Mathematical Proofs
in Complement of the Book

Principles of Abstract Interpretation

MIT Press, 2021

Patrick Cousot

New York University

December 29, 2020

1 Mathematical Proofs of Chapter 4

Proof of Lemma 4.18 The lemma trivially holds if $\mathsf{escape}[\![\mathtt{S}]\!] = \mathtt{ff}$. Otherwise $\mathsf{escape}[\![\mathtt{S}]\!] = \mathtt{tt}$ 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 $\mathsf{escape}[\![\mathtt{Sl}]\!] = \mathtt{tt}$, 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 $\mathsf{escape}[\![\mathtt{Sl}']\!] = \mathtt{tt}$ 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 4.15, 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 to lemma 4.17, proving $\mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \neq \mathsf{after}[\![\mathtt{Sl}']\!]$;
  - If $\mathsf{escape}[\![\mathtt{S}]\!] = \mathtt{tt}$ 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 $\mathsf{escape}[\![\mathtt{S}_t]\!] = \mathsf{escape}[\![\mathtt{S}]\!] = \mathtt{tt}$, $\mathsf{after}[\![\mathtt{S}_t]\!] = \mathsf{after}[\![\mathtt{S}]\!]$, $\mathsf{break\text{-}to}[\![\mathtt{S}_t]\!] = \mathsf{break\text{-}to}[\![\mathtt{S}]\!]$, and $\mathsf{break\text{-}to}[\![\mathtt{S}]\!] \neq \mathsf{after}[\![\mathtt{S}]\!]$ by induction hypothesis because $\delta(\mathtt{S}_t) = \delta(\mathtt{S}) + 1$, 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 $\mathtt{S} ::= \mathtt{\{\ Sl\ \}}$. $\square$

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\qquad\qquad\qquad\qquad\wr\text{definition (41.3) of } \alpha^{\exists l}_{\text{use,mod}}[\![\texttt{S}]\!] \text{ for } \texttt{Sl} ::= \epsilon\ \texttt{S}\wr\\
=\ &\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\wr\text{definition of } \mathcal{S}^*[\![\ \epsilon\ \texttt{S}]\!]\wr\\
=\ &\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\wr\text{(6.15) so that } \mathcal{S}^*[\![\ \epsilon\ ]\!] = \{\langle\pi_0\textsf{at}[\![\texttt{S}]\!],\ \textsf{at}[\![\texttt{S}]\!]\rangle \mid \pi_0\textsf{at}[\![\texttt{S}]\!] \in \mathbb{T}^+\} \text{ and } \langle\pi_0\textsf{at}[\![\texttt{S}]\!],\ \textsf{at}[\![\texttt{S}]\!]\rangle \in\\
&\qquad\ \ \mathcal{S}^*[\![\texttt{S}]\!] \text{ by (6.11)}\wr\\
=\ &\alpha^{\exists l}_{\text{use,mod}}[\![\texttt{Sl}]\!]\ (\mathcal{S}^*[\![\texttt{S}]\!])\ L_b, L_e\qquad\qquad\wr\text{definition (41.3) of } \alpha^{\exists l}_{\text{use,mod}}[\![\texttt{S}]\!]\wr\\
=\ &\alpha^{\exists l}_{\text{use,mod}}[\![\texttt{S}]\!]\ (\mathcal{S}^*[\![\texttt{S}]\!])\ L_b, L_e\\
&\qquad\wr\text{(41.3) because } \textsf{after}[\![\texttt{Sl}]\!] = \textsf{after}[\![\texttt{S}]\!],\ \textsf{escape}[\![\texttt{Sl}]\!] = \textsf{escape}[\![\texttt{S}]\!], \text{ and } \textsf{break-to}[\![\texttt{Sl}]\!] =\\
&\qquad\ \ \textsf{break-to}[\![\texttt{S}]\!] \text{ when } \texttt{Sl}' = \epsilon\wr\\
\subseteq\ &\widehat{\mathcal{S}}^{\exists l}[\![\texttt{S}]\!]\ L_b, L_e\qquad\qquad\wr\text{induction hypothesis for theorem 41.24}\wr\\
=\ &\widehat{\mathcal{S}}^{\exists l}[\![\texttt{S}]\!]\ L_b, (\widehat{\mathcal{S}}^{\exists l}[\![\ \epsilon\ ]\!]\ L_b, L_e)\qquad\wr\text{because } \widehat{\mathcal{S}}^{\exists l}[\![\ \epsilon\ ]\!]\ L_b, L_e \triangleq L_e \text{ by (41.22)}\wr
\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, $\alpha^{\exists l}_{\text{use,mod}}[\![\texttt{Sl}]\!]\ L_b, L_e = \alpha^{\exists l}_{\text{use,mod}}[\![\texttt{Sl}']\!]\ L_b, L_e \subseteq \widehat{\mathcal{S}}^{\exists l}[\![\texttt{Sl}']\!]\ L_b, (\widehat{\mathcal{S}}^{\exists l}[\![\texttt{S}]\!]\ L_b, L_e) \triangleq \widehat{\mathcal{S}}^{\exists l}[\![\texttt{Sl}]\!]\ L_b, L_e$ because $\widehat{\mathcal{S}}^{\exists l}[\![\texttt{S}]\!]\ L_b, L_e = L_e$ when $\texttt{S}$ is empty.

- Otherwise, $\texttt{Sl}' \neq \epsilon$ and $\texttt{S} \neq \texttt{\{ ...\{ }\ \epsilon\ \texttt{\}... \}}$ so, by lemma 4.16, $\textsf{after}[\![\texttt{S}]\!] \notin \textsf{in}[\![\texttt{S}]\!]$. In that case, let us calculate □

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

$= \bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [1, n-1] \,.\, \forall j \in [1, i-1] \,.\, \mathtt{x} \notin \mathtt{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathtt{use}[\![\mathtt{a}_i]\!]\} \cup (\!\!|\, \ell_n = \mathsf{after}[\![\mathtt{S1}]\!] \;?\; L_e \;⨾\; \varnothing \,|\!\!) \cup (\!\!|\, \mathsf{escape}[\![\mathtt{S1}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S1}]\!] \;?\; L_b \;⨾\; \varnothing \,|\!\!) \mid \langle \pi_0,\, \pi_1 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S1}]\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \dots \xrightarrow{\mathtt{a}_{n-1}} \ell_n\}$ ≀By lemma 41.8, omitting the useless parameters of $\mathtt{use}$ and $\mathtt{mod}$∫

$= \bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [1, n-1] \,.\, \forall j \in [1, i-1] \,.\, \mathtt{x} \notin \mathtt{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathtt{use}[\![\mathtt{a}_i]\!]\} \cup (\!\!|\, \ell_n = \mathsf{after}[\![\mathtt{S}]\!] \;?\; L_e \;⨾\; \varnothing \,|\!\!) \cup (\!\!|\, \mathsf{escape}[\![\mathtt{S1}']\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S1}']\!] \;?\; L_b \;⨾\; \varnothing \,|\!\!) \cup (\!\!|\, \mathsf{escape}[\![\mathtt{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] \;?\; L_b \;⨾\; \varnothing \,|\!\!) \mid \langle \pi_0,\, \pi_1 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S1}']\!] \cup \{\langle \pi_0 \frown \pi_2,\, \pi_2 \frown \pi_3 \rangle \mid \langle \pi_0,\, \pi_2 \rangle \in \boldsymbol{\mathcal{S}}^+[\![\mathtt{S1}']\!] \wedge \langle \pi_0 \frown \pi_2,\, \pi_3 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}]\!]\} \wedge \pi_1 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \dots \xrightarrow{\mathtt{a}_{n-1}} \ell_n\}$

≀definitions of $\boldsymbol{\mathcal{S}}^*[\![\mathtt{S1}]\!]$, $\mathsf{after}[\![\mathtt{S1}]\!] = \mathsf{after}[\![\mathtt{S}]\!]$ in section 4.2.2, $\mathsf{escape}[\![\mathtt{S1}]\!] \triangleq \mathsf{escape}[\![\mathtt{S1}']\!] \vee \mathsf{escape}[\![\mathtt{S}]\!]$, and $\mathsf{break\text{-}to}[\![\mathtt{S1}']\!] \triangleq \mathsf{break\text{-}to}[\![\mathtt{S}]\!] \triangleq \mathsf{break\text{-}to}[\![\mathtt{S1}]\!]$ in section 4.2.4 ∫

$= \bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [1, n-1] \,.\, \forall j \in [1, i-1] \,.\, \mathtt{x} \notin \mathtt{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathtt{use}[\![\mathtt{a}_i]\!]\} \cup (\!\!|\, \ell_n = \mathsf{after}[\![\mathtt{S}]\!] \;?\; L_e \;⨾\; \varnothing \,|\!\!) \cup (\!\!|\, \mathsf{escape}[\![\mathtt{S1}']\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S1}']\!] \;?\; L_b \;⨾\; \varnothing \,|\!\!) \cup (\!\!|\, \mathsf{escape}[\![\mathtt{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] \;?\; L_b \;⨾\; \varnothing \,|\!\!) \mid \langle \pi_0,\, \pi_1 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S1}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \dots \xrightarrow{\mathtt{a}_{n-1}} \ell_n\} \cup$
$\bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [1, n-1] \,.\, \forall j \in [1, i-1] \,.\, \mathtt{x} \notin \mathtt{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathtt{use}[\![\mathtt{a}_i]\!]\} \cup (\!\!|\, \ell_n = \mathsf{after}[\![\mathtt{S}]\!] \;?\; L_e \;⨾\; \varnothing \,|\!\!) \cup (\!\!|\, \mathsf{escape}[\![\mathtt{S1}']\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S1}']\!] \;?\; L_b \;⨾\; \varnothing \,|\!\!) \cup (\!\!|\, \mathsf{escape}[\![\mathtt{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] \;?\; L_b \;⨾\; \varnothing \,|\!\!) \mid \langle \pi_0,\, \pi_2 \rangle \in \boldsymbol{\mathcal{S}}^+[\![\mathtt{S1}']\!] \wedge \langle \pi_0 \frown \pi_2,\, \pi_3 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}]\!] \wedge \pi_2 \frown \pi_3 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \dots \xrightarrow{\mathtt{a}_{n-1}} \ell_n\}$

≀definition of $\cup$ and definition of $\in$ so $\langle \pi_0,\, \pi_1 \rangle = \langle \pi_0 \frown \pi_2,\, \pi_2 \frown \pi_3 \rangle$∫

$\subseteq \bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [1, m-1] \,.\, \forall j \in [1, i-1] \,.\, \mathtt{x} \notin \mathtt{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathtt{use}[\![\mathtt{a}_i]\!]\} \cup (\!\!|\, \mathsf{escape}[\![\mathtt{S1}']\!] \wedge \ell_m = \mathsf{break\text{-}to}[\![\mathtt{S1}']\!] \;?\; L_b \;⨾\; \varnothing \,|\!\!) \mid \langle \pi_0,\, \pi_1 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S1}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \dots \xrightarrow{\mathtt{a}_{m-1}} \ell_m\} \cup$
$\bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [1, n-1] \,.\, \forall j \in [1, i-1] \,.\, \mathtt{x} \notin \mathtt{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathtt{use}[\![\mathtt{a}_i]\!]\} \cup (\!\!|\, \ell_n = \mathsf{after}[\![\mathtt{S}]\!] \;?\; L_e \;⨾\; \varnothing \,|\!\!) \cup (\!\!|\, \mathsf{escape}[\![\mathtt{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] \;?\; L_b \;⨾\; \varnothing \,|\!\!) \mid \langle \pi_0,\, \pi_1 \rangle \in \boldsymbol{\mathcal{S}}^+[\![\mathtt{S1}']\!] \wedge \langle \pi_0',\, \pi_3 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}]\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \dots \xrightarrow{\mathtt{a}_{m-1}} \ell_m \wedge \ell_m = \mathsf{after}[\![\mathtt{S1}']\!] \wedge \pi_3 = \ell_m \xrightarrow{\mathtt{a}_m} \ell_{m+1} \xrightarrow{\mathtt{a}_{m+1}} \dots \xrightarrow{\mathtt{a}_{n-1}} \ell_n\}$

≀— For the first term, $\langle \pi_0,\, \pi_1 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S1}']\!]$, π_1 ends in ℓ_n, and $\ell_n = \mathsf{after}[\![\mathtt{S}]\!]$ is impossible because $\mathtt{S1}'$ and $\mathtt{S}$ are not empty. Moreover, if $\ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] = \mathsf{break\text{-}to}[\![\mathtt{S1}']\!]$ then $\mathtt{a}_{n-1}$ is a break, so $\mathsf{escape}[\![\mathtt{S1}']\!]$ holds. L_b is included in $(\!\!|\, \mathsf{escape}[\![\mathtt{S1}']\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S1}']\!] \;?\; L_b \;⨾\; \varnothing \,|\!\!)$ and so $(\!\!|\, \mathsf{escape}[\![\mathtt{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] \;?\; L_b \;⨾\; \varnothing \,|\!\!)$ is redundant. Finally, renaming $n \leftarrow m$.∫

≀— For the second term, if $\ell_n = \mathsf{break\text{-}to}[\![\mathtt{S1}']\!] = \mathsf{break\text{-}to}[\![\mathtt{S}]\!]$ then $\mathtt{a}_{n-1}$ is a break, so $\mathsf{escape}[\![\mathtt{S}]\!]$ holds. L_b is included in $(\!\!|\, \mathsf{escape}[\![\mathtt{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] \;?\; L_b \;⨾\; \varnothing \,|\!\!)$ and so $(\!\!|\, \mathsf{escape}[\![\mathtt{S1}']\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S1}']\!] \;?\; L_b \;⨾\; \varnothing \,|\!\!)$ is redundant. Moreover, $\pi_2 \frown \pi_3 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \dots \xrightarrow{\mathtt{a}_{n-1}} \ell_n$ is decomposed into $\pi_2 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \dots \xrightarrow{\mathtt{a}_{m-1}} \ell_m$ and $\pi_3 = \ell_m \xrightarrow{\mathtt{a}_m} \ell_{m+1} \xrightarrow{\mathtt{a}_{m+1}} \dots \xrightarrow{\mathtt{a}_{n-1}} \ell_n$ where, by $\langle \pi_0,\, \pi_2 \rangle \in \boldsymbol{\mathcal{S}}^+[\![\mathtt{S1}']\!]$ and $\langle \pi_0 \frown \pi_2,\, \pi_3 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}]\!]$, $\ell_m = \mathsf{after}[\![\mathtt{S1}']\!] = \mathsf{at}[\![\mathtt{S}]\!]$. Moreover, $\pi_0 \frown \pi_2$ is generalized to π_0' (whence inclusion) and π_2 is renamed into π_1. ∫

$$
\begin{aligned}
&= \bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [1, m-1] \,.\, \forall j \in [1, i-1] \,.\, \mathtt{x} \notin \mathtt{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathtt{use}[\![\mathtt{a}_i]\!]\} \cup \llparenthesis\, \mathsf{escape}[\![\mathtt{S1}']\!] \wedge \ell_m = \mathsf{break\text{-}to}[\![\mathtt{S1}']\!] \mathrel{?} L_b \mathrel{⸾} \varnothing \,\rrparenthesis \mid \langle \pi_0,\ \pi_1 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S1}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \ldots \xrightarrow{\mathtt{a}_{m-1}} \ell_m\} \cup {} \\
&\quad \bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [m, n-1] \,.\, \forall j \in [1, i-1] \,.\, \mathtt{x} \notin \mathtt{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathtt{use}[\![\mathtt{a}_i]\!]\} \cup \llparenthesis\, \ell_n = \mathsf{after}[\![\mathtt{S}]\!] \mathrel{?} L_e \mathrel{⸾} \varnothing \,\rrparenthesis \cup \llparenthesis\, \mathsf{escape}[\![\mathtt{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] \mathrel{?} L_b \mathrel{⸾} \varnothing \,\rrparenthesis \mid \langle \pi_0,\ \pi_1 \rangle \in \boldsymbol{\mathcal{S}}^+[\![\mathtt{S1}']\!] \wedge \langle \pi_0',\ \pi_3 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}]\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \ldots \xrightarrow{\mathtt{a}_{m-1}} \ell_m \wedge \ell_m = \mathsf{after}[\![\mathtt{S1}']\!] \wedge \pi_3 = \ell_m \xrightarrow{\mathtt{a}_m} \ell_{m+1} \xrightarrow{\mathtt{a}_{m+1}} \ldots \xrightarrow{\mathtt{a}_{n-1}} \ell_n\}
\end{aligned}
$$

⟅because the case $i \in [1, m-1]$ of the second term is already incorporated in the first term⟆

$$
\begin{aligned}
&= \bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [1, m-1] \,.\, \forall j \in [1, i-1] \,.\, \mathtt{x} \notin \mathtt{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathtt{use}[\![\mathtt{a}_i]\!]\} \cup \llparenthesis\, \ell_m = \mathsf{after}[\![\mathtt{S1}']\!] \mathrel{?} \Big(\bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [m, n-1] \,.\, \forall j \in [1, i-1] \,.\, \mathtt{x} \notin \mathtt{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathtt{use}[\![\mathtt{a}_i]\!]\} \cup \llparenthesis\, \ell_n = \mathsf{after}[\![\mathtt{S}]\!] \mathrel{?} L_e \mathrel{⸾} \varnothing \,\rrparenthesis \cup \llparenthesis\, \mathsf{escape}[\![\mathtt{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] \mathrel{?} L_b \mathrel{⸾} \varnothing \,\rrparenthesis \mid \langle \pi_0',\ \pi_3 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}]\!] \wedge \pi_3 = \ell_m \xrightarrow{\mathtt{a}_m} \ell_{m+1} \xrightarrow{\mathtt{a}_{m+1}} \ldots \xrightarrow{\mathtt{a}_{n-1}} \ell_n\}\Big) \mathrel{⸾} \varnothing \,\rrparenthesis \cup \llparenthesis\, \mathsf{escape}[\![\mathtt{S1}']\!] \wedge \ell_m = \mathsf{break\text{-}to}[\![\mathtt{S1}']\!] \mathrel{?} L_b \mathrel{⸾} \varnothing \,\rrparenthesis \mid \langle \pi_0,\ \pi_1 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S1}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \ldots \xrightarrow{\mathtt{a}_{m-1}} \ell_m\}
\end{aligned}
$$

⟅incorporating the second term in the first term, in case $\ell_m = \mathsf{after}[\![\mathtt{S1}']\!]$⟆

$$
\begin{aligned}
&\subseteq \bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [1, m-1] \,.\, \forall j \in [1, i-1] \,.\, \mathtt{x} \notin \mathtt{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathtt{use}[\![\mathtt{a}_i]\!]\} \cup \llparenthesis\, \ell_m = \mathsf{after}[\![\mathtt{S1}']\!] \mathrel{?} (\bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [m, n-1] \,.\, \forall j \in [m, i-1] \,.\, \mathtt{x} \notin \mathtt{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathtt{use}[\![\mathtt{a}_i]\!]\} \cup \llparenthesis\, \ell_n = \mathsf{after}[\![\mathtt{S}]\!] \mathrel{?} L_e \mathrel{⸾} \varnothing \,\rrparenthesis \cup \llparenthesis\, \mathsf{escape}[\![\mathtt{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] \mathrel{?} L_b \mathrel{⸾} \varnothing \,\rrparenthesis \mid \langle \pi_0',\ \pi_3 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}]\!] \wedge \pi_3 = \ell_m \xrightarrow{\mathtt{a}_m} \ell_{m+1} \xrightarrow{\mathtt{a}_{m+1}} \ldots \xrightarrow{\mathtt{a}_{n-1}} \ell_n\}) \mathrel{⸾} \varnothing \,\rrparenthesis \cup \llparenthesis\, \mathsf{escape}[\![\mathtt{S1}']\!] \wedge \ell_m = \mathsf{break\text{-}to}[\![\mathtt{S1}']\!] \mathrel{?} L_b \mathrel{⸾} \varnothing \,\rrparenthesis \mid \langle \pi_0,\ \pi_1 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S1}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \ldots \xrightarrow{\mathtt{a}_{m-1}} \ell_m\}
\end{aligned}
$$

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

$$
\begin{aligned}
&= \bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [1, m-1] \,.\, \forall j \in [1, i-1] \,.\, \mathtt{x} \notin \mathtt{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathtt{use}[\![\mathtt{a}_i]\!]\} \cup \llparenthesis\, \ell_m = \mathsf{after}[\![\mathtt{S1}']\!] \mathrel{?} (\bigcup\{\alpha^{l}_{\mathtt{use},\mathtt{mod}}[\![\mathtt{S}]\!]\ L_b, L_e\ \langle \pi_0',\ \pi_3 \rangle \mid \langle \pi_0',\ \pi_3 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}]\!]\}) \mathrel{⸾} \varnothing \,\rrparenthesis \cup \llparenthesis\, \mathsf{escape}[\![\mathtt{S1}']\!] \wedge \ell_m = \mathsf{break\text{-}to}[\![\mathtt{S1}']\!] \mathrel{?} L_b \mathrel{⸾} \varnothing \,\rrparenthesis \mid \langle \pi_0,\ \pi_1 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S1}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \ldots \xrightarrow{\mathtt{a}_{m-1}} \ell_m\}
\end{aligned}
$$

⟅lemma 41.8⟆

$$
\subseteq \bigcup\{\alpha^{l}_{\mathtt{use},\mathtt{mod}}[\![\mathtt{S1}']\!]\ L_b, (\boldsymbol{\mathcal{S}}^{\exists l}[\![\mathtt{S}]\!]\ L_b, L_e)\ \langle \pi_0,\ \pi_1 \rangle \mid \langle \pi_0,\ \pi_1 \rangle \in \widehat{\boldsymbol{\mathcal{S}}}^*[\![\mathtt{S1}']\!]\}
$$

⟅lemma 41.8 and (41.3)⟆

$$
= \alpha^{\exists l}_{\mathtt{use},\mathtt{mod}}[\![\mathtt{S1}']\!](\boldsymbol{\mathcal{S}}^*[\![\mathtt{S1}']\!])\ L_b, (\widehat{\boldsymbol{\mathcal{S}}}^{\exists l}[\![\mathtt{S}]\!]\ L_b, L_e)
$$

⟅definition (41.3) of $\alpha^{\exists l}_{\mathtt{use},\mathtt{mod}}$⟆

$$
\subseteq \widehat{\boldsymbol{\mathcal{S}}}^{\exists l}[\![\mathtt{S1}']\!]\ L_b, (\widehat{\boldsymbol{\mathcal{S}}}^{\exists l}[\![\mathtt{S}]\!]\ L_b, L_e)
$$

⟅induction hypothesis of theorem 41.24: $\alpha^{\exists l}_{\mathtt{use},\mathtt{mod}}[\![\mathtt{S1}']\!](\widehat{\boldsymbol{\mathcal{S}}}^*[\![\mathtt{S1}']\!])\ L_b, (\widehat{\boldsymbol{\mathcal{S}}}^{\exists l}[\![\mathtt{S}]\!]\ L_b, L_e) \subseteq \widehat{\boldsymbol{\mathcal{S}}}^{\exists l}[\![\mathtt{S1}']\!]\ L_b, (\widehat{\boldsymbol{\mathcal{S}}}^{\exists l}[\![\mathtt{S}]\!]\ L_b, L_e)$, Q.E.D.⟆

- For the ***empty statement list*** $\mathtt{Sl} ::= \epsilon$, we have $\mathcal{S}^*[\![\mathtt{Sl}]\!] = \{\langle \pi_0\ell, \ell\rangle\}$ by (6.15), where $\ell = \mathsf{at}[\![\mathtt{Sl}]\!]$ and so

$$\begin{aligned}
& \alpha^{\exists l}_{\mathsf{use,mod}}[\![\mathtt{Sl}]\!]\ (\mathcal{S}^*[\![\mathtt{Sl}]\!])\ L_b, L_e \\
= {} & \bigcup\{\alpha^{l}_{\mathsf{use,mod}}[\![\mathtt{Sl}]\!]\ L_b, L_e\ \langle \pi_0,\ \pi_1\rangle \mid \langle \pi_0,\ \pi_1\rangle\ \in\ \mathcal{S}^*[\![\mathtt{Sl}]\!]\} && \text{(41.3)} \\
= {} & \bigcup\{\alpha^{l}_{\mathsf{use,mod}}[\![\mathtt{Sl}]\!]\ L_b, L_e\ \langle \pi_0,\ \pi_1\rangle \mid \langle \pi_0,\ \pi_1\rangle\ \in\ \{\langle \pi_0\ell,\ \ell\rangle\}\} && \text{definition of } \mathcal{S}^*[\![\mathtt{Sl}]\!] \\
= {} & \alpha^{\exists l}_{\mathsf{use,mod}}[\![\mathtt{Sl}]\!]\ L_b, L_e\ \langle \pi_0\ell,\ \ell\rangle && \text{definitions of } \in \text{ and } \cup \\
= {} & \{\mathtt{x} \in \mathbb{V} \mid (\ell = \mathsf{after}[\![\mathtt{Sl}]\!] \wedge \mathtt{x} \in L_e) \vee (\mathsf{escape}[\![\mathtt{Sl}]\!] \wedge \ell = \mathsf{break\text{-}to}[\![\mathtt{Sl}]\!] \wedge \mathtt{x} \in L_b)\} && \text{(41.3)} \\
= {} & L_e \qquad \ell = \mathsf{at}[\![\mathtt{Sl}]\!] = \mathsf{after}[\![\mathtt{Sl}]\!] \text{ in appendix 4.2.1 and } \mathsf{escape}[\![\mathtt{Sl}]\!] = \mathit{ff} \text{ in 4.2.4 when } \mathtt{Sl} = \epsilon
\end{aligned}$$

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

$$\begin{aligned}
& \widehat{\mathcal{S}}^{\forall d}[\![\mathtt{if\ (B)\ S}_t]\!]\ D_b, D_e \\
= {} & \neg\widehat{\mathcal{S}}^{\exists l}[\![\mathtt{if\ (B)\ S}_t]\!]\ \neg D_b, \neg D_e && \text{definition of } \widehat{\mathcal{S}}^{\forall d}[\![\mathtt{S}]\!] \text{ as dual of } \widehat{\mathcal{S}}^{\exists l}[\![\mathtt{S}]\!] \\
= {} & \neg(\mathbb{use}[\![\mathtt{B}]\!] \cup \neg D_e \cup \widehat{\mathcal{S}}^{\exists l}[\![\mathtt{S}_t]\!]\ \neg D_b, \neg D_e) && \text{(41.22)} \\
= {} & \neg\, \mathbb{use}[\![\mathtt{B}]\!] \cap \neg\neg D_e \cap \neg\widehat{\mathcal{S}}^{\exists l}[\![\mathtt{S}_t]\!]\ \neg D_b, \neg D_e) && \text{De Morgan's laws} \\
= {} & \neg\, \mathbb{use}[\![\mathtt{B}]\!] \cap D_e \cap \widehat{\mathcal{S}}^{\forall d}[\![\mathtt{S}_t]\!]\ D_b, D_e && \text{structural induction hypothesis}
\end{aligned}$$

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

$$\begin{aligned}
& \mathcal{M}^{\dagger}[\![\mathtt{S}]\!]\langle \underline{\varrho},\ \varepsilon\rangle \\
\triangleq {} & \mathcal{M}^{\dagger}\langle \underline{\varrho},\ \varepsilon\rangle(\widehat{\mathcal{S}}^{*}_{\mathbb{s}}[\![\mathtt{S}]\!]) && \text{(44.26)} \\
= {} & \{\langle \pi,\ \mathtt{R}'\rangle \mid \pi \in \widehat{\mathcal{S}}^{*}_{\mathbb{s}}[\![\mathtt{S}]\!] \wedge \langle \mathit{tt},\ \mathtt{R}'\rangle = \mathcal{M}^{t}\langle \rho,\ \varepsilon\rangle\pi\} && \text{(44.25)} \\
= {} & \{\langle \pi,\ \varepsilon\rangle \mid \pi \in \widehat{\mathcal{S}}^{*}_{\mathbb{s}}[\![\mathtt{S}]\!]\} && \text{because } \mathcal{M}^{t}\langle \underline{\varrho},\ \varepsilon\rangle\pi \triangleq \langle \mathit{tt},\ \varepsilon\rangle \text{ by (44.24)} \\
\triangleq {} & \widehat{\mathcal{M}}^{\dagger}[\![\mathtt{S}]\!]\langle \underline{\varrho},\ \varepsilon\rangle && \text{(44.41)}
\end{aligned}$$

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

$$\begin{aligned}
& \mathcal{M}^{\dagger}[\![\mathtt{Sl}]\!]\ \langle \underline{\varrho},\ \mathtt{R}\rangle \\
= {} & \mathcal{M}^{\dagger}\langle \underline{\varrho},\ \mathtt{R}\rangle(\widehat{\mathcal{S}}^{*}_{\mathbb{s}}[\![\mathtt{Sl}]\!]) && \text{(44.26)} \\
= {} & \{\langle \pi,\ \mathtt{R}'\rangle \mid \pi \in \widehat{\mathcal{S}}^{*}_{\mathbb{s}}[\![\mathtt{Sl}]\!] \wedge \langle \mathit{tt},\ \mathtt{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R}\rangle\pi\} && \text{(44.25)}
\end{aligned}$$

$$= \{\langle \pi,\ \mathtt{R}'\rangle \mid \pi \in \{\langle \mathsf{at}[\![\mathtt{S1}]\!],\ \rho\rangle \mid \rho \in \mathbb{E}\mathrm{v}\} \wedge \langle \mathrm{tt},\ \mathtt{R}'\rangle = \boldsymbol{\mathcal{M}}^t\langle \underline{\varrho},\ \mathtt{R}\rangle\pi\} \qquad \text{(42.10)}$$

$$= \{\langle\langle \mathsf{at}[\![\mathtt{S1}]\!],\ \rho\rangle,\ \mathtt{R}'\rangle \mid \rho \in \mathbb{E}\mathrm{v} \wedge \langle \mathrm{tt},\ \mathtt{R}'\rangle = \boldsymbol{\mathcal{M}}^t\langle \underline{\varrho},\ \mathtt{R}\rangle(\langle \mathsf{at}[\![\mathtt{S1}]\!],\ \rho\rangle)\} \qquad \text{(definition of } \in\text{)}$$

$$= \{\langle\langle \mathsf{at}[\![\mathtt{S1}]\!],\ \rho\rangle,\ \mathtt{R}'\rangle \mid \rho \in \mathbb{E}\mathrm{v} \wedge \langle \mathtt{L} : \mathtt{B},\ \mathtt{R}'\rangle = \mathsf{fstnxt}(\mathtt{R}) \wedge \langle \underline{\varrho},\ \langle \mathsf{at}[\![\mathtt{S1}]\!],\ \rho\rangle\rangle \in \boldsymbol{\mathcal{S}}^{\mathsf{r}}[\![\mathtt{L} : \mathtt{B}]\!]\}$$

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

$$= \widehat{\boldsymbol{\mathcal{M}}}^{\dagger}[\![\mathtt{S1}]\!]\langle \underline{\varrho},\ \mathtt{R}\rangle \qquad \text{(44.43)}$$

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

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

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

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

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

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

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

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

- In case (44.49) of an iteration statement $\mathtt{S} ::= \mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b$, we apply corollary 18.33 so we have to calculate the abstract transformer that satisfies the commutation property for an iterate X of the concrete transformer $\mathscr{F}^{*}_{\mathbb{S}}[\![\mathtt{S}]\!]$ (which traces must be of the form $\pi\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle$).

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

$$= \boldsymbol{\mathcal{M}}^{\dagger}\langle \underline{\varrho},\ \mathtt{R}\rangle(\{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathrm{v}\} \cup \{\pi_2\langle \ell',\ \rho\rangle\langle \mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle \mid \pi_2\langle \ell',\ \rho\rangle \in X \wedge \boldsymbol{\mathcal{B}}[\![\mathtt{B}]\!]\,\rho = \mathrm{ff} \wedge \ell' = \ell\} \cup \{\pi_2\langle \ell',\ \rho\rangle\langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho\rangle\cdot\pi_3 \mid \pi_2\langle \ell',\ \rho\rangle \in X \wedge \boldsymbol{\mathcal{B}}[\![\mathtt{B}]\!]\,\rho = \mathrm{tt} \wedge \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho\rangle\cdot\pi_3 \in \widehat{\boldsymbol{\mathcal{S}}}^{\,*}_{\mathbb{s}}[\![\mathtt{S}_b]\!] \wedge \ell' = \ell\}) \qquad \text{(42.6)}$$

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

$$\text{(Galois connection (44.30), so that, by lemma 11.37, } \boldsymbol{\mathcal{M}}^{\dagger}\langle \underline{\varrho},\ \mathtt{R}\rangle \text{ preserves joins)}$$

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

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

$$\boldsymbol{\mathcal{M}}^{\dagger}\langle \underline{\varrho},\ \mathtt{R}\rangle(\{\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle \mid \rho \in \mathbb{E}\mathrm{v}\}$$

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

— The second case is that of the loop exit

$\mathcal{M}^{\dagger}\langle\underline{\varrho},\ \mathtt{R}\rangle(\{\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle\mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle \mid \pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\,\rho = \mathsf{ff}\})$

$= \{\langle\pi, \mathtt{R}'\rangle \mid \pi \in \{\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!], \rho\rangle\langle\mathsf{after}[\![\mathtt{S}]\!], \rho\rangle \mid \pi_2\langle\mathsf{at}[\![\mathtt{S}]\!], \rho\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\rho = \mathsf{ff}\} \wedge \langle\mathsf{tt}, \mathtt{R}'\rangle = \mathcal{M}^{t}\langle\underline{\varrho}, \mathtt{R}\rangle\pi\}$ ≀(44.25)∫

$= \{\langle\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle\mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle,\ \mathtt{R}'\rangle \mid \pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\ \rho = \mathsf{ff} \wedge \langle\mathsf{tt},\ \mathtt{R}'\rangle = \mathcal{M}^{t}\langle\underline{\varrho}, \mathtt{R}\rangle(\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle\mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle)\}$ ≀definition of $\in$∫

$= \{\langle\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle\mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle,\ \mathtt{R}'\rangle \mid \pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\ \rho = \mathsf{ff} \wedge \exists \mathtt{R}'' \in \mathbb{R}\ .\ \mathcal{M}^{t}\langle\underline{\varrho}, \mathtt{R}\rangle(\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle) = \langle\mathsf{tt}, \mathtt{R}''\rangle \wedge \mathcal{M}^{t}\langle\underline{\varrho}, \mathtt{R}''\rangle(\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle\mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle) = \langle\mathsf{tt}, \mathtt{R}'\rangle\}$ ≀lemma 44.37∫

$= \{\langle\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle\mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle, \mathtt{R}'\rangle \mid \langle\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle, \mathtt{R}''\rangle \in \{\langle\pi, \mathtt{R}''\rangle \mid \pi \in X \wedge \langle\mathsf{tt}, \mathtt{R}''\rangle = \mathcal{M}^{t}\langle\underline{\varrho}, \mathtt{R}\rangle\pi\} \wedge \mathcal{B}[\![\mathtt{B}]\!]\ \rho = \mathsf{ff} \wedge \mathcal{M}^{t}\langle\underline{\varrho},\ \mathtt{R}''\rangle(\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle\mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle) = \langle\mathsf{tt},\ \mathtt{R}'\rangle\}$

≀X is an iterate of the concrete transformer $\mathcal{F}_{\mathbb{S}}^{*}[\![\mathtt{S}]\!]$ so its traces must be of the form $\pi\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle$∫

$= \{\langle\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle\mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle,\ \mathtt{R}'\rangle \mid \langle\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle,\ \mathtt{R}''\rangle \in \mathcal{M}^{\dagger}\langle\underline{\varrho},\ \mathtt{R}\rangle X \wedge \mathcal{B}[\![\mathtt{B}]\!]\ \rho = \mathsf{ff} \wedge \mathcal{M}^{t}\langle\underline{\varrho}, \mathtt{R}''\rangle(\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle\mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle) = \langle\mathsf{tt},\ \mathtt{R}'\rangle\}$ ≀(44.25) ∫

$= \{\langle\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle\mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle,\ \varepsilon\rangle \mid \langle\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle,\ \varepsilon\rangle \in \mathcal{M}^{\dagger}\langle\underline{\varrho},\ \mathtt{R}\rangle X \wedge \mathcal{B}[\![\mathtt{B}]\!]\ \rho = \mathsf{ff}\} \cup \{\langle\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle\mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle,\ \mathtt{R}'\rangle \mid \langle\pi_2\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle,\ \mathtt{R}''\rangle \in \mathcal{M}^{\dagger}\langle\underline{\varrho},\ \mathtt{R}\rangle X \wedge \mathcal{B}[\![\mathtt{B}]\!]\ \rho = \mathsf{ff} \wedge \mathtt{R}'' \notin \mathbb{R}_{\varepsilon} \wedge \mathcal{M}^{t}\langle\underline{\varrho},\ \mathtt{R}''\rangle(\langle\mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle\mathsf{after}[\![\mathtt{S}]\!],\ \rho\rangle) = \langle\mathsf{tt},\ \mathtt{R}'\rangle\}$

≀case analysis and $\mathcal{M}^{t}\langle\underline{\varrho},\ \varepsilon\rangle\pi \triangleq \langle\mathsf{tt},\ \varepsilon\rangle$ in (44.24)∫

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

There are two subsubcases, depending on whether $\mathtt{R}''''$ is empty or not.

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

$= \{\langle \pi_2\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho\rangle\pi_3,\ \varepsilon\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle,\ \mathtt{R}''\rangle \in \mathcal{M}^{+}\langle \underline{\varrho},\ \mathtt{R}\rangle X \wedge \mathcal{B}[\![\mathtt{B}]\!]\,\rho = \mathsf{tt} \wedge \mathtt{R}'' \notin \mathbb{R}_\varepsilon \wedge \langle \mathtt{L}\ :\ \mathtt{B},\ \varepsilon\rangle = \mathsf{fstnxt}(\mathtt{R}'') \wedge \langle \underline{\varrho},\ \langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\rangle \in \mathcal{S}^{\mathfrak{r}}[\![\mathtt{L}\ :\ \mathtt{B}]\!] \wedge \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho\rangle\pi_3 \in \widehat{\mathcal{S}}^{\,*}_{\mathbb{S}}[\![\mathtt{S}_b]\!]\}$ ≀(44.24)∫

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

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

$= \{\langle \pi_2\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho\rangle\pi_3,\ \mathtt{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle,\ \mathtt{R}''\rangle \in \mathcal{M}^{+}\langle \underline{\varrho},\ \mathtt{R}\rangle X \wedge \mathcal{B}[\![\mathtt{B}]\!]\,\rho = \mathsf{tt} \wedge \mathtt{R}'' \notin \mathbb{R}_\varepsilon \wedge \langle \mathtt{L}\ :\ \mathtt{B},\ \mathtt{R}''''\rangle = \mathsf{fstnxt}(\mathtt{R}'') \wedge \langle \underline{\varrho},\ \langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho\rangle\rangle \in \mathcal{S}^{\mathfrak{r}}[\![\mathtt{L}\ :\ \mathtt{B}]\!] \wedge \mathtt{R}'''' \notin \mathbb{R}_\varepsilon \wedge \langle \mathtt{L}'\ :\ \mathtt{B}',\ \mathtt{R}'''\rangle = \mathsf{fstnxt}(\mathtt{R}'''') \wedge \langle \underline{\varrho},\ \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho\rangle\rangle \in \mathcal{S}^{\mathfrak{r}}[\![\mathtt{L}'\ :\ \mathtt{B}']\!] \wedge \langle\langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho\rangle\pi_3,\ \mathtt{R}'\rangle \in \mathcal{M}^{+}[\![\mathtt{S}_b]\!]\langle \underline{\varrho},\ \mathtt{R}'''\rangle\}$ ≀(44.24)∫

— Grouping all cases together we get the term (44.50) defining $\widehat{\mathcal{F}}^{+}[\![\mathtt{S}]\!]\langle \underline{\varrho},\ \mathtt{R}\rangle\ (\mathcal{M}^{+}\langle \underline{\varrho},\ \mathtt{R}\rangle X)$ and so corollary 18.33 and the commutation condition $\mathcal{M}^{+}\langle \underline{\varrho},\ \mathtt{R}\rangle(\mathcal{F}^{*}_{\mathbb{S}}[\![\mathtt{S}]\!](X)) = \widehat{\mathcal{F}}^{+}[\![\mathtt{S}]\!]\langle \underline{\varrho},\ \mathtt{R}\rangle\ (\mathcal{M}^{+}\langle \underline{\varrho},\ \mathtt{R}\rangle(X))$ for the iterates X of $\mathcal{F}^{*}_{\mathbb{S}}[\![\mathtt{S}]\!]$ yield $\widehat{\mathcal{M}}^{+}[\![\mathtt{S}]\!]\langle \underline{\varrho},\ \mathtt{R}\rangle \triangleq \mathsf{lfp}^{\subseteq}(\widehat{\mathcal{F}}^{+}[\![\mathtt{S}]\!]\langle \underline{\varrho},\ \mathtt{R}\rangle)$ that is (44.49).

- In case (44.48) of a break statement `S ::= ℓ break ;`

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

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

$= \{\langle \pi,\ \mathtt{R}'\rangle \mid \pi \in \{\langle \ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \cup \{\langle \ell,\ \rho\rangle\langle \mathsf{break\text{-}to}[\![\mathtt{S}]\!],\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \wedge \langle \mathsf{tt},\ \mathtt{R}'\rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R}\rangle\pi\}$ ≀(42.14)∫

$= \{\langle\langle \ell,\ \rho\rangle,\ \mathtt{R}''\rangle \mid \langle \mathsf{tt},\ \mathtt{R}''\rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R}\rangle\langle \ell,\ \rho\rangle\} \cup \{\langle\langle \ell,\ \rho\rangle\langle \mathsf{break\text{-}to}[\![\mathtt{S}]\!],\ \rho\rangle,\ \mathtt{R}''\rangle \mid \langle \mathsf{tt},\ \mathtt{R}''\rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R}\rangle(\langle \ell,\ \rho\rangle\langle \mathsf{break\text{-}to}[\![\mathtt{S}]\!],\ \rho\rangle)\}$ ≀definitions of ∪ and ∈∫

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

$\wr \mathtt{R} \notin \mathbb{R}_\varepsilon$, case analysis on $\mathtt{R}' \in \mathbb{R}_\varepsilon$, 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 $\mathtt{S}$, or in the true branch $\mathtt{S}_t$.

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

— (2) — Assume $\ell = \mathsf{after}[\![\mathtt{S}]\!]$.

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

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

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

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

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

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

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

$\wr$definition of $\in$ so that π_1 and π_1' must end with $\mathsf{after}[\![\mathtt{S}]\!]$ and definition (47.16) of $\mathsf{seqval}[\![\mathtt{y}]\!]$$\wr$

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

$\wr$definitions of $\in$ and of trace concatenation $\frown\wr$

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

$\wr$definition (47.18) of $\mathsf{diff}\wr$

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

— (2.a) — 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 false branch, we have,

(1)

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

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

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

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

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

$\wr$letting $\rho = \boldsymbol{\varrho}(\pi_0 \mathsf{at}[\![\mathtt{S}]\!])$, $\nu = \boldsymbol{\varrho}(\pi_0' \mathsf{at}[\![\mathtt{S}]\!])\mathtt{x}'$ so that $\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}'\} \,.\, \boldsymbol{\varrho}(\pi_0 \mathsf{at}[\![\mathtt{S}]\!])\mathtt{z} = \boldsymbol{\varrho}(\pi_0' \mathsf{at}[\![\mathtt{S}]\!])\mathtt{z}$ 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 $\mathsf{trace}_0' \mathsf{at}[\![\mathtt{S}]\!]$ (otherwise, this is $\subseteq$)$\wr$

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

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

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

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

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

Described 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)` $\mathtt{S}_t$ 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 classic coarser overapproximation is to ignore values, that is, that variables may have only one value making the test false.

— (2.b) — Else, if both executions $\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket\pi_1\mathsf{after}\llbracket\mathtt{S}\rrbracket$ and $\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket\pi_1'\mathsf{after}\llbracket\mathtt{S}\rrbracket$ are through the true branch, we have,

(1)

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

$\wr$case $\mathcal{B}\llbracket\mathtt{B}\rrbracket\varrho(\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket) = \mathtt{tt}$ and $\mathcal{B}\llbracket\mathtt{B}\rrbracket\varrho(\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket) = \mathtt{ff}\wr$

$$= \{\langle\mathtt{x}',\ \mathtt{y}\rangle \mid \exists\pi_0,\pi_1,\pi_0',\pi_1'\ .\ \mathcal{B}\llbracket\mathtt{B}\rrbracket\varrho(\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket) = \mathtt{tt} \wedge \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1\mathsf{after}\llbracket\mathtt{S}\rrbracket \in \widehat{\mathcal{S}}^{+\infty}\llbracket\mathtt{S}_t\rrbracket(\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket) \wedge \mathcal{B}\llbracket\mathtt{B}\rrbracket\varrho(\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket) = \mathtt{tt} \wedge \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1'\mathsf{after}\llbracket\mathtt{S}\rrbracket \in \widehat{\mathcal{S}}^{+\infty}\llbracket\mathtt{S}_t\rrbracket(\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket) \wedge (\forall\mathtt{z} \in \mathcal{V}\setminus\{\mathtt{x}'\}\ .\ \varrho(\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket)\mathtt{z} = \varrho(\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket)\mathtt{z}) \wedge (\varrho(\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1\mathsf{after}\llbracket\mathtt{S}\rrbracket)\mathtt{y} \neq \varrho(\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1'\mathsf{after}\llbracket\mathtt{S}\rrbracket)\mathtt{y})\}$$

$\wr$definition of $\in\wr$

$$= \{\langle\mathtt{x}',\ \mathtt{y}\rangle \mid \exists\langle\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket,\ \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1\mathsf{after}\llbracket\mathtt{S}_t\rrbracket\pi_2\rangle, \langle\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket,\ \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1'\mathsf{after}\llbracket\mathtt{S}_t\rrbracket\pi_2'\rangle \in \mathcal{S}^{+\infty}\llbracket\mathtt{S}_t\rrbracket\ .\ \mathcal{B}\llbracket\mathtt{B}\rrbracket\varrho(\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket) = \mathtt{tt} \wedge \mathcal{B}\llbracket\mathtt{B}\rrbracket\varrho(\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket) = \mathtt{tt} \wedge (\forall\mathtt{z} \in \mathcal{V}\setminus\{\mathtt{x}'\}\ .\ \varrho(\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket)\mathtt{z} = \varrho(\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket)\mathtt{z}) \wedge \mathsf{after}\llbracket\mathtt{S}_t\rrbracket \notin \pi_1 \wedge \mathsf{after}\llbracket\mathtt{S}_t\rrbracket \notin \pi_1' \wedge (\varrho(\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1\mathsf{after}\llbracket\mathtt{S}\rrbracket)\mathtt{y} \neq \varrho(\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1'\mathsf{after}\llbracket\mathtt{S}\rrbracket)\mathtt{y})\}$$

$\wr\mathsf{after}\llbracket\mathtt{S}\rrbracket = \mathsf{after}\llbracket\mathtt{S}_t\rrbracket$, $\pi_2 = \pi_2' = \ni$, definition (6.6) of $\varrho\wr$

$$= \{\langle\mathtt{x}',\ \mathtt{y}\rangle \mid \exists\langle\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket,\ \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1\mathsf{after}\llbracket\mathtt{S}_t\rrbracket\pi_2\rangle, \langle\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket,\ \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1'\mathsf{after}\llbracket\mathtt{S}_t\rrbracket\pi_2'\rangle \in \mathcal{S}^{+\infty}\llbracket\mathtt{S}_t\rrbracket\ .\ \mathcal{B}\llbracket\mathtt{B}\rrbracket\varrho(\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket) = \mathtt{tt} \wedge \mathcal{B}\llbracket\mathtt{B}\rrbracket\varrho(\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket) = \mathtt{tt} \wedge (\forall\mathtt{z} \in \mathcal{V}\setminus\{\mathtt{x}'\}\ .\ \varrho(\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket)\mathtt{z} = \varrho(\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket)\mathtt{z}) \wedge \mathsf{after}\llbracket\mathtt{S}_t\rrbracket \notin \pi_1 \wedge \mathsf{after}\llbracket\mathtt{S}_t\rrbracket \notin \pi_1' \wedge \mathsf{diff}(\mathsf{seqval}\llbracket\mathtt{y}\rrbracket(\mathsf{after}\llbracket\mathtt{S}_t\rrbracket)(\pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket \frown \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1\mathsf{after}\llbracket\mathtt{S}_t\rrbracket,\ \mathsf{after}\llbracket\mathtt{S}_t\rrbracket\pi_2),\ \mathsf{seqval}\llbracket\mathtt{y}\rrbracket(\mathsf{after}\llbracket\mathtt{S}_t\rrbracket)(\pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket \frown \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1'\mathsf{after}\llbracket\mathtt{S}_t\rrbracket,\ \mathsf{after}\llbracket\mathtt{S}_t\rrbracket\pi_2'))\}$$

$\wr$definition (47.18) of diff and (47.16) of $\mathsf{seqval}\llbracket\mathtt{y}\rrbracket\wr$

$$\subseteq \{\langle\mathtt{x}',\ \mathtt{y}\rangle \mid \exists\langle\bar{\pi}_0,\ \bar{\pi}_1\mathsf{after}\llbracket\mathtt{S}_t\rrbracket\pi_2\rangle, \langle\bar{\pi}_0',\ \bar{\pi}_1'\mathsf{after}\llbracket\mathtt{S}_t\rrbracket\pi_2'\rangle \in \mathcal{S}^{+\infty}\llbracket\mathtt{S}_t\rrbracket\ .\ \mathcal{B}\llbracket\mathtt{B}\rrbracket\varrho(\bar{\pi}_0) = \mathtt{tt} \wedge \mathcal{B}\llbracket\mathtt{B}\rrbracket\varrho(\bar{\pi}_0') = \mathtt{tt} \wedge (\forall\mathtt{z} \in \mathcal{V}\setminus\{\mathtt{x}'\}\ .\ \varrho(\bar{\pi}_0)\mathtt{z} = \varrho(\bar{\pi}_0')\mathtt{z}) \wedge \mathsf{after}\llbracket\mathtt{S}_t\rrbracket \notin \bar{\pi}_1 \wedge \mathsf{after}\llbracket\mathtt{S}_t\rrbracket \notin \bar{\pi}_1' \wedge \mathsf{diff}(\mathsf{seqval}\llbracket\mathtt{y}\rrbracket(\mathsf{after}\llbracket\mathtt{S}_t\rrbracket)(\bar{\pi}_0 \frown \bar{\pi}_1\mathsf{after}\llbracket\mathtt{S}_t\rrbracket,\ \mathsf{after}\llbracket\mathtt{S}_t\rrbracket\pi_2),\ \mathsf{seqval}\llbracket\mathtt{y}\rrbracket(\mathsf{after}\llbracket\mathtt{S}_t\rrbracket)(\bar{\pi}_0' \frown \bar{\pi}_1'\mathsf{after}\llbracket\mathtt{S}_t\rrbracket,\ \mathsf{after}\llbracket\mathtt{S}_t\rrbracket\pi_2'))\}$$

$\wr$letting $\bar{\pi}_0 = \pi_0\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket$, $\bar{\pi}_1 = \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1$, $\bar{\pi}_0' = \pi_0'\mathsf{at}\llbracket\mathtt{S}\rrbracket \xrightarrow{\mathtt{B}} \mathsf{at}\llbracket\mathtt{S}_t\rrbracket$, and $\bar{\pi}_1' = \mathsf{at}\llbracket\mathtt{S}_t\rrbracket\pi_1'\wr$

$\subseteq \{\langle \mathtt{x}', \mathtt{y}\rangle \mid \exists \rho, \nu \;.\; \rho(\mathtt{x}') \neq \nu \wedge \mathcal{B}[\![\mathtt{B}]\!]\rho = \mathtt{tt} \wedge \mathcal{B}[\![\mathtt{B}]\!]\rho[\mathtt{x}' \leftarrow \nu] = \mathtt{tt}\} \cap \{\langle \mathtt{x}', \mathtt{y}\rangle \mid \exists \langle \bar{\pi}_0, \bar{\pi}_1 \mathsf{after}[\![\mathtt{S}_t]\!]\pi_2\rangle, \langle \bar{\pi}_0', \bar{\pi}_1' \mathsf{after}[\![\mathtt{S}_t]\!]\pi_2'\rangle \in \mathcal{S}^{+\infty}[\![\mathtt{S}_t]\!] \;.\; (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}'\} \;.\; \boldsymbol{\varrho}(\bar{\pi}_0)\mathtt{z} = \boldsymbol{\varrho}(\bar{\pi}_0')\mathtt{z}) \wedge \mathsf{after}[\![\mathtt{S}_t]\!] \notin \bar{\pi}_1 \wedge \mathsf{after}[\![\mathtt{S}_t]\!] \notin \bar{\pi}_1' \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!](\mathsf{after}[\![\mathtt{S}_t]\!])(\bar{\pi}_0 \frown \bar{\pi}_1 \mathsf{after}[\![\mathtt{S}_t]\!], \mathsf{after}[\![\mathtt{S}_t]\!]\pi_2), \mathsf{seqval}[\![\mathtt{y}]\!](\mathsf{after}[\![\mathtt{S}_t]\!])(\bar{\pi}_0' \frown \bar{\pi}_1' \mathsf{after}[\![\mathtt{S}_t]\!], \mathsf{after}[\![\mathtt{S}_t]\!]\pi_2'))\}$

$\wr$letting $\rho = \boldsymbol{\varrho}(\bar{\pi}_0)$ and $\nu = \boldsymbol{\varrho}(\bar{\pi}_0')(\mathtt{x}')$$\wr$

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

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

$\wr$definition of$\subseteq$ and definition (47.25) of $\alpha^{\mathsf{d}}$$\wr$

Described in words for that second case, the initial value of $\mathtt{x}'$ flows to the value of $\mathtt{y}$ by the true branch of the conditional `if (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 $\mathtt{y}$ in $\mathtt{S}_t$.

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

$\wr$by structural induction hypothesis , definition (47.48) of nondet, and definition of the left restriction $\rceil$ of a relation in section 2.2.2$\wr$

$\subseteq \widehat{\overline{\mathcal{S}}}^{\exists}_{\mathsf{diff}}[\![\mathtt{S}_t]\!]\,\mathsf{after}[\![\mathtt{S}_t]\!]$ $\wr$A coarse overapproximation ignoring values$\wr$

— (2.c–d) — Otherwise, one execution is through the true branch (let us denote it $\pi_0\mathsf{at}[\![\mathtt{S}]\!]\pi_1\mathsf{after}[\![\mathtt{S}]\!]$) and the other is through the false branch (let it be $\pi_0'\mathsf{at}[\![\mathtt{S}]\!]\pi_1'\mathsf{after}[\![\mathtt{S}]\!]$), we have (the other case is symmetric),

(1)

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

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

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

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

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

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

$\wr$by definition (6.6) of ϱ so that $\varrho(\pi_0'\mathsf{at}[\![\mathtt{S}]\!]) = \varrho(\pi_0'\mathsf{at}[\![\mathtt{S}]\!] \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_t]\!])$$\wr$

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

$\wr$letting $\pi_0'\mathsf{at}[\![\mathtt{S}_t]\!] = \pi_0'\mathsf{at}[\![\mathtt{S}]\!] \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_t]\!]$, commutativity of $\wedge$$\wr$

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

$\wr$because 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}$$\wr$

Described 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 counterexample 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 $\mathtt{y}$.

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

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

$\wr$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 $\exists \rho, \nu\ .\ \rho(\mathtt{x}') \neq \nu \wedge \mathcal{B}[\![\mathtt{B}]\!]\rho = \mathtt{tt} \wedge \mathcal{B}[\![\mathtt{B}]\!]\rho[\mathtt{x}' \leftarrow \nu] = \mathtt{ff}$. Therefore, by definition (47.48) of nondet, $\mathtt{x}' \in \mathsf{nondet}(\mathtt{B}, \neg\mathtt{B})$$\wr$

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

$\wr$Because $\{\mathtt{x} \mid \exists\pi_0,\pi_1 \;.\; \mathsf{at}[\![\mathtt{S}]\!]\pi_1\mathsf{after}[\![\mathtt{S}]\!] \in \widehat{\boldsymbol{\mathcal{S}}}^*[\![\mathtt{S}]\!](\pi_0\mathsf{at}[\![\mathtt{S}]\!]) \wedge \varrho(\pi_0\mathsf{at}[\![\mathtt{S}]\!]\pi_1\mathsf{after}[\![\mathtt{S}]\!])\mathtt{x} \neq \varrho(\pi_0\mathsf{at}[\![\mathtt{S}]\!])\mathtt{x}\} \subseteq \mathsf{mod}[\![\mathtt{S}]\!]$, 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). $\wr$

$= \mathsf{nondet}(\mathtt{B}, \neg\mathtt{B}) \times \mathsf{mod}[\![\mathtt{S}_t]\!]$ $\wr$definition of the Cartesian product$\wr$

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

$\wr$$\mathsf{nondet}(\mathtt{B}, \neg\mathtt{B})$ can be overapproximated by the set of variables $\mathtt{x}'$ occurring in the Boolean expression $\mathtt{B}$ as defined in exercise 3.3$\wr$

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

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

$\square$

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

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

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

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

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

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

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

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

$\wr$ definition $\in$ and if ℓ has multiple occurrences in $\pi_1'\ell\pi_2'$, we choose the first one, same for $\pi_1'\ell\pi_2'$ $\int$

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

$\wr$ letting $\bar{\pi}_0\mathsf{at}[\![S_t]\!] = \pi_0\mathsf{at}[\![S]\!] \xrightarrow{B} \mathsf{at}[\![S_t]\!]$, $\bar{\pi}_0'\mathsf{at}[\![S_t]\!] = \pi_0'\mathsf{at}[\![S]\!] \xrightarrow{B} \mathsf{at}[\![S_t]\!]$ so that by definition (6.6) of $\boldsymbol{\varrho}$, $\boldsymbol{\varrho}(\bar{\pi}_0\mathsf{at}[\![S_t]\!]) = \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![S]\!])$ and $\boldsymbol{\varrho}(\bar{\pi}_0'\mathsf{at}[\![S_t]\!]) = \boldsymbol{\varrho}(\pi_0'\mathsf{at}[\![S]\!])$ $\int$

$\subseteq \{\langle x',\ y\rangle \mid \exists\pi_0, \pi_0' \ .\ \mathcal{B}[\![B]\!]\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![S_t]\!]) = \mathsf{tt} \wedge \mathcal{B}[\![B]\!]\boldsymbol{\varrho}(\pi_0'\mathsf{at}[\![S_t]\!]) = \mathsf{tt} \wedge (\forall z \in \mathbb{V} \setminus \{x'\}\ .\ \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![S_t]\!])z = \boldsymbol{\varrho}(\pi_0'\mathsf{at}[\![S_t]\!])z)\} \cap \{\langle x',\ y\rangle \mid \exists\pi_0, \pi_1, \pi_2, \pi_0', \pi_1', \pi_2' \ .\ \mathsf{at}[\![S_t]\!]\pi_1\ell\pi_2 \in \widehat{\mathcal{S}}^*[\![S_t]\!](\pi_0\mathsf{at}[\![S_t]\!]) \wedge \mathsf{at}[\![S_t]\!]\pi_1'\ell\pi_2' \in \widehat{\mathcal{S}}^*[\![S_t]\!](\pi_0'\mathsf{at}[\![S_t]\!]) \wedge (\forall z \in \mathbb{V} \setminus \{x'\}\ .\ \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![S_t]\!])z = \boldsymbol{\varrho}(\pi_0'\mathsf{at}[\![S_t]\!])z) \wedge \ell \notin \pi_1 \wedge \ell \notin \pi_1' \wedge \mathsf{diff}(\mathsf{seqval}[\![y]\!]\ell(\pi_0\mathsf{at}[\![S_t]\!]\pi_1\ell,\ \ell\pi_2), \mathsf{seqval}[\![y]\!]\ell(\pi_0'\mathsf{at}[\![S_t]\!]\pi_1'\ell,\ \ell\pi_2'))\}$ $\wr$ definitions of $\exists$ and of $\subseteq$ $\int$

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

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

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

$\wr$ definition (47.25) of α^{d} $\int$

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

$\wr$ structural induction hypothesis $\int$

$= \mathcal{S}^{\mathsf{d}}[\![S_t]\!]\ \ell\ \rceil\ \mathsf{nondet}(B, B)$ $\wr$ definition (47.48) of nondet $\int$

Described inn words, the initial value of x' flows to the value of y at ℓ in the true branch S_t 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 at ℓ in S_t.

$\subseteq \mathcal{S}^{\mathsf{d}}[\![S_t]\!]\ \ell$

$\wr$ A coarse overapproximation ignoring values, that is, that the conditional holds for only one value of x' $\int$ □

Proof of (47.63) 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 (**??**). So the soundness of (47.63) follows from the following (3):

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

The proof of (3) is an application of exercise 18.18. $\langle C, \sqsubseteq, \bot, \sqcup\rangle$ is the complete lattice $\langle\wp(\wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})), \subseteq, \varnothing, \cup\rangle$. $\langle\mathcal{A}, \preccurlyeq, 0, \curlyvee\rangle$ is the complete lattice $\langle\mathbb{P}^{\mathrm{d}}, \subseteq^{\mathrm{d}}, \bot^{\mathrm{d}}, \cup^{\mathrm{d}}\rangle$. The Galois connection $\langle C, \sqsubseteq\rangle \xleftrightarrow[\alpha]{\gamma} \langle\mathcal{A}, \preccurlyeq\rangle$ is given by lemma 47.26. The transformer f is (**??**). It preserves arbitrary nonempty unions so it is continuous. The transformer g is (47.63). It preserves arbitrary nonempty 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 semicommutation condition

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

By exercise 18.18, 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 $\varnothing$.

In practice, we have discovered $\mathcal{F}^{\mathsf{diff}}[\![\mathtt{while}\;\ell\;\mathtt{(B)}\;\mathtt{S}_b]\!]$ knowing $\mathcal{F}^*[\![\mathtt{while}\;\ell\;\mathtt{(B)}\;\mathtt{S}_b]\!]$ and α^{d} by rewriting until getting a formula of the form $\mathcal{F}^{\mathsf{diff}}[\![\mathtt{while}\;\ell\;\mathtt{(B)}\;\mathtt{S}_b]\!] \circ \alpha^{\mathrm{d}}$ and using $\dot{\subseteq}$-overapproximations to ignore values in the static analysis. By exercise 18.18, we conclude that

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

The proof of semicommutation (4) is by calculational design as follows. By definition (47.18) of diff, we do not have to compare futures of prefix traces in which one is a prefix of the other.

$$\begin{array}{l} \alpha^{\mathrm{d}}(\{\mathcal{F}^*[\![\mathtt{while}\;\ell\;\mathtt{(B)}\;\mathtt{S}_b]\!]\,X\})\,\ell' \\ = \{\langle\mathtt{x},\,\mathtt{y}\rangle \mid \mathcal{F}^*[\![\mathtt{while}\;\ell\;\mathtt{(B)}\;\mathtt{S}_b]\!]\,X \in \mathcal{D}(\ell')\langle\mathtt{x},\,\mathtt{y}\rangle\} \qquad \text{(definition (47.25) of } \alpha^{\mathrm{d}}\text{)} \\ = \{\langle\mathtt{x},\,\mathtt{y}\rangle \mid \exists\langle\pi_0,\,\pi_1\rangle, \langle\pi_0',\,\pi_1'\rangle \in \mathcal{F}^*[\![\mathtt{while}\;\ell\;\mathtt{(B)}\;\mathtt{S}_b]\!]\,X\;.\;(\forall\mathtt{z} \in \mathbb{V}\setminus\{\mathtt{x}\}\;.\;\varrho(\pi_0)\mathtt{z} = \varrho(\pi_0')\mathtt{z}) \wedge \\ \quad \mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0,\pi_1), \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0',\pi_1'))\} \qquad \text{(definition (47.19) of } \mathcal{D}\ell\langle\mathtt{x},\,\mathtt{y}\rangle\text{)} \end{array}$$

$$\begin{array}{l} = \{\langle\mathtt{x},\,\mathtt{y}\rangle \mid \exists\langle\pi_0\ell,\,\ell\pi_1\rangle, \langle\pi_0'\ell,\,\ell\pi_1'\rangle \in \mathcal{F}^*[\![\mathtt{while}\;\ell\;\mathtt{(B)}\;\mathtt{S}_b]\!]\,X\;.\;(\forall\mathtt{z} \in \mathbb{V}\setminus\{\mathtt{x}\}\;. \\ \quad \varrho(\pi_0\ell)\mathtt{z} = \varrho(\pi_0'\ell)\mathtt{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell,\ell\pi_1), \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0'\ell,\ell\pi_1'))\} \\ \qquad \text{(because } \langle\pi_0\ell',\,\ell''\pi_1\rangle \notin \mathcal{F}^*[\![\mathtt{while}\;\ell\;\mathtt{(B)}\;\mathtt{S}_b]\!](X) \text{ when } \ell' \neq \ell \text{ or } \ell'' \neq \ell\text{)} \end{array} \tag{5}$$

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

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.

$$\mathcal{F}^*[\![\texttt{while}\,\ell\;(\texttt{B})\;\texttt{S}_b]\!](X) \;\triangleq\; \{\langle\pi_0\ell,\;\ell\rangle\} \qquad \textbf{(A)} \qquad \textbf{(??)}$$

$$\cup\,\{\langle\pi_0\ell,\;\ell\pi_2\ell \xrightarrow{\texttt{B}} \mathsf{at}[\![\texttt{S}_b]\!]\pi_3\ell''\rangle \mid \langle\pi_0\ell,\;\ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathtt{tt} \qquad \textbf{(B)}$$

$$\wedge\,\langle\pi_0\ell\pi_2\ell \xrightarrow{\texttt{B}} \mathsf{at}[\![\texttt{S}_b]\!],\;\mathsf{at}[\![\texttt{S}_b]\!]\pi_3\ell''\rangle \in \mathcal{S}^*[\![\texttt{S}_b]\!]\}$$

$$\cup\,\{\langle\pi_0\ell,\;\ell\pi_2\ell \xrightarrow{\neg(\texttt{B})} \mathsf{after}[\![\texttt{S}]\!]\rangle \mid \langle\pi_0\ell,\;\ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\texttt{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathtt{ff}\} \qquad \textbf{(C)}$$

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 $\mathsf{seqval}[\![\texttt{y}]\!]\ell'(\pi_0\ell,\ell) = \varrho(\pi_0\ell)\texttt{y}$ by (47.16). Whether $\ell\pi_1'$ is determined by **(A)**, **(B)**, or **(C)** we have in all cases that $\mathsf{seqval}[\![\texttt{y}]\!]\ell'(\pi_0'\ell,\ell\pi_1') = \varrho(\pi_0'\ell) \frown \sigma$ where σ is a possibly empty sequence of values of $\texttt{y}$ at $\ell' = \ell$. By definition (47.18) of diff, we don't care about σ because $\mathsf{diff}(\mathsf{seqval}[\![\texttt{y}]\!]\ell'(\pi_0\ell,\ell\pi_1), \mathsf{seqval}[\![\texttt{y}]\!]\ell'(\pi_0'\ell,\ell\pi_1'))$ is true if and only if $\varrho(\pi_0\ell)\texttt{y} \neq \varrho(\pi_0'\ell)$. In that case, we have

(5)

$$= \{\langle\texttt{x},\;\texttt{y}\rangle \mid \exists\langle\pi_0\ell,\;\ell\pi_1\rangle,\langle\pi_0'\ell,\;\ell\pi_1'\rangle \in \mathcal{F}^*[\![\texttt{while}\,\ell\;(\texttt{B})\;\texttt{S}_b]\!]\;X\;.\;(\forall\texttt{z} \in \mathbb{V}\setminus\{\texttt{x}\}\;.\;\varrho(\pi_0\ell)\texttt{z} = \varrho(\pi_0'\ell)\texttt{z}) \wedge \varrho(\pi_0\ell)\texttt{y} \neq \varrho(\pi_0\ell)\texttt{y}\}$$

$$\subseteq \{\langle\texttt{x},\;\texttt{y}\rangle \mid \exists\pi_0\ell,\pi_0'\ell\;.\;(\forall\texttt{z} \in \mathbb{V}\setminus\{\texttt{x}\}\;.\;\varrho(\pi_0\ell)\texttt{z} = \varrho(\pi_0'\ell)\texttt{z}) \wedge (\varrho(\pi_0\ell)\texttt{y} \neq \varrho(\pi_0'\ell)\texttt{y})\} \quad \text{(definition of} \subseteq\text{)}$$

$$= \{\langle\texttt{x},\;\texttt{y}\rangle \mid \exists\rho,\nu\;.\;\rho(\texttt{y}) \neq \rho[\texttt{x} \leftarrow \nu](\texttt{y})\}$$

$$\text{(letting } \rho = \varrho(\pi_0\ell),\; \rho[\texttt{x} \leftarrow \nu] = \varrho(\pi_0'\ell) \text{ and exercise 6.8)}$$

$$= \{\langle\texttt{x},\;\texttt{x}\rangle \mid \texttt{x} \in \mathbb{V}\} \quad \text{(definition (19.10) of the environment assignment)}$$

$$= \mathbb{1}_{\mathbb{V}} \quad \text{(definition of the identity relation on the set } \mathbb{V} \text{ of variables in section 2.2.2)}$$

— **(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

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

$= \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell'')$ where $\langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathrm{tt} \wedge \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!],\ \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell''\rangle \in \mathcal{S}^*[\![\mathtt{S}_b]\!]$ ⟅**(B)** with $\ell'' \in \mathsf{in}[\![\mathtt{S}_b]\!]$⟆

$= \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell)$ where $\langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathrm{tt}$

⟅definition (47.16) of $\mathsf{seqval}[\![\mathtt{y}]\!]$ because $\langle\pi_0\ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!],\ \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell''\rangle \in \mathcal{S}^*[\![\mathtt{S}_b]\!]$ 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

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

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

$= \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell)$ where $\langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathrm{tt}$

⟅definition (47.16) of $\mathsf{seqval}[\![\mathtt{y}]\!]$ because $\langle\pi_0\ell\pi_2\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!],\ \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{break\text{-}to}[\![\mathtt{S}]\!]\rangle \in \mathcal{S}^*[\![\mathtt{S}_b]\!]$ 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

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

$= \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\neg(\mathtt{B})} \mathsf{after}[\![\mathtt{S}]\!])$ where $\langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathrm{ff}$ ⟅**(C)**⟆

$= \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell)$ where $\langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathrm{ff}$ ⟅definition (47.16) of $\mathsf{seqval}[\![\mathtt{y}]\!]$⟆

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

(5)

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

$\subseteq \{\langle\mathtt{x},\ \mathtt{y}\rangle \mid \exists\langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X\ .\ \exists\langle\pi_0'\ell,\ \ell\pi_1'\rangle \in \mathcal{F}^*[\![\mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b]\!]\ X\ .\ (\forall \mathtt{z} \in \mathcal{V} \setminus \{\mathtt{x}\}\ .\ \boldsymbol{\varrho}(\pi_0\ell)\mathtt{z} = \boldsymbol{\varrho}(\pi_0'\ell)\mathtt{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0'\ell, \ell\pi_1'))\}$ (6)
⟅abstracting away the value of the conditions⟆

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–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

$$
\begin{aligned}
& (6) \\
= \ & \{\langle \mathtt{x},\ \mathtt{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}^*[\![\mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b]\!]\,X \,.\, (\forall \mathtt{z} \in \mathcal{V}\setminus\{\mathtt{x}\} \,.\, \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_2\ell), \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0'\ell, \ell\pi_1'))\} \\
\subseteq \ & \{\langle \mathtt{x},\ \mathtt{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 \mathtt{z} \in \mathcal{V}\setminus\{\mathtt{x}\} \,.\, \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_2\ell), \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0'\ell, \ell\pi_2'\ell))\} \\
& \hfill \wr\text{abstracting away the value of the conditions}\wr \\
\subseteq \ & \{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \exists\langle \pi_0,\ \pi_1\rangle, \langle \pi_0',\ \pi_1'\rangle \in X \,.\, (\forall \mathtt{z} \in \mathcal{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'))\} \\
& \hfill \wr\text{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, \text{ and } \ell' = \ell \text{ in case } (\mathbf{1})\wr \\
= \ & \{\langle \mathtt{x},\ \mathtt{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 \mathtt{z} \in \mathcal{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'))\}\} \hfill \wr\text{definition of } \in\wr \\
= \ & \{\langle \mathtt{x},\ \mathtt{y}\rangle \mid X \in \mathcal{D}\ell\langle \mathtt{x},\ \mathtt{y}\rangle\} \hfill \wr\text{definition (47.19) of } \mathcal{D}\ell\langle \mathtt{x}',\ \mathtt{y}\rangle\wr \\
= \ & \alpha^{\mathrm{d}}(\{X\})\ell \hfill \wr\text{definition (47.25) of } \alpha^{\mathrm{d}}\wr
\end{aligned}
$$

– **(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 $\ell'' = \mathsf{after}[\![\mathtt{S}_b]\!] = \mathsf{at}[\![\mathtt{S}]\!] = \ell$ and the prefix observation stops there, just before the next iteration or the loop exit. We have

$$
\begin{aligned}
& (6) \\
= \ & \{\langle \mathtt{x},\ \mathtt{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}^*[\![\mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b]\!]\,X \,.\, (\forall \mathtt{z} \in \mathcal{V}\setminus\{\mathtt{x}\} \,.\, \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_2\ell), \mathsf{seqval}[\![\mathtt{y}]\!]\ell(\pi_0'\ell, \ell\pi_1'))\} \\
& \hfill \wr\text{case } (\mathbf{1}) \text{ so } \ell' = \ell = \mathsf{at}[\![\mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b]\!]\wr \\
= \ & \{\langle \mathtt{x},\ \mathtt{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{\ \mathtt{B}\ } \mathsf{at}[\![\mathtt{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) = \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]\!] \wedge \ell'' = \mathsf{after}[\![\mathtt{S}_b]\!] = \mathsf{at}[\![\mathtt{S}]\!] = \\
& \ell\} \,.\, (\forall \mathtt{z} \in \mathcal{V}\setminus\{\mathtt{x}\} \,.\, \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_2\ell), \mathsf{seqval}[\![\mathtt{y}]\!]\ell(\pi_0'\ell, \ell\pi_1'))\} \\
& \hfill \wr\text{case } (\mathbf{Bb}) \text{ for } \ell\pi_1'\wr \\
= \ & \{\langle \mathtt{x},\ \mathtt{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{\ \mathtt{B}\ } \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell\rangle \,.\, \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]\!] \wedge (\forall \mathtt{z} \in \mathcal{V}\setminus\{\mathtt{x}\} \,.\, \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_2\ell), \mathsf{seqval}[\![\mathtt{y}]\!]\ell(\pi_0'\ell, \ell\pi_2'\ell \xrightarrow{\ \mathtt{B}\ } \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell))\} \\
& \hfill \wr\text{definition of } \in \text{ and } \ell'' = \ell\wr
\end{aligned}
$$

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

$$\cup$$

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

≀By definition (47.16) of $\mathsf{seqval}[\![\mathtt{y}]\!]$ and (47.18) of diff, there is an instance of ℓ in $\ell\pi_2\ell$ and one in $\ell\pi_2'\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell$ at which the values of $\mathtt{y}$ do differ, whereas they were the same previously. So there are two possible cases in which this ℓ is either in $\ell\pi_2'\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!]$ or in $\mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell$. So we have $\mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!]\ell(\pi_0\ell,\ell\pi_2\ell), \mathsf{seqval}[\![\mathtt{y}]\!]\ell(\pi_0'\ell,\ell\pi_2'\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell)) = \mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!]\ell(\pi_0\ell,\ell\pi_2\ell), \mathsf{seqval}[\![\mathtt{y}]\!]\ell(\pi_0'\ell,\ell\pi_2'\ell)) \vee \mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!]\ell(\pi_0\ell,\ell\pi_2\ell), \mathsf{seqval}[\![\mathtt{y}]\!]\ell(\pi_0'\ell\pi_2'\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!], \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell))$≀

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

$$\cup$$

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

≀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 $\ell\pi_2\ell \neq \ell$ because otherwise we would be in case (**1–A**)), X is an iterate of $\mathcal{F}^*[\![\mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b]\!]$, and so, by (**??**), can be written in the form $\ell\pi_2\ell = \ell\pi_2''\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3''\ell$ (where $\ell\pi_2''\ell$ may be reduced to ℓ for the first iteration) with $\ell\pi_2''\ell \in X$, $\mathcal{B}[\![\mathtt{B}]\!]\varrho(\pi_0\ell\pi_2''\ell) = \mathrm{tt}$ and $\langle\pi_0\ell\pi_2''\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!], \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3'\ell\rangle \in \mathcal{S}^*[\![\mathtt{S}_b]\!]$. Moreover if the difference on $\mathtt{y}$ is in $\ell\pi_2''\ell$, the case is covered by the first term.≀ (7)

$$\subseteq \alpha^{\mathrm{d}}(\{X\})\ell$$

$$\cup$$

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

$\wr$ because $\varrho(\pi) = \varrho(\pi \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!])$ $\wr$

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

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

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

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

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

$\wr$ lemma 47.59 with $\boldsymbol{\mathcal{S}} \leftarrow X$ and $\boldsymbol{\mathcal{S}}' \leftarrow \{\langle \pi_0\ell, \ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!]\pi\rangle \mid \langle \pi_0\ell \xrightarrow{\mathtt{B}} \mathsf{at}[\![\mathtt{S}_b]\!], \mathsf{at}[\![\mathtt{S}_b]\!]\pi\rangle \in \{\langle \pi, \pi'\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}_b]\!] \mid \boldsymbol{\mathcal{B}}[\![\mathtt{B}]\!]\varrho(\pi)\}\}$ $\wr$

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

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

$= \alpha^{\mathrm{d}}(\{X\})\ell \cup (\alpha^{\mathrm{d}}(\{X\})\ell \fatsemi (\alpha^{\mathrm{d}}(\{\boldsymbol{\mathcal{S}}^*[\![\mathtt{S}_b]\!]\})\ell \rceil \mathsf{nondet}(\mathtt{B}, \mathtt{B})))$ $\wr$ lemma 47.62 $\wr$

$= \alpha^{\mathrm{d}}(\{X\})\ell \cup (\alpha^{\mathrm{d}}(\{X\})\ell \fatsemi (\alpha^{\mathrm{d}}(\{\boldsymbol{\mathcal{S}}^{+\infty}[\![\mathtt{S}_b]\!]\})\ell) \rceil \mathsf{nondet}(\mathtt{B}, \mathtt{B}))$ $\wr$ lemma 47.23 $\wr$

$\subseteq \alpha^{\mathrm{d}}(\{X\})\ell \cup (\alpha^{\mathrm{d}}(\{X\})\ell \fatsemi (\widehat{\overline{\boldsymbol{\mathcal{S}}}}^{\exists}_{\mathsf{diff}}[\![\mathtt{S}_b]\!]\,\ell \rceil \mathsf{nondet}(\mathtt{B}, \mathtt{B})))$ $\wr$ induction hypothesis (47.32), $\fatsemi$ and $\rceil$ are $\subseteq$-increasing $\wr$

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

The possible choices for $\langle \pi_0'\ell, \ell\pi_1'\rangle \in \boldsymbol{\mathcal{F}}^*[\![\mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b]\!]\, X$ 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 $\{\langle\pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \mid \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]\}$. In that case, we have

$$
\begin{aligned}
&(5)\\
&= \{\langle\mathrm{x},\ \mathrm{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 \\
&\quad \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]\!]\}\ .\ (\forall \mathrm{z} \in \mathbb{V} \setminus \{\mathrm{x}\}\ .\ \boldsymbol{\varrho}(\pi_0\ell)\mathrm{z} = \\
&\quad \boldsymbol{\varrho}(\pi_0'\ell)\mathrm{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathrm{y}]\!]\ell'(\pi_0\ell,\ell\pi_1), \mathsf{seqval}[\![\mathrm{y}]\!]\ell'(\pi_0'\ell,\ell\pi_1'))\} \qquad \text{\textit{\{case (\textbf{1–Bb–Bb})\}}}\\
&= \{\langle\mathrm{x},\ \mathrm{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}]\!]\boldsymbol{\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\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 \\
&\quad 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 \mathrm{z} \in \mathbb{V} \setminus \{\mathrm{x}\}\ .\ \boldsymbol{\varrho}(\pi_0'\ell)\mathrm{z} = \\
&\quad \boldsymbol{\varrho}(\pi_0'\ell)\mathrm{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathrm{y}]\!]\ell'(\pi_0\ell,\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell), \mathsf{seqval}[\![\mathrm{y}]\!]\ell'(\pi_0'\ell,\ell\pi_2'\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell))\}\\
&\quad \text{\textit{\{definition of $\in$\}}}\\
&\subseteq \{\langle\mathrm{x},\mathrm{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,\\
&\quad \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \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}}\\
&\quad \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}]\!]\boldsymbol{\varrho}(\pi)\} \wedge (\forall \mathrm{z} \in \mathbb{V} \setminus \{\mathrm{x}\}\ .\ \boldsymbol{\varrho}(\pi_0'\ell)\mathrm{z} = \boldsymbol{\varrho}(\pi_0'\ell)\mathrm{z}) \wedge \\
&\quad \mathsf{diff}(\mathsf{seqval}[\![\mathrm{y}]\!]\ell'(\pi_0\ell,\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell), \mathsf{seqval}[\![\mathrm{y}]\!]\ell'(\pi_0'\ell,\ell\pi_2'\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell))\} \text{\textit{\{definition of}}\\
&\quad \text{\textit{$\in$\}}}\\
&= \{\langle\mathrm{x},\mathrm{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,\\
&\quad \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \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}}\\
&\quad \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}]\!]\boldsymbol{\varrho}(\pi)\} \wedge (\forall \mathrm{z} \in \mathbb{V} \setminus \{\mathrm{x}\}\ .\ \boldsymbol{\varrho}(\pi_0'\ell)\mathrm{z} = \boldsymbol{\varrho}(\pi_0'\ell)\mathrm{z}) \wedge \\
&\quad \mathsf{diff}(\mathsf{seqval}[\![\mathrm{y}]\!]\ell(\pi_0\ell,\ell\pi_2\ell), \mathsf{seqval}[\![\mathrm{y}]\!]\ell(\pi_0'\ell,\ell\pi_2'\ell))\}\\
&\qquad \text{\textit{\{by definition (47.18) of diff, and definition (47.16) of $\mathsf{seqval}[\![\mathrm{y}]\!]$ because in case (1), $\ell' = \ell$}}\\
&\qquad \text{\textit{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}}$}}\\
&\qquad \text{\textit{$\mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell$ and at ℓ after $\pi_0\ell\pi_2\ell$. The same holds for $\pi_0'\ell\pi_2'\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell$.\}}}\\
&\subseteq \{\langle\mathrm{x},\ \mathrm{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 \mathrm{z} \in \mathbb{V} \setminus \{\mathrm{x}\}\ .\ \boldsymbol{\varrho}(\pi_0'\ell)\mathrm{z} = \boldsymbol{\varrho}(\pi_0'\ell)\mathrm{z}) \wedge \\
&\quad \mathsf{diff}(\mathsf{seqval}[\![\mathrm{y}]\!]\ell(\pi_0\ell,\ell\pi_2\ell), \mathsf{seqval}[\![\mathrm{y}]\!]\ell(\pi_0'\ell,\ell\pi_2'\ell))\} \qquad \text{\textit{\{definition of $\subseteq$\}}}\\
&\subseteq \alpha^{\mathrm{d}}(\{X\})\ell \qquad \text{\textit{\{definition (47.25) of α^{d}\}}}
\end{aligned}
$$

— Summing up for case **(1)** we get (5) $\subseteq \mathbb{1}_{\mathbb{V}} \cup \alpha^{\mathrm{d}}(\{X\})\ell \cup (\alpha^{\mathrm{d}}(\{X\})\ell \mathbin{⨾} \widehat{\overrightarrow{\mathcal{S}}}^{\exists}_{\mathsf{diff}}[\![\mathtt{S}_b]\!]\ \ell)\ \rceil\ \mathsf{nondet}(\mathtt{B},\mathtt{B})$ which yields (47.63.a) of the form

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

However, the term $X(\ell)$ does not appear in (47.63.a) because it can be simplified using exercise 15.8.

—— **(2)** Else, if the dependency observation point ℓ' on prefix traces is in the loop body $\mathtt{S}_b$ after zero or more loop iterations. So the two traces $\ell\pi_1$ and $\ell\pi_1'$ in (5) cannot be generated by (**??.A**). The case $\ell' = \ell = \mathsf{after}[\![\mathtt{S}_b]\!] = \mathsf{at}[\![\mathtt{S}]\!]$ has already been considered in case **(1)** (for subcases involving **(B)** and **(C)**). By definition (47.16) of $\mathsf{seqval}[\![\mathtt{y}]\!]$ the case $\ell' = \mathsf{at}[\![\mathtt{S}_b]\!]$ is equivalent to $\ell' = \mathsf{at}[\![\mathtt{S}]\!]$ already considered in **(1)** because the evaluation of Boolean expressions has no side effect so the value of variables $\mathtt{y}$ at $\mathsf{at}[\![\mathtt{S}_b]\!]$ and $\mathsf{at}[\![\mathtt{S}]\!]$ are the same. Similarly, the value of variables $\mathtt{y}$ before a `break ;` statement at labels in $\mathsf{breaks\text{-}of}[\![\mathtt{S}_b]\!]$ that can escape the loop body $\mathtt{S}_b$ is the same as the value at $\mathsf{break\text{-}to}[\![\mathtt{S}_b]\!] = \mathsf{after}[\![\mathtt{S}]\!]$ and will be handled with case **(3)**.

It follows that in this case **(2)** we only have to consider the case $\ell' \in \mathsf{in}[\![\mathtt{S}_b]\!] \setminus (\{\mathsf{at}[\![\mathtt{S}_b]\!], \mathsf{after}[\![\mathtt{S}_b]\!]\} \cup \mathsf{breaks\text{-}of}[\![\mathtt{S}_b]\!])$ 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 $\mathtt{S}_b$ after zero or more loop iterations and the observation along these two traces stops in the loop body.

$$
\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 \{\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\ \mathtt{B}\ } \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell''\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge{}\\
&\mathcal{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathsf{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 \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}_b]\!]\}\ .\ (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}\}\ .\ \boldsymbol{\varrho}(\pi_0\ell)\mathtt{z} =\\
&\boldsymbol{\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{(case \textbf{2–B–B})}\\
=\ &\{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\ \mathtt{B}\ } \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell''\rangle\ .\ \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathsf{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 \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}_b]\!] \wedge \exists \langle \pi_0'\ell,\ \ell\pi_2'\ell \xrightarrow{\ \mathtt{B}\ } \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3'\ell''\rangle\ .\ \langle \pi_0'\ell,\ \ell\pi_2'\ell\rangle \in{}\\
&X \wedge \mathcal{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi_0'\ell\pi_2'\ell) = \mathsf{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 \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}_b]\!] \wedge (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}\}\ .\ \boldsymbol{\varrho}(\pi_0\ell)\mathtt{z} =\\
&\boldsymbol{\varrho}(\pi_0'\ell)\mathtt{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\ \mathtt{B}\ } \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell''), \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0'\ell, \ell\pi_2'\ell \xrightarrow{\ \mathtt{B}\ } \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3'\ell''))\}\\
&\text{(definition } \in\text{)}\\
\subseteq\ &\{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\ \mathtt{B}\ } \mathsf{at}[\![\mathtt{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{\ \mathtt{B}\ } \mathsf{at}[\![\mathtt{S}_b]\!],\ \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell''\rangle \in{}\\
&\{\langle \pi, \pi'\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}_b]\!] \mid \mathcal{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi)\} \wedge \exists \langle \pi_0'\ell,\ \ell\pi_2'\ell \xrightarrow{\ \mathtt{B}\ } \mathsf{at}[\![\mathtt{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{\ \mathtt{B}\ }\\
&\mathsf{at}[\![\mathtt{S}_b]\!],\ \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3'\ell''\rangle \in \{\langle \pi, \pi'\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}_b]\!] \mid \mathcal{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi)\} \wedge (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}\}\ .\ \boldsymbol{\varrho}(\pi_0\ell)\mathtt{z} = \boldsymbol{\varrho}(\pi_0'\ell)\mathtt{z}) \wedge{}\\
&\mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\ \mathtt{B}\ } \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3\ell''), \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0'\ell, \ell\pi_2'\ell \xrightarrow{\ \mathtt{B}\ } \mathsf{at}[\![\mathtt{S}_b]\!]\pi_3'\ell''))\} \quad \text{(definition of } \in\text{)}
\end{aligned}
$$

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

$\cup$

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

$\cup$

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

≀by definition (47.18) of diff and (47.16) of $\mathsf{seqval}[\![y]\!]\ell'$, there is an instance of ℓ' in both $\ell\pi_2'\ell \xrightarrow{\mathrm{B}} \mathsf{at}[\![S_b]\!]\pi_3'\ell''$ and $\ell\pi_2'\ell \xrightarrow{\mathrm{B}} \mathsf{at}[\![S_b]\!]\pi_3'\ell''$ before which the values of y at ℓ' and at which they differ. There are four cases (indeed three by symmetry), depending on whether the occurrence of ℓ'' is before or after the transition $\xrightarrow{\mathrm{B}}$.≀

$\subseteq \alpha^{\mathrm{d}}(\{X\})\ell' \cup$

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

≀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.≀

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

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

— **(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)

$= \{\langle x,\ y\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_1\rangle \in \big\{\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathrm{B}} \mathsf{at}[\![S_b]\!]\pi_3\ell''\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \boldsymbol{\mathcal{B}}[\![B]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{tt} \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathrm{B}} \mathsf{at}[\![S_b]\!],\ \mathsf{at}[\![S_b]\!]\pi_3\ell''\rangle \in \boldsymbol{\mathcal{S}}^*[\![S_b]\!]\big\}\ .\ \exists\langle \pi_0'\ell,\ \ell\pi_1'\rangle \in \big\{\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\neg(\mathrm{B})} \mathsf{after}[\![S]\!]\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \boldsymbol{\mathcal{B}}[\![B]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{ff}\big\}\ .\ (\forall z \in \mathbb{V} \setminus \{x\}\ .\ \varrho(\pi_0\ell)z = \varrho(\pi_0'\ell)z) \wedge \mathsf{diff}(\mathsf{seqval}[\![y]\!]\ell'(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![y]\!]\ell'(\pi_0'\ell, \ell\pi_1'))\}$ ≀case **2–B–C**≀

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

⦅This case is handled exactly as the previous one because 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 $\ell\pi_2\ell \xrightarrow{\neg(\mathtt{B})} \mathsf{after}[\![\mathtt{S}]\!]$ and the loop exit $\ell \xrightarrow{\neg(\mathtt{B})} \mathsf{after}[\![\mathtt{S}]\!]$ does not affect the variable y.⦆

— **(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 $\mathtt{S}_b$ after zero or more loop iterations and the observation along these two traces stops at the loop exit.

$$
\begin{aligned}
&(5)\\
= &\ \{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_1\rangle, \langle \pi_0'\ell,\ \ell\pi_1'\rangle \in \{\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\neg(\mathtt{B})} \mathsf{after}[\![\mathtt{S}]\!]\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in \\
&\quad X \wedge \mathcal{B}[\![\mathtt{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathrm{ff}\} \ .\ (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}\}\ .\ \boldsymbol{\varrho}(\pi_0\ell)\mathtt{z} = \boldsymbol{\varrho}(\pi_0'\ell)\mathtt{z}) \wedge \\
&\quad \mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathtt{y}]\!]\ell'(\pi_0'\ell, \ell\pi_1'))\} \qquad \text{⦅case 2–C–C⦆}\\
\subseteq &\ \alpha^{\mathrm{d}}(\{X\})\ell' \cup \big(\alpha^{\mathrm{d}}(\{X\})\ell \,\mathbin{⨟}\, ((\widehat{\boldsymbol{\mathcal{S}}}^{\exists}_{\mathsf{diff}}[\![\mathtt{S}_b]\!]\ \ell')\ \rceil\ \mathsf{nondet}(\mathtt{B}, \mathtt{B}))\big)
\end{aligned}
$$

⦅This case is handled exactly as the two previous ones because , 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 $\ell\pi_2\ell \xrightarrow{\neg(\mathtt{B})} \mathsf{after}[\![\mathtt{S}]\!]$ and the loop exit $\ell \xrightarrow{\neg(\mathtt{B})} \mathsf{after}[\![\mathtt{S}]\!]$ does not affect the variable y. Similarly for the second trace $\ell\pi_1'$.⦆

— Summing up for case (2), we get (5) $\subseteq \alpha^{\mathrm{d}}(\{X\})\ell' \cup \big(\alpha^{\mathrm{d}}(\{X\})\ell \,⨟\, ((\widehat{\boldsymbol{\mathcal{S}}}^{\exists}_{\mathsf{diff}}[\![\mathtt{S}_b]\!]\ \ell')\ \rceil\ \mathsf{nondet}(\mathtt{B}, \mathtt{B}))\big)$ which yields (47.63.b) of the form

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

where the term $X(\ell')$ does not appear in (47.63.b) by the simplification following from exercise 15.8.

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

$$
\begin{aligned}
&(5)\\
= &\ \{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_1\rangle, \langle \pi_0'\ell,\ \ell\pi_1'\rangle \in \boldsymbol{\mathcal{F}}^*[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b]\!]\ X\ .\ (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}\}\ .\ \boldsymbol{\varrho}(\pi_0\ell)\mathtt{z} = \\
&\quad \boldsymbol{\varrho}(\pi_0'\ell)\mathtt{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!](\mathsf{after}[\![\mathtt{S}]\!])(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathtt{y}]\!](\mathsf{after}[\![\mathtt{S}]\!])(\pi_0'\ell, \ell\pi_1'))\}\\
&\qquad \text{⦅}\ell' = \mathsf{after}[\![\mathtt{S}]\!]\text{⦆}
\end{aligned}
$$

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

≀The only cases in (**??**) where $\ell' = \mathsf{after}[\![\mathtt{S}]\!]$ is reachable is either via **(C)** for normal termination after zero or more iterations or via **(B)** through a `break ;` in the loop body $\mathtt{S}_b$ 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)

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

≀definition of $\in$ and $\ell' = \mathsf{after}[\![\mathtt{S}]\!]$∫

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

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

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 because in both cases the condition $\mathtt{B}$ is false, we have $\ell\pi_2\ell = \ell$ and $\ell\pi_2'\ell = \ell$.

(9)

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

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

⦃because if $\mathtt{x} \notin \mathsf{nondet}(\neg\mathtt{B}, \neg\mathtt{B})$ then $\mathtt{x} \in \mathsf{det}(\neg\mathtt{B}, \neg\mathtt{B})$ so $\mathscr{B}[\![\neg\mathtt{B}]\!]\varrho(\pi_0\ell)$ and $\mathscr{B}[\![\neg\mathtt{B}]\!]\varrho(\pi_0'\ell)$ would imply $\varrho(\pi_0\ell)\mathtt{x} = \varrho(\pi_0'\ell)\mathtt{x}$. Therefore $\varrho(\pi_0\ell) = \varrho(\pi_0'\ell)$ in contradiction to $\varrho(\pi_0\ell)\mathtt{y} \neq \varrho(\pi_0'\ell)\mathtt{y}$.⦄

– **(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 because in both cases the condition $\mathtt{B}$ is true, we have $\ell\pi_2\ell \neq \ell$ and $\ell\pi_2'\ell \neq \ell$

(9)

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

⦃case **(3–C–C.b)** and X belongs to the iterates of $\mathscr{F}^*[\![\mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b]\!]$ so this is possible only when $\mathscr{B}[\![\mathtt{B}]\!]\varrho(\pi_0\ell) = \mathrm{tt}$ and $\mathscr{B}[\![\mathtt{B}]\!]\varrho(\pi_0'\ell) = \mathrm{tt}$ and definition (47.48) of nondet⦄

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

⦃because $\varrho(\pi_0\ell\pi_2\ell)\mathtt{y} \neq \varrho(\pi_0'\ell\pi_2'\ell)\mathtt{y}$ implies $\mathsf{diff}(\mathsf{seqval}[\![\mathtt{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathtt{y}]\!]\ell(\pi_0'\ell, \ell\pi_2'\ell))$⦄

$\subseteq \alpha^{\mathrm{d}}(\{X\})\ell$ ⦃definition (47.25) of α^{d}⦄

– **(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)

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

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

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

⦃because , by definition (47.48) of nondet, if $\mathtt{x} \notin \mathsf{nondet}(\mathtt{B}, \neg\mathtt{B})$ then $\mathtt{x} \in \mathsf{det}(\mathtt{B}, \neg\mathtt{B})$ so by (47.48), $\mathscr{B}[\![\mathtt{B}]\!]\varrho(\pi_0\ell)$ and $\mathscr{B}[\![\neg\mathtt{B}]\!]\varrho(\pi_0'\ell)$ would imply $\varrho(\pi_0\ell)\mathtt{x} = \varrho(\pi_0'\ell)\mathtt{x}$ and therefore $\varrho(\pi_0\ell) = \varrho(\pi_0'\ell)$. X being included in the iterates of $\mathscr{F}^*[\![\mathtt{while}\ \ell\ (\mathtt{B})\ \mathtt{S}_b]\!]$ and, by exercises 17.13 and 17.21, the language being deterministic, this would imply that $\ell\pi_2\ell = \ell$, in contradiction to $\mathscr{B}[\![\mathtt{B}]\!]\varrho(\pi_0\ell) = \mathrm{tt}$ and $\mathscr{B}[\![\mathtt{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathrm{ff}$⦄

$= \{\langle x,\ y\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_2''\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell\rangle\ .\ \langle \pi_0\ell,\ \ell\pi_2''\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell) = \mathsf{tt} \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2''\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell) = \mathsf{ff} \wedge \langle \pi_0\ell\pi_2''\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \wedge \exists\langle \pi_0'\ell,\ \ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0'\ell) = \mathsf{ff} \wedge (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi_0'\ell)\mathsf{z}) \wedge \varrho(\pi_0\ell\pi_2''\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell)\mathsf{y} \neq \varrho(\pi_0'\ell)\mathsf{y}\} \rceil\ \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$

≀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 $\ell\pi_2\ell = \ell\pi_2''\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell$ (where $\ell\pi_2''\ell$ may be reduced to ℓ for the first iteration) with $\ell\pi_2''\ell \in X$, $\mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2''\ell) = \mathsf{tt}$ and $\langle \pi_0\ell\pi_2''\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]$≀

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

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

$= \{\langle x,\ y\rangle \mid \exists \pi_0\ell\pi_2''\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}[\![\mathsf{S}]\!], \pi_0'\ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}[\![\mathsf{S}]\!]\ .\ \langle \pi_0\ell,\ \ell\pi_2''\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell\rangle \in X \wedge \langle \pi_0\ell\pi_2''\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell,\ \ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}' \wedge \langle \pi_0'\ell,\ \ell\rangle \in X \wedge \langle \pi_0'\ell,\ \ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}' \wedge (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi_0'\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\mathsf{after}[\![\mathsf{S}]\!](\pi_0\ell\pi_2''\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!]), \mathsf{seqval}[\![\mathsf{y}]\!]\mathsf{after}[\![\mathsf{S}]\!](\pi_0'\ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!]))\} \rceil\ \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$

≀where $\mathcal{S}' = \{\langle \pi_1'\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell,\ \ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_1'\ell) = \mathsf{tt} \wedge \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2''\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell) = \mathsf{ff} \wedge \langle \pi_1'\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3'\ell\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]\} \cup \{\langle \pi_0'\ell,\ \ell \xrightarrow{\neg\mathsf{B}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0'\ell) = \mathsf{ff}\}$≀

$\subseteq (\alpha^{\mathsf{d}}(\{X\})\ \ell\ ⨟\ \alpha^{\mathsf{d}}(\{\mathcal{S}'\})\ \mathsf{after}[\![\mathsf{S}]\!]) \rceil\ \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$

≀lemma 47.59 with $\ell_0 \leftarrow \ell$, $\ell' \leftarrow \ell$, and $\ell \leftarrow \mathsf{after}[\![\mathsf{S}]\!]$≀

We have to calculate the second term

$$\alpha^{\mathsf{d}}(\{\mathcal{S}'\})\ \mathsf{after}[\![\mathsf{S}]\!] \tag{10}$$

$= \{\langle x,\ y\rangle \mid \mathcal{S}' \in \mathcal{D}(\mathsf{after}[\![\mathsf{S}]\!])\langle x,\ y\rangle\}$ ≀definition (47.25) of α^{d}≀

$= \{\langle x,\ y\rangle \mid \exists\langle \pi_0, \pi_1\rangle, \langle \pi_0', \pi_1'\rangle \in \mathcal{S}'\ .\ (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0)\mathsf{z} = \varrho(\pi_0')\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\mathsf{after}[\![\mathsf{S}]\!](\pi_0, \pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]\mathsf{after}[\![\mathsf{S}]\!](\pi_0', \pi_1'))\}$ ≀definition (47.19) of $\mathcal{D}^{\ell}\langle x,\ y\rangle$≀

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

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

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

≀definition (6.6) of ϱ, definition (47.16) of $\mathsf{seqval}\llbracket \mathrm{y}\rrbracket$ and program labeling so that $\mathsf{after}\llbracket \mathrm{S}\rrbracket$ does not appear in the trace (in particular $\ell \neq \mathsf{after}\llbracket \mathrm{S}\rrbracket$), and definition (47.18) of diff≀

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

≀because if $\mathrm{x} \notin \mathsf{nondet}(\neg\mathrm{B}, \neg\mathrm{B})$ then $\mathrm{x} \in \mathsf{det}(\neg\mathrm{B}, \neg\mathrm{B})$ so by (47.48), $\mathcal{B}\llbracket \neg\mathrm{B}\rrbracket \varrho(\pi_0\ell\pi''_2\ell \xrightarrow{\mathrm{B}} \mathsf{at}\llbracket \mathrm{S}_b\rrbracket \pi'_3\ell)$, and $\mathcal{B}\llbracket \neg\mathrm{B}\rrbracket \varrho(\pi'_0\ell)$, we would have $\varrho(\pi_0\ell\pi''_2\ell \xrightarrow{\mathrm{B}} \mathsf{at}\llbracket \mathrm{S}_b\rrbracket \pi'_3\ell) = \varrho(\pi'_0\ell)$,, which with $\forall \mathrm{z} \in \mathbb{V} \setminus \{\mathrm{x}\} \ .\ \varrho(\pi'_2\ell \xrightarrow{\mathrm{B}} \mathsf{at}\llbracket \mathrm{S}_b\rrbracket \pi'_3\ell)\mathrm{z} = \varrho(\pi'_0\ell)\mathrm{z}$, would imply $\forall \mathrm{z} \in \mathbb{V} \setminus \{\mathrm{x}\} \ .\ \varrho(\pi'_2\ell \xrightarrow{\mathrm{B}} \mathsf{at}\llbracket \mathrm{S}_b\rrbracket \pi'_3\ell) = \varrho(\pi'_0\ell)$, in contradiction to $\varrho(\pi'_2\ell \xrightarrow{\mathrm{B}} \mathsf{at}\llbracket \mathrm{S}_b\rrbracket \pi'_3\ell)\mathrm{y} \neq \varrho(\pi'_0\ell)\mathrm{y})$≀

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

≀letting $\pi_0\mathsf{at}\llbracket \mathrm{S}_b\rrbracket \leftarrow \pi'_2\ell \xrightarrow{\mathrm{B}} \mathsf{at}\llbracket \mathrm{S}_b\rrbracket$ with $\varrho(\pi'_2\ell \xrightarrow{\mathrm{B}} \mathsf{at}\llbracket \mathrm{S}_b\rrbracket) = \varrho(\pi'_2\ell)$, $\pi_0\mathsf{at}\llbracket \mathrm{S}_b\rrbracket \leftarrow \pi'_2\ell \xrightarrow{\mathrm{B}} \mathsf{at}\llbracket \mathrm{S}_b\rrbracket \pi'_3\ell$, and $\pi_1\ell \leftarrow \pi'_3\ell$ ≀

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

≀because when $\mathrm{x} \neq \mathrm{y}$, $\varrho(\pi'_0\mathsf{at}\llbracket \mathrm{S}_b\rrbracket)\mathrm{y} = \varrho(\pi_0\mathsf{at}\llbracket \mathrm{S}_b\rrbracket)\mathrm{y}$≀

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

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

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

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

$\wr$A coarse approximation is to consider the variables $\mathtt{y} \neq \mathtt{x}$ appearing to the left of an assignment in $\mathtt{S}_b$, a necessary condition for $\mathtt{y}$ to be modified by the execution of $\mathtt{S}_b$ in which 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). $\int$

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

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

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

(8)

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

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

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

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

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

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

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

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

— **(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 $\mathtt{S}_b$. By symmetry of diff this also covers the inverse case.

(8)

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

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

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

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

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

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

$\wr$by lemma 47.59 where $\boldsymbol{\mathcal{S}}' = \{\langle \pi\ell,\ \ell \xrightarrow{\mathrm{B}} \mathsf{at}[\![\mathrm{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathrm{S}]\!]\rangle \mid \mathcal{B}[\![\mathrm{B}]\!]\boldsymbol{\varrho}(\pi\ell) = \mathsf{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathrm{S}_b]\!] \wedge \langle \pi\ell \xrightarrow{\mathrm{B}} \mathsf{at}[\![\mathrm{S}_b]\!], \mathsf{at}[\![\mathrm{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathrm{S}]\!]\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathrm{S}_b]\!]\} \cup \{\langle \pi\ell,\ \ell \xrightarrow{\neg(\mathrm{B})} \mathsf{after}[\![\mathrm{S}]\!]\rangle \mid \mathcal{B}[\![\mathrm{B}]\!]\boldsymbol{\varrho}(\pi\ell) = \mathsf{ff}\}$ with $\pi_0\ell_0 \leftarrow \pi_0\ell$, $\ell_0\pi_1\ell' \leftarrow \ell\pi_2\ell$, $\ell \leftarrow \mathsf{after}[\![\mathrm{S}]\!]$, $\ell'\pi_2\ell \leftarrow \ell \xrightarrow{\mathrm{B}} \mathsf{at}[\![\mathrm{S}_b]\!]\pi_3\ell'' \xrightarrow{\texttt{break}} \mathsf{after}[\![\mathrm{S}]\!]$, $\ell\pi_3 \leftarrow \mathsf{after}[\![\mathrm{S}]\!]$ so $\pi_3 = \ni$, and $\pi_0'\ell_0 \leftarrow \pi_0'\ell$, $\ell_0\pi_1'\ell' \leftarrow \ell_0\pi_2'\ell$, $\ell'\pi_2'\ell \leftarrow \ell \xrightarrow{\mathrm{B}} \mathsf{at}[\![\mathrm{S}_b]\!]$, $\ell\pi_3' \leftarrow \mathsf{after}[\![\mathrm{S}]\!]$ so $\pi_3' = \ni$ $\wr$

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

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

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

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

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

⟅definition of $\mathcal{S}'$ and the other two combinations have already been considered in (**3–B–B**) and (**2–C–C**)⟆

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

⟅$\langle\pi\ell \xrightarrow{B} \mathsf{at}[\![S_b]\!],\ \mathsf{at}[\![S_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{after}[\![S]\!]\rangle \in \mathcal{S}^*[\![S_b]\!]$ so, by definition of program labeling in section 4.2, $\mathsf{after}[\![S]\!] \neq \mathsf{at}[\![S_b]\!]$ cannot appear in $\mathsf{at}[\![S_b]\!]\pi_3\ell''$. Therefore, by definitions (6.6) of ϱ and (47.16) of $\mathsf{seqval}[\![y]\!]\ell$, $\mathsf{seqval}[\![y]\!](\mathsf{after}[\![S]\!])(\pi_0\ell, \ell\pi_2\ell \xrightarrow{B} \mathsf{at}[\![S_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{after}[\![S]\!]) = \varrho(\pi\ell \xrightarrow{B} \mathsf{at}[\![S_b]\!]\pi_3\ell'')$ and $\mathsf{seqval}[\![y]\!](\mathsf{after}[\![S]\!])(\pi'\ell, \ell\pi_2'\ell \xrightarrow{\neg(B)} \mathsf{after}[\![S]\!]) = \varrho(\pi'\ell\pi_2'\ell)$. We conclude by definition (47.18) of diff⟆

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

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

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

⟅definition of $\cup$⟆

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

(because if $y \neq x$ then $\varrho(\pi\ell)y = \varrho(\pi'\ell)y = \varrho(\pi'\ell \xrightarrow{\neg(B)} \mathsf{after}[\![S]\!])y$ so for the value of y to be different in $\varrho(\pi\ell \xrightarrow{B} \mathsf{at}[\![S_b]\!]\pi_3\ell'' \xrightarrow{\mathtt{break}} \mathsf{after}[\![S]\!]) = \varrho(\pi\ell \xrightarrow{B} \mathsf{at}[\![S_b]\!]\pi_3\ell'') = \varrho(\pi'\ell \xrightarrow{B} \mathsf{at}[\![S_b]\!]\pi_3\ell'')$, y must be modified during the execution $\mathsf{at}[\![S_b]\!]\pi_3\ell''$ 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 $\mathsf{mod}[\![S]\!]$ of variables that may be modified by the execution of S is syntactically defined as in (47.50).
)

$(\mathbb{1}_{\mathbb{V}} \cup \{\langle x, y\rangle \mid x \in \mathbb{V} \wedge y \in \mathsf{mod}[\![S_b]\!]\}) \rceil \mathsf{nondet}(B, \neg B)$ (definition of the identity relation $\mathbb{1}$ and $\cup$)

$= \mathbb{1}_{\mathsf{nondet}(B,\neg B)} \cup (\mathsf{nondet}(B, \neg B) \times \mathsf{mod}[\![S_b]\!])$ (definition of $\rceil$)

– Summing up for cases (**3–B–B**) and (**3–C–C**), we get

$(5) \subseteq \alpha^{\mathrm{d}}(\{X\})\ell \fatsemi \Big(\big(\bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![S_b]\!]} \widehat{\boldsymbol{\mathcal{S}}}^{\exists}_{\mathsf{diff}}[\![S_b]\!]\ell''\big) \rceil \mathsf{nondet}(B, B)\Big) \cup \mathbb{1}_{\mathsf{nondet}(B,\neg B)} \cup (\mathsf{nondet}(B, \neg B) \times \mathsf{mod}[\![S_b]\!])$.

— Summing up for all subcases of (**3**) for a dependency observation point $\ell' = \mathsf{after}[\![S]\!]$, we would get a term (47.63.c) of the form

$$
\begin{aligned}
\llparenthesis\, \ell' = \mathsf{after}[\![S]\!] \;?\; (&\mathbb{1}_{\mathsf{nondet}(\neg B,\neg B)} \cup X(\ell) \cup \\
&(X(\ell) \fatsemi (\mathbb{1}_{\mathsf{nondet}(\neg B,\neg B)} \cup \mathsf{nondet}(\neg B, \neg B) \times \mathsf{mod}[\![S_b]\!])) \rceil \mathsf{nondet}(B, \neg B) \cup \\
&X(\ell) \fatsemi \Big(\Big(\bigcup_{\ell'' \in \mathsf{breaks\text{-}of}[\![S_b]\!]} \widehat{\boldsymbol{\mathcal{S}}}^{\exists}_{\mathsf{diff}}[\![S_b]\!]\,\ell''\Big) \rceil \mathsf{nondet}(B, B)\Big) \cup \\
&\quad \mathbb{1}_{\mathsf{nondet}(B,\neg B)} \cup (\mathsf{nondet}(B, \neg B) \times \mathsf{mod}[\![S_b]\!])) \,\text{\textcircled{:}}\, \varnothing \,\rrparenthesis.
\end{aligned} \tag{47.63.c$'$}
$$

that can be simplified as follows (while losing precision)

(5)

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

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

$\wr$because $\mathsf{nondet}(\mathtt{B}_1,\mathtt{B}_2) \subseteq \mathbb{V}$ so $\mathbb{1}_{\mathsf{nondet}(\mathtt{B}_1,\mathtt{B}_2)} \subseteq \mathbb{1}_{\mathbb{V}}$ and definition of $\rceil$$\int$

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

$\wr$because $⨾$ distributes over $\cup$$\int$

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

$\wr$idempotency law for $\cup$ and $⨾$ distributes over $\cup$$\int$

After simplification, we get a term (47.63.c) of the form

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

For fixpoints X of $\mathcal{F}^{\mathrm{diff}}[\![\mathtt{while}\;\ell\;\mathtt{(B)}\;\mathtt{S}_b]\!]$, we have $\mathbb{1}_{\mathbb{V}} \subseteq X(\ell)$ by (47.63.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 (47.63.c) of the form

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

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

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

proving pointwise semicommutation. □

5 Mathematical Proofs of Chapter 48

Proof of Lemma 48.63 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 $\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0) = \Omega^{\mathrm{r}}_{\mathrm{s}}$ in case (48.47.8) of an occurs check, we have $\gamma^{\mathrm{r}}_{\mathrm{s}}(\Omega^{\mathrm{r}}_{\mathrm{s}}) = \varnothing$ 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, $\boldsymbol{\tau}_2 \notin \mathbb{V}_{\mathbb{t}}$ in case (48.47.8). It follows, by definition (48.51) of γ_{e} that $\gamma_{\mathsf{e}}(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) = \gamma_{\mathsf{e}}(\alpha \doteq \boldsymbol{\tau}_2) = \varnothing$ because otherwise, there would be some $\boldsymbol{\varrho}$ such that $\boldsymbol{\varrho}(\boldsymbol{\tau}_1) = \boldsymbol{\varrho}(f(\dots\alpha\dots)$ which would be an infinite object not in $\mathbf{P}^{\nu}$, as shown in lemma 48.9.

- By lemma 48.58, 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, \dots, \boldsymbol{\tau}^n_1) \doteq g(\boldsymbol{\tau}^1_2, \dots, \boldsymbol{\tau}^m_2)) \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0) && \wr \text{test (48.47.1) is } \mathtt{tt} \wr \\
= \ & \gamma_{\mathsf{e}}(f(\boldsymbol{\tau}^1_1, \dots, \boldsymbol{\tau}^n_1) \doteq f(\boldsymbol{\tau}^1_2, \dots, \boldsymbol{\tau}^n_2)) \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0) && \wr \text{test (48.47.2) is } \mathtt{ff} \wr \\
= \ & \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(f(\boldsymbol{\tau}^1_1, \dots, \boldsymbol{\tau}^n_1)) = \boldsymbol{\varrho}(f(\boldsymbol{\tau}^1_2, \dots, \boldsymbol{\tau}^n_2))\} \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0) && \wr \text{definition (48.51) of } \gamma_{\mathsf{e}} \wr \\
= \ & \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \bigwedge_{i=1}^{n} \boldsymbol{\varrho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\varrho}(\boldsymbol{\tau}^i_2)\} && \wr \text{definition (48.7) of assignment application} \wr \\
= \ & \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) && \wr \text{definition of } \textstyle\bigcap \wr \\
= \ & (\{\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)\} \\
& && \wr \textstyle\bigcap \text{ is associative and commutative} \wr \\
= \ & (\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)\} && \wr \text{definition (48.51)x of } \gamma_{\mathsf{e}} \wr \\
= \ & \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) && \wr \text{induction hypothesis and } \textstyle\bigcap \text{ commutative} \wr \\
= \ & \mathsf{let}\ \vartheta_1 = \mathsf{unify}((\boldsymbol{\tau}^1_i, \boldsymbol{\tau}^1_2, \vartheta_0)\ \mathsf{in} \\
& \quad \dots \\
& \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) && \wr \text{recurrence hypothesis, } j < n \wr \\
= \ & \mathsf{let}\ \vartheta_1 = \mathsf{unify}(\boldsymbol{\tau}^1_i, \boldsymbol{\tau}^1_2, \vartheta_0)\ \mathsf{in} \\
& \quad \dots \\
& \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)\}
\end{aligned}
$$

$\wr \bigcap$ is associative and commutative $\wr$

$$
\begin{aligned}
&= \mathsf{let}\ \vartheta_1 = \mathsf{unify}(\boldsymbol{\tau}_i^1, \boldsymbol{\tau}_2^1, \vartheta_0)\ \mathsf{in} \\
&\qquad \ldots \\
&\qquad\quad \mathsf{let}\ \vartheta_j = \mathsf{unify}(\boldsymbol{\tau}_i^j, \boldsymbol{\tau}_2^j, \vartheta_{j-1})\ \mathsf{in} \\
&\qquad\qquad \mathsf{let}\ \vartheta_{j+1} = \mathsf{unify}(\boldsymbol{\tau}_i^{j+1}, \boldsymbol{\tau}_2^{j+1}, \vartheta_j)\ \mathsf{in} \\
&\qquad\qquad\quad \bigcap_{i=j+2}^{n} \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\boldsymbol{\tau}_i^1) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2^i)\} \cap \gamma_s^r(\vartheta_{j+1}) && \wr \text{induction hypothesis and } \bigcap \text{ commutative} \wr \\
&= \mathsf{let}\ \vartheta_1 = \mathsf{unify}(\boldsymbol{\tau}_i^1, \boldsymbol{\tau}_2^1, \vartheta_0)\ \mathsf{in} \\
&\qquad \ldots \\
&\qquad\quad \mathsf{let}\ \vartheta_j = \mathsf{unify}(\boldsymbol{\tau}_i^n, \boldsymbol{\tau}_2^n, \vartheta_{n-1})\ \mathsf{in} \\
&\qquad\qquad \bigcap_{i=n+2}^{n} \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\boldsymbol{\tau}_i^1) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2^i)\} \cap \gamma_s^r(\vartheta_n) && \wr \text{by recurrence when } j+1=n \wr \\
&= \mathsf{let}\ \vartheta_1 = \mathsf{unify}(\boldsymbol{\tau}_i^1, \boldsymbol{\tau}_2^1, \vartheta_0)\ \mathsf{in} \\
&\qquad \ldots \\
&\qquad\quad \mathsf{let}\ \vartheta_j = \mathsf{unify}(\boldsymbol{\tau}_i^n, \boldsymbol{\tau}_2^n, \vartheta_{n-1})\ \mathsf{in} \\
&\qquad\qquad \gamma_s^r(\vartheta_n)
\end{aligned}
$$

$\wr$ because $\bigcap_{i=n+2}^{n}\{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\boldsymbol{\tau}_i^1) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2^i)\} = \bigcap \varnothing = \mathbf{P}^\nu$ is the identity for $\cap$ $\wr$

- In case (48.47.7), we have

$$
\begin{aligned}
& \gamma_e(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) \cap \gamma_s^r(\vartheta_0) \\
&= \gamma_e(\alpha \doteq \alpha) \cap \gamma_s^r(\vartheta_0) && \wr \alpha \in \mathbb{V}_{\mathfrak{t}} \text{ by test (48.47.7)} \wr \\
&= \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\alpha)\} \cap \gamma_s^r(\vartheta_0) && \wr \text{definition (48.51) of } \gamma_e \wr \\
&= \mathbf{P}^\nu \cap \gamma_s^r(\vartheta_0) && \wr \text{because } \boldsymbol{\varrho} \in \mathbf{P}^\nu \triangleq \mathbb{V}_{\mathfrak{t}} \to \mathbf{T} \text{ by (48.6)} \wr \\
&= \gamma_s^r(\vartheta_0) && \wr \mathbf{P}^\nu \text{ is the identity for } \cap \wr \\
&= \gamma_s^r(\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0)) && \wr \text{definition of} \mathsf{unify} \text{ in case (48.47.7)} \wr
\end{aligned}
$$

- In case (48.47.11), we have

$$
\begin{aligned}
& \gamma_e(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) \cap \gamma_s^r(\vartheta_0) \\
&= \gamma_e(\alpha \doteq \boldsymbol{\tau}_2) \cap \gamma_s^r(\vartheta_0)
\end{aligned}
$$

$\wr$ where $\alpha \in \mathbb{V}_{\mathfrak{t}}$ by test (48.47.9), $\alpha \notin \mathsf{vars}[\![\boldsymbol{\tau}_2]\!]$ because test (48.47.8) is ff, $\alpha \notin \mathsf{dom}(\vartheta_0)$ by test (48.47.10), and $\boldsymbol{\tau}_2 \notin \mathbb{V}_{\mathfrak{t}}$ because test (48.47.1) is ff $\wr$

$$
\begin{aligned}
&= \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2)\} \cap \gamma_s^r(\vartheta_0) && \wr \text{definition (48.51) of } \gamma_e \wr \\
&= \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2)\} \cap \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\vartheta_0(\beta))\} && \wr \text{definition (48.52) of } \gamma_s^r \wr \\
&= \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2) \wedge \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\vartheta_0(\beta))\} && \wr \text{definition of } \cap \wr
\end{aligned}
$$

$= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \forall \beta \in \mathbb{V}_{t} \mathrel{.} \boldsymbol{\varrho}(\beta) = \llparenthesis\, \beta = \alpha \mathrel{?} \boldsymbol{\varrho}(\vartheta_0(\beta)[\beta \in \mathsf{vars}[\![\boldsymbol{\tau}_2]\!] \leftarrow \boldsymbol{\tau}_2]) \mathrel{⸮} \boldsymbol{\varrho}(\boldsymbol{\tau}_2[\alpha \leftarrow \vartheta_0(\beta)])\, \rrparenthesis\}$

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

$= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \forall \beta \in \mathbb{V}_{t} \mathrel{.} \boldsymbol{\varrho}(\beta) = \llparenthesis\, \beta = \alpha \mathrel{?} \boldsymbol{\varrho}(\vartheta_0(\beta)[\beta \in \mathsf{vars}[\![\boldsymbol{\tau}_2]\!] \leftarrow \boldsymbol{\tau}_2]) \mathrel{⸮} \boldsymbol{\varrho}(\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\}(\vartheta_0(\beta)))\, \rrparenthesis\}$

$\wr$by exercise 48.60 where $\boldsymbol{\tau}' = \vartheta_0(\beta)$$\wr$

$= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \forall \beta \in \mathbb{V}_{t} \mathrel{.} \boldsymbol{\varrho}(\beta) = \llparenthesis\, \beta = \alpha \mathrel{?} \boldsymbol{\varrho}(\vartheta_0(\boldsymbol{\tau}_2)) \mathrel{⸮} \boldsymbol{\varrho}(\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\}(\vartheta_0(\beta)))\, \rrparenthesis\}$ $\wr$by exercise 48.62$\wr$

$= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \forall \beta \in \mathbb{V}_{t} \mathrel{.} \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\llparenthesis\, \beta = \alpha \mathrel{?} \vartheta_0(\boldsymbol{\tau}_2) \mathrel{⸮} (\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\} \circ \vartheta_0)(\beta)\, \rrparenthesis)\}$

$\wr$definitions the conditional and function composition $\circ$$\wr$

$= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \forall \beta \in \mathbb{V}_{t} \mathrel{.} \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\llparenthesis\, \beta = \alpha \mathrel{?} (\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\} \circ \vartheta_0)(\alpha) \mathrel{⸮} (\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\} \circ \vartheta_0)(\beta)\, \rrparenthesis)\}$

$\wr$because $X \notin \mathsf{dom}(\vartheta_0)$ 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$

$= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \forall \beta \in \mathbb{V}_{t} \mathrel{.} \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\} \circ \vartheta_0)(\beta)$ $\wr$definition of the conditional$\wr$

$= \gamma^{\mathsf{r}}_{\mathsf{s}}\{\langle\alpha,\ \boldsymbol{\tau}_2\rangle\} \circ \vartheta_0$ $\wr$definition (48.52) of $\gamma^{\mathsf{r}}_{\mathsf{s}}$$\wr$

$= \gamma^{\mathsf{r}}_{\mathsf{s}}(\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0))$ $\wr$(48.47.11)$\wr$

- 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 $\boldsymbol{\tau}_2 \notin \mathbb{V}_{t}$ because test (48.47.1) is ff.

  $\gamma_{\mathsf{e}}(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0)$

  $= \gamma_{\mathsf{e}}(\alpha \doteq \boldsymbol{\tau}_2) \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0)$ $\wr\boldsymbol{\tau}_1 = \alpha\wr$

  $= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2) \wedge \forall \beta \in \mathbb{V}_{t} \mathrel{.} \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\vartheta_0(\beta))\}$

  $\wr$definition (48.51) of γ_{e}, (48.52) of $\gamma^{\mathsf{r}}_{\mathsf{s}}$, and definition of $\cap$$\wr$

  $= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\vartheta_0(\alpha)) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2) \wedge \forall \beta \in \mathbb{V}_{t} \mathrel{.} \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\vartheta_0(\beta))\}$

  $\wr\alpha \in \mathsf{dom}(\vartheta_0)$ so $\boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\vartheta_0(\beta)) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2)$$\wr$

  $= \gamma_{\mathsf{e}}(\vartheta_0(\alpha) \doteq \boldsymbol{\tau}_2) \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0)$ $\wr$definition (48.51) of γ_{e}, (48.52) of $\gamma^{\mathsf{r}}_{\mathsf{s}}$, and definition of $\cap$$\wr$

  $= \gamma^{\mathsf{r}}_{\mathsf{s}}(\mathsf{unify}(\vartheta_0(\alpha), \boldsymbol{\tau}_2, \vartheta_0))$ $\wr$induction hypothesis of lemma 48.63$\wr$

  $= \gamma^{\mathsf{r}}_{\mathsf{s}}(\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0))$ $\wr$(48.47.12)$\wr$

- In case (48.47.13) we are back to (48.47.11) or (48.47.12) by the symmetry argument of remark 48.49. □

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

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

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

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 (48.68.2), …, (48.68.4), and by case analysis on the conditional.

The first call at (48.68.12) satisfies the preinvariant of (48.39) because $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0 \in \mathbf{T}^\nu$ by hypothesis and $T_0 = \varnothing \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu$;

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 (48.68.5), $\boldsymbol{\tau}_j \in \mathbf{T}^\nu$ by hypothesis on the intermediate call, so $\boldsymbol{\tau}_j^i \in \mathbf{T}^\nu$, $i = 1, \ldots, n$, $j = 1, 2$, by the test (48.68.1). 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 $T_i \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu \wedge \forall \alpha \in \mathsf{dom}(T_0) \,.\, T_0(\alpha) = T_i(\alpha)$. Then, by induction on the sequence of calls to lub, $\boldsymbol{\tau}^{i+1} \in \mathbf{T}^\nu$ and $T_{i+1} \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu \wedge \mathsf{vars}[\![\boldsymbol{\tau}^{i+1}]\!] \subseteq \mathsf{dom}(T_{i+1}) \wedge \forall \alpha \in \mathsf{dom}(T_i) \,.\, T_i(\alpha) = T_{i+1}(\alpha)$. 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 (48.68.5) satisfies (48.39) because $\boldsymbol{\tau}^i \in \mathbf{T}^\nu$, $i = 1, \ldots, n$, implies $f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n) \in \mathbf{T}^\nu$ and $\mathsf{vars}[\![f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)]\!] = \bigcup_{i=1}^n \mathsf{vars}[\![\boldsymbol{\tau}^i]\!]$;
- The case (48.68.7) is trivial because $\beta \in \mathbf{T}^\nu$, $T' = T_0$, and $\beta \in \mathsf{dom}(T_0)$;
- In case (48.68.9), $T_0 \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu$ by hypothesis, $\beta \in \mathbf{T}^\nu$, and $\beta \in \mathbb{V}_{\mathfrak{t}} \setminus \mathsf{dom}(T_0)$ by the test (48.68.8) so $T' = \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0] \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu$ 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 (48.68.9).

For $T \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu$, 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 $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \in \mathsf{T}^\nu$ and $T_0 \in \wp(\mathbb{V}_{\mathbb{t}} \times \mathsf{T}^\nu \times \mathsf{T}^\nu)$, 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 (48.68.2), …, (48.68.4), and by case analysis for the conditional.

- In case (48.68.5), 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 $\forall \alpha \in \mathsf{vars}[\![\boldsymbol{\tau}^i]\!] \subseteq \mathsf{dom}(T_i)\ .\ T_i(\alpha) = T_{i+1}(\alpha)$. Therefore, by (13), $\forall \alpha \in \mathsf{vars}[\![\boldsymbol{\tau}^i]\!]\ .\ \vartheta_j(T_{i+1})(\boldsymbol{\tau}^i) = \vartheta_j(T_i)(\boldsymbol{\tau}^i)$. 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 (48.68.7), (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 (48.68.9), $\bar{\varsigma}_j(T')\boldsymbol{\tau} = \vartheta_j(\langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])\beta = \mathsf{if}\ \beta \in \mathsf{dom}(T)\ \mathsf{then\ let}\ \langle \boldsymbol{\tau}_1',\ \boldsymbol{\tau}_2' \rangle = \langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0](\beta)\ \mathsf{in}\ \boldsymbol{\tau}_j'\ \mathsf{else}\ \alpha = \boldsymbol{\tau}_j$, $j = 1, 2$. □

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

Lemma 16 For all $\boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \in \mathsf{T}^\nu$, 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 (48.68.12) does terminate.

Lemma 16 follows by definition of the infimum $\overline{\varnothing}^\nu$ in cases (48.68.11).

Otherwise, at (48.68.12), $\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2) = \boldsymbol{\tau}$ 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 theorem 48.31, 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 theorem 48.31, 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 given in figure 18 to construct this substitution ϑ' given any upper bound $\boldsymbol{\tau}'$.

Example 19 The assumption (17.13) prevents a call like $\mathsf{lub}'(f(a, b), f(b, a), \varnothing, f(\alpha, \alpha), \boldsymbol{\varepsilon}, \varnothing)$ where $f(\alpha, \alpha)$ is not an upper bound of $\{f(a, b), f(b, a)\}$. □

Example 20 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

$\mathsf{lub}'(f(g(a), g(g(a)), g(a), b, b), f(g(b), g(h(b)), g(b), a, a), \varnothing, f(g(\alpha), \beta, g(\alpha), \gamma, U), \boldsymbol{\varepsilon})$

$\quad \mathsf{lub}'(g(a), g(b), \varnothing, g(\alpha), \boldsymbol{\varepsilon})$ (17.2b)

$\quad\quad \mathsf{lub}'(a, b, \varnothing, \alpha, \boldsymbol{\varepsilon})$ (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)

$\quad \mathsf{lub}'(g(g(a)), g(h(b)), \{\langle \beta, \langle a, b \rangle \rangle\}, \beta, \{\langle \alpha, \beta \rangle\})$ (17.3b)

$\quad\quad \mathsf{lub}(g(a), h(b), \{\langle \beta, \langle a, b \rangle \rangle\})$ (17.2a)

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

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

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

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

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

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

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

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

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

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

$= \langle f(g(\beta), g(\gamma), g(\beta), \alpha, \alpha), \{\langle \alpha, \langle b, a \rangle \rangle, \langle \beta, \langle a, b \rangle \rangle, \langle \gamma, \langle g(a), h(b) \rangle \rangle\}, \{\langle \alpha, \beta \rangle, \langle \beta, g(\gamma) \rangle, \langle \gamma, \alpha \rangle, \langle U, \alpha \rangle\} \rangle$ (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 21 For all $\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}, \boldsymbol{\tau}', \boldsymbol{\tau}'' \in \mathbf{T}^\nu, T_0, T, T'' \in \wp(\mathbb{V}_{\mathfrak{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta' \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu$, 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 21 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 (48.68.2), …, (48.68.5). 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 (48.68.2), …, (48.68.4) while, by induction on the sequence of calls to lub' (17.2b), …, (17.4b) is abstracted to that of (48.68.2), …, (48.68.4). It follows that $\langle \boldsymbol{\tau}, T \rangle$ at (48.68.12) is equal to $\langle \boldsymbol{\tau}, T \rangle$ at (17.14). □

The following lemma 22 proves the well-typing of algorithm lub'.

Lemma 22 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}' \in \mathbf{T}^\nu$, $T_0 \in \wp(\mathbb{V}_{\mathfrak{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2 \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$ 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 $\exists \gamma \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\tau}' = \gamma$ at (17.6) and (17.8). □

Proof of Lemma 22 Notice that Lemmas 11, 14, and 16 are valid for lub' because 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 definition (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 because 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 23 shows that variables recorded in T_0 are for nonmatching subterms only.

Lemma 23 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \in \mathbf{T}^\nu$ and $T_0 \in \wp(\mathbb{V}_{\mathfrak{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, if $\mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0)$ is (recursively) called from the main call $\mathsf{lub}(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing)$, then for all $\boldsymbol{\tau}_1', \boldsymbol{\tau}_1'^1, \ldots, \boldsymbol{\tau}_1'^n, \boldsymbol{\tau}_2', \boldsymbol{\tau}_2'^1, \ldots, \boldsymbol{\tau}_2'^n \in \mathbf{T}^\nu$,

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

□

Proof of Lemma 23 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 23 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 (48.68.9) for which (48.68.1) 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 23 holds for all calls from the main call (17.14). $\square$

Lemma 24 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}, \boldsymbol{\tau}' \in \mathbf{T}^\nu$, $T_0, T \in \mathbb{V}_{\mathfrak{t}} \nrightarrow (\mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$ 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

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

Proof of Lemma 24 We prove the stronger property that the following preinvariant and postinvariant do hold for any call $\langle \boldsymbol{\tau}, T, \vartheta' \rangle = \mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$.

$$\begin{array}{ll} \text{preinvariant} & (\exists \beta \in \mathsf{dom}(T_0) \,.\, T_0(\beta) = \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle \wedge \boldsymbol{\tau}' = \gamma) \Rightarrow (\gamma \in \mathsf{dom}(\vartheta_0) \wedge \vartheta_0(\gamma) = \beta) \\ \text{postinvariant} & (\exists \beta \in \mathsf{dom}(T) \,.\, T(\beta) = \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle \wedge \boldsymbol{\tau}' = \gamma) \Rightarrow (\gamma \in \mathsf{dom}(\vartheta') \wedge \vartheta'(\gamma) = \beta) \end{array} \tag{25}$$

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 (25) holds vacuously at the first call (17.14) because $T_0 = \varnothing$;
- For the induction step, we proceed by case analysis.
  - In case (17.5a), there is no recursive call to lub' and, by lemma 23, the premise of the postinvariant of (25) 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 (25) 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 (25) holds at (17.5b) for T_n and ϑ_n.
  - In case (17.7), we know by the test (17.6) and lemma 22 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 $\vartheta_0(\gamma) = \beta$. Because $T = T_0$ 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 (25). $\square$

Let us prove the converse of lemma 24.

Lemma 26 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu$, $T_0, T \in \wp(\mathbb{V}_{\mathfrak{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$ 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

$$\forall \beta, \gamma \in \mathbb{V}_{\mathfrak{t}} \,.\, (\gamma \in \mathsf{dom}(\vartheta_0) \wedge \vartheta_0(\gamma) = \beta) \Rightarrow (\beta \in \mathsf{dom}(T_0)). \quad \square$$

Proof of Lemma 26 We prove the stronger property that the following preinvariant and postinvariant do hold for any call $\langle \boldsymbol{\tau},\ T,\ \vartheta' \rangle = \mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$.

$$\begin{array}{ll} \text{preinvariant} & \forall \beta, \gamma \in \mathbb{V}_{\mathfrak{t}} \,.\, (\gamma \in \mathsf{dom}(\vartheta_0) \wedge \vartheta_0(\gamma) = \beta) \Rightarrow (\beta \in \mathsf{dom}(T_0)) \\ \text{postinvariant} & \forall \beta, \gamma \in \mathbb{V}_{\mathfrak{t}} \,.\, (\gamma \in \mathsf{dom}(\vartheta') \wedge \vartheta'(\gamma) = \beta) \Rightarrow (\beta \in \mathsf{dom}(T)) \end{array} \tag{27}$$

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 basis, $\vartheta_0 = \boldsymbol{\varepsilon}$ so $\mathsf{dom}(\vartheta_0) = \varnothing$ so the preinvariant (27) 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 $\vartheta'(\gamma) = f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n) \notin \mathbb{V}_{\mathfrak{t}}$ so that the postcondition holds vacuously;
  - In case (17.5b), the preinvariant of the first recursive call (17.2a) holds by the preinvariant of (27) 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 (27) 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 (27) 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 $\beta \in \mathsf{dom}(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0]) = \mathsf{dom}(T)$. $\square$

The next lemma 28 shows how the term variables are used.

Lemma 28 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu$, $T_0, T \in \wp(\mathcal{V}_{\mathfrak{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1^0, \vartheta_2^0, \vartheta' \in \mathcal{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$ 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

$$\begin{array}{ll} \text{preinvariant} & \mathsf{vars}[\![\vartheta_0(\mathcal{V}_{\mathfrak{t}})]\!] \subseteq \mathsf{dom}(T_0) \\ \text{postinvariant} & \mathsf{vars}[\![\vartheta'(\mathcal{V}_{\mathfrak{t}})]\!] \subseteq \mathsf{dom}(T) \end{array} \tag{29}$$

(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 28 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), $\vartheta_0 = \boldsymbol{\varepsilon}$ so $\mathsf{vars}[\![\vartheta_0(\mathcal{V}_{\mathfrak{t}})]\!] = \mathsf{vars}[\![\varnothing]\!] = \varnothing \subseteq \mathsf{dom}(T_0)$;
- Otherwise the preinvariant of (29) holds for T_0 and ϑ_0 at the first recursive call (17.2b). Assume, by induction hypothesis, that $\mathsf{vars}[\![\vartheta_{i-1}(\mathcal{V}_{\mathfrak{t}})]\!] \subseteq \mathsf{dom}(T_{i-1})$ 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 $\mathsf{vars}[\![\vartheta_i(\mathcal{V}_{\mathfrak{t}})]\!] \subseteq \mathsf{dom}(T_i)$ after that call, which is also the preinvariant of the next call, if any. By recurrence, $\mathsf{vars}[\![\vartheta'(\mathcal{V}_{\mathfrak{t}})]\!] = \mathsf{vars}[\![\vartheta_n(\mathcal{V}_{\mathfrak{t}})]\!] \subseteq \mathsf{dom}(T_n) = \mathsf{dom}(T)$ in case the call (17) to lub' terminates at (17.5b);
- If lub' terminates at (17.5a), there are two cases.
  - $\mathsf{vars}[\![\vartheta'(\{\gamma\})]\!] = \mathsf{vars}[\![f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\{\gamma\})]\!] = \mathsf{vars}[\![f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)]\!] = \bigcup_{i=1}^n \mathsf{vars}[\![\boldsymbol{\tau}^i]\!]$. By lemma 11 and 21, we have $\mathsf{vars}[\![\boldsymbol{\tau}^i]\!] \subseteq \mathsf{dom}(T_i)$, $i = 1, \ldots, n$ and $\mathsf{dom}(T_i) \subseteq \mathsf{dom}(T_n)$ so that $\bigcup_{i=1}^n \mathsf{vars}[\![\boldsymbol{\tau}^i]\!] \subseteq \bigcup_{i-1}^n \mathsf{dom}(T_i) \subseteq \mathsf{dom}(T_n) = \mathsf{dom}(T)$;
  - $\mathsf{vars}[\![\vartheta'(\mathcal{V}_{\mathfrak{t}} \setminus \{\gamma\})]\!] = \mathsf{vars}[\![f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\mathcal{V}_{\mathfrak{t}} \setminus \{\gamma\})]\!] = \mathsf{vars}[\![\vartheta_0(\mathcal{V}_{\mathfrak{t}} \setminus \{\gamma\})]\!] \subseteq \mathsf{vars}[\![\vartheta_0(\mathcal{V}_{\mathfrak{t}})]\!]$ which, by the preinvariant (29), is included in $\mathsf{dom}(T_0)$. By lemma 11 and 21, $\mathsf{dom}(T_{i=1}) \subseteq \mathsf{dom}(T_i)$, $i = 1, \ldots, n$ so that, by transitivity, $\mathsf{dom}(T_0) \subseteq \mathsf{dom}(T_n) = \mathsf{dom}(T)$. Therefore $\mathsf{vars}[\![\vartheta'(\mathcal{V}_{\mathfrak{t}} \setminus \{\gamma\})]\!] \subseteq \mathsf{dom}(T)$;
  - Because $\vartheta'(\mathcal{V}_{\mathfrak{t}}) = \vartheta'(\{\gamma\}) \cup \vartheta'(\mathcal{V}_{\mathfrak{t}} \setminus \{\gamma\})$, we conclude that $\mathsf{vars}[\![\vartheta'(\mathcal{V}_{\mathfrak{t}})]\!] = \mathsf{vars}[\![\vartheta'(\{\gamma\}) \cup \vartheta'(\mathcal{V}_{\mathfrak{t}} \setminus \{\gamma\})]\!] = \mathsf{vars}[\![\vartheta'(\{\gamma\})]\!] \cup \mathsf{vars}[\![\vartheta'(\mathcal{V}_{\mathfrak{t}} \setminus \{\gamma\})]\!] \subseteq \mathsf{dom}(\vartheta') \cup \mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta')$; □
- If lub' terminates at (17.7) then the postinvariant directly follows from the preinvariant of (29) because $T = T_0$ 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 $\mathsf{vars}[\![\vartheta'(\mathbb{V}_{\mathfrak{t}}\setminus\{\gamma\})]\!] = \mathsf{vars}[\![\beta[\gamma \leftarrow \vartheta_0](\mathbb{V}_{\mathfrak{t}}\setminus\{\gamma\})]\!] = \mathsf{vars}[\![\vartheta_0(\mathbb{V}_{\mathfrak{t}}\setminus\{\gamma\})]\!] \subseteq \mathsf{vars}[\![\vartheta_0(\mathbb{V}_{\mathfrak{t}})]\!] \subseteq \mathsf{dom}(T_0)$, by the preinvariant of (29). 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 because vars preserves joins. □

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

Lemma 30 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}' \in \mathbf{T}^\nu, T_0, T \in \wp(\mathbb{V}_{\mathfrak{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1^0, \vartheta_2^0, \vartheta' \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$ 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

$$\vartheta_1^0(\boldsymbol{\tau}') = \boldsymbol{\tau}_1 \wedge \vartheta_2^0(\boldsymbol{\tau}') = \boldsymbol{\tau}_2. \tag{31}$$ □

Proof of Lemma 30 For the first call at (17.14), (31) 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 (31) holds before the recursive calls (17.2b), …, (17.4b) because 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 32 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu$, $T_0, T \in \wp(\mathbb{V}_{\mathfrak{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1^0, \vartheta_2^0, \vartheta' \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$ 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

$$\begin{array}{lll} \text{preinvariant} & \forall j = 1, 2\ .\ \forall \alpha \in \mathsf{dom}(\vartheta_0)\ .\ \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_0)(\vartheta_0(\alpha)) & (33) \\ \text{postinvariant} & \forall j = 1, 2\ .\ \forall \alpha \in \mathsf{dom}(\vartheta')\ .\ \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T)(\vartheta'(\alpha)) \wedge \bar{\varsigma}_j(T)(\boldsymbol{\tau}) = \boldsymbol{\tau}_j & \end{array}$$ □

Proof of Lemma 32 Notice again that lemma 11, 14, and 16 are valid for lub' because they do not involve the extra parameters $\boldsymbol{\tau}', \vartheta_0$, or result ϑ'. It follows, by lemma 14, that the postinvariant of (33) satisfies $\bar{\varsigma}_j(T)(\boldsymbol{\tau}) = \boldsymbol{\tau}_j$, $j = 1, 2$. The proof of (33) 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 (33) holds vacuously for the main call (17.14) because $\vartheta_0 = \boldsymbol{\varepsilon}$ so $\mathsf{dom}(\vartheta_0) = \varnothing$;
- Assume that the preinvariant (33) 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 $\forall j = 1,2 \,.\, \forall \alpha \in \mathsf{dom}(\vartheta') \,.\, \vartheta^0_j(\alpha) = \bar{\varsigma}_j(T_0)(\vartheta'(\alpha))$ at the first recursive call (17.2b).

Assume that $\forall j = 1,2 \,.\, \forall \alpha \in \mathsf{dom}(\vartheta_{i-1}) \,.\, \vartheta^0_j(\alpha) = \bar{\varsigma}_j(T_{i-1})(\vartheta_{i-1}(\alpha))$ before the i^{th} recursive call. By induction on the sequence of calls to lub', the postinvariant of (33) holds. Therefore we have $\forall j = 1,2 \,.\, \forall \alpha \in \mathsf{dom}(\vartheta_i) \,.\, \vartheta^0_j(\alpha) = \bar{\varsigma}_j(T_i)(\vartheta_i(\alpha))$ before the $i+1^{\text{th}}$ call. By recurrence, all recursive calls do satisfy (33).

We must also show that the intermediate call satisfies the postinvariant of (33). We proceed by cases.

- In case (17.5b), we have $T = T_n$ and ϑ_n which satisfy the postinvariant of (33), as shown above.
- In case (17.5a), the postinvariant is $\forall j = 1,2 \,.\, \forall \alpha \in \mathsf{dom}(f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0]) \,.\, \vartheta^0_j(\alpha) = \bar{\varsigma}_j(T_n)(f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\alpha))$.
  - If $\alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\}$, we must show that $\vartheta^0_j(\alpha) = \bar{\varsigma}_j(T_n)(\vartheta_0(\alpha))$.
    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 28, $\mathsf{vars}[\![\vartheta_0(\mathbb{V}_{\mathbb{t}})]\!] \subseteq \mathsf{dom}(T_0)$ 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 $\forall \alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\} \,.\, \bar{\varsigma}_j(T_0)\boxtimes_0(\boxtimes) = \bar{\varsigma}_j(T_n)\boxtimes_0(\boxtimes)$. By the preinvariant of (33), we have $\forall \alpha \in \mathsf{dom}(\vartheta_0) \,.\, \vartheta^0_j(\alpha) = \bar{\varsigma}_j(T_0)(\vartheta_0(\alpha))$. Therefore, by transitivity, $\vartheta^0_j(\alpha) = \bar{\varsigma}_j(T_n)(\vartheta_0(\alpha))$.
  - Otherwise $\alpha = \gamma$, in which case we must show that $\vartheta^0_j(\gamma) = \bar{\varsigma}_j(T_n)(f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n))$. By lemma 30, (48.42) of lemma 48.40, and (17.5a), we have $\vartheta^0_j(\gamma) = \vartheta^0_j(\boldsymbol{\tau}') = \boldsymbol{\tau}_j = \bar{\varsigma}_j(T)(\boldsymbol{\tau}) = \bar{\varsigma}_j(T)(f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n))$.
- In case (17.7), the postinvariant of (31) immediately follows from the preinvariant because $T = T_0$ and $\vartheta' = \vartheta_0$;
- In case (17.9), we must show that $\forall j = 1,2 \,.\, \forall \alpha \in \mathsf{dom}(\beta[\gamma \leftarrow \vartheta_0]) \,.\, \vartheta^0_j(\alpha) = \bar{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])(\beta[\gamma \leftarrow \vartheta_0](\alpha))$. There are two cases.
  - If $\alpha = \gamma$ then we must prove that $\vartheta^0_j(\gamma) = \bar{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])(\beta)$, that is, by (13), $\vartheta^0_j(\gamma) = \boldsymbol{\tau}_j$. It is not possible that $\gamma \in \mathsf{dom}(\vartheta_0)$ because otherwise, we would have $\forall \beta \in \mathsf{dom}(T_0) \,.\, T_0(\beta) \neq \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle$ because the test (17.6) is ff and $\boldsymbol{\tau}' = \gamma \in \mathbb{V}_{\mathbb{t}}$ by lemma 22, which is in contradiction to (the contrapositive of) lemma 26. Therefore $\vartheta_0(\gamma) = \gamma$ by (48.30). It follows that we have to prove that $\vartheta^0_j(\vartheta_0(\gamma)) = \boldsymbol{\tau}_j$, which directly follows from the preinvariant of (31);
  - Otherwise, $\alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\}$ and we must show that $\vartheta^0_j(\alpha) = \bar{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])(\vartheta_0(\alpha))$. The test (17.8) implies $\beta \notin \mathsf{dom}(T_0)$ and so $\beta \notin \mathsf{vars}[\![\vartheta_0(\alpha)]\!]$ because $\mathsf{vars}[\![\vartheta_0(\mathbb{V}_{\mathbb{t}})]\!] \subseteq \mathsf{dom}(T_0)$ by (29) of lemma 28. 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 (31) 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 34 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu$, $T_0, T \in \wp(\mathbb{V}_{\mathfrak{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$ 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.

$$\mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![\boldsymbol{\tau}']\!] \qquad (35)$$ □

Proof of Lemma 34 The proof of (35) 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 $\langle\boldsymbol{\tau},\ T,\ \vartheta'\rangle = \mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$. We proceed by case analysis of the returned values $\langle\boldsymbol{\tau},\ T,\ \vartheta'\rangle$.

- In case (17.5a), we have $\mathsf{dom}(\vartheta') = \mathsf{dom}(f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0]) = \mathsf{dom}(\vartheta_0) \cup \{\gamma\} = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![\boldsymbol{\tau}']\!]$ because $\vartheta' = \gamma$ by the test (17.a);
- In case (17.5b), we have $\mathsf{dom}(\vartheta_i) = \mathsf{dom}(\vartheta_{i-1}) \cup \mathsf{vars}[\![\boldsymbol{\tau}^i]\!]$, $i = 1, \ldots, n$, by induction hypothesis on the sequence of calls to lub'. It follows that $\mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta_n) = \mathsf{dom}(\vartheta_0) \cup \bigcup_{i=1}^n \mathsf{vars}[\![\boldsymbol{\tau}^i]\!] = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)]\!] = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![\boldsymbol{\tau}']\!]$;
- In case (17.7), we have $\vartheta' = \beta[\gamma \leftarrow \vartheta_0]$ so $\mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta_0) \cup \{\gamma\} = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![\boldsymbol{\tau}']\!]$ because $\boldsymbol{\tau}' = \gamma$ by lemma 22;
- Finally, in case (17.9), $\mathsf{dom}(\vartheta') = \mathsf{dom}(\beta[\gamma \leftarrow \vartheta_0]) = \mathsf{dom}(\vartheta_0) \cup \{\gamma\} = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![\boldsymbol{\tau}']\!]$ because $\boldsymbol{\tau}' = \gamma$ by lemma 22. □ □

Lemma 36 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}'^0, \boldsymbol{\tau}^{n-1}, \boldsymbol{\tau}^n, \boldsymbol{\tau}^{m-1}.\boldsymbol{\tau}^m \in \mathbf{T}^\nu$, $T_n, T_m \in \wp(\mathbb{V}_{\mathfrak{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, consider any computation trace for the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}'^0, \boldsymbol{\varepsilon}, \varnothing)$ 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 21, this also holds for calls to lub' independently of the other two parameters. □

Proof of Lemma 36 By (12) in lemma 11, lemma 21, (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 21, the reasoning is the same for lub'). The only possible executions are the following.

- If one execution follows the true branch of (48.68.1), so does the other because they have the same parameters. By recurrence and induction on the sequence of calls for (48.68.2), …, (48.68.4) 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 (48.68.7) then obviously $\boldsymbol{\tau}^k = \boldsymbol{\tau}^m = \beta$;
- Both calls cannot go through (48.68.9) because 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 (48.68.9) 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 (48.68.9) then the call $\langle\boldsymbol{\tau}^m, T_m\rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_{m-1})$ must go through (48.68.7) because $\mathsf{dom}(T_k) \subseteq \mathsf{dom}(T_{m-1})$ with $\beta \in \mathsf{dom}(T_{m-1})$ so that $\boldsymbol{\tau}^k = \boldsymbol{\tau}^m = \beta$. □ □

Lemma 37 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu$, $T_0, T \in \wp(\mathbb{V}_{\mathfrak{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$ 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.

$$\forall\alpha \in \mathsf{dom}(\vartheta_0)\ .\ \vartheta_0(\alpha) = \vartheta'(\alpha) \qquad (38)$$ □

Proof of Lemma 37 The proof of (35) 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 $\langle\boldsymbol{\tau},\ T,\ \vartheta'\rangle = \mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$. 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 $\gamma \in \mathsf{dom}(\vartheta_0)$. Because the main call starts with $\boldsymbol{\varepsilon}$ and by (35) 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 $\boldsymbol{\tau}'^k = \gamma$ because (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 (31) of lemma 30, $\vartheta_j^0(\boldsymbol{\tau}'^k) = \vartheta_j^0(\gamma) = \boldsymbol{\tau}_j^k$. 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 (31) of lemma 30, 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 36, 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 22, and lemma 24 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 $\gamma \in \mathsf{dom}(\vartheta_0)$ because otherwise, we would have $\forall\beta \in \mathsf{dom}(T_0)\ .\ T_0(\beta) \neq \langle\boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2\rangle$ because the test (17.6) is ff and $\boldsymbol{\tau}' = \gamma \in \mathbb{V}_{\mathfrak{t}}$ by lemma 22, which is in contradiction to (the contrapositive of) lemma 26. It follows that $\forall\alpha \in \mathsf{dom}(\vartheta_0)\ .\ \vartheta_0(\alpha) = \beta[\gamma \leftarrow \vartheta_0](\alpha) = \vartheta'(\alpha)$ because $\alpha \neq \gamma$. □ □

Lemma 39 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu$, $T_0, T \in \wp(\mathbb{V}_{\mathfrak{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$ 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.

$$\vartheta'(\boldsymbol{\tau}') = \boldsymbol{\tau} \tag{40}$$ □

Proof of Lemma 39 The proof of (40) 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 $\langle\boldsymbol{\tau}, T, \vartheta'\rangle = \mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$. 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 $\mathsf{dom}(\vartheta_1) = \mathsf{dom}(\vartheta_0) \cup \mathbb{vars}[\![\boldsymbol{\tau}_1']\!]$ by (35) of lemma 34, 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

$$\begin{aligned}\mathsf{dom}(\vartheta_i) = \mathsf{dom}(\vartheta_0) \cup \bigcup_{j=1}^{i} \mathbb{vars}[\![\boldsymbol{\tau}_j']\!] \wedge \\ \forall j \in [1, i]\ .\ \forall\alpha \in \mathsf{dom}(\vartheta_j)\ .\ \vartheta_i(\alpha) = \vartheta_j(\alpha) \wedge \\ \forall j \in [1, i]\ .\ \vartheta_i(\boldsymbol{\tau}_j') = \vartheta_j(\boldsymbol{\tau}_j') = \boldsymbol{\tau}^j\end{aligned} \tag{41}$$

  - At the next $i + 1^{\text{th}}$ call, we have
    1. By (35) of lemma 34 and recurrence hypothesis (41), $\mathsf{dom}(\vartheta_{i+1}) = \mathsf{dom}(\vartheta_i) \cup \mathbb{vars}[\![\boldsymbol{\tau}_{i+1}']\!] = \mathsf{dom}(\vartheta_0) \cup \bigcup_{j=1}^{i} \mathbb{vars}[\![\boldsymbol{\tau}_j']\!] \cup \mathbb{vars}[\![\boldsymbol{\tau}_{i+1}']\!] = \mathsf{dom}(\vartheta_0) \cup \bigcup_{j=1}^{i+1} \mathbb{vars}[\![\boldsymbol{\tau}_j']\!]$;

2. By (38) of lemma 37, we have $\forall \alpha \in \mathsf{dom}(\vartheta_i)$. $\vartheta_i(\alpha) = \vartheta_{i+1}(\alpha)$ so that by recurrence hypothesis (41), $\forall j \in [1, i+1]$. $\forall \alpha \in \mathsf{dom}(\vartheta_j)$. $\vartheta_{i+1}(\alpha) = \vartheta_i(\alpha) = \vartheta_j(\alpha)$
3. By (1)., $\forall j \in [1, i+1]$. $\mathbb{vars}[\![\boldsymbol{\tau}'_j]\!] \subseteq \mathsf{dom}(\vartheta_j) \subseteq \mathsf{dom}(\vartheta_{i+1})$ 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 $\forall j \in [1, i+1]$. $\vartheta_{i+1}(\boldsymbol{\tau}'_j) = \vartheta_j(\boldsymbol{\tau}'_j) = \boldsymbol{\tau}^j$. $\square$

By recurrence, (41) 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 24, 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 22, we have $\vartheta'(\boldsymbol{\tau}') = \beta[\gamma \leftarrow \vartheta_0](\gamma) = \beta = \boldsymbol{\tau}$. $\square$

Proof of Theorem 48.103 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 21, 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 $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \varnothing, \boldsymbol{\tau}', \boldsymbol{\varepsilon}, \varnothing)$ terminates (by lemma 16 and 21) 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 (40) of lemma 39). 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 lemma 21 that $\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)$ is the $\preceq_{\simeq^\nu}$-least upper bound of $[\boldsymbol{\tau}_1]_{\simeq^\nu}$ and $[\boldsymbol{\tau}_2]_{\simeq^\nu}$. $\square$

6 Bibliography

[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. Laboratoire IMAG, Université de Grenoble Alpes, Sept. 1977 (271, 284, 428, 736, 36).

[2] Patrick Cousot and Radhia Cousot. "Automatic Synthesis of Optimal Invariant Assertions: Mathematical Foundations." *SIGART Newsl.* 64 (1977), pp. 1–12 (269, 428, 580, 36).

[3] Michael Karr. "Affine Relationships Among Variables of a Program." *Acta Inf.* 6 (1976), pp. 133–151 (475, 478, 636, 641, 651, 12).

[4] Gary A. Kildall. "A Unified Approach to Global Program Optimization." In *POPL*. ACM Press, 1973, pp. 194–206 (34, 111, 263, 271, 337, 362, 431, 521, 636, 651, 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 (636, 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 (636, 651, 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 (636, 651, 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 (414, 537, 636, 651, 12).

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

Figure 18: The modified least upper bound algorithm