathsf{dom}(T_0)$, $\bar{\varsigma}_j(T_0)\beta \triangleq \mathsf{let}\ \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle = T_0(\beta)\ \mathsf{in}\ \boldsymbol{\tau}_j = \mathsf{let}\ \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle = T_n(\beta)\ \mathsf{in}\ \boldsymbol{\tau}_j = \bar{\varsigma}_j(T_n)\beta$. By Lemma 27, $\mathsf{vars}[\![\vartheta_0(\mathcal{V})]\!] \subseteq \mathsf{dom}(T_0)$ so, in particular, $\forall \alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\} \,.\, \mathsf{vars}[\![\vartheta_0(\alpha)]\!] \subseteq \mathsf{dom}(T_0)$. This implies that $\forall \alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\} \,.\, \forall \beta \in \mathsf{vars}[\![\vartheta_0(\alpha)]\!] \,.\, \bar{\varsigma}_j(T_0)\beta = \bar{\varsigma}_j(T_n)\beta$. By (48.30) and (48.30), we infer that $\forall \alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\} \,.\, \bar{\varsigma}_j(T_0)\boxtimes_{\odot}(\boxtimes) = \bar{\varsigma}_j(T_n)\boxtimes_{\odot}(\boxtimes)$. By the preinvariant of (32), we have $\forall \alpha \in \mathsf{dom}(\vartheta_0) \,.\, \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_0)(\vartheta_0(\alpha))$. Therefore, by transitivity, $\vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_n)(\vartheta_0(\alpha))$.
  - Otherwise $\alpha = \gamma$, in which case we must show that $\vartheta_j^0(\gamma) = \bar{\varsigma}_j(T_n)(f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n))$. By Lemma 29, (48.42) of Lemma 48.40, and (17.5a), we have $\vartheta_j^0(\gamma) = \vartheta_j^0(\boldsymbol{\tau}') = \boldsymbol{\tau}_j = \bar{\varsigma}_j(T)(\boldsymbol{\tau}) = \bar{\varsigma}_j(T)(f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n))$.
- In case (17.7), the postinvariant of (30) immediately follows from the preinvariant since $T = T_0$ and $\vartheta' = \vartheta_0$;
- In case (17.9), we must show that $\forall j = 1, 2 \,.\, \forall \alpha \in \mathsf{dom}(\beta[\gamma \leftarrow \vartheta_0]) \,.\, \vartheta_j^0(\alpha) = \bar{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])(\beta[\gamma \leftarrow \vartheta_0](\alpha))$. There are two cases.
  - If $\alpha = \gamma$ then we must prove that $\vartheta_j^0(\gamma) = \bar{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])(\beta)$, that is, by (13), $\vartheta_j^0(\gamma) = \boldsymbol{\tau}_j$. It is not possible that $\gamma \in \mathsf{dom}(\vartheta_0)$ since otherwise, we would have $\forall \beta \in \mathsf{dom}(T_0) \,.\, T_0(\beta) \neq \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle$ since the test (17.6) is $\mathtt{ff}$ and $\boldsymbol{\tau}' = \gamma \in \mathcal{V}$ by Lemma 21, which is in contradiction with (the contrapositive of) Lemma 25. Therefore $\vartheta_0(\gamma) = \gamma$ by (48.30). It follows that we have to prove that $\vartheta_j^0(\vartheta_0(\gamma)) = \boldsymbol{\tau}_j$, which directly follows from the preinvariant of (30);
  - Otherwise, $\alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\}$ and we must show that $\vartheta_j^0(\alpha) = \bar{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])(\vartheta_0(\alpha))$. The test (17.8) implies $\beta \notin \mathsf{dom}(T_0)$ and so $\beta \notin \mathsf{vars}[\![\vartheta_0(\alpha)]\!]$ since $\mathsf{vars}[\![\vartheta_0(\mathcal{V})]\!] \subseteq \mathsf{dom}(T_0)$ by (28) of Lemma 27. Therefore, by (13), $\forall \gamma \in \mathsf{vars}[\![\vartheta_0(\alpha)]\!] \,.\, \bar{\varsigma}_j(T_0)(\gamma) = \bar{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])(\gamma)$. It follows, by (48.30) and (48.30), that $\bar{\varsigma}_j(T_0)(\vartheta_0(\alpha)) = \bar{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])(\vartheta_0(\alpha))$. We conclude, by the preinvariant (30) and transitivity that $\bar{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])(\vartheta_0(\alpha)) = \vartheta_j^0(\alpha)$. □ □

Lemma 33 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}'_0, \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu$, $T_0, T \in \wp(\mathbb{V} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}'_0, \varepsilon)$ with hypothesis $\vartheta_1(\boldsymbol{\tau}'_0) = \boldsymbol{\tau}_1^0 \wedge \vartheta_2(\boldsymbol{\tau}'_0) = \boldsymbol{\tau}_2^0$ and returns $\langle \boldsymbol{\tau}, T, \vartheta' \rangle$, then the following postinvariant holds after the call.

$$\mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![\boldsymbol{\tau}']\!] \tag{34}$$ □

Proof of Lemma 33 The proof of (34) is by induction on the sequence of calls to lub' and, for any given call, by recurrence to handle the recursive calls at (17.2b), (17.3b),…, (17.4b), and by case analysis for the conditional.

Consider any intermediate call $\langle \boldsymbol{\tau}, T, \vartheta' \rangle = \mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}'_0, \varepsilon)$. We proceed by case analysis of the returned values $\langle \boldsymbol{\tau}, T, \vartheta' \rangle$.

- In case (17.5a), we have $\mathsf{dom}(\vartheta') = \mathsf{dom}(f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0]) = \mathsf{dom}(\vartheta_0) \cup \{\gamma\} = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![\boldsymbol{\tau}']\!]$ since $\vartheta' = \gamma$ by the test (17.a);
- In case (17.5b), we have $\mathsf{dom}(\vartheta_i) = \mathsf{dom}(\vartheta_{i-1}) \cup \mathsf{vars}[\![\boldsymbol{\tau}^i]\!]$, $i = 1, \dots, n$, by induction hypothesis on the sequence of calls to lub'. It follows that $\mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta_n) = \mathsf{dom}(\vartheta_0) \cup \bigcup_{i=1}^n \mathsf{vars}[\![\boldsymbol{\tau}^i]\!] = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)]\!] = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![\boldsymbol{\tau}']\!]$;
- In case (17.7), we have $\vartheta' = \beta[\gamma \leftarrow \vartheta_0]$ so $\mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta_0) \cup \{\gamma\} = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![\boldsymbol{\tau}']\!]$ since $\boldsymbol{\tau}' = \gamma$ by Lemma 21;
- Finally, in case (17.9), $\mathsf{dom}(\vartheta') = \mathsf{dom}(\beta[\gamma \leftarrow \vartheta_0]) = \mathsf{dom}(\vartheta_0) \cup \{\gamma\} = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![\boldsymbol{\tau}']\!]$ since $\boldsymbol{\tau}' = \gamma$ by Lemma 21. □ □

Lemma 35 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}'^0, \boldsymbol{\tau}^{n-1}, \boldsymbol{\tau}^n, \boldsymbol{\tau}^{m-1}.\boldsymbol{\tau}^m \in \mathbf{T}^\nu$, $T_n, T_m \in \wp(\mathbb{V} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, consider any computation trace for the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}'^0, \varepsilon, \varnothing)$ at (17.14) with hypothesis $\vartheta_1(\boldsymbol{\tau}'^0) = \boldsymbol{\tau}_1^0 \wedge \vartheta_2(\boldsymbol{\tau}'^0) = \boldsymbol{\tau}_2^0$. Assume that in this computation trace, a call $\langle \boldsymbol{\tau}^k, T_k \rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_{k-1})$ is followed by a later call $\langle \boldsymbol{\tau}^m, T_m \rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_{m-1})$ with the same parameters $\boldsymbol{\tau}_1$ and $\boldsymbol{\tau}_2$. Then $\boldsymbol{\tau}^k = \boldsymbol{\tau}^m$.

By Lemma 20, this also holds for calls to lub' independently of the other two parameters.

□

Proof of Lemma 35 By (12) in Lemma 11, Lemma 20, (17.2a), …, (17.4a), and (17.2b), …, (17.4b) and recurrence, the successive calls of lub and lub' in the trace have parameters T_i and result T_{i+1} with increasing domains and preservation of the previous values so that $\forall \alpha \in \mathsf{dom}(T_k) \,.\, T_k(\alpha) = T_m(\alpha)$.

To prove that $\boldsymbol{\tau}^k = \boldsymbol{\tau}^m$, we consider the calls $\langle \boldsymbol{\tau}^k, T_k \rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_{k-1})$ and the later $\langle \boldsymbol{\tau}^m, T_m \rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_{m-1})$ to lub (by Lemma 20, the reasoning is the same for lub'). The only possible executions are the following.

- If one execution follows the true branch of (48.67.1), so does the other since they have the same parameters. By recurrence and induction on the sequence of calls for (48.67.2), …, (48.67.4) with $\forall \alpha \in \mathsf{dom}(T_{i-1}) \,.\, T_{i-1}(\alpha) = T_i(\alpha)$, $i = 1, \ldots, n$, we have $\boldsymbol{\tau}^k = f({\boldsymbol{\tau}^1}^k, \ldots, {\boldsymbol{\tau}^n}^k) = f({\boldsymbol{\tau}^1}^m, \ldots, {\boldsymbol{\tau}^n}^m) = \boldsymbol{\tau}^m$;

- If both calls go through (48.67.7) then obviously $\boldsymbol{\tau}^k = \boldsymbol{\tau}^m = \beta$;

- Both calls cannot go through (48.67.9) since the first ones (which is $\langle \boldsymbol{\tau}^k, T_k \rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_{k-1})$) that goes through (48.67.9) will add β to the $\mathsf{dom}(T_k) \subseteq \mathsf{dom}(T_{m-1})$;

- If $\langle \boldsymbol{\tau}^k, T_k \rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_{k-1})$ goes through (48.67.9) then the call $\langle \boldsymbol{\tau}^m, T_m \rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_{m-1})$ must go through (48.67.7) since $\mathsf{dom}(T_k) \subseteq \mathsf{dom}(T_{m-1})$ with $\beta \in \mathsf{dom}(T_{m-1})$ so that $\boldsymbol{\tau}^k = \boldsymbol{\tau}^m = \beta$. □ □

Lemma 36 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}'_0, \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu$, $T_0, T \in \wp(\mathbb{V} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}'_0, \varepsilon)$ with hypothesis $\vartheta_1(\boldsymbol{\tau}'_0) = \boldsymbol{\tau}_1^0 \wedge \vartheta_2(\boldsymbol{\tau}'_0) = \boldsymbol{\tau}_2^0$ and returns $\langle \boldsymbol{\tau},\ T,\ \vartheta' \rangle$, then the following postinvariant holds after the call.

$$\forall \alpha \in \mathsf{dom}(\vartheta_0) \,.\, \vartheta_0(\alpha) = \vartheta'(\alpha) \tag{37}$$ □

Proof of Lemma 36 The proof of (34) is by induction on the sequence of calls to lub' and, for any given call, by recurrence to handle the recursive calls at (17.2b), (17.3b),…, (17.4b), and by case analysis for the conditional.

Consider any intermediate call $\langle \boldsymbol{\tau}, T, \vartheta' \rangle = \mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}'_0, \varepsilon)$. We proceed by case analysis of the returned values $\langle \boldsymbol{\tau},\ T,\ \vartheta' \rangle$.

- In case (17.5a), we have $\forall \alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\} \,.\, \vartheta_0(\alpha) = f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\alpha) = \vartheta'(\alpha)$.

  It may also be that $\gamma \in \mathsf{dom}(\vartheta_0)$. Since the main call starts with ε and by (34) the domain of ϑ_0 grows along the calls, there must be a previous call that added γ to $\mathsf{dom}(\vartheta_0)$. At that previous call, say $\mathsf{lub}'(\boldsymbol{\tau}_1^k, \boldsymbol{\tau}_2^k, T_0^k, \boldsymbol{\tau}'^k, \vartheta_0^k)$, we had $\boldsymbol{\tau}'^k = \gamma$ since (17.5a) and (17.9) are the two only cases where the domain of ϑ_0^k is extending with γ. By the initial hypothesis and (30) of Lemma 29, $\vartheta_j^0(\boldsymbol{\tau}'^k) = \vartheta_j^0(\gamma) = \boldsymbol{\tau}_j^k$. At the current call $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ where $\boldsymbol{\tau}'_0 = \gamma$, we also have, by the initial hypothesis and (30) of Lemma 29, that $\vartheta_j^0(\boldsymbol{\tau}') = \vartheta_j^0(\gamma) = \boldsymbol{\tau}_j$. By transitivity $\boldsymbol{\tau}_j^k = \boldsymbol{\tau}_j$. So the current and previous calls had the same first two parameters. It follows, by Lemma 35, that they have the same results. This implies that necessarily, $\vartheta_0(\gamma) = f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)$.

- In case (17.5b), we have $\forall \alpha \in \mathsf{dom}(\vartheta_{i-1}) \,.\, \vartheta_{i=1}(\alpha) = \vartheta_i(\alpha), i = 1, \ldots, n$, by induction hypothesis on the sequence of calls to lub'. It follows, by transitivity, that $\forall \alpha \in \mathsf{dom}(\vartheta_0) \,.\, \vartheta_0(\alpha) = \vartheta_n(\alpha) = \vartheta'(\alpha)$;

- In case (17.7), for all $\alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\}$, we have $\vartheta_0(\alpha) = \beta[\gamma \leftarrow \vartheta_0](\alpha) = \vartheta'(\alpha)$. We may also have $\gamma \in \mathsf{dom}(\vartheta_0)$, in which case the test (17.6), Lemma 21, and Lemma 23 imply that $\vartheta_0(\gamma) = \beta$ so $\vartheta_0(\gamma) = \beta = \beta[\gamma \leftarrow \vartheta_0](\gamma) = \vartheta'(\gamma)$;

- Finally, in case (17.9), it is not possible that $\gamma \in \mathsf{dom}(\vartheta_0)$ since otherwise, we would have $\forall \beta \in \mathsf{dom}(T_0) \, . \, T_0(\beta) \neq \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle$ since the test (17.6) is ff and $\boldsymbol{\tau}' = \gamma \in \mathbb{V}$ by Lemma 21, which is in contradiction with (the contrapositive of) Lemma 25. It follows that $\forall \alpha \in \mathsf{dom}(\vartheta_0) \, . \, \vartheta_0(\alpha) = \beta[\gamma \leftarrow \vartheta_0](\alpha) = \vartheta'(\alpha)$ since $\alpha \neq \gamma$. □ □

Lemma 38 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^{\nu}$, $T_0, T \in \wp(\mathbb{V} \times \mathbf{T}^{\nu} \times \mathbf{T}^{\nu})$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V} \nrightarrow \mathbf{T}^{\nu}$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \varepsilon)$ with hypothesis $\vartheta_1(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_1^0 \wedge \vartheta_2(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_2^0$ and returns $\langle \boldsymbol{\tau}, T, \vartheta' \rangle$, then the following postinvariant holds after the call.

$$\vartheta'(\boldsymbol{\tau}') = \boldsymbol{\tau} \tag{39}$$ □

Proof of Lemma 38 The proof of (39) is by induction on the sequence of calls to lub' and, for any given call, by recurrence to handle the recursive calls at (17.2b), (17.3b),…, (17.4b), and by case analysis for the conditional.

Consider any intermediate call $\langle \boldsymbol{\tau}, T, \vartheta' \rangle = \mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \varepsilon)$. We proceed by case analysis of the returned values $\langle \boldsymbol{\tau}, T, \vartheta' \rangle$.

- In case (17.5a), we have $\vartheta'(\boldsymbol{\tau}') = f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\gamma) = f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n) = \boldsymbol{\tau}$;

- In case (17.5b), we handle (17.2b), …, (17.4b) by recurrence.

  - For the basis at (17.2b), we have $\mathsf{dom}(\vartheta_1) = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![\boldsymbol{\tau}_1']\!]$ by (34) of Lemma 33, and $\vartheta_1(\boldsymbol{\tau}_1') = \boldsymbol{\tau}^1$, by induction on the sequence of calls to lub';
  - Assume, by recurrence hypothesis, that for the i^{th} call (17.2b), …, (17.4b), $i \in [1, n[$, we have

$$\begin{gathered}\mathsf{dom}(\vartheta_i) = \mathsf{dom}(\vartheta_0) \cup \bigcup_{j=1}^{i} \mathsf{vars}[\![\boldsymbol{\tau}_j']\!] \wedge \\ \forall j \in [1, i] \, . \, \forall \alpha \in \mathsf{dom}(\vartheta_j) \, . \, \vartheta_i(\alpha) = \vartheta_j(\alpha) \wedge \\ \forall j \in [1, i] \, . \, \vartheta_i(\boldsymbol{\tau}_j') = \vartheta_j(\boldsymbol{\tau}_j') = \boldsymbol{\tau}^j\end{gathered} \tag{40}$$

  - At the next $i + 1^{\text{th}}$ call, we have

    1. By (34) of Lemma 33 and recurrence hyp. (40), $\mathsf{dom}(\vartheta_{i+1}) = \mathsf{dom}(\vartheta_i) \cup \mathsf{vars}[\![\boldsymbol{\tau}_{i+1}']\!] = \mathsf{dom}(\vartheta_0) \cup \bigcup_{j=1}^{i} \mathsf{vars}[\![\boldsymbol{\tau}_j']\!] \cup \mathsf{vars}[\![\boldsymbol{\tau}_{i+1}']\!] = \mathsf{dom}(\vartheta_0) \cup \bigcup_{j=1}^{i+1} \mathsf{vars}[\![\boldsymbol{\tau}_j']\!]$;
    2. By (37) of Lemma 36, we have $\forall \alpha \in \mathsf{dom}(\vartheta_i) \, . \, \vartheta_i(\alpha) = \vartheta_{i+1}(\alpha)$ so that by recurrence hyp. (40), $\forall j \in [1, i+1] \, . \, \forall \alpha \in \mathsf{dom}(\vartheta_j) \, . \, \vartheta_{i+1}(\alpha) = \vartheta_i(\alpha) = \vartheta_j(\alpha)$

3. By (1)., $\forall j \in [1, i+1]$. $\mathsf{vars}[\![\boldsymbol{\tau}'_j]\!] \subseteq \mathsf{dom}(\vartheta_j) \subseteq \mathsf{dom}(\vartheta_{i+1})$ and by (2)., $\forall \alpha \in \mathsf{dom}(\vartheta_j)$. $\vartheta_{i+1}(\alpha) = \vartheta_j(\alpha)$ so that, by (48.30) and (48.30), $\forall j \in [1, i]$. $\vartheta_{i+1}(\boldsymbol{\tau}'_j) = \vartheta_i(\boldsymbol{\tau}'_j) = \vartheta_j(\boldsymbol{\tau}'_j) = \boldsymbol{\tau}^j$. Moreover, $\vartheta_{i+1}(\boldsymbol{\tau}'_{i+1}) = \boldsymbol{\tau}^{i+1}$, by induction on the sequence of calls to lub'. Grouping all cases $j \in [1, i]$ and $j = i+1$ together, we have $\forall j \in [1, i+1]$. $\vartheta_{i+1}(\boldsymbol{\tau}'_j) = \vartheta_j(\boldsymbol{\tau}'_j) = \boldsymbol{\tau}^j$. □

By recurrence, (40) holds for $i = n$. Therefore $\vartheta'(\boldsymbol{\tau}') = \vartheta_n(f(\boldsymbol{\tau}'_1, \ldots, \boldsymbol{\tau}'_n)) = f(\vartheta_n(\boldsymbol{\tau}'_1), \ldots, \vartheta_n(\boldsymbol{\tau}'_n)) = f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n) = \boldsymbol{\tau}$.

- In case (17.7), we have $\exists \beta \in \mathsf{dom}(T_0)$. $T_0(\beta) = \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle \wedge \boldsymbol{\tau}' = \gamma$ so that by Lemma 23, we have $\gamma \in \mathsf{dom}(\vartheta_0) \wedge \vartheta_0(\gamma) = \beta$. It follows that $\vartheta'(\boldsymbol{\tau}') = \vartheta_0(\gamma) = \beta = \boldsymbol{\tau}$.
- Finally, in case (17.9), by (17.9) and Lemma 21, we have $\vartheta'(\boldsymbol{\tau}') = \beta[\gamma \leftarrow \vartheta_0](\gamma) = \beta = \boldsymbol{\tau}$. □

Proof of Theorem 48.100 By Lemma 16, $[\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)]_{\simeq^\nu}$ is a $\preceq_{\simeq^\nu}$-upper-bound of $[\boldsymbol{\tau}_1]_{\simeq^\nu}$ and $[\boldsymbol{\tau}_2]_{\simeq^\nu}$. By Lemma 20, so is $[\mathsf{lgc}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)]_{\simeq^\nu}$.

Now if $[\boldsymbol{\tau}']_{\simeq^\nu}$ is any $\preceq_{\simeq^\nu}$-upper-bound of $[\boldsymbol{\tau}_1]_{\simeq^\nu}$ and $[\boldsymbol{\tau}_2]_{\simeq^\nu}$ then by Exercise 48.16, $\exists \vartheta_1, \vartheta_2$. $\vartheta_1(\boldsymbol{\tau}') = \boldsymbol{\tau}_1 \wedge \vartheta_2(\boldsymbol{\tau}') = \boldsymbol{\tau}_2$, which is the precondition (17.13). It follows that the call to $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \varnothing, \boldsymbol{\tau}', \varepsilon, \varnothing)$ terminates (by Lemma 16 and 20) and returns $\langle \mathsf{lgc}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2), T, \vartheta' \rangle$ such that $\vartheta'(\boldsymbol{\tau}') = \mathsf{lgc}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)$ (by (39) of Lemma 38). By Exercise 48.16, this means that $\mathsf{lgc}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2) \preceq_{\simeq^\nu} [\boldsymbol{\tau}']_{\simeq^\nu}$. This proves by Lem. 20) that $\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)$ is the $\preceq_{\simeq^\nu}$-least upper-bound of $[\boldsymbol{\tau}_1]_{\simeq^\nu}$ and $[\boldsymbol{\tau}_2]_{\simeq^\nu}$. □

[1] Patrick Cousot. *Asynchronous iterative methods for solving a fixed point system of monotone equations in a complete lattice*. Tech. rep. R.R. 88. 15 p. Grenoble, France: Laboratoire IMAG, Université scientifique et médicale de Grenoble, Sept. 1977 (37).

[2] Patrick Cousot and Radhia Cousot. "Automatic synthesis of optimal invariant assertions: Mathematical foundations". *SIGART Newsl.* 64 (1977), pp. 1–12 (37).

[3] Michael Karr. "Affine Relationships Among Variables of a Program". *Acta Inf.* 6 (1976), pp. 133–151 (12).

[4] Gary A. Kildall. "A Unified Approach to Global Program Optimization". In: *POPL*. ACM Press, 1973, pp. 194–206 (12).

[5] Oleg Kiselyov. "Effects Without Monads: Non-determinism - Back to the Meta Language". In: *ML/OCaml*. Vol. 294. EPTCS. 2017, pp. 15–40 (12).

[6] Jens Knoop, Dirk Koschützki, and Bernhard Steffen. "Basic-Block Graphs: Living Dinosaurs?" In: *CC*. Vol. 1383. Lecture Notes in Computer Science. Springer, 1998, pp. 65–79 (12).

[7] Jens Knoop and Oliver Rüthing. "Constant Propagation on the Value Graph: Simple Constants and Beyond". In: *CC*. Vol. 1781. Lecture Notes in Computer Science. Springer, 2000, pp. 94–109 (12).

[8] Pedro López-García, Francisco Bueno, and Manuel V. Hermenegildo. "Automatic Inference of Determinacy and Mutual Exclusion for Logic Programs Using Mode and Type Analyses". *New Generation Comput.* 28.2 (2010), pp. 177–206 (12).

[9] Markus Müller-Olm and Oliver Rüthing. "On the Complexity of Constant Propagation". In: *ESOP*. Vol. 2028. Lecture Notes in Computer Science. Springer, 2001, pp. 190–205 (12).

[10] Mark N. Wegman and F. Kenneth Zadeck. "Constant Propagation with Conditional Branches". *ACM Trans. Program. Lang. Syst.* 13.2 (1991), pp. 181–210 (12).