Mathematical Proofs in Complement of the Book

Principles of Abstract Interpretation

MIT Press, 2021

Patrick Cousot

New York University

April 21, 2021

Contents

1 Mathematical Proofs of Chapter 4

Proof of lemma 4.18 The lemma trivially holds if $\mathsf{escape}[\![\mathsf{S}]\!] = \mathsf{ff}$. Otherwise $\mathsf{escape}[\![\mathsf{S}]\!] = \mathsf{tt}$ and the proof is by induction on the distance $\delta(\mathsf{S})$ of S to the root of the abstract syntax tree of P (where $\delta(\mathsf{P}) = 0$).

- 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, $\mathtt{Sl} \neq \{\ \ldots\{\ \epsilon\ \}\ldots\ \}$, $\mathsf{after}[\![\mathtt{Sl}']\!] = \mathsf{at}[\![\mathtt{S}]\!]$, $\mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \triangleq \mathsf{break\text{-}to}[\![\mathtt{Sl}]\!]$, $\mathsf{at}[\![\mathtt{S}]\!] \in \mathsf{in}[\![\mathtt{S}]\!]$ 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 $\mathtt{S} \neq \{\ \ldots\{\ \epsilon\ \}\ldots\ \}$, $\mathsf{after}[\![\mathtt{S}]\!] = \mathsf{after}[\![\mathtt{Sl}]\!]$, $\mathsf{break\text{-}to}[\![\mathtt{S}]\!] \triangleq \mathsf{break\text{-}to}[\![\mathtt{Sl}]\!]$, $\mathsf{break\text{-}to}[\![\mathtt{Sl}]\!] \neq \mathsf{after}[\![\mathtt{Sl}]\!]$ by induction hypothesis, so $\mathsf{break\text{-}to}[\![\mathtt{S}]\!] \neq \mathsf{after}[\![\mathtt{S}]\!]$.

- If $\mathtt{S} ::= \mathbf{if}\ \ell\ (\mathtt{B})\ \mathtt{S}_t$ 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 $\mathtt{S} ::= \mathbf{if}\ \ell\ (\mathtt{B})\ \mathtt{S}_t\ \mathbf{else}\ \mathtt{S}_f$ and $\mathtt{S} ::= \{\ \mathtt{Sl}\ \}$. $\square$

---

2 Mathematical Proofs of Chapter 41

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

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

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

$= \widehat{\boldsymbol{S}}^{\exists l}[\![\mathtt{S}]\!]\ L_b, (\widehat{\boldsymbol{S}}^{\exists l}[\![\ \epsilon\ ]\!]\ L_b, L_e)$ $\quad$ ⦃because $\widehat{\boldsymbol{S}}^{\exists l}[\![\ \epsilon\ ]\!]\ L_b, L_e \triangleq L_e$ by (41.22)⦄

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

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

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

$$\alpha^{\exists l}_{\mathbb{use},\mathbb{mod}}[\![\mathtt{Sl}]\!]\ L_b, L_e$$

$$= \bigcup\{\alpha^{l}_{\mathbb{use},\mathbb{mod}}[\![\mathtt{Sl}]\!]\ L_b, L_e\ \langle\pi_0,\ \pi_1\rangle \mid \langle\pi_0,\ \pi_1\rangle\ \in\ \boldsymbol{S}^*[\![\mathtt{Sl}]\!]\}$$

⦃definition (41.3) of $\alpha^{\exists l}_{\mathbb{use},\mathbb{mod}}[\![\mathtt{S}]\!]$⦄

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

⦃By lemma 41.8, omitting the useless parameters of $\mathbb{use}$ and $\mathbb{mod}$⦄

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

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

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

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

$\subseteq \bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [1,m-1] \;.\; \forall j \in [1,i-1] \;.\; \mathtt{x} \notin \mathbb{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathbb{use}[\![\mathtt{a}_i]\!]\} \cup (\!\lvert\, \mathsf{escape}[\![\mathtt{Sl}']\!] \wedge \ell_m = \mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \;?\; L_b \;\colon \varnothing \,\rvert\!) \mid \langle\pi_0,\ \pi_1\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{Sl}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \ldots \xrightarrow{\mathtt{a}_{m-1}} \ell_m\} \cup$

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

> ⟨— For the first term, $\langle\pi_0,\ \pi_1\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{Sl}']\!]$, π_1 ends in ℓ_n, and $\ell_n = \mathsf{after}[\![\mathtt{S}]\!]$ is impossible because $\mathtt{Sl}'$ and $\mathtt{S}$ are not empty. Moreover, if $\ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] = \mathsf{break\text{-}to}[\![\mathtt{Sl}']\!]$ then $\mathtt{a}_{n-1}$ is a break, so $\mathsf{escape}[\![\mathtt{Sl}']\!]$ holds. L_b is included in $(\!\lvert\, \mathsf{escape}[\![\mathtt{Sl}']\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \;?\; L_b \;\colon \varnothing \,\rvert\!)$ and so $(\!\lvert\, \mathsf{escape}[\![\mathtt{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] \;?\; L_b \;\colon \varnothing \,\rvert\!)$ is redundant. Finally, renaming $n \leftarrow m$.⟩
>
> ⟨— For the second term, if $\ell_n = \mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] = \mathsf{break\text{-}to}[\![\mathtt{S}]\!]$ then $\mathtt{a}_{n-1}$ is a break, so $\mathsf{escape}[\![\mathtt{S}]\!]$ holds. L_b is included in $(\!\lvert\, \mathsf{escape}[\![\mathtt{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] \;?\; L_b \;\colon \varnothing \,\rvert\!)$ and so $(\!\lvert\, \mathsf{escape}[\![\mathtt{Sl}']\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \;?\; L_b \;\colon \varnothing \,\rvert\!)$ is redundant. Moreover, $\pi_2 \frown \pi_3 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \ldots \xrightarrow{\mathtt{a}_{n-1}} \ell_n$ is decomposed into $\pi_2 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \ldots \xrightarrow{\mathtt{a}_{m-1}} \ell_m$ and $\pi_3 = \ell_m \xrightarrow{\mathtt{a}_m} \ell_{m+1} \xrightarrow{\mathtt{a}_{m+1}} \ldots \xrightarrow{\mathtt{a}_{n-1}} \ell_n$ where, by $\langle\pi_0,\ \pi_2\rangle \in \boldsymbol{\mathcal{S}}^+[\![\mathtt{Sl}']\!]$ and $\langle\pi_0 \frown \pi_2,\ \pi_3\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}]\!]$, $\ell_m = \mathsf{after}[\![\mathtt{Sl}']\!] = \mathsf{at}[\![\mathtt{S}]\!]$. Moreover, $\pi_0 \frown \pi_2$ is generalized to π'_0 (whence inclusion) and π_2 is renamed into π_1. ⟩

$= \bigcup\{\{\mathtt{x} \in \mathbb{V} \mid \exists i \in [1,m-1] \;.\; \forall j \in [1,i-1] \;.\; \mathtt{x} \notin \mathbb{mod}[\![\mathtt{a}_j]\!] \wedge \mathtt{x} \in \mathbb{use}[\![\mathtt{a}_i]\!]\} \cup (\!\lvert\, \mathsf{escape}[\![\mathtt{Sl}']\!] \wedge \ell_m = \mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \;?\; L_b \;\colon \varnothing \,\rvert\!) \mid \langle\pi_0,\ \pi_1\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{Sl}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathtt{a}_1} \ell_2 \xrightarrow{\mathtt{a}_2} \ldots \xrightarrow{\mathtt{a}_{m-1}} \ell_m\} \cup$

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

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

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

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

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

$= \bigcup\{\{\mathsf{x} \in \mathbb{V} \mid \exists i \in [1, m-1] \,.\, \forall j \in [1, i-1] \,.\, \mathsf{x} \notin \mathbb{mod}[\![\mathsf{a}_j]\!] \wedge \mathsf{x} \in \mathbb{use}[\![\mathsf{a}_i]\!]\} \cup (\![\, \ell_m = \mathsf{after}[\![\mathtt{Sl}']\!] \mathrel{?} (\bigcup\{\alpha^{l}_{\mathbb{use},\mathbb{mod}}[\![\mathtt{S}]\!]\, L_b, L_e\, \langle \pi'_0, \pi_3 \rangle \mid \langle \pi'_0, \pi_3 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{S}]\!]\}) \mathrel{⁏} \varnothing \,]\!) \cup (\![\, \mathsf{escape}[\![\mathtt{Sl}']\!] \wedge \ell_m = \mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \mathrel{?} L_b \mathrel{⁏} \varnothing \,]\!) \mid \langle \pi_0, \pi_1 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{Sl}']\!] \wedge \pi_1 = \ell_1 \xrightarrow{\mathsf{a}_1} \ell_2 \xrightarrow{\mathsf{a}_2} \ldots \xrightarrow{\mathsf{a}_{m-1}} \ell_m\}$ $\wr$lemma 41.8$\wr$

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

$\wr$lemma 41.8 and (41.3)$\wr$

$= \alpha^{\exists l}_{\mathbb{use},\mathbb{mod}}[\![\mathtt{Sl}']\!](\boldsymbol{\mathcal{S}}^*[\![\mathtt{Sl}']\!])\, L_b, (\widehat{\boldsymbol{\mathcal{S}}}^{\exists l}[\![\mathtt{S}]\!]\, L_b, L_e)$ $\wr$definition (41.3) of $\alpha^{\exists l}_{\mathbb{use},\mathbb{mod}}$$\wr$

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

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

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

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

$= \bigcup\{\alpha^{l}_{\mathbb{use},\mathbb{mod}}[\![\mathtt{Sl}]\!]\, L_b, L_e\, \langle \pi_0, \pi_1 \rangle \mid \langle \pi_0, \pi_1 \rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathtt{Sl}]\!]\}$ $\wr$(41.3)$\wr$

$= \bigcup\{\alpha^{l}_{\mathbb{use},\mathbb{mod}}[\![\mathtt{Sl}]\!]\, L_b, L_e\, \langle \pi_0, \pi_1 \rangle \mid \langle \pi_0, \pi_1 \rangle \in \{\langle \pi_0 \ell, \ell \rangle\}\}$ $\wr$definition of $\boldsymbol{\mathcal{S}}^*[\![\mathtt{Sl}]\!]$$\wr$

$= \alpha^{\exists l}_{\mathbb{use},\mathbb{mod}}[\![\mathtt{Sl}]\!]\, L_b, L_e\, \langle \pi_0 \ell, \ell \rangle$ $\wr$definitions of $\in$ and $\cup$$\wr$

$= \{\mathsf{x} \in \mathbb{V} \mid (\ell = \mathsf{after}[\![\mathtt{Sl}]\!] \wedge \mathsf{x} \in L_e) \vee (\mathsf{escape}[\![\mathtt{Sl}]\!] \wedge \ell = \mathsf{break\text{-}to}[\![\mathtt{Sl}]\!] \wedge \mathsf{x} \in L_b)\}$ $\wr$(41.3)$\wr$

$= L_e$ $\wr \ell = \mathsf{at}[\![\mathtt{Sl}]\!] = \mathsf{after}[\![\mathtt{Sl}]\!]$ in appendix 4.2.1 and $\mathsf{escape}[\![\mathtt{Sl}]\!] = \mathrm{ff}$ in 4.2.4 when $\mathtt{Sl} = \epsilon \wr$

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,

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

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

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

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

$$
\begin{aligned}
& \mathcal{M}^{+}[\![\mathtt{Sl}]\!]\ \langle \underline{\varrho},\ \mathtt{R} \rangle \\
=\ & \mathcal{M}^{+}\langle \underline{\varrho},\ \mathtt{R} \rangle(\widehat{\mathcal{S}}^{*}_{\mathbb{s}}[\![\mathtt{Sl}]\!]) && \wr (44.26) \wr \\
=\ & \{\langle \pi,\ \mathtt{R}' \rangle \mid \pi \in \widehat{\mathcal{S}}^{*}_{\mathbb{s}}[\![\mathtt{Sl}]\!] \wedge \langle \mathrm{tt},\ \mathtt{R}' \rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R} \rangle \pi\} && \wr (44.25) \wr \\
=\ & \{\langle \pi,\ \mathtt{R}' \rangle \mid \pi \in \{\langle \mathsf{at}[\![\mathtt{Sl}]\!],\ \rho \rangle \mid \rho \in \mathbb{Ev}\} \wedge \langle \mathrm{tt},\ \mathtt{R}' \rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R} \rangle \pi\} && \wr (42.10) \wr \\
=\ & \{\langle \langle \mathsf{at}[\![\mathtt{Sl}]\!],\ \rho \rangle,\ \mathtt{R}' \rangle \mid \rho \in \mathbb{Ev} \wedge \langle \mathrm{tt},\ \mathtt{R}' \rangle = \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R} \rangle(\langle \mathsf{at}[\![\mathtt{Sl}]\!],\ \rho \rangle)\} && \wr \text{definition of} \in \wr \\
=\ & \{\langle \langle \mathsf{at}[\![\mathtt{Sl}]\!],\ \rho \rangle,\ \mathtt{R}' \rangle \mid \rho \in \mathbb{Ev} \wedge \langle \mathtt{L} : \mathtt{B},\ \mathtt{R}' \rangle = \mathsf{fstnxt}(\mathtt{R}) \wedge \langle \underline{\varrho},\ \langle \mathsf{at}[\![\mathtt{Sl}]\!],\ \rho \rangle \rangle \in \mathcal{S}^{\mathfrak{r}}[\![\mathtt{L} : \mathtt{B}]\!]\} \\
& \wr (44.24) \text{ with } \mathcal{M}^{t}\langle \underline{\varrho},\ \mathtt{R}' \rangle \ni\ = \langle \mathrm{tt},\ \mathtt{R}' \rangle \wr \\
=\ & \widehat{\mathcal{M}}^{+}[\![\mathtt{Sl}]\!]\langle \underline{\varrho},\ \mathtt{R} \rangle && \wr (44.43) \wr
\end{aligned}
$$

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

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

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

$= \{\langle\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle,\ \mathsf{R}'\rangle \mid \rho \in \mathbb{E}\mathbb{v} \wedge \langle \mathsf{tt},\ \mathsf{R}'\rangle = \mathscr{M}^t\langle\underline{\varrho},\ \mathsf{R}\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle)\}$ ⁅definition of ∈⁆

$= \{\langle\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle,\ \mathsf{R}'\rangle \mid \rho \in \mathbb{E}\mathbb{v} \wedge \langle \mathsf{L} : \mathsf{B},\ \mathsf{R}'\rangle = \mathsf{fstnxt}(\mathsf{R}) \wedge \langle\underline{\varrho},\ \langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L} : \mathsf{B}]\!]\}$
⁅(44.24) with $\mathscr{M}^t\langle\underline{\varrho},\ \mathsf{R}'\rangle\ni = \langle \mathsf{tt},\ \mathsf{R}'\rangle$⁆

$= \widehat{\mathscr{M}}^{+}[\![\mathsf{S}]\!]\langle\underline{\varrho},\ \mathsf{R}\rangle$ ⁅(44.44)⁆

- In case (44.50) of an iteration statement $\mathsf{S} ::= \texttt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b$, we apply corollary 18.34 so we have to calculate the abstract transformer that satisfies the commutation property for an iterate X of the concrete transformer $\mathscr{F}^{*}_{\mathbb{S}}[\![\mathsf{S}]\!]$ (which traces must be of the form $\pi\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle$).

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

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

$= \mathscr{M}^{+}\langle\underline{\varrho},\ \mathsf{R}\rangle(\{\langle\ell,\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\}) \cup \mathscr{M}^{+}\langle\underline{\varrho},\ \mathsf{R}\rangle(\{\pi_2\langle\ell',\ \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho\rangle \mid \pi_2\langle\ell',\ \rho\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\,\rho = \mathsf{ff} \wedge \ell' = \ell\}) \cup \mathscr{M}^{+}\langle\underline{\varrho},\ \mathsf{R}\rangle(\{\pi_2\langle\ell',\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle \cdot \pi_3 \mid \pi_2\langle\ell',\ \rho\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\,\rho = \mathsf{tt} \wedge \langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle \cdot \pi_3 \in \widehat{\mathcal{S}}^{*}_{\mathbb{s}}[\![\mathsf{S}_b]\!] \wedge \ell' = \ell\})$
⁅Galois connection (44.30), so that, by lemma 11.38, $\mathscr{M}^{+}\langle\underline{\varrho},\ \mathsf{R}\rangle$ preserves joins⁆

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

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

$\mathscr{M}^{+}\langle\underline{\varrho},\ \mathsf{R}\rangle(\{\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\}$

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

— The second case is that of the loop exit

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

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

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

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

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

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

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

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

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

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

$\wr$because $(\langle \mathsf{tt},\ \mathsf{R}'\rangle = \mathcal{M}^t\langle \underline{\varrho},\ \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho\rangle)) \Leftrightarrow (\langle \mathsf{L}' : \mathsf{B}',\ \mathsf{R}'\rangle = \mathsf{fstnxt}(\mathsf{R}'') \wedge \mathsf{R}' \in \mathbb{R}_\varepsilon \wedge \langle \underline{\varrho},\ \langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L}' : \mathsf{B}']\!]) \vee (\langle \mathsf{L}' : \mathsf{B}',\ \mathsf{R}'''\rangle = \mathsf{fstnxt}(\mathsf{R}'') \wedge \langle \underline{\varrho},\ \langle \mathsf{at}[\![\mathsf{S}]\!],\ \overline{\rho}\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L}' : \mathsf{B}']\!] \wedge \mathsf{R}''' \notin \mathbb{R}_\varepsilon \wedge \langle \mathsf{L}'' : \mathsf{B}'',\ \mathsf{R}'\rangle = \mathsf{fstnxt}(\mathsf{R}''') \wedge \langle \underline{\varrho},\ \langle \mathsf{after}[\![\mathsf{S}]\!],\ \rho\rangle\rangle \in \mathcal{S}^{\mathsf{r}}[\![\mathsf{L}'' : \mathsf{B}'']\!])$ as shown previously while proving the second term in case (44.47) of a conditional statement $\mathsf{S} ::= \mathbf{if}\ ^{\ell}\ (\mathsf{B})\ \mathsf{S}_t$ $\wr$

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

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

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

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

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

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

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

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

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

≀(44.25)≀

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

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

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

$= \{\langle\pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle\pi_3,\ \mathsf{R}'\rangle \mid \langle\pi_2\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle,\ \mathsf{R}''\rangle \in \mathcal{M}^+\langle\underline{\varrho},\ \mathsf{R}\rangle X \wedge \mathcal{B}[\![\mathsf{B}]\!]\,\rho = \mathrm{tt} \wedge \mathcal{M}^t\langle\underline{\varrho},\ \mathsf{R}''\rangle(\langle \mathsf{at}[\![\mathsf{S}]\!],\ \rho\rangle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle) = \langle \mathrm{tt},\ \mathsf{R}'''\rangle \wedge \langle\langle \mathsf{at}[\![\mathsf{S}_b]\!],\ \rho\rangle\pi_3,\ \mathsf{R}'\rangle \in \mathcal{M}^+[\![\mathsf{S}_b]\!]\langle\underline{\varrho},\ \mathsf{R}'''\rangle\}$ ≀(44.26) and (44.25), $\wedge$ commutative≀

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

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

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

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

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

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

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

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

$\langle \mathsf{at}\llbracket \mathsf{S}_b \rrbracket,\ \rho\rangle\pi_3 \in \widehat{\boldsymbol{\mathcal{S}}}^*_{\mathbb{s}}\llbracket \mathsf{S}_b\rrbracket$. We get

$= \big\{\langle \pi_2\langle \mathsf{at}\llbracket \mathsf{S}\rrbracket,\ \rho\rangle\langle \mathsf{at}\llbracket \mathsf{S}_b\rrbracket,\ \rho\rangle\pi_3,\ \varepsilon\rangle \mid \langle \pi_2\langle \mathsf{at}\llbracket \mathsf{S}\rrbracket,\ \rho\rangle,\ \mathsf{R}''\rangle \in \boldsymbol{\mathcal{M}}^{\dagger}\langle \underline{\varrho},\ \mathsf{R}\rangle X \wedge \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\,\rho = \mathsf{tt} \wedge \mathsf{R}'' \notin \mathbb{R}_{\varepsilon} \wedge \langle \mathsf{L} : \mathsf{B}, \varepsilon\rangle = \mathsf{fstnxt}(\mathsf{R}'') \wedge \langle \underline{\varrho},\ \langle \mathsf{at}\llbracket \mathsf{S}\rrbracket, \rho\rangle\rangle \in \boldsymbol{\mathcal{S}}^{\mathsf{r}}\llbracket \mathsf{L} : \mathsf{B}\rrbracket \wedge \langle \mathsf{at}\llbracket \mathsf{S}_b\rrbracket,\ \rho\rangle\pi_3 \in \widehat{\boldsymbol{\mathcal{S}}}^*_{\mathbb{s}}\llbracket \mathsf{S}_b\rrbracket\big\}$ $\wr$(44.24)$\int$

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

$= \big\{\langle \pi_2\langle \mathsf{at}\llbracket \mathsf{S}\rrbracket, \rho\rangle\langle \mathsf{at}\llbracket \mathsf{S}_b\rrbracket, \rho\rangle\pi_3, \mathsf{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}\llbracket \mathsf{S}\rrbracket, \rho\rangle, \mathsf{R}''\rangle \in \boldsymbol{\mathcal{M}}^{\dagger}\langle \underline{\varrho}, \mathsf{R}\rangle X \wedge \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\rho = \mathsf{tt} \wedge \mathsf{R}'' \notin \mathbb{R}_{\varepsilon} \wedge \langle \mathsf{L} : \mathsf{B}, \mathsf{R}''''\rangle = \mathsf{fstnxt}(\mathsf{R}'') \wedge \langle \underline{\varrho}, \langle \mathsf{at}\llbracket \mathsf{S}\rrbracket, \rho\rangle\rangle \in \boldsymbol{\mathcal{S}}^{\mathsf{r}}\llbracket \mathsf{L} : \mathsf{B}\rrbracket \wedge \mathsf{R}'''' \notin \mathbb{R}_{\varepsilon} \wedge \boldsymbol{\mathcal{M}}^{t}\langle \underline{\varrho}, \mathsf{R}''''\rangle\langle \mathsf{at}\llbracket \mathsf{S}_b\rrbracket,\ \rho\rangle = \langle \mathsf{tt},\ \mathsf{R}'''\rangle \wedge \langle\langle \mathsf{at}\llbracket \mathsf{S}_b\rrbracket,\ \rho\rangle\pi_3,\ \mathsf{R}'\rangle \in \boldsymbol{\mathcal{M}}^{\dagger}\llbracket \mathsf{S}_b\rrbracket\langle \underline{\varrho},\ \mathsf{R}'''\rangle\big\}$

$= \big\{\langle \pi_2\langle \mathsf{at}\llbracket \mathsf{S}\rrbracket,\ \rho\rangle\langle \mathsf{at}\llbracket \mathsf{S}_b\rrbracket,\ \rho\rangle\pi_3,\ \mathsf{R}'\rangle \mid \langle \pi_2\langle \mathsf{at}\llbracket \mathsf{S}\rrbracket,\ \rho\rangle,\ \mathsf{R}''\rangle \in \boldsymbol{\mathcal{M}}^{\dagger}\langle \underline{\varrho},\ \mathsf{R}\rangle X \wedge \boldsymbol{\mathcal{B}}\llbracket \mathsf{B}\rrbracket\ \rho = \mathsf{tt} \wedge \mathsf{R}'' \notin \mathbb{R}_{\varepsilon} \wedge \langle \mathsf{L} : \mathsf{B},\ \mathsf{R}''''\rangle = \mathsf{fstnxt}(\mathsf{R}'') \wedge \langle \underline{\varrho},\ \langle \mathsf{at}\llbracket \mathsf{S}\rrbracket,\ \rho\rangle\rangle \in \boldsymbol{\mathcal{S}}^{\mathsf{r}}\llbracket \mathsf{L} : \mathsf{B}\rrbracket \wedge \mathsf{R}'''' \notin \mathbb{R}_{\varepsilon} \wedge \langle \mathsf{L}' : \mathsf{B}',\ \mathsf{R}'''\rangle = \mathsf{fstnxt}(\mathsf{R}'''') \wedge \langle \underline{\varrho},\ \langle \mathsf{at}\llbracket \mathsf{S}_b\rrbracket,\ \rho\rangle\rangle \in \boldsymbol{\mathcal{S}}^{\mathsf{r}}\llbracket \mathsf{L}' : \mathsf{B}'\rrbracket \wedge \langle\langle \mathsf{at}\llbracket \mathsf{S}_b\rrbracket,\ \rho\rangle\pi_3,\ \mathsf{R}'\rangle \in \boldsymbol{\mathcal{M}}^{\dagger}\llbracket \mathsf{S}_b\rrbracket\langle \underline{\varrho},\ \mathsf{R}'''\rangle\big\}$ $\wr$(44.24)$\int$

— Grouping all cases together we get the term (44.51) defining $\widehat{\boldsymbol{\mathcal{F}}}^{\dagger}\llbracket \mathsf{S}\rrbracket\langle \underline{\varrho}, \mathsf{R}\rangle(\boldsymbol{\mathcal{M}}^{\dagger}\langle \underline{\varrho}, \mathsf{R}\rangle X)$ and so corollary 18.34 and the commutation condition $\boldsymbol{\mathcal{M}}^{\dagger}\langle \underline{\varrho},\ \mathsf{R}\rangle(\boldsymbol{\mathcal{F}}^*_{\mathbb{S}}\llbracket \mathsf{S}\rrbracket(X)) = \widehat{\boldsymbol{\mathcal{F}}}^{\dagger}\llbracket \mathsf{S}\rrbracket\langle \underline{\varrho},\ \mathsf{R}\rangle\ (\boldsymbol{\mathcal{M}}^{\dagger}\langle \underline{\varrho},\ \mathsf{R}\rangle(X))$ for the iterates X of $\boldsymbol{\mathcal{F}}^*_{\mathbb{S}}\llbracket \mathsf{S}\rrbracket$ yield $\widehat{\boldsymbol{\mathcal{M}}}^{\dagger}\llbracket \mathsf{S}\rrbracket\langle \underline{\varrho},\ \mathsf{R}\rangle \triangleq \mathsf{lfp}^{\subseteq}\,(\widehat{\boldsymbol{\mathcal{F}}}^{\dagger}\llbracket \mathsf{S}\rrbracket\langle \underline{\varrho},\ \mathsf{R}\rangle)$ that is (44.50).

- In case (44.49) of a break statement $\mathsf{S} ::= \ell$ `break` ;

$\boldsymbol{\mathcal{M}}^{\dagger}\llbracket \mathsf{S}\rrbracket\ \langle \underline{\varrho},\ \mathsf{R}\rangle$

$= \big\{\langle \pi,\ \mathsf{R}'\rangle \mid \pi \in \widehat{\boldsymbol{\mathcal{S}}}^*_{\mathbb{s}}\llbracket \mathsf{S}\rrbracket \wedge \langle \mathsf{tt},\ \mathsf{R}'\rangle = \boldsymbol{\mathcal{M}}^{t}\langle \underline{\varrho},\ \mathsf{R}\rangle\pi\big\}$ $\wr$(44.26) and (44.25)$\int$

$= \big\{\langle \pi,\ \mathsf{R}'\rangle \mid \pi \in \{\langle \ell, \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \cup \{\langle \ell, \rho\rangle\langle \mathsf{break\text{-}to}\llbracket \mathsf{S}\rrbracket, \rho\rangle \mid \rho \in \mathbb{E}\mathbb{v}\} \wedge \langle \mathsf{tt}, \mathsf{R}'\rangle = \boldsymbol{\mathcal{M}}^{t}\langle \underline{\varrho}, \mathsf{R}\rangle\pi\big\}$ $\wr$(42.14)$\int$

$= \big\{\langle\langle \ell,\ \rho\rangle,\ \mathsf{R}''\rangle \mid \langle \mathsf{tt},\ \mathsf{R}''\rangle = \boldsymbol{\mathcal{M}}^{t}\langle \underline{\varrho},\ \mathsf{R}\rangle\langle \ell,\ \rho\rangle\big\} \cup \big\{\langle\langle \ell,\ \rho\rangle\langle \mathsf{break\text{-}to}\llbracket \mathsf{S}\rrbracket,\ \rho\rangle,\ \mathsf{R}''\rangle \mid \langle \mathsf{tt},\ \mathsf{R}''\rangle = \boldsymbol{\mathcal{M}}^{t}\langle \underline{\varrho},\ \mathsf{R}\rangle(\langle \ell,\ \rho\rangle\langle \mathsf{break\text{-}to}\llbracket \mathsf{S}\rrbracket,\ \rho\rangle)\big\}$ $\wr$definitions of $\cup$ and $\in$$\int$

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

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

---

4 Mathematical Proofs of Chapter 47

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

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

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

$$
\begin{array}{l}
\alpha^{\mathrm{d}}(\{\boldsymbol{\mathcal{S}}^{+\infty}[\![\mathsf{S}]\!]\})\,\mathsf{after}[\![\mathsf{S}]\!]\\
= \alpha^{\mathrm{d}}(\{\boldsymbol{\mathcal{S}}^{*}[\![\mathsf{S}]\!]\})\,\mathsf{after}[\![\mathsf{S}]\!] \hfill \text{(lemma 47.23)}\\
= \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \boldsymbol{\mathcal{S}}^{*}[\![\mathsf{S}]\!] \in \mathcal{D}(\mathsf{after}[\![\mathsf{S}]\!])\langle \mathsf{x}',\ \mathsf{y}\rangle\}\\
\hfill \text{(definition (47.25) of } \alpha^{\mathrm{d}}\text{)}\\
= \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \langle \pi_0,\ \pi_1\rangle, \langle \pi'_0,\ \pi'_1\rangle \in \boldsymbol{\mathcal{S}}^{*}[\![\mathsf{S}]\!]\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\}\ .\ \boldsymbol{\varrho}(\pi_0)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0)\mathsf{z}) \wedge\\
\quad \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))\} \quad \text{(definition (47.19) of}\\
\quad \mathcal{D}\ell\langle \mathsf{x}',\ \mathsf{y}\rangle\text{)}\\
= \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \langle \pi_0,\ \pi_1\rangle, \langle \pi'_0,\ \pi'_1\rangle \in \{\langle \pi\mathsf{at}[\![\mathsf{S}]\!],\ \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid\\
\quad \boldsymbol{\mathscr{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{ff}\} \cup \{\langle \pi\mathsf{at}[\![\mathsf{S}]\!],\ \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \boldsymbol{\mathscr{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi\mathsf{at}[\![\mathsf{S}]\!]) =\\
\quad \mathsf{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\boldsymbol{\mathcal{S}}}^{+\infty}[\![\mathsf{S}_t]\!](\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\}\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\}\ .\ \boldsymbol{\varrho}(\pi_0)\mathsf{z} =\\
\quad \boldsymbol{\varrho}(\pi'_0)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0, \pi_1), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0, \pi'_1))\}\\
\hfill \text{(definition of } \boldsymbol{\mathcal{S}}^{*}[\![\mathsf{S}]\!] \text{ in (6.9), (6.19), and (6.18) so that } \mathsf{after}[\![\mathsf{S}]\!] = \mathsf{after}[\![\mathsf{S}_t]\!]\text{)}\\
= \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \langle \pi_0,\ \pi_1\mathsf{after}[\![\mathsf{S}]\!]\rangle, \langle \pi'_0,\ \pi'_1\mathsf{after}[\![\mathsf{S}]\!]\rangle \in \{\langle \pi\mathsf{at}[\![\mathsf{S}]\!],\ \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid\\
\quad \boldsymbol{\mathscr{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{ff}\} \cup \{\langle \pi\mathsf{at}[\![\mathsf{S}]\!],\ \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \boldsymbol{\mathscr{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi\mathsf{at}[\![\mathsf{S}]\!]) =\\
\quad \mathsf{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\boldsymbol{\mathcal{S}}}^{+\infty}[\![\mathsf{S}_t]\!](\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\}\ .\ \boldsymbol{\varrho}(\pi_0)\mathsf{z} =\\
\quad \boldsymbol{\varrho}(\pi'_0)\mathsf{z}) \wedge \mathsf{diff}(\boldsymbol{\varrho}(\pi_0 \frown \pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y},\ \boldsymbol{\varrho}(\pi'_0 \frown \pi'_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\}\\
\hfill \text{(definition of } \in \text{ so that } \pi_1 \text{ and } \pi'_1 \text{ must end with } \mathsf{after}[\![\mathsf{S}]\!] \text{ and definition (47.16)}\\
\hfill \text{of } \mathsf{seqval}[\![\mathsf{y}]\!]\text{)}\\
= \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!], \pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!] \in \{\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \mid\\
\quad \boldsymbol{\mathscr{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{ff}\} \cup \{\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \mid \boldsymbol{\mathscr{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{tt} \wedge\\
\quad \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\boldsymbol{\mathcal{S}}}^{+\infty}[\![\mathsf{S}_t]\!](\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\}\ .\ \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z} =\\
\quad \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z}) \wedge \mathsf{diff}(\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y},\ \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\}\\
\hfill \text{(definitions of } \in \text{ and of trace concatenation } \frown\text{)}\\
= \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!], \pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!] \in \{\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \hfill (1)\\
\quad \mathsf{after}[\![\mathsf{S}]\!] \mid \boldsymbol{\mathscr{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{ff}\} \cup \{\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \mid\\
\quad \boldsymbol{\mathscr{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\boldsymbol{\mathcal{S}}}^{+\infty}[\![\mathsf{S}_t]\!](\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\} \wedge\\
\quad (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\}\ .\ \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z}) \wedge (\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq\\
\quad \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\}\\
\hfill \text{(definition (47.18) of diff)}
\end{array}
$$

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

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

$$
\begin{aligned}
&(1)\\
= \;& \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!], \pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \;.\; \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!]) = \\
&\mathsf{ff} \wedge \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{ff} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \;.\; \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z}) \wedge \\
&(\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\}\\
&\qquad\qquad \text{(case } \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{ff} \text{ and } \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{ff}\text{)}\\
= \;& \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \pi_0\mathsf{at}[\![\mathsf{S}]\!], \pi'_0\mathsf{at}[\![\mathsf{S}]\!] \;.\; \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{ff} \wedge \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{ff} \wedge (\forall \mathsf{z} \in \\
&\mathbb{V} \setminus \{\mathsf{x}'\} \;.\; \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z}) \wedge (\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{y} \neq \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]))\mathsf{y}\}\\
&\qquad\qquad \text{(definition (6.6) of } \boldsymbol{\varrho} \text{ so that } \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} = \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!]\mathsf{y})\text{)}\\
= \;& \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \rho, \nu \;.\; \mathscr{B}[\![\mathsf{B}]\!]\rho = \mathsf{ff} \wedge \mathscr{B}[\![\mathsf{B}]\!]\rho[\mathsf{x}' \leftarrow \nu] = \mathsf{ff} \wedge \rho(\mathsf{y}) \neq \rho[\mathsf{x}' \leftarrow \nu]\mathsf{y}\}
\end{aligned}
$$

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

$$
\begin{aligned}
= \;& \{\langle \mathsf{x}',\ \mathsf{x}'\rangle \mid \exists \rho, \nu \;.\; \rho(\mathsf{x}') \neq \nu \wedge \mathscr{B}[\![\mathsf{B}]\!]\rho = \mathsf{ff} \wedge \mathscr{B}[\![\mathsf{B}]\!]\rho[\mathsf{x}' \leftarrow \nu] = \mathsf{ff}\}\\
&\qquad\qquad \text{(because } \rho[\mathsf{x}' \leftarrow \nu](\mathsf{y}) = \rho(\mathsf{y}) \text{ when } \mathsf{y} \neq \mathsf{x}'\text{)}\\
= \;& \{\langle \mathsf{x}',\ \mathsf{x}'\rangle \mid \mathsf{x}' \in \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B})\} \qquad \text{(definition (47.48) of nondet)}\\
= \;& \mathbb{1}_{\mathbb{V}} \rceil \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B}) \qquad \text{(definition of left restriction } \rceil\text{)}\\
\subseteq \;& \mathbb{1}_{\mathbb{V}}
\end{aligned}
$$

Described in words for that first case, the initial value of x' flows to the value of x' by the false branch of the conditional `if` $(\mathsf{B})\ \mathsf{S}_t$ when there are at least two different values of x' for which B is false. (If there is only one, 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 $\pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!]$ and $\pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!]$ are through the true branch, we have,

$$
\begin{aligned}
&(1)\\
= \;& \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \exists \pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!], \pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!] \in \{\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \mid \\
&\mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi\mathsf{at}[\![\mathsf{S}]\!]) = \mathsf{tt} \wedge \mathsf{at}[\![\mathsf{S}_t]\!]\pi'\mathsf{after}[\![\mathsf{S}]\!] \in \widehat{\boldsymbol{\mathcal{S}}}^{+\infty}[\![\mathsf{S}_t]\!](\pi\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\} \wedge \\
&(\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \;.\; \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!])\mathsf{z}) \wedge (\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \\
&\boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\}
\end{aligned}
$$

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

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

$$\wr\text{definition of } \in\wr$$

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists \langle \pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!], \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}_t]\!]\pi_2\rangle, \langle \pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!], \mathsf{at}[\![\mathsf{S}_t]\!]\pi'_1\mathsf{after}[\![\mathsf{S}_t]\!]\pi'_2\rangle \in \boldsymbol{\mathcal{S}}^{+\infty}[\![\mathsf{S}_t]\!] \;.\; \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]) = \mathtt{tt} \wedge \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]) = \mathtt{tt} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \;.\; \boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!])\mathsf{z}) \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \pi_1 \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \pi'_1 \wedge (\boldsymbol{\varrho}(\pi_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \boldsymbol{\varrho}(\pi'_0\mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_t]\!]\pi'_1\mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\}$

$$\wr\mathsf{after}[\![\mathsf{S}]\!] = \mathsf{after}[\![\mathsf{S}_t]\!], \pi_2 = \pi'_2 = \ni, \text{definition (6.6) of } \boldsymbol{\varrho}\wr$$

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

$$\wr\text{definition (47.18) of diff and (47.16) of } \mathsf{seqval}[\![\mathsf{y}]\!]\wr$$

$\subseteq \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists \langle \bar{\pi}_0, \bar{\pi}_1\mathsf{after}[\![\mathsf{S}_t]\!]\pi_2\rangle, \langle \bar{\pi}_0', \bar{\pi}_1'\mathsf{after}[\![\mathsf{S}_t]\!]\pi'_2\rangle \in \boldsymbol{\mathcal{S}}^{+\infty}[\![\mathsf{S}_t]\!] \;.\; \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\bar{\pi}_0) = \mathtt{tt} \wedge \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\bar{\pi}_0') = \mathtt{tt} \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \;.\; \boldsymbol{\varrho}(\bar{\pi}_0)\mathsf{z} = \boldsymbol{\varrho}(\bar{\pi}_0')\mathsf{z}) \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \bar{\pi}_1 \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \bar{\pi}_1' \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}_t]\!])(\bar{\pi}_0 \frown \bar{\pi}_1\mathsf{after}[\![\mathsf{S}_t]\!], \mathsf{after}[\![\mathsf{S}_t]\!]\pi_2), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}_t]\!])(\bar{\pi}_0' \frown \bar{\pi}_1'\mathsf{after}[\![\mathsf{S}_t]\!], \mathsf{after}[\![\mathsf{S}_t]\!]\pi'_2))\}$

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

$\subseteq \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists \rho, \nu \;.\; \rho(\mathsf{x}') \neq \nu \wedge \mathscr{B}[\![\mathsf{B}]\!]\rho = \mathtt{tt} \wedge \mathscr{B}[\![\mathsf{B}]\!]\rho[\mathsf{x}' \leftarrow \nu] = \mathtt{tt}\} \cap \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists \langle \bar{\pi}_0, \bar{\pi}_1\mathsf{after}[\![\mathsf{S}_t]\!]\pi_2\rangle, \langle \bar{\pi}_0', \bar{\pi}_1'\mathsf{after}[\![\mathsf{S}_t]\!]\pi'_2\rangle \in \boldsymbol{\mathcal{S}}^{+\infty}[\![\mathsf{S}_t]\!] \;.\; (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \;.\; \boldsymbol{\varrho}(\bar{\pi}_0)\mathsf{z} = \boldsymbol{\varrho}(\bar{\pi}_0')\mathsf{z}) \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \bar{\pi}_1 \wedge \mathsf{after}[\![\mathsf{S}_t]\!] \notin \bar{\pi}_1' \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}_t]\!])(\bar{\pi}_0 \frown \bar{\pi}_1\mathsf{after}[\![\mathsf{S}_t]\!], \mathsf{after}[\![\mathsf{S}_t]\!]\pi_2), \mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}_t]\!])(\bar{\pi}_0' \frown \bar{\pi}_1'\mathsf{after}[\![\mathsf{S}_t]\!], \mathsf{after}[\![\mathsf{S}_t]\!]\pi'_2))\}$

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

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

$= \{\langle \mathsf{x}', \mathsf{y}\rangle \mid \exists \rho, \nu \,.\, \rho(\mathsf{x}') \neq \nu \wedge \mathcal{B}[\![\mathsf{B}]\!]\rho = \mathrm{tt} \wedge \mathcal{B}[\![\mathsf{B}]\!]\rho[\mathsf{x}' \leftarrow \nu] = \mathrm{tt}\} \cap \alpha^{\mathrm{d}}(\{\boldsymbol{\mathcal{S}}^{+\infty}[\![\mathsf{S}_t]\!]\})\,\mathsf{after}[\![\mathsf{S}_t]\!]$ $\wr$definition of$\subseteq$ and definition (47.25) of $\alpha^{\mathrm{d}}\wr$

Described in words for that second case, the initial value of x' flows to the value of y by the true branch of the conditional **if** $(\mathsf{B})\ \mathsf{S}_t$ when there are at least two different values of x' for which B is true and x' flows to the value of y in S_t.

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

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

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

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

(1)

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

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

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

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

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

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

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

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

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

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

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

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

Described in words for that third case, x' flows to x' if and only if changing x' changes the Boolean expression B, and when B is true, S_t changes x' to a value different from that when B is false. A counterexample is `if (x' != 1) x' = 1 ;`.

Moreover, x' flows to $\mathsf{y} \neq \mathsf{x}'$ if and only if changing x' changes the Boolean expression B and when B is true, S_t changes y.

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

(grouping cases together)

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

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

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

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

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

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

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

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

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

$\square$

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

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

$= \{\langle \mathsf{x}',\ \mathsf{y}\rangle \mid \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}]\!] \in \mathcal{D}\ell\langle \mathsf{x}',\ \mathsf{y}\rangle\}$ $\quad$ ⟅definition (47.25) of α^{d}⟆

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

⟅definition (47.19) of $\mathcal{D}\ell\langle \mathsf{x}',\ \mathsf{y}\rangle$⟆

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

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

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

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

⟅definition $\in$ and if ℓ has multiple occurrences in $\pi'_1\ell\pi'_2$, we choose the first one, same for $\pi'_1\ell\pi'_2$⟆

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

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

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

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

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

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

⦃definition (47.25) of α^{d}⦄

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

⦃structural induction hypothesis⦄

$= \boldsymbol{\mathcal{S}}^{\mathsf{d}}[\![\mathsf{S}_t]\!]\,\ell \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})$ ⦃definition (47.48) of nondet⦄

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** $(\mathsf{B})\ \mathsf{S}_t$ 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.

$\subseteq \boldsymbol{\mathcal{S}}^{\mathsf{d}}[\![\mathsf{S}_t]\!]\,\ell$

⦃A coarse overapproximation ignoring values, that is, that the conditional holds for only one value of x'⦄ □

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 (17.4). So the soundness of (47.63) follows from the following (3):

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

The proof of (3) is an application of exercise 18.19. $\langle \mathscr{C}, \sqsubseteq, \bot, \sqcup\rangle$ is the complete lattice $\langle \wp(\wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})), \subseteq, \emptyset, \cup\rangle$. $\langle \mathscr{A}, \preccurlyeq, 0, \curlyvee\rangle$ is the complete lattice $\langle \mathbb{P}^{\mathsf{d}}, \subseteq^{\mathsf{d}}, \bot^{\mathsf{d}}, \cup^{\mathsf{d}}\rangle$. The Galois connection $\langle \mathscr{C}, \sqsubseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle \mathscr{A}, \preccurlyeq\rangle$ is given by lemma 47.26. The transformer f is (17.4). 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 $\subseteq^{\mathsf{d}}$ and $\cup^{\mathsf{d}}$ defined pointwise). The main point of the proof is to check the semicommutation condition

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

By exercise 18.19, 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 $\mathscr{F}^*[\![\texttt{while}\ \ell\ (\texttt{B})\ \texttt{S}_b]\!]$ from $\varnothing$.

In practice, we have discovered $\mathscr{F}^{\text{diff}}[\![\texttt{while}\ \ell\ (\texttt{B})\ \texttt{S}_b]\!]$ knowing $\mathscr{F}^*[\![\texttt{while}\ \ell\ (\texttt{B})\ \texttt{S}_b]\!]$ and α^{d} by rewriting until getting a formula of the form $\mathscr{F}^{\text{diff}}[\![\texttt{while}\ \ell\ (\texttt{B})\ \texttt{S}_b]\!] \circ \alpha^{\mathrm{d}}$ and using $\dot\subseteq$-overapproximations to ignore values in the static analysis. By exercise 18.19, we conclude that

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

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.

$\alpha^{\mathrm{d}}(\{\mathscr{F}^*[\![\texttt{while}\ \ell\ (\texttt{B})\ \texttt{S}_b]\!]\ X\})\ \ell'$

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \mathscr{F}^*[\![\texttt{while}\ \ell\ (\texttt{B})\ \texttt{S}_b]\!]\ X \in \mathcal{D}(\ell')\langle \mathsf{x},\ \mathsf{y}\rangle\}$

(definition (47.25) of α^{d})

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

(definition (47.19) of $\mathcal{D}\ell\langle \mathsf{x},\ \mathsf{y}\rangle$)

$$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_1\rangle, \langle \pi'_0\ell,\ \ell\pi'_1\rangle \in \mathscr{F}^*[\![\texttt{while}\ \ell\ (\texttt{B})\ \texttt{S}_b]\!]\ X\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_1))\} \tag{5}$$

(because $\langle \pi_0\ell',\ \ell''\pi_1\rangle \notin \mathscr{F}^*[\![\texttt{while}\ \ell\ (\texttt{B})\ \texttt{S}_b]\!](X)$ when $\ell' \neq \ell$ or $\ell'' \neq \ell$)

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

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

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

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

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

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

— **(1)** If the dependency observation point ℓ' is at loop entry then

$$\ell' = \ell = \mathsf{at}[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!].$$

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 $\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell) = \boldsymbol{\varrho}(\pi_0\ell)\mathsf{y}$ by (47.16). Whether $\ell\pi'_1$ is determined by **(A)**, **(B)**, or **(C)** we have in all cases that $\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_1) = \boldsymbol{\varrho}(\pi'_0\ell) \frown \sigma$ where σ is a possibly empty sequence of values of y at $\ell' = \ell$. By definition (47.18) of diff, we don't care about σ because

$$\mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_1))$$

is true if and only if $\boldsymbol{\varrho}(\pi_0\ell)\mathsf{y} \neq \boldsymbol{\varrho}(\pi'_0\ell)$. In that case, we have

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

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

– In case **(Ba)**, we have

$$
\begin{aligned}
& \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_1)\\
=\ & \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'') \text{ where } \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \boldsymbol{\mathscr{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) =\\
& \mathtt{tt} \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!] \qquad \wr \textbf{(B)} \text{ with } \ell'' \in \mathsf{in}[\![\mathsf{S}_b]\!] \wr\\
=\ & \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_2\ell) \text{ where } \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \boldsymbol{\mathscr{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathtt{tt}\\
& \qquad \wr \text{definition (47.16) of } \mathsf{seqval}[\![\mathsf{y}]\!] \text{ because } \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \in\\
& \qquad \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!] \text{ with } \ell'' \in \mathsf{in}[\![\mathsf{S}_b]\!] \text{ so that } \ell \text{ cannot appear in the trace } \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \wr
\end{aligned}
$$

- In case **(Bc)**, we have

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

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

- In case **(C)**, we have

$$
\begin{aligned}
& \mathsf{seqval}[\![\mathsf{y}]\!]^{\ell\prime}(\pi_0{}^{\ell}, {}^{\ell}\pi_1) \\
= \; & \mathsf{seqval}[\![\mathsf{y}]\!]^{\ell\prime}(\pi_0{}^{\ell}, {}^{\ell}\pi_2{}^{\ell} \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]) \text{ where } \langle \pi_0{}^{\ell},\ {}^{\ell}\pi_2{}^{\ell}\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0{}^{\ell}\pi_2{}^{\ell}) = \mathsf{ff} \\
& \wr\textbf{(C)}\wr \\
= \; & \mathsf{seqval}[\![\mathsf{y}]\!]^{\ell\prime}(\pi_0{}^{\ell}, {}^{\ell}\pi_2{}^{\ell}) \text{ where } \langle \pi_0{}^{\ell},\ {}^{\ell}\pi_2{}^{\ell}\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0{}^{\ell}\pi_2{}^{\ell}) = \mathsf{ff} \\
& \hfill \wr\text{definition (47.16) of } \mathsf{seqval}[\![\mathsf{y}]\!]\wr
\end{aligned}
$$

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

$$
\begin{aligned}
& (5) \\
= \; & \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0{}^{\ell},\ {}^{\ell}\pi_1\rangle, \langle \pi'_0{}^{\ell},\ {}^{\ell}\pi'_1\rangle \in \mathscr{F}^*[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!]\, X\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ . \\
& \boldsymbol{\varrho}(\pi_0{}^{\ell})\mathsf{z} = \boldsymbol{\varrho}(\pi'_0{}^{\ell})\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]^{\ell\prime}(\pi_0{}^{\ell}, {}^{\ell}\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]^{\ell\prime}(\pi'_0{}^{\ell}, {}^{\ell}\pi'_1))\} \\
\subseteq \; & \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0{}^{\ell},\ {}^{\ell}\pi_2{}^{\ell}\rangle \in X\ .\ \exists\langle \pi'_0{}^{\ell},\ {}^{\ell}\pi'_1\rangle \in \mathscr{F}^*[\![\mathtt{while}\ \ell\ (\mathsf{B}) \\
& \mathsf{S}_b]\!]\ X\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \boldsymbol{\varrho}(\pi_0{}^{\ell})\mathsf{z} = \boldsymbol{\varrho}(\pi'_0{}^{\ell})\mathsf{z}) \wedge \\
& \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]^{\ell\prime}(\pi_0{}^{\ell}, {}^{\ell}\pi_2{}^{\ell}), \mathsf{seqval}[\![\mathsf{y}]\!]^{\ell\prime}(\pi'_0{}^{\ell}, {}^{\ell}\pi'_1))\} \qquad (6) \\
& \hfill \wr\text{abstracting away the value of the conditions}\wr
\end{aligned}
$$

The possible choices for $\langle \pi'_0{}^{\ell},\ {}^{\ell}\pi'_1\rangle \in \mathscr{F}^*[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!]\, X$ 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

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

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

(abstracting away the value of the conditions)

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

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

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

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid X \in \mathcal{D}\ell\langle \mathsf{x},\ \mathsf{y}\rangle\}$ (definition (47.19) of $\mathcal{D}\ell\langle \mathsf{x}',\ \mathsf{y}\rangle$)

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

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

(6)

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

(case **(1)** so $\ell' = \ell = \mathsf{at}[\![\texttt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!]$)

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X\ .\ \exists\langle \pi'_0\ell,\ \ell\pi'_1\rangle \in \{\langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \mid \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \boldsymbol{\mathscr{B}}[\![\mathsf{B}]\!]\varrho(\pi'_0\ell\pi'_2\ell) = \mathsf{tt} \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!] \wedge \ell'' = \mathsf{after}[\![\mathsf{S}_b]\!] = \mathsf{at}[\![\mathsf{S}]\!] = \ell\}\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_1))\}$ (case **(Bb)** for $\ell\pi'_1$)

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

(definition of $\in$ and $\ell'' = \ell$)

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

$\cup$

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

≀By definition (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]$ and (47.18) of diff, there is an instance of ℓ in $\ell\pi_2\ell$ and one in $\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell$ at which the values of y do differ, whereas they were the same previously. So there are two possible cases in which this ℓ is either in $\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]$ or in $\mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell$. So we have $\mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell)) = \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_2\ell)) \vee \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell))$≀

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

$\cup$

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

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

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

$\cup$

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

$\wr$because $\boldsymbol{\varrho}(\pi) = \boldsymbol{\varrho}(\pi \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket\mathsf{S}_b\rrbracket)$$\wr$

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

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

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

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

$\subseteq \alpha^{\mathsf{d}}(\{X\})\ell \cup (\alpha^{\mathsf{d}}(\{X\})\ell \mathbin{⨾} \alpha^{\mathsf{d}}(\{\{\langle \pi_0\ell,\ \ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket\mathsf{S}_b\rrbracket\pi\rangle \mid \langle \pi_0\ell \xrightarrow{\mathsf{B}} \mathsf{at}\llbracket\mathsf{S}_b\rrbracket,\ \mathsf{at}\llbracket\mathsf{S}_b\rrbracket\pi\rangle \in \{\langle\pi,$ $\pi'\rangle \in \boldsymbol{\mathcal{S}}^*\llbracket\mathsf{S}_b\rrbracket \mid \mathscr{B}\llbracket\mathsf{B}\rrbracket\boldsymbol{\varrho}(\pi)\}\}\})\ell)$

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

$= \alpha^{\mathsf{d}}(\{X\})\ell \cup (\alpha^{\mathsf{d}}(\{X\})\ell \mathbin{⨾} \alpha^{\mathsf{d}}(\{\{\langle\pi,\ \pi'\rangle \in \boldsymbol{\mathcal{S}}^*\llbracket\mathsf{S}_b\rrbracket \mid \mathscr{B}\llbracket\mathsf{B}\rrbracket\boldsymbol{\varrho}(\pi)\}\})\ell)$

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

$= \alpha^{\mathsf{d}}(\{X\})\ell \cup (\alpha^{\mathsf{d}}(\{X\})\ell \mathbin{⨾} (\alpha^{\mathsf{d}}(\{\boldsymbol{\mathcal{S}}^*\llbracket\mathsf{S}_b\rrbracket\})\ell \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})))$ $\wr$lemma 47.62$\wr$

$= \alpha^{\mathsf{d}}(\{X\})\ell \cup (\alpha^{\mathsf{d}}(\{X\})\ell \mathbin{⨾} (\alpha^{\mathsf{d}}(\{\boldsymbol{\mathcal{S}}^{+\infty}\llbracket\mathsf{S}_b\rrbracket\})\ell) \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B}))$ $\wr$lemma 47.23$\wr$

$\subseteq \alpha^{\mathsf{d}}(\{X\})\ell \cup (\alpha^{\mathsf{d}}(\{X\})\ell \mathbin{⨾} (\widehat{\overline{\boldsymbol{\mathcal{S}}}}{}^{\exists}_{\mathsf{diff}}\llbracket\mathsf{S}_b\rrbracket\ \ell \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})))$

$\wr$induction hypothesis (47.32), $⨾$ and $\rceil$ are $\subseteq$-increasing$\wr$

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

The possible choices for $\langle\pi'_0\ell,\ \ell\pi'_1\rangle \in \mathcal{F}^*[\![\texttt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!]\ X$ 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 $\{\langle\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \mid \langle\pi_0\ell, \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!]\}$. In that case, we have

$$
\begin{aligned}
&(5)\\
=\ & \{\langle\mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle\pi_0\ell,\ \ell\pi_1\rangle, \langle\pi'_0\ell,\ \ell\pi'_1\rangle \in \{\langle\pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \mid \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!]\}\ .\ (\forall\mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \boldsymbol{\varrho}(\pi_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell\prime(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]\ell\prime(\pi'_0\ell, \ell\pi'_1))\}\\
& \qquad \text{\textrm{case} \textbf{(1–Bb–Bb)}}\\
=\ & \{\langle\mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle\pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle\ .\ \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!] \wedge \exists\langle\pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle\ .\\
& \langle\pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \mathcal{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi'_0\ell\pi'_2\ell) = \mathsf{tt} \wedge \langle\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!] \wedge (\forall\mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell\prime(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell\prime(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell))\}\\
& \qquad \text{definition of } \in\\
\subseteq\ & \{\langle\mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle\pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle\ .\ \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \{\langle\pi,\ \pi'\rangle \in \boldsymbol{\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}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \{\langle\pi,\ \pi'\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi)\} \wedge (\forall\mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell\prime(\pi_0\ell, \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell\prime(\pi'_0\ell, \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell))\}\\
& \qquad \text{definition of } \in\\
=\ & \{\langle\mathsf{x},\ \mathsf{y}\rangle \mid \exists\langle\pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle\ .\ \langle\pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \langle\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \{\langle\pi,\ \pi'\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi)\} \wedge \exists\langle\pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle\ .\ \langle\pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \langle\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \{\langle\pi,\ \pi'\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!] \mid \mathcal{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi)\} \wedge (\forall\mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0\ell)\mathsf{z}) \wedge\\
& \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_2\ell))\}
\end{aligned}
$$

$\wr$by definition (47.18) of diff, and definition (47.16) of seqval$[\![\mathsf{y}]\!]$ because in case **(1)**, $\ell\prime = \ell$ does not appear in $\xrightarrow{\mathsf{B}}$ at$[\![\mathsf{S}_b]\!]\pi_3$ and the value of y is the same at ℓ after $\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}}$ at$[\![\mathsf{S}_b]\!]\pi_3\ell$ and at ℓ after $\pi_0\ell\pi_2\ell$. The same holds for $\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}}$ at$[\![\mathsf{S}_b]\!]\pi'_3\ell$. $\int$

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

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

— Summing up for case **(1)** we get (5) $\subseteq \mathbb{1}_{\mathbb{V}} \cup \alpha^{\mathrm{d}}(\{X\})\ell \cup (\alpha^{\mathrm{d}}(\{X\})\ell \,\mathbin{\raisebox{0.5ex}{;}}\, \widehat{\overline{\boldsymbol{\mathcal{S}}}}^{\exists}_{\mathrm{diff}}[\![\mathsf{S}_b]\!]\ \ell)\ \rceil$ nondet(B, B) which yields (47.63.a) of the form

$$\llparenthesis\ \ell\prime = \ell\ \text{?}\ \mathbb{1}_{\mathbb{V}} \cup X(\ell) \cup \big(X(\ell) \,;\, ((\widehat{\overline{\boldsymbol{\mathcal{S}}}}^{\exists}_{\mathrm{diff}}[\![\mathsf{S}_b]\!]\ \ell)\ \rceil\ \mathsf{nondet}(\mathsf{B},\mathsf{B}))\big) \,\text{:}\, \varnothing\ \rrparenthesis\ .$$

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 $\ell\prime$ on prefix traces is in the loop body S_b after zero or more loop iterations. So the two traces $\ell\pi_1$ and $\ell\pi'_1$ in (5) cannot be generated by (17.4.**A**). The case $\ell\prime = \ell =$ after$[\![\mathsf{S}_b]\!]$ = at$[\![\mathsf{S}]\!]$ has already been considered in case **(1)** (for subcases involving **(B)** and **(C)**). By definition (47.16) of seqval$[\![\mathsf{y}]\!]$ the case $\ell\prime$ = at$[\![\mathsf{S}_b]\!]$ is equivalent to $\ell\prime$ = at$[\![\mathsf{S}]\!]$ already considered in **(1)** because the evaluation of Boolean expressions has no side effect so the value of variables y at at$[\![\mathsf{S}_b]\!]$ and at$[\![\mathsf{S}]\!]$ are the same. Similarly, the value of variables y before a **`break`** ; statement at labels in breaks-of$[\![\mathsf{S}_b]\!]$ that can escape the loop body S_b is the same as the value at break-to$[\![\mathsf{S}_b]\!]$ = after$[\![\mathsf{S}]\!]$ and will be handled with case **(3)**.

It follows that in this case **(2)** we only have to consider the case

$$\ell\prime \in \mathsf{in}[\![\mathsf{S}_b]\!] \setminus (\{\mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{after}[\![\mathsf{S}_b]\!]\} \cup \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!])$$

and the two traces $\ell\pi_1$ and $\ell\pi'_1$ in (5) are generated by **(B)** or **(C)**. There are three cases to consider.

— **(2–B–B)** The dependency observation point $\ell\prime$ 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.

(5)

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

$\wr$case **2–B–B**$\int$

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

$\wr$definition $\in\wr$

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

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

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

$$\cup$$

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

$$\cup$$

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

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

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

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

$\wr$For the second term where $\ell\prime$ 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.$\int$

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

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

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

(5)

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

$\wr$case **2–B–C**$\int$

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

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

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

(5)

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

$\wr$case **2–C–C**$\int$

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

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

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

$$⦇\, \ell\prime \in \mathsf{in}[\![\mathsf{S}_b]\!] \;?\; \big(X(\ell) \mathbin{⨾} ((\widehat{\boldsymbol{\mathcal{S}}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\,\ell\prime)\,\rceil\,\mathsf{nondet}(\mathsf{B},\mathsf{B}))\big) \;:\; \varnothing \,⦈.$$

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

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

(5)

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

⟨$\ell\prime = \mathsf{after}[\![\mathsf{S}]\!]$⟩

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

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

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

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

(8)

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

$\wr$definition of $\in$ and $\ell\prime = \mathsf{after}[\![\mathsf{S}]\!]$$\wr$

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

$\wr$$X$ is an iterate of $\mathscr{F}^*[\![\texttt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!]$ so ${}^\ell\pi_2{}^\ell$ and ${}^\ell\pi'_2{}^\ell$ are iterates of the loop body. By definition of the labeling in section 4.2, $\mathsf{after}[\![\mathsf{S}]\!]$ 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 $\mathsf{seqval}[\![y]\!]\mathsf{after}[\![\mathsf{S}]\!]$ that $\mathsf{diff}(\mathsf{seqval}[\![y]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0{}^\ell, {}^\ell\pi_2{}^\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]), \mathsf{seqval}[\![y]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0{}^\ell, {}^\ell\pi'_2{}^\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])) = \mathsf{diff}(\mathsf{seqval}[\![y]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0{}^\ell\pi_2{}^\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!]), \mathsf{seqval}[\![y]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'_0{}^\ell\pi'_2{}^\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!], \mathsf{after}[\![\mathsf{S}]\!])) = \mathsf{diff}(\mathsf{seqval}[\![y]\!](\ell)(\pi_0{}^\ell\pi_2{}^\ell, \ell), \mathsf{seqval}[\![y]\!](\ell)(\pi'_0{}^\ell\pi'_2{}^\ell, \ell)) = \varrho(\pi_0{}^\ell\pi_2{}^\ell)y \neq \varrho(\pi'_0{}^\ell\pi'_2{}^\ell)y$ $\wr$

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 B is false, we have ${}^\ell\pi_2{}^\ell = \ell$ and ${}^\ell\pi'_2{}^\ell = \ell$.

(9)

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

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

$\wr$because if $x \notin \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B})$ then $x \in \mathsf{det}(\neg\mathsf{B}, \neg\mathsf{B})$ so $\mathscr{B}[\![\neg\mathsf{B}]\!]\varrho(\pi_0{}^\ell)$ and $\mathscr{B}[\![\neg\mathsf{B}]\!]\varrho(\pi'_0{}^\ell)$ would imply $\varrho(\pi_0{}^\ell)x = \varrho(\pi'_0{}^\ell)x$. Therefore $\varrho(\pi_0{}^\ell) = \varrho(\pi'_0{}^\ell)$ in contradiction to $\varrho(\pi_0{}^\ell)y \neq \varrho(\pi'_0{}^\ell)y$.$\wr$

– **(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 B is true, we have ${}^\ell\pi_2{}^\ell \neq \ell$ and ${}^\ell\pi'_2{}^\ell \neq \ell$

(9)

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

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

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

≀because $\varrho(\pi_0\ell\pi_2\ell)\mathsf{y} \neq \varrho(\pi'_0\ell\pi'_2\ell)\mathsf{y}$ implies $\mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_2\ell))$∫

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

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

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

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

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

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

≀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 $\ell\pi''_2\ell \in X$, $\mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi''_2\ell) = \mathrm{tt}$ and $\langle \pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!]$∫

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

≀definition (6.6) of $\boldsymbol{\varrho}$, 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≀

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

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

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

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

We have to calculate the second term

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

≀grouping cases together≀

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

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

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

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

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

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

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

(8)

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

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

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

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

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

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

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

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

$\wr ⨟$ and $\rceil$ 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 S_b. By symmetry of diff this also covers the inverse case.

(8)

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

$\wr$case **(3–B–C)**$\wr$

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

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

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

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

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

⦃definition of $\in$⦄

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

> ⦃by lemma 47.59 where $\boldsymbol{\mathcal{S}}' = \{\langle \pi\ell,\ \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi\ell) = \mathsf{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle \pi\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!]\} \cup \{\langle \pi\ell,\ \ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathscr{B}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi\ell) = \mathsf{ff}\}$ with $\pi_0\ell_0 \leftarrow \pi_0\ell$, $\ell_0\pi_1\ell' \leftarrow \ell\pi_2\ell$, $\ell \leftarrow \mathsf{after}[\![\mathsf{S}]\!]$, $\ell'\pi_2\ell \leftarrow \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell'' \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]$, $\ell\pi_3 \leftarrow \mathsf{after}[\![\mathsf{S}]\!]$ so $\pi_3 = \ni$, and $\pi'_0\ell_0 \leftarrow \pi'_0\ell$, $\ell_0\pi'_1\ell' \leftarrow \ell_0\pi'_2\ell$, $\ell'\pi'_2\ell \leftarrow \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]$, $\ell\pi'_3 \leftarrow \mathsf{after}[\![\mathsf{S}]\!]$ so $\pi'_3 = \ni$ ⦄

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

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

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

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

⟅definition (47.19) of $\mathcal{D}^{\ell}\langle \mathsf{x},\ \mathsf{y}\rangle$⟆

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

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

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

⟅$\langle \pi^{\ell} \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3{}^{\ell\prime\prime} \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!]$ so, by definition of program labeling in section 4.2, $\mathsf{after}[\![\mathsf{S}]\!] \neq \mathsf{at}[\![\mathsf{S}_b]\!]$ cannot appear in $\mathsf{at}[\![\mathsf{S}_b]\!]\pi_3{}^{\ell\prime\prime}$. Therefore, by definitions (6.6) of $\boldsymbol{\varrho}$ and (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]^{\ell}$, $\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi_0{}^{\ell}, {}^{\ell}\pi_2{}^{\ell} \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3{}^{\ell\prime\prime} \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]) = \boldsymbol{\varrho}(\pi^{\ell} \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3{}^{\ell\prime\prime})$ and $\mathsf{seqval}[\![\mathsf{y}]\!](\mathsf{after}[\![\mathsf{S}]\!])(\pi'^{\ell}, {}^{\ell}\pi'_2{}^{\ell} \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]) = \boldsymbol{\varrho}(\pi'^{\ell}\pi'_2{}^{\ell})$. We conclude by definition (47.18) of diff⟆

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

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

$$= \bigcup_{\ell'' \in \text{breaks-of}[\![\mathsf{S}_b]\!]} \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \pi^{\ell} \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3{}^{\ell''} \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!], \pi'^{\ell} \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\ .$$

$\langle \pi^{\ell} \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3{}^{\ell''} \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!] \wedge (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \boldsymbol{\varrho}(\pi^{\ell})\mathsf{z} = \boldsymbol{\varrho}(\pi'^{\ell})\mathsf{z}) \wedge \boldsymbol{\varrho}(\pi^{\ell} \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3{}^{\ell''} \xrightarrow{\mathsf{break}} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y} \neq \boldsymbol{\varrho}(\pi'^{\ell} \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!])\mathsf{y})\} \rceil \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$

(definition of $\cup$)

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

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

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

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

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

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

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

$$\begin{aligned}&(\!| \ell' = \mathsf{after}[\![\mathsf{S}]\!]\ ?\ (\mathbb{1}_{\mathsf{nondet}(\neg\mathsf{B},\neg\mathsf{B})} \cup X(\ell) \cup \\ &\quad (X(\ell) ⨾ (\mathbb{1}_{\mathsf{nondet}(\neg\mathsf{B},\neg\mathsf{B})} \cup \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B}) \times \mathsf{mod}[\![\mathsf{S}_b]\!])) \rceil \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B}) \cup \\ &\qquad X(\ell) ⨾ \Big(\Big(\bigcup_{\ell'' \in \text{breaks-of}[\![\mathsf{S}_b]\!]} \widehat{\overline{\boldsymbol{\mathcal{S}}}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ {}^{\ell''}\Big) \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})\Big) \cup \\ &\qquad\quad \mathbb{1}_{\mathsf{nondet}(\mathsf{B},\neg\mathsf{B})} \cup (\mathsf{nondet}(\mathsf{B}, \neg\mathsf{B}) \times \mathsf{mod}[\![\mathsf{S}_b]\!]))\ ⸨\ \varnothing\ |\!).\end{aligned} \tag{47.63.c$'$}$$

that can be simplified as follows (while losing precision)

(5)

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

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

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

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

$\wr$because $;$ distributes over $\cup$$\wr$

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

$\wr$idempotency law for $\cup$ and $;$ distributes over $\cup$$\wr$

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

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

For fixpoints X of $\boldsymbol{\mathscr{F}}^{\mathrm{diff}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathsf{S}_b]\!]$, 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

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

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

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

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 $\boldsymbol{\varrho}(\boldsymbol{\tau}_1) = \boldsymbol{\varrho}(f(\ldots \alpha \ldots)$ 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, \ldots, \boldsymbol{\tau}^n_1) \doteq g(\boldsymbol{\tau}^1_2, \ldots, \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, \ldots, \boldsymbol{\tau}^n_1) \doteq f(\boldsymbol{\tau}^1_2, \ldots, \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, \ldots, \boldsymbol{\tau}^n_1)) = \boldsymbol{\varrho}(f(\boldsymbol{\tau}^1_2, \ldots, \boldsymbol{\tau}^n_2))\} \cap \gamma^{\mathsf{r}}_{\mathsf{s}}(\vartheta_0) && \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 } \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 \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 } \bigcap \\
& \quad \text{commutative} \wr \\
= \;& \mathsf{let}\ \vartheta_1 = \mathsf{unify}((\boldsymbol{\tau}^1_i, \boldsymbol{\tau}^1_2, \vartheta_0)\ \mathsf{in} \\
& \quad \ldots \\
& \quad\quad \mathsf{let}\ \vartheta_j = \mathsf{unify}(\boldsymbol{\tau}^j_i, \boldsymbol{\tau}^j_2, \vartheta_{j-1})\ \mathsf{in} \\
& \quad\quad\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
\end{aligned}
$$

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

- In case (48.47.7), we have

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

- In case (48.47.11), we have

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

(where $\alpha \in \mathbb{V}_{\mathfrak{t}}$ by test (48.47.9), $\alpha \notin \mathrm{vars}[\![\boldsymbol{\tau}_2]\!]$ 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)

$$
= \{\boldsymbol{\varrho} \in \mathbf{P}^\nu \mid \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2)\} \cap \gamma_s^r(\vartheta_0) \qquad \text{(definition (48.51) of } \gamma_e\text{)}
$$

$= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2)\} \cap \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\vartheta_0(\beta))\}$ ≀definition (48.52) of $\gamma^{\mathrm{r}}_{\mathrm{s}}$≀

$= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \boldsymbol{\varrho}(\alpha) = \boldsymbol{\varrho}(\boldsymbol{\tau}_2) \wedge \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = \boldsymbol{\varrho}(\vartheta_0(\beta))\}$ ≀definition of $\cap$≀

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

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

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

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

$= \{\boldsymbol{\varrho} \in \mathbf{P}^{\nu} \mid \forall \beta \in \mathbb{V}_{\mathfrak{t}} \,.\, \boldsymbol{\varrho}(\beta) = (\!| \beta = \alpha \mathrel{?} \boldsymbol{\varrho}(\vartheta_0(\boldsymbol{\tau}_2)) \mathrel{\mathring{:}} \boldsymbol{\varrho}(\{\langle\alpha, \boldsymbol{\tau}_2\rangle\}(\vartheta_0(\beta))) |\!)\}$

≀by exercise 48.62≀

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

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

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

≀because $X \notin \mathsf{dom}(\vartheta_0)$ so $(\{\langle\alpha, \boldsymbol{\tau}_2\rangle\} \circ \vartheta_0)(\alpha) = \{\langle\alpha, \boldsymbol{\tau}_2\rangle\}(\vartheta_0(\alpha)) = \{\langle\alpha, \boldsymbol{\tau}_2\rangle\}(\alpha) = \boldsymbol{\tau}_2$≀

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

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

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

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

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

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

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

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

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

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

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

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

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

- 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

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

□

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 $\boldsymbol{\tau}_j^i \in \mathbf{T}^\nu$, $i = 1, \dots, n$, $j = 1, 2$, 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 $T_i \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu \wedge \forall \alpha \in \mathsf{dom}(T_0) \mathrel{.} T_0(\alpha) = T_i(\alpha)$. Then, by induction on the sequence of calls to lub, $\boldsymbol{\tau}^{i+1} \in \mathbf{T}^\nu$ and $T_{i+1} \in \mathbb{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^\nu \times \mathbf{T}^\nu \wedge \mathbb{vars}[\![\boldsymbol{\tau}^{i+1}]\!] \subseteq \mathsf{dom}(T_{i+1}) \wedge \forall \alpha \in \mathsf{dom}(T_i) \mathrel{.} T_i(\alpha) = T_{i+1}(\alpha)$. By transitivity, $\forall \alpha \in \mathsf{dom}(T_0) \mathrel{.} T_0(\alpha) = T_{i+1}(\alpha)$. □

  By recurrence for $i = n$, $T' = T_n$ at (48.68.5) satisfies (48.39) because $\boldsymbol{\tau}^i \in \mathbf{T}^\nu$, $i = 1, \dots, n$, implies $f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n) \in \mathbf{T}^\nu$ and $\mathbb{vars}[\![f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)]\!] = \bigcup_{i=1}^n \mathbb{vars}[\![\boldsymbol{\tau}^i]\!]$;
- 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 $\beta \in \mathbb{vars}[\![\langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0]]\!] = \mathbb{vars}[\![T']\!]$. □

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

$$\bar{\varsigma}_1(T')\boldsymbol{\tau} \;=\; \boldsymbol{\tau}_1 \quad \text{and} \quad \bar{\varsigma}_2(T')\boldsymbol{\tau} \;=\; \boldsymbol{\tau}_2 \qquad (15) \quad \square$$

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 $\forall \alpha \in \mathbb{vars}[\![\boldsymbol{\tau}^i]\!] \subseteq \mathsf{dom}(T_i) \;.\; T_i(\alpha) = T_{i+1}(\alpha)$. Therefore, by (13), $\forall \alpha \in \mathbb{vars}[\![\boldsymbol{\tau}^i]\!] \;.\; \vartheta_j(T_{i+1})(\boldsymbol{\tau}^i) = \vartheta_j(T_i)(\boldsymbol{\tau}^i)$. It follows by (48.30) that $\vartheta_j(T_n)(f(\boldsymbol{\tau}^1, \boldsymbol{\tau}^2, \ldots, \boldsymbol{\tau}^n)) = f(\vartheta_j(T_n)(\boldsymbol{\tau}^1), \vartheta_j(T_n)(\boldsymbol{\tau}^2), \ldots, \vartheta_j(T_n)(\boldsymbol{\tau}^n)) = f(\vartheta_j(T_1)(\boldsymbol{\tau}^1), \vartheta_j(T_2)(\boldsymbol{\tau}^2), \ldots, \vartheta_j(T_n)(\boldsymbol{\tau}^n)) = f(\boldsymbol{\tau}_j^1, \ldots, \boldsymbol{\tau}_j^n) = \boldsymbol{\tau}_j$, $j = 1, 2$;
- In case (48.68.7), (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), $\bar{\varsigma}_j(T')\boldsymbol{\tau} = \vartheta_j(\langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])\beta = \mathsf{if}\ \beta \in \mathsf{dom}(T)\ \mathsf{then\ let}\ \langle \boldsymbol{\tau}_1',\ \boldsymbol{\tau}_2' \rangle = \langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0](\beta)\ \mathsf{in}\ \boldsymbol{\tau}_j'\ \mathsf{else}\ \alpha = \boldsymbol{\tau}_j$, $j = 1, 2$. $\square$

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

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

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 $\bar{\varnothing}^\nu$ 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, $[\boldsymbol{\tau}_j]_{\simeq^\nu} \preceq_{\simeq^\nu} [\boldsymbol{\tau}]_{\simeq^\nu} = [\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)]_{\simeq^\nu}$. $\square$

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 $\boldsymbol{\tau}'$.

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

Figure 18: The modified least upper bound algorithm

Example 19 The assumption (17.13) prevents a call like $\text{lub}'(f(a,b), f(b,a), \varnothing, f(\alpha,\alpha), \boldsymbol{\varepsilon}, \varnothing)$ 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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Lemma 21 For all $\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}, \boldsymbol{\tau}', \boldsymbol{\tau}'' \in \mathbf{T}^{\nu}$, $T_0, T, T'' \in \wp(\mathcal{V}_{\mathfrak{t}} \times \mathbf{T}^{\nu} \times \mathbf{T}^{\nu})$, and $\vartheta_0, \vartheta' \in \mathcal{V}_{\mathfrak{t}} \nrightarrow \mathbf{T}^{\nu}$, 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). $\square$

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). $\square$

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. $\square$

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 $\boldsymbol{\tau}_1', {\boldsymbol{\tau}_1'}^1, \ldots, {\boldsymbol{\tau}_1'}^n, \boldsymbol{\tau}_2', {\boldsymbol{\tau}_2'}^1, \ldots, {\boldsymbol{\tau}_2'}^n \in \mathbf{T}^\nu$,

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

$\square$

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

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

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

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

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

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

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

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

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 $\vartheta' = f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0]$. So if $\alpha \in \mathsf{dom}(\vartheta') \setminus \{\gamma\}$ then the postinvariant follows from the preinvariant. For $\gamma \in \mathsf{dom}(\vartheta')$, we have $\vartheta'(\gamma) = f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n) \notin \mathbb{V}_{\mathbb{t}}$ 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 $\beta \in \mathsf{dom}(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0]) = \mathsf{dom}(T)$. □

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

Lemma 28 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu, T_0, T \in \wp(\mathbb{V}_{\mathbb{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1^0, \vartheta_2^0, \vartheta' \in \mathbb{V}_{\mathbb{t}} \nrightarrow \mathbf{T}^\nu$, 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

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

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

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 $\mathbb{vars}[\![\vartheta_0(\mathbb{V}_t)]\!] = \mathbb{vars}[\![\varnothing]\!] = \varnothing \subseteq \mathsf{dom}(T_0)$;

- Otherwise the preinvariant of (29) holds for T_0 and ϑ_0 at the first recursive call (17.2b). Assume, by induction hypothesis, that $\mathbb{vars}[\![\vartheta_{i-1}(\mathbb{V}_t)]\!] \subseteq \mathsf{dom}(T_{i-1})$ 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 $\mathbb{vars}[\![\vartheta_i(\mathbb{V}_t)]\!] \subseteq \mathsf{dom}(T_i)$ after that call, which is also the preinvariant of the next call, if any. By recurrence, $\mathbb{vars}[\![\vartheta'(\mathbb{V}_t)]\!] = \mathbb{vars}[\![\vartheta_n(\mathbb{V}_t)]\!] \subseteq \mathsf{dom}(T_n) = \mathsf{dom}(T)$ in case the call (17) to lub' terminates at (17.5b);

- If lub' terminates at (17.5a), there are two cases.

    - $\mathbb{vars}[\![\vartheta'(\{\gamma\})]\!] = \mathbb{vars}[\![f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\{\gamma\})]\!] = \mathbb{vars}[\![f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)]\!] = \bigcup_{i=1}^n \mathbb{vars}[\![\boldsymbol{\tau}^i]\!]$. By lemma 11 and 21, we have $\mathbb{vars}[\![\boldsymbol{\tau}^i]\!] \subseteq \mathsf{dom}(T_i)$, $i = 1, \dots, n$ and $\mathsf{dom}(T_i) \subseteq \mathsf{dom}(T_n)$ so that $\bigcup_{i=1}^n \mathbb{vars}[\![\boldsymbol{\tau}^i]\!] \subseteq \bigcup_{i-1}^n \mathsf{dom}(T_i) \subseteq \mathsf{dom}(T_n) = \mathsf{dom}(T)$;
    - $\mathbb{vars}[\![\vartheta'(\mathbb{V}_t \setminus \{\gamma\})]\!] = \mathbb{vars}[\![f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\mathbb{V}_t \setminus \{\gamma\})]\!] = \mathbb{vars}[\![\vartheta_0(\mathbb{V}_t \setminus \{\gamma\})]\!] \subseteq \mathbb{vars}[\![\vartheta_0(\mathbb{V}_t)]\!]$ which, by the preinvariant (29), is included in $\mathsf{dom}(T_0)$. By lemma 11 and 21, $\mathsf{dom}(T_{i=1}) \subseteq \mathsf{dom}(T_i)$, $i = 1, \dots, n$ so that, by transitivity, $\mathsf{dom}(T_0) \subseteq \mathsf{dom}(T_n) = \mathsf{dom}(T)$. Therefore $\mathbb{vars}[\![\vartheta'(\mathbb{V}_t \setminus \{\gamma\})]\!] \subseteq \mathsf{dom}(T)$;
    - Because $\vartheta'(\mathbb{V}_t) = \vartheta'(\{\gamma\}) \cup \vartheta'(\mathbb{V}_t \setminus \{\gamma\})$, we conclude that $\mathbb{vars}[\![\vartheta'(\mathbb{V}_t)]\!] = \mathbb{vars}[\![\vartheta'(\{\gamma\}) \cup \vartheta'(\mathbb{V}_t \setminus \{\gamma\})]\!] = \mathbb{vars}[\![\vartheta'(\{\gamma\})]\!] \cup \mathbb{vars}[\![\vartheta'(\mathbb{V}_t \setminus \{\gamma\})]\!] \subseteq \mathsf{dom}(\vartheta') \cup \mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta')$; □

- 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 $\mathbb{vars}[\![\vartheta'(\{\gamma\})]\!] = \mathbb{vars}[\![\beta[\gamma \leftarrow \vartheta_0](\{\gamma\})]\!] = \mathbb{vars}[\![\{\beta\}]\!] = \{\beta\} \subseteq \mathsf{dom}(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle [\beta \leftarrow T_0]) = \mathsf{dom}(T)$;
    - Moreover $\mathbb{vars}[\![\vartheta'(\mathbb{V}_t \setminus \{\gamma\})]\!] = \mathbb{vars}[\![\beta[\gamma \leftarrow \vartheta_0](\mathbb{V}_t \setminus \{\gamma\})]\!] = \mathbb{vars}[\![\vartheta_0(\mathbb{V}_t \setminus \{\gamma\})]\!] \subseteq \mathbb{vars}[\![\vartheta_0(\mathbb{V}_t)]\!] \subseteq \mathsf{dom}(T_0)$, 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 $\mathbb{vars}$ 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 $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}' \in \mathbf{T}^\nu, T_0, T \in \wp(\mathbb{V}_t \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1^0, \vartheta_2^0, \vartheta' \in \mathbb{V}_t \nrightarrow \mathbf{T}^\nu$, 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'. $\square$

Lemma 32 For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu, T_0, T \in \wp(\mathbb{V}_{\mathbb{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1^0, \vartheta_2^0, \vartheta' \in \mathbb{V}_{\mathbb{t}} \nrightarrow \mathbf{T}^\nu$, 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

$$\text{preinvariant} \quad \forall j = 1, 2 \;.\; \forall \alpha \in \mathsf{dom}(\vartheta_0) \;.\; \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_0)(\vartheta_0(\alpha)) \tag{33}$$

$$\text{postinvariant} \quad \forall j = 1, 2 \;.\; \forall \alpha \in \mathsf{dom}(\vartheta') \;.\; \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T)(\vartheta'(\alpha)) \wedge \bar{\varsigma}_j(T)(\boldsymbol{\tau}) = \boldsymbol{\tau}_j \qquad \square$$

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

  Assume that $\forall j = 1, 2 \;.\; \forall \alpha \in \mathsf{dom}(\vartheta_{i-1}) \;.\; \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_{i-1})(\vartheta_{i-1}(\alpha))$ before the i^{th} recursive call. By induction on the sequence of calls to lub', the postinvariant of (33) holds. Therefore we have $\forall j = 1, 2 \;.\; \forall \alpha \in \mathsf{dom}(\vartheta_i) \;.\; \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_i)(\vartheta_i(\alpha))$ before the $i + 1^{\text{th}}$ call. By recurrence, all recursive calls do satisfy (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 $\forall j = 1, 2 \;.\; \forall \alpha \in \mathsf{dom}(f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0]) \;.\; \vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_n)(f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\alpha))$.
    - If $\alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\}$, we must show that $\vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_n)(\vartheta_0(\alpha))$.

By lemma 11, $\forall\alpha \in \mathsf{dom}(T_{i-1})$. $T_{i-1}(\alpha) = T_i(\alpha)$, $i = 1,\dots,n$ so that, by transitivity, $\forall\alpha \in \mathsf{dom}(T_0)$. $T_0(\alpha) = T_n(\alpha)$. Therefore, by (13), for all $\beta \in \mathsf{dom}(T_0)$, $\bar{\varsigma}_j(T_0)\beta \triangleq \mathsf{let}\ \langle\boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2\rangle = T_0(\beta)\ \mathsf{in}\ \boldsymbol{\tau}_j = \mathsf{let}\ \langle\boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2\rangle = T_n(\beta)\ \mathsf{in}\ \boldsymbol{\tau}_j = \bar{\varsigma}_j(T_n)\beta$. By lemma 28, $\mathsf{vars}[\![\vartheta_0(\mathbb{V}_{\mathfrak{t}})]\!] \subseteq \mathsf{dom}(T_0)$ 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 $\forall\alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\}$. $\bar{\varsigma}_j(T_0)⊠_{\Theta}(⊠) = \bar{\varsigma}_j(T_n)⊠_{\Theta}(⊠)$. By the preinvariant of (33), we have $\forall\alpha \in \mathsf{dom}(\vartheta_0)$. $\vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_0)(\vartheta_0(\alpha))$. Therefore, by transitivity, $\vartheta_j^0(\alpha) = \bar{\varsigma}_j(T_n)(\vartheta_0(\alpha))$.

  - Otherwise $\alpha = \gamma$, in which case we must show that $\vartheta_j^0(\gamma) = \bar{\varsigma}_j(T_n)(f(\boldsymbol{\tau}^1,\dots,\boldsymbol{\tau}^n))$. By lemma 30, (48.42) of lemma 48.40, and (17.5a), we have $\vartheta_j^0(\gamma) = \vartheta_j^0(\boldsymbol{\tau}')$ $= \boldsymbol{\tau}_j = \bar{\varsigma}_j(T)(\boldsymbol{\tau}) = \bar{\varsigma}_j(T)(f(\boldsymbol{\tau}^1,\dots,\boldsymbol{\tau}^n))$.

- In case (17.7), the postinvariant of (31) immediately follows from the preinvariant because $T = T_0$ and $\vartheta' = \vartheta_0$;
- In case (17.9), we must show that $\forall j = 1,2$. $\forall\alpha \in \mathsf{dom}(\beta[\gamma \leftarrow \vartheta_0])$. $\vartheta_j^0(\alpha) = \bar{\varsigma}_j(\langle\boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2\rangle[\beta \leftarrow T_0])(\beta[\gamma \leftarrow \vartheta_0](\alpha))$. There are two cases.
  - If $\alpha = \gamma$ then we must prove that $\vartheta_j^0(\gamma) = \bar{\varsigma}_j(\langle\boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2\rangle[\beta \leftarrow T_0])(\beta)$, that is, by (13), $\vartheta_j^0(\gamma) = \boldsymbol{\tau}_j$. It is not possible that $\gamma \in \mathsf{dom}(\vartheta_0)$ 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. Therefore $\vartheta_0(\gamma) = \gamma$ by (48.30). It follows that we have to prove that $\vartheta_j^0(\vartheta_0(\gamma)) = \boldsymbol{\tau}_j$, which directly follows from the preinvariant of (31);
  - Otherwise, $\alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\}$ and we must show that $\vartheta_j^0(\alpha) = \bar{\varsigma}_j(\langle\boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2\rangle[\beta \leftarrow T_0])(\vartheta_0(\alpha))$.
    The test (17.8) implies $\beta \notin \mathsf{dom}(T_0)$ and so $\beta \notin \mathsf{vars}[\![\vartheta_0(\alpha)]\!]$ because $\mathsf{vars}[\![\vartheta_0(\mathbb{V}_{\mathfrak{t}})]\!] \subseteq \mathsf{dom}(T_0)$ 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 $\mathsf{dom}(\vartheta') = \mathsf{dom}(f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0]) = \mathsf{dom}(\vartheta_0) \cup \{\gamma\} = \mathsf{dom}(\vartheta_0) \cup \mathbb{vars}[\![\boldsymbol{\tau}']\!]$ because $\vartheta' = \gamma$ by the test (17.a);
- In case (17.5b), we have $\mathsf{dom}(\vartheta_i) = \mathsf{dom}(\vartheta_{i-1}) \cup \mathbb{vars}[\![\boldsymbol{\tau}^i]\!]$, $i = 1, \ldots, n$, by induction hypothesis on the sequence of calls to lub'. It follows that $\mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta_n) = \mathsf{dom}(\vartheta_0) \cup \bigcup_{i=1}^{n} \mathbb{vars}[\![\boldsymbol{\tau}^i]\!] = \mathsf{dom}(\vartheta_0) \cup \mathbb{vars}[\![f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)]\!] = \mathsf{dom}(\vartheta_0) \cup \mathbb{vars}[\![\boldsymbol{\tau}']\!]$;
- In case (17.7), we have $\vartheta' = \beta[\gamma \leftarrow \vartheta_0]$ so $\mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta_0) \cup \{\gamma\} = \mathsf{dom}(\vartheta_0) \cup \mathbb{vars}[\![\boldsymbol{\tau}']\!]$ because $\boldsymbol{\tau}' = \gamma$ by lemma 22;
- Finally, in case (17.9), $\mathsf{dom}(\vartheta') = \mathsf{dom}(\beta[\gamma \leftarrow \vartheta_0]) = \mathsf{dom}(\vartheta_0) \cup \{\gamma\} = \mathsf{dom}(\vartheta_0) \cup \mathbb{vars}[\![\boldsymbol{\tau}']\!]$ 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 $\boldsymbol{\tau}^k = f(\boldsymbol{\tau}^{1^k}, \ldots, \boldsymbol{\tau}^{nk}) = f(\boldsymbol{\tau}^{1^m}, \ldots, \boldsymbol{\tau}^{nm}) = \boldsymbol{\tau}^m$;
- 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 $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu, T_0, T \in \wp(\mathbb{V}_{\mathbb{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V}_{\mathbb{t}} \nrightarrow \mathbf{T}^\nu$, 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.

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

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 $\boldsymbol{\tau}' = \gamma \in \mathbb{V}_{\mathbb{t}}$ 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 $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\nu, T_0, T \in \wp(\mathbb{V}_{\mathbb{t}} \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V}_{\mathbb{t}} \nrightarrow \mathbf{T}^\nu$, 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.

$$\vartheta'(\boldsymbol{\tau}') = \boldsymbol{\tau} \qquad (40) \quad \square$$

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 $\vartheta'(\boldsymbol{\tau}') = f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\gamma) = f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n) = \boldsymbol{\tau}$;
- In case (17.5b), we handle (17.2b), …, (17.4b) by recurrence.
  - For the basis at (17.2b), we have $\mathsf{dom}(\vartheta_1) = \mathsf{dom}(\vartheta_0) \cup \mathsf{vars}[\![\boldsymbol{\tau}_1']\!]$ by (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
$$\begin{gathered}\mathsf{dom}(\vartheta_i) = \mathsf{dom}(\vartheta_0) \cup \bigcup_{j=1}^{i} \mathsf{vars}[\![\boldsymbol{\tau}_j']\!] \wedge \qquad (41)\\ \forall j \in [1, i] \;.\; \forall \alpha \in \mathsf{dom}(\vartheta_j) \;.\; \vartheta_i(\alpha) = \vartheta_j(\alpha) \wedge \\ \forall j \in [1, i] \;.\; \vartheta_i(\boldsymbol{\tau}_j') = \vartheta_j(\boldsymbol{\tau}_j') = \boldsymbol{\tau}^j\end{gathered}$$
  - At the next $i + 1^{\text{th}}$ call, we have
    1. By (35) of lemma 34 and recurrence hypothesis (41), $\mathsf{dom}(\vartheta_{i+1}) = \mathsf{dom}(\vartheta_i) \cup \mathsf{vars}[\![\boldsymbol{\tau}_{i+1}']\!] = \mathsf{dom}(\vartheta_0) \cup \bigcup_{j=1}^{i} \mathsf{vars}[\![\boldsymbol{\tau}_j']\!] \cup \mathsf{vars}[\![\boldsymbol{\tau}_{i+1}']\!] = \mathsf{dom}(\vartheta_0) \cup \bigcup_{j=1}^{i+1} \mathsf{vars}[\![\boldsymbol{\tau}_j']\!]$;
    2. By (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)., $\forall j \in [1, i+1] \;.\; \mathsf{vars}[\![\boldsymbol{\tau}_j']\!] \subseteq \mathsf{dom}(\vartheta_j) \subseteq \mathsf{dom}(\vartheta_{i+1})$ and by (2)., $\forall \alpha \in \mathsf{dom}(\vartheta_j) \;.\; \vartheta_{i+1}(\alpha) = \vartheta_j(\alpha)$ so that, by (48.30) and (48.30), $\forall j \in [1, i] \;.\; \vartheta_{i+1}(\boldsymbol{\tau}_j') = \vartheta_i(\boldsymbol{\tau}_j') = \vartheta_j(\boldsymbol{\tau}_j') = \boldsymbol{\tau}^j$. Moreover, $\vartheta_{i+1}(\boldsymbol{\tau}_{i+1}') = \boldsymbol{\tau}^{i+1}$, by induction on the sequence of calls to lub'. Grouping all cases $j \in [1, i]$ and $j = i + 1$ together, we have $\forall j \in [1, i+1] \;.\; \vartheta_{i+1}(\boldsymbol{\tau}_j') = \vartheta_j(\boldsymbol{\tau}_j') = \boldsymbol{\tau}^j$. □

  By recurrence, (41) holds for $i = n$. Therefore $\vartheta'(\boldsymbol{\tau}') = \vartheta_n(f(\boldsymbol{\tau}_1', \dots, \boldsymbol{\tau}_n')) = f(\vartheta_n(\boldsymbol{\tau}_1'), \dots, \vartheta_n(\boldsymbol{\tau}_n')) = f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n) = \boldsymbol{\tau}$.
- 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 $\vartheta'(\boldsymbol{\tau}') = \beta[\gamma \leftarrow \vartheta_0](\gamma) = \beta = \boldsymbol{\tau}$. □

Proof of theorem 48.103 By lemma 16, $[\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)]_{\simeq^v}$ is a $\preceq_{\simeq^v}$-upper bound of $[\boldsymbol{\tau}_1]_{\simeq^v}$ and $[\boldsymbol{\tau}_2]_{\simeq^v}$. By lemma 21, so is $[\mathsf{lgc}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)]_{\simeq^v}$.

Now if $[\boldsymbol{\tau}']_{\simeq^v}$ is any $\preceq_{\simeq^v}$-upper bound of $[\boldsymbol{\tau}_1]_{\simeq^v}$ and $[\boldsymbol{\tau}_2]_{\simeq^v}$ 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 $\mathsf{lgc}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2) \preceq_{\simeq^v} [\boldsymbol{\tau}']_{\simeq^v}$. This proves by lemma 21 that $\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)$ is the $\preceq_{\simeq^v}$-least upper bound of $[\boldsymbol{\tau}_1]_{\simeq^v}$ and $[\boldsymbol{\tau}_2]_{\simeq^v}$. $\square$

---

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 (p. 257, 269, 409, 698, 38).

[2] Patrick Cousot and Radhia Cousot. "Automatic Synthesis of Optimal Invariant Assertions: Mathematical Foundations." *SIGART Newsl.* 64 (1977), pp. 1–12 (p. 255, 409, 551, 38).

[3] Michael Karr. "Affine Relationships Among Variables of a Program." *Acta Inf.* 6 (1976), pp. 133–151 (p. 453, 456, 603, 608, 617, 12).

[4] Gary A. Kildall. "A Unified Approach to Global Program Optimization." In *POPL.* ACM Press, 1973, pp. 194–206 (p. 32, 109, 250, 257, 321, 344, 412, 497, 603, 617, 12).

[5] Oleg Kiselyov. "Effects Without Monads: Non–Determinism — Back to the Meta Language." In *ML/OCaml.* Vol. 294. EPTCS. 2017, pp. 15–40 (p. 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 (p. 603, 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 (p. 603, 617, 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 (p. 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 (p. 603, 617, 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 (p. 397, 513, 603, 617, 12).