# Mathematical proofs
# in complement of the book

# Principles of Abstract Interpretation

## (MIT Press, 2021)

Patrick Cousot

New York University

July 20, 2020

## 1 Mathematical proofs of chapter 4

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

- For $\mathtt{Sl} ::= \mathtt{Sl}'\ \mathtt{S}$, $\delta(\mathtt{Sl}') = \delta(\mathtt{S}) = \delta(\mathtt{Sl})+1$. So, in case $\mathsf{escape}[\![\mathtt{Sl}]\!] = \mathtt{tt}$, we have $\mathsf{break\text{-}to}[\![\mathtt{Sl}]\!] \neq \mathsf{after}[\![\mathtt{Sl}]\!]$ by induction hypothesis. By def. $\mathsf{escape}[\![\mathtt{Sl}]\!] \triangleq \mathsf{escape}[\![\mathtt{Sl}']\!] \vee \mathsf{escape}[\![\mathtt{S}]\!]$, there are two subcases.
  - If $\mathsf{escape}[\![\mathtt{Sl}']\!] = \mathtt{tt}$ then, on one hand, $\mathtt{Sl} \neq \mathtt{\{}\ \ldots\mathtt{\{}\ \epsilon\ \mathtt{\}}\ldots\ \mathtt{\}}$, $\mathsf{after}[\![\mathtt{Sl}']\!] = \mathsf{at}[\![\mathtt{S}]\!]$, $\mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \triangleq \mathsf{break\text{-}to}[\![\mathtt{Sl}]\!]$, $\mathsf{at}[\![\mathtt{S}]\!] \in \mathsf{in}[\![\mathtt{S}]\!]$ 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 with Lemma 4.17, proving $\mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \neq \mathsf{after}[\![\mathtt{Sl}']\!]$;
  - If $\mathsf{escape}[\![\mathtt{S}]\!] = \mathtt{tt}$ then $\mathtt{S} \neq \mathtt{\{}\ \ldots\mathtt{\{}\ \epsilon\ \mathtt{\}}\ldots\ \mathtt{\}}$, $\mathsf{after}[\![\mathtt{S}]\!] = \mathsf{after}[\![\mathtt{Sl}]\!]$, $\mathsf{break\text{-}to}[\![\mathtt{S}]\!] \triangleq \mathsf{break\text{-}to}[\![\mathtt{Sl}]\!]$, $\mathsf{break\text{-}to}[\![\mathtt{Sl}]\!] \neq \mathsf{after}[\![\mathtt{Sl}]\!]$ by induction hypothesis, so $\mathsf{break\text{-}to}[\![\mathtt{S}]\!] \neq \mathsf{after}[\![\mathtt{S}]\!]$.
- If $\mathtt{S} ::= \mathtt{if}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_t$ then $\mathsf{escape}[\![\mathtt{S}_t]\!] = \mathsf{escape}[\![\mathtt{S}]\!] = \mathtt{tt}$, $\mathsf{after}[\![\mathtt{S}_t]\!] = \mathsf{after}[\![\mathtt{S}]\!]$, $\mathsf{break\text{-}to}[\![\mathtt{S}_t]\!] = \mathsf{break\text{-}to}[\![\mathtt{S}]\!]$, and $\mathsf{break\text{-}to}[\![\mathtt{S}]\!] \neq \mathsf{after}[\![\mathtt{S}]\!]$ by induction hypothesis since $\delta(\mathtt{S}_t) = \delta(\mathtt{S}) + 1$, so $\mathsf{break\text{-}to}[\![\mathtt{S}_t]\!] \neq \mathsf{after}[\![\mathtt{S}_t]\!]$.
- The proof is similar for $\mathtt{S} ::= \mathtt{if}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_t\ \mathtt{else}\ \mathtt{S}_f$ and $\mathtt{S} ::= \mathtt{\{}\ \mathtt{Sl}\ \mathtt{\}}$.

□

## 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 $\mathcal{S}^*[\![\mathtt{Sl}]\!] = \mathcal{S}^*[\![\mathtt{Sl}']\!] \cup \{\langle \pi_1,\ \pi_2 \frown \pi_3\rangle \mid \langle \pi_1,\ \pi_2\rangle \in \mathcal{S}^*[\![\mathtt{Sl}']\!] \wedge \langle \pi_1 \frown \pi_2,\ \pi_3\rangle \in \mathcal{S}^*[\![\mathtt{S}]\!]\}$.

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

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

$= \bigcup\{\alpha^{l}_{\mathtt{use},\mathtt{mod}}[\![\epsilon\ \mathtt{S}]\!]\ L_b, L_e\ \langle \pi_0,\ \pi_1\rangle \mid \langle \pi_0,\ \pi_1\rangle \in \mathcal{S}^*[\![\epsilon\ \mathtt{S}]\!]\}$
〈def. (41.3) of $\alpha^{\exists l}_{\mathtt{use},\mathtt{mod}}[\![\mathtt{S}]\!]$ for $\mathtt{Sl} ::= \epsilon\ \mathtt{S}$〉

$= \bigcup\{\alpha^{l}_{\mathtt{use},\mathtt{mod}}\ L_b, L_e\ \langle \pi_0{}^{\ell},\ \pi_1\rangle \mid \langle \pi_0{}^{\ell},\ \pi_1\rangle \in \mathcal{S}^*[\![\epsilon]\!] \cup \{\langle \pi_0{}^{\ell},\ \pi_2 \frown \pi_3\rangle \mid \langle \pi_0{}^{\ell},\ \pi_2\rangle \in \mathcal{S}^+[\![\epsilon]\!] \wedge \langle \pi_0{}^{\ell} \frown \pi_2,\ \pi_3\rangle \in \mathcal{S}^*[\![\mathtt{S}]\!]\}\}$
〈def. $\mathcal{S}^*[\![\epsilon\ \mathtt{S}]\!]$〉

$= \bigcup\{\alpha^{l}_{\mathtt{use},\mathtt{mod}}\ L_b, L_e\ \langle \pi_0,\ \pi_1\rangle \mid \langle \pi_0,\ \pi_1\rangle \in \mathcal{S}^*[\![\mathtt{S}]\!]\}\}$
〈(6.15) so that $\mathcal{S}^*[\![\epsilon]\!] = \{\langle \pi_0\mathtt{at}[\![\mathtt{S}]\!],\ \mathtt{at}[\![\mathtt{S}]\!]\rangle \mid \pi_0\mathtt{at}[\![\mathtt{S}]\!] \in \mathbb{T}^+\}$ and $\langle \pi_0\mathtt{at}[\![\mathtt{S}]\!],\ \mathtt{at}[\![\mathtt{S}]\!]\rangle \in \mathcal{S}^*[\![\mathtt{S}]\!]$ by (6.11)〉

$= \alpha^{\exists l}_{\mathtt{use},\mathtt{mod}}[\![\mathtt{Sl}]\!]\ (\mathcal{S}^*[\![\mathtt{S}]\!])\ L_b, L_e$
〈def. (41.3) of $\alpha^{\exists l}_{\mathtt{use},\mathtt{mod}}[\![\mathtt{S}]\!]$〉

$= \alpha^{\exists l}_{\mathtt{use},\mathtt{mod}}[\![\mathtt{S}]\!]\ (\mathcal{S}^*[\![\mathtt{S}]\!])\ L_b, L_e$
〈(41.3) since $\mathtt{after}[\![\mathtt{Sl}]\!] = \mathtt{after}[\![\mathtt{S}]\!]$, $\mathtt{escape}[\![\mathtt{Sl}]\!] = \mathtt{escape}[\![\mathtt{S}]\!]$, and $\mathtt{break\text{-}to}[\![\mathtt{Sl}]\!] = \mathtt{break\text{-}to}[\![\mathtt{S}]\!]$ when $\mathtt{Sl}' = \epsilon$〉

$\subseteq \widehat{\mathcal{S}}^{\exists l}[\![\mathtt{S}]\!]\ L_b, L_e$
〈ind. hyp. for Theorem 41.24〉

$= \widehat{\mathcal{S}}^{\exists l}[\![\mathtt{S}]\!]\ L_b, (\widehat{\mathcal{S}}^{\exists l}[\![\epsilon]\!]\ L_b, L_e)$
〈since $\widehat{\mathcal{S}}^{\exists l}[\![\epsilon]\!]\ L_b, L_e \triangleq L_e$ by (41.22)〉

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

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

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

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

$= \bigcup\{\alpha^{l}_{\mathtt{use},\mathtt{mod}}[\![\mathtt{Sl}]\!]\ L_b, L_e\ \langle \pi_0,\ \pi_1\rangle \mid \langle \pi_0,\ \pi_1\rangle \in \mathcal{S}^*[\![\mathtt{Sl}]\!]\}$
〈def. (41.3) of $\alpha^{\exists l}_{\mathtt{use},\mathtt{mod}}[\![\mathtt{S}]\!]$〉

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

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

(def. $\mathcal{S}^*[\![\mathtt{Sl}]\!]$, $\mathsf{after}[\![\mathtt{Sl}]\!] = \mathsf{after}[\![\mathtt{S}]\!]$ 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)

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

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

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

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

(— For the second term, if $\ell_n = \mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] = \mathsf{break\text{-}to}[\![\mathtt{S}]\!]$ then $\mathsf{a}_{n-1}$ is a break, so $\mathsf{escape}[\![\mathtt{S}]\!]$ holds. $L_b$ is included in $(\, \mathsf{escape}[\![\mathtt{S}]\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{S}]\!] \;?\; L_b \,:\, \varnothing \,)$ and so $(\, \mathsf{escape}[\![\mathtt{Sl}']\!] \wedge \ell_n = \mathsf{break\text{-}to}[\![\mathtt{Sl}']\!] \;?\; L_b \,:\, \varnothing \,)$ is redundant. Moreover, $\pi_2 \frown \pi_3 = \ell_1 \xrightarrow{\mathsf{a}_1} \ell_2 \xrightarrow{\mathsf{a}_2} \dots \xrightarrow{\mathsf{a}_{n-1}} \ell_n$ is decomposed into $\pi_2 = \ell_1 \xrightarrow{\mathsf{a}_1} \ell_2 \xrightarrow{\mathsf{a}_2} \dots \xrightarrow{\mathsf{a}_{m-1}} \ell_m$ and $\pi_3 = \ell_m \xrightarrow{\mathsf{a}_m} \ell_{m+1} \xrightarrow{\mathsf{a}_{m+1}} \dots \xrightarrow{\mathsf{a}_{n-1}} \ell_n$ where, by $\langle \pi_0, \pi_2 \rangle \in \mathcal{S}^+[\![\mathtt{Sl}']\!]$ and $\langle \pi_0 \frown \pi_2, \pi_3 \rangle \in \mathcal{S}^*[\![\mathtt{S}]\!]$, $\ell_m = \mathsf{after}[\![\mathtt{Sl}']\!] = \mathsf{at}[\![\mathtt{S}]\!]$. Moreover, $\pi_0 \frown \pi_2$ is generalized to $\pi'_0$ (whence inclusion) and $\pi_2$ is renamed into $\pi_1$.)

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

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

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

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

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

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

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

Lemma 41.8

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

Lemma 41.8 and (41.3)

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

def. (41.3) of $\alpha^{\exists l}_{\mathtt{use},\mathtt{mod}}$

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

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

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

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

□

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

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

All other cases are similar. □

# 3 Mathematical proofs of chapter 44

**Proof of Theorem 44.38** • In case (44.41) of an empty temporal specification $\varepsilon$, we have

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

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

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

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

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

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

$= \widehat{\mathscr{M}}^\dagger[\![\mathtt{Sl}]\!] \langle \underline{\varrho},\ \mathtt{R} \rangle$ ⟅(44.43)⟆

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

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

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

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

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

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

  $= \widehat{\mathscr{M}}^\dagger[\![\mathtt{S}]\!] \langle \underline{\varrho},\ \mathtt{R} \rangle$ ⟅(44.44)⟆

- In case (44.49) of an iteration statement $\mathtt{S} ::= \mathtt{while}^{\ell}\ \mathtt{(B)}\ \mathtt{S}_b$, we apply Corollary 18.31 so we have to calculate the abstract transformer that satisfies the commutation property for an iterate $X$ of the concrete transformer $\mathscr{F}^*_{\mathbb{S}}[\![\mathtt{S}]\!]$ (which traces must be of the form $\pi\langle \mathsf{at}[\![\mathtt{S}]\!],\ \rho \rangle$).

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

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

  $= \mathscr{M}^\dagger \langle \underline{\varrho},\ \mathtt{R} \rangle (\{\langle \ell,\ \rho \rangle \mid \rho \in \mathbb{E}\mathsf{v}\}) \cup \mathscr{M}^\dagger \langle \underline{\varrho},\ \mathtt{R} \rangle (\{\pi_2 \langle \ell',\ \rho \rangle \langle \mathsf{after}[\![\mathtt{S}]\!],\ \rho \rangle \mid \pi_2 \langle \ell',\ \rho \rangle \in X \wedge \mathscr{B}[\![\mathtt{B}]\!]\ \rho = \mathtt{ff} \wedge \ell' = \ell\}) \cup \mathscr{M}^\dagger \langle \underline{\varrho},\ \mathtt{R} \rangle (\{\pi_2 \langle \ell',\ \rho \rangle \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho \rangle \cdot \pi_3 \mid \pi_2 \langle \ell',\ \rho \rangle \in X \wedge \mathscr{B}[\![\mathtt{B}]\!]\ \rho = \mathtt{tt} \wedge \langle \mathsf{at}[\![\mathtt{S}_b]\!],\ \rho \rangle \cdot \pi_3 \in \widehat{\mathscr{S}}^*_{\mathbb{S}}[\![\mathtt{S}_b]\!] \wedge \ell' = \ell\})$
  ⟅Galois connection (44.30), so that, by Lemma 11.34, $\mathscr{M}^\dagger \langle \underline{\varrho},\ \mathtt{R} \rangle$ preserves joins⟆

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

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

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

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

  — The second case is that of the loop exit

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⟅(44.26) and (44.25), ∧ commutative⟆

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

— If $\mathtt{R}'' \in \mathscr{R}_{\varepsilon}$, then

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

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

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

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

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

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

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

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

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

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

— Grouping all cases together we get the term (44.50) defining $\widehat{\mathscr{F}}^{\dagger}[\![\mathsf{S}]\!]\langle \underline{\varrho},\ \mathsf{R}\rangle\ (\mathscr{M}^{\dagger}\langle \underline{\varrho},\ \mathsf{R}\rangle X)$ and so Corollary 18.31 and the commutation condition $\mathscr{M}^{\dagger}\langle \underline{\varrho},\ \mathsf{R}\rangle(\mathscr{F}^{*}_{\mathbb{S}}[\![\mathsf{S}]\!](X)) = \widehat{\mathscr{F}}^{\dagger}[\![\mathsf{S}]\!]\langle \underline{\varrho},\ \mathsf{R}\rangle\ (\mathscr{M}^{\dagger}\langle \underline{\varrho},\ \mathsf{R}\rangle(X))$ for the iterates $X$ of $\mathscr{F}^{*}_{\mathbb{S}}[\![\mathsf{S}]\!]$ yield $\widehat{\mathscr{M}}^{\dagger}[\![\mathsf{S}]\!]\langle \underline{\varrho},\ \mathsf{R}\rangle \triangleq \mathsf{lfp}^{\subseteq}\,(\widehat{\mathscr{F}}^{\dagger}[\![\mathsf{S}]\!]\langle \underline{\varrho},\ \mathsf{R}\rangle)$ that is (44.49).

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

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

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

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

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

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

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

# 4 Mathematical proofs of chapter 47

**Proof** (47.47) There are three cases depending on whether the program label $\ell$ is at or after statement $\mathsf{S}$, or in the true branch $\mathsf{S}_t$.

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

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

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

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

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

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

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

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

$\wr$def. $\in$ so that $\pi_1$ and $\pi'_1$ must end with $\mathsf{after}[\![\mathsf{S}]\!]$ and def. (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]\int$

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

$$\text{⟅def. } \in \text{ and trace concatenation } \frown \text{⟆}$$

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

$$\text{⟅def. (47.18) of diff⟆}$$

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

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

(??)

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

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

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

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

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

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

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

$$\text{⟅since } \rho[\mathsf{x}' \leftarrow \nu](\mathsf{y}) = \rho(\mathsf{y}) \text{ when } \mathsf{y} \neq \mathsf{x}'\text{⟆}$$

$$= \{\langle \mathsf{x}',\ \mathsf{x}'\rangle \mid \mathsf{x}' \in \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B})\} \qquad \text{⟅def. (47.48) of nondet⟆}$$

$$= \mathbb{1}_{\mathscr{V}} \rceil \mathsf{nondet}(\neg\mathsf{B}, \neg\mathsf{B}) \qquad \text{⟅def. left restriction } \rceil\text{⟆}$$

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

In words for that first case, the initial value of $\mathsf{x}'$ flows to the value of $\mathsf{x}'$ by the false branch of the conditional `if (B)` $\mathsf{S}_t$ when there are at least two different values of $\mathsf{x}'$ for which $\mathsf{B}$ is false. (If

there is only one, $\mathsf{x}'$ is constant on the false branch. This can be disproved by a constancy analysis [**DBLP:conf/popl/Kildall73**, **DBLP:journals/toplas/WegmanZ91**, **DBLP:journals/acta/Karr76**, **DBLP:conf/cc/KnoopKS98**, **DBLP:conf/cc/KnoopR00**, **DBLP:conf/esop/Muller-OlmR01**] or a determinacy analysis [**DBLP:journals/ngc/Lopez-GarciaBH10**, **DBLP:journals/corr/abs-1905-06544**].) A classical coarser over-approximation is to ignore values *i.e.* that variables may have only one value making the test false.

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

(??)

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

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

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

$$\text{〖def. } \in\text{〗}$$

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

$$\text{〖after}[\![\mathsf{S}]\!] = \mathsf{after}[\![\mathsf{S}_t]\!], \pi_2 = \pi'_2 = \ni, \text{ def. (6.6) of } \varrho\text{〗}$$

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

$$\text{〖def. (47.18) of diff and (47.16) of seqval}[\![\mathsf{y}]\!]\text{〗}$$

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

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

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

$\quad$ ⟅letting $\rho = \varrho(\bar\pi_0)$ and $\nu = \varrho(\bar\pi_0{}')(\mathsf{x}')$⟆

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

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

⟅def. ⊆ and def. (47.25) of $\alpha^{\mathrm{d}}$⟆

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

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

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

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

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

(??)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⟅letting $\rho = \varrho(\pi_0 \mathsf{at}[\![\mathsf{S}]\!])$, $\nu = \varrho(\pi'_0 \mathsf{at}[\![\mathsf{S}]\!])\mathsf{x}'$ so that $\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}'\} \,.\, \varrho(\pi_0 \mathsf{at}[\![\mathsf{S}]\!])\mathsf{z} = \varrho(\pi'_0 \mathsf{at}[\![\mathsf{S}]\!])\mathsf{z}$ implies $\varrho(\pi'_0 \mathsf{at}[\![\mathsf{S}]\!]) = \rho[\mathsf{x}' \leftarrow \nu]$. 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 def. (47.48) of nondet, $\mathsf{x}' \in \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B})$⟆

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

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

$= \mathsf{nondet}(\mathsf{B}, \neg\mathsf{B}) \times \mathsf{mod}[\![\mathsf{S}_t]\!]$ ⟅def. 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 over-approximated by the set of variables $\mathsf{x}'$ occurring in the boolean expression $\mathsf{B}$ as defined in Exercise 3.3⟆

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

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

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

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

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

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

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

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

⟅since if $\langle \pi_0,\ \pi_1 \rangle$ (or $\langle \pi'_0,\ \pi'_1 \rangle$) has the form $\langle \pi \mathsf{at}[\![\mathsf{S}]\!],\ \mathsf{at}[\![\mathsf{S}]\!] \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!] \rangle$ then $\ell$ does not appear in $\pi_1$ (resp. $\pi'_1$) 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⟆

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

⟅def. $\in$ and if $\ell$ has multiple occurrences in $\pi'_1{}^\ell\pi'_2$, we choose the first one, same for $\pi'_1{}^\ell\pi'_2$⟆

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

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

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

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

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

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

⟅def. (47.25) of $\alpha^{\mathrm{d}}$⟆

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

⟅structural induction hypothesis⟆

$= \mathscr{S}^{\mathrm{d}}[\![\mathsf{S}_t]\!]\,\ell \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})$ ⟅def. (47.48) of nondet⟆

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

$\subseteq \mathscr{S}^{\mathrm{d}}[\![\mathsf{S}_t]\!]\,\ell$

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

**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 (**??**):

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

The proof of (**??**) is an application of Exercise 18.17. $\langle C, \sqsubseteq, \bot, \sqcup\rangle$ is the complete lattice $\langle \wp(\wp(\mathbb{T}^+ \times \mathbb{T}^{+\infty})), \subseteq, \varnothing, \cup\rangle$. $\langle \mathcal{A}, \preccurlyeq, 0, \curlyvee\rangle$ is the complete lattice $\langle \mathbb{P}^{\mathrm{d}}, \subseteq^{\mathrm{d}}, \bot^{\mathrm{d}}, \cup^{\mathrm{d}}\rangle$. The Galois connection $\langle C, \sqsubseteq\rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathcal{A}, \preccurlyeq\rangle$ is given by Lemma 47.26. The transformer $f$ is (17.4). It preserves arbitrary non-empty unions so it is continuous. The transformer $g$ is (47.63). It preserves arbitrary non-empty unions pointwise so it is pointwise continuous (*i.e.* for $\subseteq^{\mathrm{d}}$ and $\cup^{\mathrm{d}}$ defined pointwise). The main point of the proof is to check the semi-commutation condition

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

By Exercise 18.17, 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 $\mathscr{F}^*[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b]\!]$ from $\varnothing$.

In practice, we have discovered $\mathscr{F}^{\mathsf{diff}}[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b]\!]$ knowing $\mathscr{F}^*[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b]\!]$ and $\alpha^{\mathrm{d}}$ by rewriting until getting a formula of the form $\mathscr{F}^{\mathsf{diff}}[\![\mathtt{while}\ \ell\ \mathtt{(B)}\ \mathtt{S}_b]\!] \circ \alpha^{\mathrm{d}}$ and using $\dot{\subseteq}$-over-approximations to ignore values in the static analysis. By Exercise 18.17, we conclude that

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

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

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

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

For each of these case, we have to consider all possible ways the traces $\ell\pi_1$ and $\ell\pi'_1$ in (**??**) can go through the dependency observation program point $\ell'$. The definition of $\mathscr{F}^*$ below shows all possible choices **(A)**, **(B)**, or **(C)** of $\ell\pi_1$ and $\ell\pi'_1$ in (**??**). 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 (**??**) which reduces the number of cases to be considered.

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

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

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

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

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

—— **(1)** If the dependency observation point $\ell'$ is at loop entry then $\ell' = \ell = \mathsf{at}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathtt{S}_b]\!]$. 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 (**??**).

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

$$\begin{aligned}
&(\texttt{??})\\
&= \{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \exists \langle \pi_0\ell,\ \ell\pi_1\rangle, \langle \pi'_0\ell,\ \ell\pi'_1\rangle \in \mathscr{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathtt{S}_b]\!]\ X\ .\ (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}\}\ .\ \varrho(\pi_0\ell)\mathtt{z} = \varrho(\pi'_0\ell)\mathtt{z}) \wedge \varrho(\pi_0\ell)\mathtt{y} \neq \varrho(\pi_0\ell)\mathtt{y}\}\\
&\subseteq \{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \exists \pi_0\ell, \pi'_0\ell\ .\ (\forall \mathtt{z} \in \mathbb{V} \setminus \{\mathtt{x}\}\ .\ \varrho(\pi_0\ell)\mathtt{z} = \varrho(\pi'_0\ell)\mathtt{z}) \wedge (\varrho(\pi_0\ell)\mathtt{y} \neq \varrho(\pi'_0\ell)\mathtt{y})\} && \text{⟅def. } \subseteq \text{⟆}\\
&= \{\langle \mathtt{x},\ \mathtt{y}\rangle \mid \exists \rho, \nu\ .\ \rho(\mathtt{y}) \neq \rho[\mathtt{x} \leftarrow \nu](\mathtt{y})\}\\
&\qquad \text{⟅letting } \rho = \varrho(\pi_0\ell), \rho[\mathtt{x} \leftarrow \nu] = \varrho(\pi'_0\ell) \text{ and Exercise 6.8⟆}\\
&= \{\langle \mathtt{x},\ \mathtt{x}\rangle \mid \mathtt{x} \in \mathbb{V}\} && \text{⟅def. (19.10) of the environment assignment⟆}
\end{aligned}$$

$= \mathbb{1}_{\mathcal{V}}$ ⟅def. identity relation on the set $\mathcal{V}$ of variables in Section 2.2.2⟆

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

– In case **(Ba)**, we have

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

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

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

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

– In case **(Bc)**, we have

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

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

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

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

– In case **(C)**, we have

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

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

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

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

(**??**)

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

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

⟅abstracting away the value of the conditions⟆

The possible choices for $\langle \pi'_0 \ell,\ \ell\pi'_1 \rangle \in \mathscr{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathsf{S}_b]\!]\ X$ 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}
&\text{(??)}\\
&= \{\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}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathsf{S}_b]\!]\ X\ .\ (\forall \mathsf{z} \in \mathcal{V}\setminus\{\mathsf{x}\}\ .\ \boldsymbol{\varrho}(\pi_0 \ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0 \ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]^{\ell'}(\pi_0 \ell, \ell\pi_2 \ell), \mathsf{seqval}[\![\mathsf{y}]\!]^{\ell'}(\pi'_0 \ell, \ell\pi'_1))\}\\
&\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 \mathcal{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))\}\\
&\qquad\qquad \text{⟅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 \mathcal{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))\}\\
&\qquad\qquad \text{⟅letting } \pi_0 \leftarrow \pi_0 \ell, \pi_1 \leftarrow \ell\pi_2 \ell, \pi'_0 \leftarrow \pi'_0 \ell, \pi'_1 \leftarrow \ell\pi'_2 \ell, \text{ and } \ell' = \ell \text{ in case } \textbf{(1)}\text{⟆}\\
&= \{\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 \mathcal{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))\}\}\\
&\qquad\qquad \text{⟅def. } \in \text{⟆}\\
&= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid X \in \mathcal{D}^{\ell}\langle \mathsf{x},\ \mathsf{y}\rangle\}\\
&\qquad\qquad \text{⟅def. (47.19) of } \mathcal{D}^{\ell}\langle \mathsf{x}',\ \mathsf{y}\rangle \text{⟆}\\
&= \alpha^{\mathrm{d}}(\{X\})^{\ell}\\
&\qquad\qquad \text{⟅def. (47.25) of } \alpha^{\mathrm{d}} \text{⟆}
\end{aligned}
$$

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

$$
\begin{aligned}
&\text{(??)}\\
&= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0 \ell,\ell\pi_2 \ell\rangle \in X\ .\ \exists \langle \pi'_0 \ell,\ \ell\pi'_1\rangle \in \mathscr{F}^*[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathsf{S}_b]\!]\ X\ .\ (\forall \mathsf{z} \in \mathcal{V}\setminus\{\mathsf{x}\}\ .\ \boldsymbol{\varrho}(\pi_0 \ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0 \ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]^{\ell}(\pi_0 \ell, \ell\pi_2 \ell), \mathsf{seqval}[\![\mathsf{y}]\!]^{\ell}(\pi'_0 \ell, \ell\pi'_1))\}\\
&\qquad\qquad \text{⟅case } \textbf{(1)} \text{ so } \ell' = \ell = \mathsf{at}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathsf{S}_b]\!] \text{⟆}\\
&= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0 \ell,\ \ell\pi_2 \ell\rangle \in X\ .\ \exists \langle \pi'_0 \ell,\ \ell\pi'_1\rangle \in \{\langle \pi'_0 \ell,\ \ell\pi'_2 \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3 \ell''\rangle \mid \langle \pi'_0 \ell,\ \ell\pi'_2 \ell\rangle \in X \wedge\\
&\quad \boldsymbol{\mathscr{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi'_0 \ell\pi'_2 \ell) = \mathrm{tt} \wedge \langle \pi'_0 \ell\pi'_2 \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3 \ell''\rangle \in \boldsymbol{\mathscr{S}}^*[\![\mathsf{S}_b]\!] \wedge \ell'' = \mathsf{after}[\![\mathsf{S}_b]\!] = \mathsf{at}[\![\mathsf{S}]\!] = \ell\}\ .\ (\forall \mathsf{z} \in \mathcal{V}\setminus\{\mathsf{x}\}\ .\ \boldsymbol{\varrho}(\pi_0 \ell)\mathsf{z} = \boldsymbol{\varrho}(\pi'_0 \ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]^{\ell}(\pi_0 \ell, \ell\pi_2 \ell), \mathsf{seqval}[\![\mathsf{y}]\!]^{\ell}(\pi'_0 \ell, \ell\pi'_1))\}\\
&\qquad\qquad \text{⟅case } \textbf{(Bb)} \text{ for } \ell\pi'_1 \text{⟆}
\end{aligned}
$$

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

(def. ∈ and $\ell'' = \ell$)

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

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

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

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

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

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

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

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

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

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

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

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

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

$$
\begin{aligned}
= {}& \alpha^{\mathrm{d}}(\{X\})\ell \cup (\alpha^{\mathrm{d}}(\{X\})\ell \fatsemi \alpha^{\mathrm{d}}(\{\{\langle \pi, \pi'\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!] \mid \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi)\}\})\ell)
\end{aligned}
$$

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

$$
= \alpha^{\mathrm{d}}(\{X\})\ell \cup (\alpha^{\mathrm{d}}(\{X\})\ell \fatsemi (\alpha^{\mathrm{d}}(\{\mathcal{S}^*[\![\mathsf{S}_b]\!]\})\ell \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B}))) \qquad ⟅\text{Lemma 47.62}⟆
$$

$$
= \alpha^{\mathrm{d}}(\{X\})\ell \cup (\alpha^{\mathrm{d}}(\{X\})\ell \fatsemi (\alpha^{\mathrm{d}}(\{\mathcal{S}^{+\infty}[\![\mathsf{S}_b]\!]\})\ell) \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B})) \qquad ⟅\text{Lemma 47.23}⟆
$$

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

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

(**??**)

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

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

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

$= \{\langle \mathsf{x},\mathsf{y}\rangle \mid \exists\langle \pi_0\ell,\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle\ .\ \langle \pi_0\ell,\ell\pi_2\ell\rangle \in X \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell\rangle \in \{\langle \pi, \pi'\rangle \in \mathscr{S}^*[\![\mathsf{S}_b]\!] \mid \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi)\} \wedge \exists\langle \pi'_0\ell,\ \ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle\ .\ \langle \pi'_0\ell,\ \ell\pi'_2\ell\rangle \in X \wedge \langle \pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \{\langle \pi,\ \pi'\rangle \in \mathscr{S}^*[\![\mathsf{S}_b]\!] \mid \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi)\} \wedge (\forall \mathsf{z} \in \mathbb{V}\setminus\{\mathsf{x}\}\ .\ \varrho(\pi'_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi_0\ell, \ell\pi_2\ell), \mathsf{seqval}[\![\mathsf{y}]\!]\ell(\pi'_0\ell, \ell\pi'_2\ell))\}$
$\wr$by def. (47.18) of diff, and def. (47.16) of $\mathsf{seqval}[\![\mathsf{y}]\!]$ since in case **(1)**, $\ell' = \ell$ does not appear in $\xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3$ and the value of $\mathsf{y}$ is the same at $\ell$ after $\pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell$ and at $\ell$ after $\pi_0\ell\pi_2\ell$. Same for $\pi'_0\ell\pi'_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell$. $\int$

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

$\subseteq \alpha^{\mathrm{d}}(\{X\})^{\ell}$ ⟅def. (47.25) of $\alpha^{\mathrm{d}}$⟆

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

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

However, the term $X(\ell)$ does not appear in (47.63.a) since it can be simplified thanks to Exercise 15.8.

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

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

— **(2–B–B)** The dependency observation point $\ell'$ on the two prefix observation traces ${}^{\ell}\pi_1$ and ${}^{\ell}\pi'_1$ in (**??**) is in the loop body $\mathsf{S}_b$ after zero or more loop iterations and the observation along these two traces stops in the loop body.

(**??**)

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0{}^{\ell},\ {}^{\ell}\pi_1\rangle, \langle \pi'_0{}^{\ell},\ {}^{\ell}\pi'_1\rangle \in \{\langle \pi_0{}^{\ell},\ {}^{\ell}\pi_2{}^{\ell} \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3{}^{\ell''}\rangle \mid \langle \pi_0{}^{\ell},\ {}^{\ell}\pi_2{}^{\ell}\rangle \in X \wedge \boldsymbol{\mathcal{B}}[\![\mathsf{B}]\!]\boldsymbol{\varrho}(\pi_0{}^{\ell}\pi_2{}^{\ell}) = \mathtt{tt} \wedge \langle \pi_0{}^{\ell}\pi_2{}^{\ell} \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3{}^{\ell''}\rangle \in \boldsymbol{\mathcal{S}}^*[\![\mathsf{S}_b]\!]\}\ .\ (\forall \mathsf{z} \in \mathcal{V} \setminus \{\mathsf{x}\}\ .\ \boldsymbol{\varrho}(\pi_0{}^{\ell})\mathsf{z} = \boldsymbol{\varrho}(\pi'_0{}^{\ell})\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]^{\ell'}(\pi_0{}^{\ell}, {}^{\ell}\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]^{\ell'}(\pi'_0{}^{\ell}, {}^{\ell}\pi'_1))\}$ ⟅case **2–B–B**⟆

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

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

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

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

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

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

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

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

— **(2–B–C/2–C–B)** The dependency observation point $\ell'$ on the two prefix observation traces $\ell\pi_1$ and $\ell\pi'_1$ in (**??**) is in the loop body $\mathsf{S}_b$ 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.

(??)

$= \{\langle \mathsf{x},\ \mathsf{y}\rangle \mid \exists \langle \pi_0 \ell,\ \ell\pi_1\rangle \in \{\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathsf{tt} \wedge \langle \pi_0\ell\pi_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3\ell''\rangle \in \mathscr{S}^*[\![\mathsf{S}_b]\!]\}\ .\ \exists\langle \pi'_0\ell,\ \ell\pi'_1\rangle \in \{\langle \pi_0\ell,\ \ell\pi_2\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \langle \pi_0\ell,\ \ell\pi_2\ell\rangle \in X \wedge \mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathsf{ff}\}\ .\ (\forall \mathsf{z} \in \mathbb{V} \setminus \{\mathsf{x}\}\ .\ \varrho(\pi_0\ell)\mathsf{z} = \varrho(\pi'_0\ell)\mathsf{z}) \wedge \mathsf{diff}(\mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi_0\ell, \ell\pi_1), \mathsf{seqval}[\![\mathsf{y}]\!]\ell'(\pi'_0\ell, \ell\pi'_1))\}$ ⟅case 2–B–C⟆

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

⟅This case is handled exactly as the previous one since the program point $\ell'$ 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.⟆

— (2–C–C) The dependency observation point $\ell'$ on the two prefix observation traces $\ell\pi_1$ and $\ell\pi'_1$ in (??) is in the loop body $\mathsf{S}_b$ after zero or more loop iterations and the observation along these two traces stops at the loop exit.

(??)

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

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

⟅This case is handled exactly as the two previous ones since, again, the program point $\ell'$ 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 (??) $\subseteq \alpha^{\mathrm{d}}(\{X\})\ell' \cup \big(\alpha^{\mathrm{d}}(\{X\})\ell \fatsemi ((\widehat{\widehat{\mathscr{S}}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell') \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B}))\big)$ which yields (47.63.b) of the form

$$\langle\!\langle\ \ell' \in \mathsf{in}[\![\mathsf{S}_b]\!] \mathbin{?} \big(X(\ell) \fatsemi ((\widehat{\widehat{\mathscr{S}}}^{\exists}_{\mathsf{diff}}[\![\mathsf{S}_b]\!]\ \ell') \rceil \mathsf{nondet}(\mathsf{B}, \mathsf{B}))\big) \mathbin{:} \varnothing\ \rangle\!\rangle.$$

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

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

(??)

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

$\wr \ell' = \mathsf{after}[\![\mathsf{S}]\!] \int$

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

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

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.

(??)

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

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

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

From there on, the development is very similar to the cases **(2.a)**, **(2.b)**, and **(2.c–d)** of the condi-

tional with execution traces that may go through the true branch (here entering the loop) or the false branch (here not entering the iteration). There are four subcases (three by symmetry).

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

(??)

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

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

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

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

(??)

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

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

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

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

$\subseteq \alpha^{\mathrm{d}}(\{X\})^\ell$ ⟅def. (47.25) of $\alpha^{\mathrm{d}}$⟆

– **(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.

(??)

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

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

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

⟅since, by def. (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), $\mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell)$ and $\mathscr{B}[\![\neg\mathsf{B}]\!]\varrho(\pi'_0\ell)$ 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 $\mathscr{F}^*[\![\mathtt{while}\ \ell\ (\mathsf{B})\ \mathsf{S}_b]\!]$ and, by Exercises 17.13 and 17.21, the language being deterministic, this would imply that $\ell\pi_2\ell = \ell$, in contradiction with $\mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell) = \mathtt{tt}$ and $\mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi_2\ell) = \mathtt{ff}$⟆

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

⟅by the argument (**??**) 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 $\ell$ for the first iteration) with $\ell\pi''_2\ell \in X$, $\mathscr{B}[\![\mathsf{B}]\!]\varrho(\pi_0\ell\pi''_2\ell) = \mathtt{tt}$ and $\langle \pi_0\ell\pi''_2\ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!],\ \mathsf{at}[\![\mathsf{S}_b]\!]\pi'_3\ell\rangle \in \mathscr{S}^*[\![\mathsf{S}_b]\!]$⟆

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

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

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

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

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

⟅Lemma 47.59 with $\ell_0 \leftarrow \ell$, $\ell' \leftarrow \ell$, and $\ell \leftarrow \mathsf{after}[\![\mathsf{S}]\!]$⟆

We have to calculate the second term

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

⟅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 $\boldsymbol{\varrho}(\pi'_0 \ell) = \rho[\mathsf{x} \leftarrow \nu]$.⟆

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

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

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

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

— **(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 $\mathsf{S}_b$.

(??)

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

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

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

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

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

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

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

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

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

(**??**)

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

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

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

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

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

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

$\wr$by Lemma 47.59 where $\mathcal{S}' = \{\langle \pi \ell, \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3 \ell'' \xrightarrow{\mathbf{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi \ell) =$
$\mathsf{tt} \wedge \ell'' \in \mathsf{breaks\text{-}of}[\![\mathsf{S}_b]\!] \wedge \langle \pi \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!], \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3 \ell'' \xrightarrow{\mathbf{break}} \mathsf{after}[\![\mathsf{S}]\!]\rangle \in \mathcal{S}^*[\![\mathsf{S}_b]\!]\} \cup \{\langle \pi \ell,$
$\ell \xrightarrow{\neg(\mathsf{B})} \mathsf{after}[\![\mathsf{S}]\!]\rangle \mid \mathcal{B}[\![\mathsf{B}]\!]\varrho(\pi \ell) = \mathsf{ff}\}$ with $\pi_0 \ell_0 \leftarrow \pi_0 \ell$, $\ell_0 \pi_1 \ell' \leftarrow \ell \pi_2 \ell$, $\ell \leftarrow \mathsf{after}[\![\mathsf{S}]\!]$,
$\ell' \pi_2 \ell \leftarrow \ell \xrightarrow{\mathsf{B}} \mathsf{at}[\![\mathsf{S}_b]\!]\pi_3 \ell'' \xrightarrow{\mathbf{break}} \mathsf{after}[\![\mathsf{S}]\!], \ell \pi_3 \leftarrow \mathsf{after}[\![\mathsf{S}]\!]$ 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 $\pi'_3 = \ni \int$

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

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

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

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

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

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

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

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

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

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

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

⟅def. $\cup$⟆

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

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

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

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

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

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

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

$$\begin{array}{l} ⦇\, \ell' = \text{after}[\![\mathsf{S}]\!] \,?\, (\mathbb{1}_{\text{nondet}(\neg\mathsf{B},\neg\mathsf{B})} \cup X(\ell) \cup \qquad (47.63.\mathrm{c}') \\ \quad (X(\ell) \fatsemi (\mathbb{1}_{\text{nondet}(\neg\mathsf{B},\neg\mathsf{B})} \cup \text{nondet}(\neg\mathsf{B}, \neg\mathsf{B}) \times \text{mod}[\![\mathsf{S}_b]\!])) \rceil \text{nondet}(\mathsf{B}, \neg\mathsf{B}) \cup \\ \quad X(\ell) \fatsemi \Big( \big( \bigcup_{\ell'' \in \text{breaks-of}[\![\mathsf{S}_b]\!]} \widehat{\widehat{\boldsymbol{\mathcal{S}}}}^{\exists}_{\text{diff}}[\![\mathsf{S}_b]\!]\ \ell'' \big) \rceil \text{nondet}(\mathsf{B}, \mathsf{B}) \Big) \cup \\ \quad \mathbb{1}_{\text{nondet}(\mathsf{B},\neg\mathsf{B})} \cup (\text{nondet}(\mathsf{B}, \neg\mathsf{B}) \times \text{mod}[\![\mathsf{S}_b]\!])) \fatsemi \varnothing \,⦈. \end{array}$$

that can be simplified as follows (while loosing precision)

(**??**)

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

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

⟅since $\text{nondet}(\mathsf{B}_1, \mathsf{B}_2) \subseteq \mathcal{V}$ so $\mathbb{1}_{\text{nondet}(\mathsf{B}_1,\mathsf{B}_2)} \subseteq \mathbb{1}_{\mathcal{V}}$ and def. ⟆⟆

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

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

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

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

For fixpoints $X$ of $\mathcal{F}^{\text{diff}}[\![\texttt{while}\ \ell\ \texttt{(B)}\ \mathsf{S}_b]\!]$, we have $\mathbb{1}_{\mathcal{V}} \subseteq X(\ell)$ by (47.63.a) so that, by the chaotic iteration theorem [**DBLP:journals/sigart/CousotC77**, **Cousot-IMAG-RR88-1977**], $\mathbb{1}_{\mathcal{V}} \cup X(\ell)$ can be replaced by $X(\ell)$. We get a term (47.63.c) of the form

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

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

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

proving pointwise semi-commutation. □

# 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 $\vartheta_0$, or not.

- If $\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0) = \Omega^{\mathrm{r}}_{\mathsf{s}}$ in case (48.47.8) of an occur-check, we have $\gamma^{\mathrm{r}}_{\mathsf{s}}(\Omega^{\mathrm{r}}_{\mathsf{s}}) = \varnothing$ by (48.46). By the test (48.47.8), $\alpha \in \mathbb{vars}[\![\boldsymbol{\tau}_2]\!]$. If $\boldsymbol{\tau}_2 = \beta \in \mathbb{V}_{\mathbb{t}}$ 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 def. (48.51) of $\gamma_{\mathsf{e}}$ that $\gamma_{\mathsf{e}}(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) = \gamma_{\mathsf{e}}(\alpha \doteq \boldsymbol{\tau}_2) = \varnothing$ since otherwise, there would be some $\boldsymbol{\rho}$ such that $\boldsymbol{\rho}(\boldsymbol{\tau}_1) = \boldsymbol{\rho}(f(\ldots\,\alpha\,\ldots)$ which would be an infinite object not in $\mathbf{P}^{\mathrm{v}}$, as shown in Lemma 48.9.

- By Lemma 48.58, unify does terminate so that, in case (48.47.6) with $\vartheta_n = \Omega^{\mathrm{r}}_{\mathsf{s}}$ 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 $\gamma^{\mathrm{r}}_{\mathsf{s}}(\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0)) = \gamma^{\mathrm{r}}_{\mathsf{s}}(\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0)) = \gamma^{\mathrm{r}}_{\mathsf{s}}(\Omega^{\mathrm{r}}_{\mathsf{s}}) = \varnothing$;

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

$$
\begin{aligned}
& \gamma_{\mathsf{e}}(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) \cap \gamma^{\mathrm{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^{\mathrm{r}}_{\mathsf{s}}(\vartheta_0) && \text{⟅test (48.47.1) is tt⟆} \\
= \; & \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^{\mathrm{r}}_{\mathsf{s}}(\vartheta_0) && \text{⟅test (48.47.2) is ff⟆} \\
= \; & \{\boldsymbol{\rho} \in \mathbf{P}^{\mathcal{V}} \mid \boldsymbol{\rho}(f(\boldsymbol{\tau}^1_1, \ldots, \boldsymbol{\tau}^n_1)) = \boldsymbol{\rho}(f(\boldsymbol{\tau}^1_2, \ldots, \boldsymbol{\tau}^n_2))\} \cap \gamma^{\mathrm{r}}_{\mathsf{s}}(\vartheta_0) && \text{⟅def. (48.51) of } \gamma_{\mathsf{e}}\text{⟆} \\
= \; & \{\boldsymbol{\rho} \in \mathbf{P}^{\mathcal{V}} \mid \bigwedge_{i=1}^{n} \boldsymbol{\rho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\rho}(\boldsymbol{\tau}^i_2)\} && \text{⟅def. (48.7) of assignment application⟆} \\
= \; & \bigcap_{i=1}^{n} \{\boldsymbol{\rho} \in \mathbf{P}^{\mathcal{V}} \mid \boldsymbol{\rho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\rho}(\boldsymbol{\tau}^i_2)\} \cap \gamma^{\mathrm{r}}_{\mathsf{s}}(\vartheta_0) && \text{⟅def. } \textstyle\bigcap\text{⟆} \\
= \; & (\{\boldsymbol{\rho} \in \mathbf{P}^{\mathcal{V}} \mid \boldsymbol{\rho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\rho}(\boldsymbol{\tau}^1_2)\} \cap \gamma^{\mathrm{r}}_{\mathsf{s}}(\vartheta_0)) \cap \bigcap_{2=1}^{n} \{\boldsymbol{\rho} \in \mathbf{P}^{\mathcal{V}} \mid \boldsymbol{\rho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\rho}(\boldsymbol{\tau}^i_2)\} \\
& && \text{⟅} \textstyle\bigcap \text{ is associative and commutative⟆} \\
= \; & (\gamma_{\mathsf{e}}(\boldsymbol{\tau}^1_i) \doteq \boldsymbol{\tau}^1_2) \cap \gamma^{\mathrm{r}}_{\mathsf{s}}(\vartheta_0)) \cap \bigcap_{2=1}^{n} \{\boldsymbol{\rho} \in \mathbf{P}^{\mathcal{V}} \mid \boldsymbol{\rho}(\boldsymbol{\tau}^1_i = \boldsymbol{\rho}(\boldsymbol{\tau}^i_2)\} && \text{⟅def. (48.51)x of } \gamma_{\mathsf{e}}\text{⟆} \\
= \; & \mathsf{let}\ \vartheta_1 = \mathsf{unify}(\boldsymbol{\tau}^1_i, \boldsymbol{\tau}^1_2, \vartheta_0)\ \mathsf{in} \\
& \quad \bigcap_{2=1}^{n} \{\boldsymbol{\rho} \in \mathbf{P}^{\mathcal{V}} \mid \boldsymbol{\rho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\rho}(\boldsymbol{\tau}^i_2)\} \cap \gamma^{\mathrm{r}}_{\mathsf{s}}(\vartheta_1) && \text{⟅ind. hyp. and } \textstyle\bigcap \text{ commutative⟆} \\
= \; & \mathsf{let}\ \vartheta_1 = \mathsf{unify}((\boldsymbol{\tau}^1_i, \boldsymbol{\tau}^1_2, \vartheta_0)\ \mathsf{in} \\
& \quad \ldots \\
& \quad\ \mathsf{let}\ \vartheta_j = \mathsf{unify}(\boldsymbol{\tau}^j_i, \boldsymbol{\tau}^j_2, \vartheta_{j-1})\ \mathsf{in} \\
& \quad\quad \bigcap_{i=j+1}^{n} \{\boldsymbol{\rho} \in \mathbf{P}^{\mathcal{V}} \mid \boldsymbol{\rho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\rho}(\boldsymbol{\tau}^i_2)\} \cap \gamma^{\mathrm{r}}_{\mathsf{s}}(\vartheta_j) && \text{⟅recurrence hyp., } j < n\text{⟆} \\
= \; & \mathsf{let}\ \vartheta_1 = \mathsf{unify}(\boldsymbol{\tau}^1_i, \boldsymbol{\tau}^1_2, \vartheta_0)\ \mathsf{in} \\
& \quad \ldots \\
& \quad\ \mathsf{let}\ \vartheta_j = \mathsf{unify}(\boldsymbol{\tau}^j_i, \boldsymbol{\tau}^j_2, \vartheta_{j-1})\ \mathsf{in} \\
& \quad\quad \{\boldsymbol{\rho} \in \mathbf{P}^{\mathcal{V}} \mid \boldsymbol{\rho}(\boldsymbol{\tau}^{j+1}_i) = \boldsymbol{\rho}(\boldsymbol{\tau}^{j+1}_2)\} \cap \gamma^{\mathrm{r}}_{\mathsf{s}}(\vartheta_j) \cap \\
& \quad\quad\quad \bigcap_{i=j+2}^{n} \{\boldsymbol{\rho} \in \mathbf{P}^{\mathcal{V}} \mid \boldsymbol{\rho}(\boldsymbol{\tau}^1_i) = \boldsymbol{\rho}(\boldsymbol{\tau}^i_2)\} && \text{⟅} \textstyle\bigcap \text{ is associative and commutative⟆}
\end{aligned}
$$

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

- In case (48.47.7), we have

$$
\begin{aligned}
&\gamma_{\mathsf{e}}(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) \\
&= \gamma_{\mathsf{e}}(\alpha \doteq \alpha) \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) && \text{⦇}\alpha \in \mathbb{V}_{\mathbb{t}} \text{ by test (48.47.7)⦈} \\
&= \{\boldsymbol{\rho} \in \mathbf{P}^\nu \mid \boldsymbol{\rho}(\alpha) = \boldsymbol{\rho}(\alpha)\} \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) && \text{⦇def. (48.51) of } \gamma_{\mathsf{e}}\text{⦈} \\
&= \mathbf{P}^\nu \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) && \text{⦇since } \boldsymbol{\rho} \in \mathbf{P}^\nu \triangleq \mathbb{V}_{\mathbb{t}} \to \mathbf{T} \text{ by (48.6)⦈} \\
&= \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) && \text{⦇}\mathbf{P}^\nu \text{ is the identity for } \cap\text{⦈} \\
&= \gamma_{\mathsf{s}}^{\mathsf{r}}(\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0)) && \text{⦇def. unify in case (48.47.7)⦈}
\end{aligned}
$$

- In case (48.47.11), we have

$$
\begin{aligned}
&\gamma_{\mathsf{e}}(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) \\
&= \gamma_{\mathsf{e}}(\alpha \doteq \boldsymbol{\tau}_2) \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) \\
&\qquad \text{⦇where } \alpha \in \mathbb{V}_{\mathbb{t}} \text{ by test (48.47.9), } \alpha \notin \mathbb{vars}[\![\boldsymbol{\tau}_2]\!] \text{ since test (48.47.8) is ff, } \alpha \notin \mathsf{dom}(\vartheta_0) \text{ by} \\
&\qquad\quad \text{test (48.47.10), and } \boldsymbol{\tau}_2 \notin \mathbb{V}_{\mathbb{t}} \text{ since test (48.47.1) is ff⦈} \\
&= \{\boldsymbol{\rho} \in \mathbf{P}^\nu \mid \boldsymbol{\rho}(\alpha) = \boldsymbol{\rho}(\boldsymbol{\tau}_2)\} \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) && \text{⦇def. (48.51) of } \gamma_{\mathsf{e}}\text{⦈} \\
&= \{\boldsymbol{\rho} \in \mathbf{P}^\nu \mid \boldsymbol{\rho}(\alpha) = \boldsymbol{\rho}(\boldsymbol{\tau}_2)\} \cap \{\boldsymbol{\rho} \in \mathbf{P}^\nu \mid \forall \beta \in \mathbb{V}_{\mathbb{t}}\ .\ \boldsymbol{\rho}(\beta) = \boldsymbol{\rho}(\vartheta_0(\beta))\} && \text{⦇def. (48.52) of } \gamma_{\mathsf{s}}^{\mathsf{r}}\text{⦈} \\
&= \{\boldsymbol{\rho} \in \mathbf{P}^\nu \mid \boldsymbol{\rho}(\alpha) = \boldsymbol{\rho}(\boldsymbol{\tau}_2) \wedge \forall \beta \in \mathbb{V}_{\mathbb{t}}\ .\ \boldsymbol{\rho}(\beta) = \boldsymbol{\rho}(\vartheta_0(\beta))\} && \text{⦇def. } \cap\text{⦈} \\
&= \{\boldsymbol{\rho} \in \mathbf{P}^\nu \mid \forall \beta \in \mathbb{V}_{\mathbb{t}}\ .\ \boldsymbol{\rho}(\beta) = [\![\, \beta = \alpha \mathbin{?} \boldsymbol{\rho}(\vartheta_0(\beta)[\beta \in \mathbb{vars}[\![\boldsymbol{\tau}_2]\!] \leftarrow \boldsymbol{\tau}_2]) \mathbin{:} \boldsymbol{\rho}(\boldsymbol{\tau}_2[\alpha \leftarrow \vartheta_0(\beta)]) \,]\!]\}
\end{aligned}
$$

$$
\begin{aligned}
&\quad \text{⟅def. (48.7) of assignment application where } \boldsymbol{\rho}(\alpha) \text{ is replaced by its equal } \boldsymbol{\rho}(\boldsymbol{\tau}_2) \text{ and for } \beta \in \mathbb{V}_t \setminus \{\alpha\}, \boldsymbol{\rho}(\beta) \text{ is replaced by its equal } \boldsymbol{\rho}(\vartheta_0(\beta))\text{⟆} \\
&= \{\boldsymbol{\rho} \in \mathbf{P}^\nu \mid \forall \beta \in \mathbb{V}_t \,.\, \boldsymbol{\rho}(\beta) = [\![\, \beta = \alpha \;⁇\; \boldsymbol{\rho}(\vartheta_0(\beta)[\beta \in \mathbb{vars}[\![\boldsymbol{\tau}_2]\!] \leftarrow \boldsymbol{\tau}_2]) \;:\; \boldsymbol{\rho}(\{\langle \alpha, \boldsymbol{\tau}_2 \rangle\}(\vartheta_0(\beta))) \,]\!]\} \\
&\qquad\qquad \text{⟅by Exercise 48.60 where } \boldsymbol{\tau}' = \vartheta_0(\beta)\text{⟆} \\
&= \{\boldsymbol{\rho} \in \mathbf{P}^\nu \mid \forall \beta \in \mathbb{V}_t \,.\, \boldsymbol{\rho}(\beta) = [\![\, \beta = \alpha \;⁇\; \boldsymbol{\rho}(\vartheta_0(\boldsymbol{\tau}_2)) \;:\; \boldsymbol{\rho}(\{\langle \alpha, \boldsymbol{\tau}_2 \rangle\}(\vartheta_0(\beta))) \,]\!]\} \quad \text{⟅by Exercise 48.62⟆} \\
&= \{\boldsymbol{\rho} \in \mathbf{P}^\nu \mid \forall \beta \in \mathbb{V}_t \,.\, \boldsymbol{\rho}(\beta) = \boldsymbol{\rho}([\![\, \beta = \alpha \;⁇\; \vartheta_0(\boldsymbol{\tau}_2) \;:\; (\{\langle \alpha, \boldsymbol{\tau}_2 \rangle\} \circ \vartheta_0)(\beta) \,]\!])\} \\
&\qquad\qquad \text{⟅def. conditional and function composition } \circ\text{⟆} \\
&= \{\boldsymbol{\rho} \in \mathbf{P}^\nu \mid \forall \beta \in \mathbb{V}_t \,.\, \boldsymbol{\rho}(\beta) = \boldsymbol{\rho}([\![\, \beta = \alpha \;⁇\; (\{\langle \alpha, \boldsymbol{\tau}_2 \rangle\} \circ \vartheta_0)(\alpha) \;:\; (\{\langle \alpha, \boldsymbol{\tau}_2 \rangle\} \circ \vartheta_0)(\beta) \,]\!])\} \\
&\qquad\qquad \text{⟅since } X \notin \mathsf{dom}(\vartheta_0) \text{ so } (\{\langle \alpha, \boldsymbol{\tau}_2 \rangle\} \circ \vartheta_0)(\alpha) = \{\langle \alpha, \boldsymbol{\tau}_2 \rangle\}(\vartheta_0(\alpha)) = \{\langle \alpha, \boldsymbol{\tau}_2 \rangle\}(\alpha) = \boldsymbol{\tau}_2\text{⟆} \\
&= \{\boldsymbol{\rho} \in \mathbf{P}^\nu \mid \forall \beta \in \mathbb{V}_t \,.\, \boldsymbol{\rho}(\beta) = \boldsymbol{\rho}(\{\langle \alpha, \boldsymbol{\tau}_2 \rangle\} \circ \vartheta_0)(\beta) \qquad \text{⟅def. conditional⟆} \\
&= \gamma_{\mathsf{s}}^{\mathsf{r}}\{\langle \alpha, \boldsymbol{\tau}_2 \rangle\} \circ \vartheta_0 \qquad \text{⟅def. (48.52) of } \gamma_{\mathsf{s}}^{\mathsf{r}}\text{⟆} \\
&= \gamma_{\mathsf{s}}^{\mathsf{r}}(\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0)) \qquad \text{⟅(48.47.11)⟆}
\end{aligned}
$$

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

$$
\begin{aligned}
&\gamma_{\mathsf{e}}(\boldsymbol{\tau}_1 \doteq \boldsymbol{\tau}_2) \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) \\
&= \gamma_{\mathsf{e}}(\alpha \doteq \boldsymbol{\tau}_2) \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) \qquad \text{⟅} \boldsymbol{\tau}_1 = \alpha\text{⟆} \\
&= \{\boldsymbol{\rho} \in \mathbf{P}^\nu \mid \boldsymbol{\rho}(\alpha) = \boldsymbol{\rho}(\boldsymbol{\tau}_2) \wedge \forall \beta \in \mathbb{V}_t \,.\, \boldsymbol{\rho}(\beta) = \boldsymbol{\rho}(\vartheta_0(\beta))\} \\
&\qquad\qquad \text{⟅def. (48.51) of } \gamma_{\mathsf{e}}\text{, (48.52) of } \gamma_{\mathsf{s}}^{\mathsf{r}}\text{, and def. } \cap\text{⟆} \\
&= \{\boldsymbol{\rho} \in \mathbf{P}^\nu \mid \boldsymbol{\rho}(\vartheta_0(\alpha)) = \boldsymbol{\rho}(\boldsymbol{\tau}_2) \wedge \forall \beta \in \mathbb{V}_t \,.\, \boldsymbol{\rho}(\beta) = \boldsymbol{\rho}(\vartheta_0(\beta))\} \\
&\qquad\qquad \text{⟅} \alpha \in \mathsf{dom}(\vartheta_0) \text{ so } \boldsymbol{\rho}(\alpha) = \boldsymbol{\rho}(\vartheta_0(\beta)) = \boldsymbol{\rho}(\boldsymbol{\tau}_2)\text{⟆} \\
&= \gamma_{\mathsf{e}}(\vartheta_0(\alpha) \doteq \boldsymbol{\tau}_2) \cap \gamma_{\mathsf{s}}^{\mathsf{r}}(\vartheta_0) \qquad \text{⟅def. (48.51) of } \gamma_{\mathsf{e}}\text{, (48.52) of } \gamma_{\mathsf{s}}^{\mathsf{r}}\text{, and def. } \cap\text{⟆} \\
&= \gamma_{\mathsf{s}}^{\mathsf{r}}(\mathsf{unify}(\vartheta_0(\alpha), \boldsymbol{\tau}_2, \vartheta_0)) \qquad \text{⟅ind. hyp. of Lemma 48.63⟆} \\
&= \gamma_{\mathsf{s}}^{\mathsf{r}}(\mathsf{unify}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \vartheta_0)) \qquad \text{⟅(48.47.12)⟆}
\end{aligned}
$$

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

□

The following Lemma **??** 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

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

□

**Proof of Lemma ??** 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) since $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0 \in \mathbf{T}^\nu$ by hypothesis and $T_0 = \varnothing \in \mathbb{V}_t \pfun \mathbf{T}^\nu \times \mathbf{T}^\nu$;

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

- In case (48.68.5), $\boldsymbol{\tau}_j \in \mathbf{T}^\nu$ by hypothesis on the intermediate call, so $\boldsymbol{\tau}_j^i \in \mathbf{T}^\nu$, $i = 1, \ldots, n$, $j = 1, 2$, by the test (48.68.1). Then we proceed by recurrence on the recursive calls.
  - For the basis $i = 0$, $T_0$ satisfies (48.39) by hypothesis on the intermediate call;
  - Assume, by recurrence hypothesis for $i \in [0, n[$, that $T_i \in \mathbb{V}_t \pfun \mathbf{T}^\nu \times \mathbf{T}^\nu \wedge \forall \alpha \in \mathsf{dom}(T_0)\ .\ T_0(\alpha) = T_i(\alpha)$. Then, by induction on the sequence of calls to lub, $\boldsymbol{\tau}^{i+1} \in \mathbf{T}^\nu$ and $T_{i+1} \in \mathbb{V}_t \pfun \mathbf{T}^\nu \times \mathbf{T}^\nu \wedge \mathbb{vars}[\![\boldsymbol{\tau}^{i+1}]\!] \subseteq \mathsf{dom}(T_{i+1}) \wedge \forall \alpha \in \mathsf{dom}(T_i)\ .\ T_i(\alpha) = T_{i+1}(\alpha)$. By transitivity, $\forall \alpha \in \mathsf{dom}(T_0)\ .\ T_0(\alpha) = T_{i+1}(\alpha)$. □

  By recurrence for $i = n$, $T' = T_n$ at (48.68.5) satisfies (48.39) since $\boldsymbol{\tau}^i \in \mathbf{T}^\nu$, $i = 1, \ldots, n$, implies $f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n) \in \mathbf{T}^\nu$ and $\mathbb{vars}[\![f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)]\!] = \bigcup_{i=1}^n \mathbb{vars}[\![\boldsymbol{\tau}^i]\!]$;
- The case (48.68.7) is trivial since $\beta \in \mathbf{T}^\nu$, $T' = T_0$, and $\beta \in \mathsf{dom}(T_0)$;
- In case (48.68.9), $T_0 \in \mathbb{V}_t \pfun \mathbf{T}^\nu \times \mathbf{T}^\nu$ by hypothesis, $\beta \in \mathbf{T}^\nu$, and $\beta \in \mathbb{V}_t \setminus \mathsf{dom}(T_0)$ by the test (48.68.8) so $T' = \langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle [\beta \leftarrow T_0] \in \mathbb{V}_t \pfun \mathbf{T}^\nu \times \mathbf{T}^\nu$ 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 **??** 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 $T \in \mathbb{V}_t \pfun \mathbf{T}^\nu \times \mathbf{T}^\nu$, 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 **??** 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 $T_0 \in \wp(\mathbb{V}_\sharp \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, 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

$$\overline{\varsigma}_1(T')\boldsymbol{\tau} \quad = \quad \boldsymbol{\tau}_1 \quad \text{and} \quad \overline{\varsigma}_2(T')\boldsymbol{\tau} \quad = \quad \boldsymbol{\tau}_2 \qquad (??)$$ □

**Proof of Lemma ??** The preinvariant is $\mathtt{tt}$. 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 $\overline{\varsigma}_1(T_i)\boldsymbol{\tau}^i = \boldsymbol{\tau}_1^i$ and $\overline{\varsigma}_2(T_i)\boldsymbol{\tau}^i = \boldsymbol{\tau}_2^i$ 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 (??) that $\forall \alpha \in \mathsf{vars}[\![\boldsymbol{\tau}^i]\!] \subseteq \mathsf{dom}(T_i)\ .\ T_i(\alpha) = T_{i+1}(\alpha)$. Therefore, by (??), $\forall \alpha \in \mathsf{vars}[\![\boldsymbol{\tau}^i]\!]\ .\ \vartheta_j(T_{i+1})(\boldsymbol{\tau}^i) = \vartheta_j(T_i)(\boldsymbol{\tau}^i)$. It follows by (48.30) that $\vartheta_j(T_n)(f(\boldsymbol{\tau}^1, \boldsymbol{\tau}^2, \ldots, \boldsymbol{\tau}^n)) = f(\vartheta_j(T_n)(\boldsymbol{\tau}^1), \vartheta_j(T_n)(\boldsymbol{\tau}^2), \ldots, \vartheta_j(T_n)(\boldsymbol{\tau}^n)) = f(\vartheta_j(T_1)(\boldsymbol{\tau}^1), \vartheta_j(T_2)(\boldsymbol{\tau}^2), \ldots, \vartheta_j(T_n)(\boldsymbol{\tau}^n)) = f(\boldsymbol{\tau}_j^1, \ldots, \boldsymbol{\tau}_j^n) = \boldsymbol{\tau}_j$, $j = 1, 2$;
- In case (48.68.7), (??) 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 (??);
- In case (48.68.9), $\overline{\varsigma}_j(T')\boldsymbol{\tau} = \vartheta_j(\langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])\beta = \mathsf{if}\ \beta \in \mathsf{dom}(T)\ \mathsf{then\ let}\ \langle \boldsymbol{\tau}_1',\ \boldsymbol{\tau}_2' \rangle = \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0](\beta)\ \mathsf{in}\ \boldsymbol{\tau}_j'\ \mathsf{else}\ \alpha = \boldsymbol{\tau}_j$, $j = 1, 2$. □

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

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

**Proof of Lemma ??** 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 ?? follows by def. of the infimum $\overline{\varnothing}^\nu$ in cases (48.68.11).

Otherwise, at (48.68.12), $\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2) = \boldsymbol{\tau}$ where $\langle \boldsymbol{\tau},\ T \rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \varnothing)$. By (48.42), $\overline{\varsigma}_j(T)\boldsymbol{\tau} = \boldsymbol{\tau}_j$, $j = 1, 2$. So by Exercise 48.16, $[\boldsymbol{\tau}_j]_{\simeq^\nu} \preceq_{\simeq^\nu} [\boldsymbol{\tau}]_{\simeq^\nu} = [\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)]_{\simeq^\nu}$. □

Let $[\boldsymbol{\tau}']_{\simeq^\nu}$ be an upper bound of $[\boldsymbol{\tau}_1]_{\simeq^\nu}$ and $[\boldsymbol{\tau}_2]_{\simeq^\nu}$ i.e. $\boldsymbol{\tau}_1 \preceq_{\simeq^\nu} \boldsymbol{\tau}'$ and $\boldsymbol{\tau}_2 \preceq_{\simeq^\nu} \boldsymbol{\tau}'$ so that, by Theorem 48.31, there exists substitutions $\vartheta_1$ and $\vartheta_2$ 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 $\vartheta'$ such that $\vartheta'(\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)) = \boldsymbol{\tau}'$.

We modify the lub algorithm into $\mathsf{lub}'$ (which calls lub) as given in Figure ?? to construct this substitution $\vartheta'$ given any upper bound $\boldsymbol{\tau}'$.

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

**Example 20** For $\boldsymbol{\tau}_1 = f(g(a), g(g(a)), g(a), b, b)$, $\boldsymbol{\tau}_2 = f(g(b), g(h(b)), g(b), a, a)$ and $\boldsymbol{\tau}' = f(g(\alpha), \beta, g(\alpha), \gamma, U)$, we have

$\mathsf{lub}'(f(g(a), g(g(a)), g(a), b, b), f(g(b), g(h(b)), g(b), a, a), \varnothing, f(g(\alpha), \beta, g(\alpha), \gamma, U), \boldsymbol{\varepsilon})$
$\quad \mathsf{lub}'(g(a), g(b), \varnothing, g(\alpha), \boldsymbol{\varepsilon})$ (??.??)
$\quad\quad \mathsf{lub}'(a, b, \varnothing, \alpha, \boldsymbol{\varepsilon})$ (??.??)
$\quad\quad = \langle \beta, \{\langle \beta, \langle a, b\rangle\rangle\}, \{\langle \alpha, \beta\rangle\}\rangle$ (??.??)
$\quad = \langle g(\beta), \{\langle \beta, \langle a, b\rangle\rangle\}, \{\langle \alpha, \beta\rangle\}\rangle$ (??.??)
$\quad \mathsf{lub}'(g(g(a)), g(h(b)), \{\langle \beta, \langle a, b\rangle\rangle\}, \beta, \{\langle \alpha, \beta\rangle\})$ (??.??)
$\quad\quad \mathsf{lub}(g(a), h(b), \{\langle \beta, \langle a, b\rangle\rangle\})$ (??.??)
$\quad\quad = \langle \gamma, \{\langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}\rangle$
$\quad = \langle g(\gamma), \{\langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}, \{\langle \alpha, \beta\rangle, \langle \beta, g(\gamma)\rangle\}\rangle$ (??.??)
$\quad \mathsf{lub}'(g(a), g(b), \{\langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}, g(\alpha), \{\langle \alpha, \beta\rangle, \langle \beta, g(\gamma)\rangle\})$ (??.??)
$\quad\quad \mathsf{lub}'(a, b, \{\langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}, \alpha, \{\langle \alpha, \beta\rangle, \langle \beta, g(\gamma)\rangle\})$ (??.??)
$\quad\quad = \langle \beta, \{\langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}, \{\langle \alpha, \beta\rangle, \langle \beta, g(\gamma)\rangle\}\rangle$ (??.??)
$\quad = \langle g(\beta), \{\langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}, \{\langle \alpha, \beta\rangle, \langle \beta, g(\gamma)\rangle\}\rangle$ (??.??)
$\quad \mathsf{lub}'(b, a, \{\langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}, \gamma, \{\langle \alpha, \beta\rangle, \langle \beta, g(\gamma)\rangle\})$ (??.??)
$\quad = \langle \alpha, \{\langle \alpha, \langle b, a\rangle\rangle, \langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}, \{\langle \alpha, \beta\rangle, \langle \beta, g(\gamma)\rangle, \langle \gamma, \alpha\rangle\}\rangle$ (??.??)
$\quad\quad \mathsf{lub}'(b, a, \{\{\langle \alpha, \langle b, a\rangle\rangle, \langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}, U, \{\langle \alpha, \beta\rangle, \langle \beta, g(\gamma)\rangle, \langle \gamma, \alpha\rangle\})$ (??.??)
$\quad = \langle \alpha, \{\{\langle \alpha, \langle b, a\rangle\rangle, \langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}, \{\langle \alpha, \beta\rangle, \langle \beta, g(\gamma)\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle, \langle U, \alpha\rangle\}\rangle$
$= \langle f(g(\beta), g(\gamma), g(\beta), \alpha, \alpha), \{\langle \alpha, \langle b, a\rangle\rangle, \langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}, \{\langle \alpha, \beta\rangle, \langle \beta, g(\gamma)\rangle, \langle \gamma, \alpha\rangle, \langle U, \alpha\rangle\}\rangle$ (??.??)

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. $\overline{\varsigma}_1(T) = \overline{\varsigma}_1(\{\langle \alpha, \langle b, a\rangle\rangle, \langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}) = \{\langle \alpha, b\rangle, \langle \beta, a\rangle, \langle \gamma, g(a)\rangle\}$;
3. $\overline{\varsigma}_1(T)(\boldsymbol{\tau}) = \{\langle \alpha, b\rangle, \langle \beta, a\rangle, \langle \gamma, g(a)\rangle\}(f(g(\beta), g(\gamma), g(\beta), \alpha, \alpha)) = f(g(a), g(g(a)), g(a), b, b) = \boldsymbol{\tau}_1$;
4. $\overline{\varsigma}_2(T) = \overline{\varsigma}_2(\{\langle \alpha, \langle b, a\rangle\rangle, \langle \beta, \langle a, b\rangle\rangle, \langle \gamma, \langle g(a), h(b)\rangle\rangle\}) = \{\langle \alpha, a\rangle, \langle \beta, b\rangle, \langle \gamma, h(b)\rangle\}$;
5. $\overline{\varsigma}_2(T)(\boldsymbol{\tau}) = \{\langle \alpha, a\rangle, \langle \beta, b\rangle, \langle \gamma, h(b)\rangle\}(f(g(\beta), g(\gamma), g(\beta), \alpha, \alpha)) = f(g(b), g(h(b)), g(b), a, a) = \boldsymbol{\tau}_2$. □

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

**Lemma 21** For all $\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}, \boldsymbol{\tau}', \boldsymbol{\tau}'' \in \mathbf{T}^\nu, T_0, T, T'' \in \wp(\mathbb{V}_t \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta' \in \mathbb{V}_t \nrightarrow \mathbf{T}^\nu$, 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 ??** 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 $\vartheta_0$, the resulting substitution $\vartheta'$, ignoring the program point (??.??) and mapping (??.??), …, (??.??) and (??.??), …, (??.??) 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 $\vartheta_0$. An exception is the test (??.??) but the two alternative yield the same result. (??.??), …, (??.??) is identical to (48.68.2), …, (48.68.4) while, by induction on the sequence of calls to lub′ (??.??), …, (??.??) 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 (??.??). □

The following Lemma ?? proves the well-typing of algorithm lub′.

**Lemma 22** For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}' \in \mathbf{T}^\nu$, $T_0 \in \wp(\mathbb{V}_t \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2 \in \mathbb{V}_t \nrightarrow \mathbf{T}^\nu$, 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 $\vartheta_1(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_1^0 \wedge \vartheta_2(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_2^0$, then the case analysis in the definition of lub′ is complete (i.e., there is no missing case) and $\exists \gamma \in \mathbb{V}_t \,.\, \boldsymbol{\tau}' = \gamma$ at (??.??) and (??.??). □

**Proof of Lemma ??** Notice that Lemmata ??, ??, and ?? are valid for lub′ since they do not involve the extra parameters $\boldsymbol{\tau}', \vartheta_0$ or result $\vartheta'$. The proof is by case analysis.

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

□

The following Lemma ?? shows that variables recorded in $T_0$ are for non-matching 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 $T_0 \in \wp(\mathbb{V}_t \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, 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 $\boldsymbol{\tau}_1', {\boldsymbol{\tau}_1'}^1, \ldots, {\boldsymbol{\tau}_1'}^n, \boldsymbol{\tau}_2', {\boldsymbol{\tau}_2'}^1, \ldots, {\boldsymbol{\tau}_2'}^n \in \mathbf{T}^\nu$,

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

$$T_0(\beta) \neq \langle \boldsymbol{\tau}'_2,\ \boldsymbol{\tau}'_1 \rangle. \qquad \square$$

**Proof of Lemma ??** 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 **??** 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 (**??.??**) to (**??.??**) for $T_n$ returned at (**??.??**) as well as for the unmodified $T_0$ returned at (**??.??**). By induction, Lemma **??** holds for all calls from the main call (**??.??**). $\square$

**Lemma 24** For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}'_0, \boldsymbol{\tau}, \boldsymbol{\tau}' \in \mathbf{T}^\nu, T_0, T \in \mathbb{V}_t \rightharpoonup (\mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V}_t \rightharpoonup \mathbf{T}^\nu$, 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 ??** We prove the stronger property that the following preinvariant and postinvariant do hold for any call $\langle \boldsymbol{\tau},\ T,\ \vartheta' \rangle = \mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$.

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

The proof is by induction on the sequence of calls to $\mathsf{lub}'$ and, for any given call, by recurrence to handle the recursive calls at (**??.??**), (**??.??**),…, (**??.??**), and by case analysis for the conditional.

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

    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 $\mathsf{lub}'$, the postinvariant (**??**) holds for $T_i$ and $\vartheta_i$, which is the preinvariant of the next recursive call, if any.

    It follows, by recurrence, that the postinvariant of (**??**) holds at (**??.??**) for $T_n$ and $\vartheta_n$.

– In case (??.??), we know by the test (??.??) and Lemma ?? that $\exists \beta \in \mathsf{dom}(T_0)\ .\ T_0(\beta) = \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle \wedge \boldsymbol{\tau}' = \gamma$ so by the preinvariant $\gamma \in \mathsf{dom}(\vartheta_0)$ and $\vartheta_0(\gamma) = \beta$. Since $T = T_0$ and $\vartheta' = \vartheta_0$, we have $\gamma \in \mathsf{dom}(\vartheta') \wedge \vartheta'(\gamma) = \beta$;
– In case (??.??), $\vartheta' = \beta[\gamma \leftarrow \vartheta_0]$, which implies the postinvariant (??).

□

Let us prove the converse of Lemma ??.

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

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

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

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

The proof is by induction on the sequence of calls to $\mathsf{lub}'$ and, for any given call, by recurrence to handle the recursive calls at (??.??), (??.??),…, (??.??), and by case analysis for the conditional.

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

**Lemma 28** For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\mathrm{v}$, $T_0, T \in \wp(\mathcal{V}_\mathrm{t} \times \mathbf{T}^\mathrm{v} \times \mathbf{T}^\mathrm{v})$, and $\vartheta_0, \vartheta_1^0, \vartheta_2^0, \vartheta' \in \mathcal{V}_\mathrm{t} \nrightarrow \mathbf{T}^\mathrm{v}$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$ with hypothesis $\vartheta_1^0(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_1^0 \wedge \vartheta_2^0(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_2^0$ and returns $\langle \boldsymbol{\tau},\ T,\ \vartheta' \rangle$, then

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

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

**Proof of Lemma ??** The proof is by induction on the sequence of calls to $\mathsf{lub}'$ and, for any given call, by recurrence to handle the recursive calls at (**??.??**), (**??.??**),…, (**??.??**), and by case analysis for the conditional.

- For the first call at (**??.??**), $\vartheta_0 = \boldsymbol{\varepsilon}$ so $\mathsf{vars}[\![\vartheta_0(\mathcal{V}_\mathrm{t})]\!] = \mathsf{vars}[\![\varnothing]\!] = \varnothing \subseteq \mathsf{dom}(T_0)$;
- Otherwise the preinvariant of (**??**) holds for $T_0$ and $\vartheta_0$ at the first recursive call (**??.??**). Assume, by induction hypothesis, that $\mathsf{vars}[\![\vartheta_{i-1}(\mathcal{V}_\mathrm{t})]\!] \subseteq \mathsf{dom}(T_{i-1})$ before the $i^{\text{th}}$ call (**??.??**),…, (**??.??**), $i \in [1, n]$. By induction hypothesis on the sequence of calls to $\mathsf{lub}'$, we have $\mathsf{vars}[\![\vartheta_i(\mathcal{V}_\mathrm{t})]\!] \subseteq \mathsf{dom}(T_i)$ after that call, which is also the preinvariant of the next call, if any. By recurrence, $\mathsf{vars}[\![\vartheta'(\mathcal{V}_\mathrm{t})]\!] = \mathsf{vars}[\![\vartheta_n(\mathcal{V}_\mathrm{t})]\!] \subseteq \mathsf{dom}(T_n) = \mathsf{dom}(T)$ in case the call (**??**) to $\mathsf{lub}'$ terminates at (**??.??**);
- If $\mathsf{lub}'$ terminates at (**??.??**), there are two cases.
  - $\mathsf{vars}[\![\vartheta'(\{\gamma\})]\!] = \mathsf{vars}[\![f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\{\gamma\})]\!] = \mathsf{vars}[\![f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)]\!] = \bigcup_{i=1}^n \mathsf{vars}[\![\boldsymbol{\tau}^i]\!]$. By Lemma **??** and **??**, we have $\mathsf{vars}[\![\boldsymbol{\tau}^i]\!] \subseteq \mathsf{dom}(T_i)$, $i = 1, \ldots, n$ and $\mathsf{dom}(T_i) \subseteq \mathsf{dom}(T_n)$ so that $\bigcup_{i=1}^n \mathsf{vars}[\![\boldsymbol{\tau}^i]\!] \subseteq \bigcup_{i-1}^n \mathsf{dom}(T_i) \subseteq \mathsf{dom}(T_n) = \mathsf{dom}(T)$;
  - $\mathsf{vars}[\![\vartheta'(\mathcal{V}_\mathrm{t} \backslash \{\gamma\})]\!] = \mathsf{vars}[\![f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\mathcal{V}_\mathrm{t} \backslash \{\gamma\})]\!] = \mathsf{vars}[\![\vartheta_0(\mathcal{V}_\mathrm{t} \backslash \{\gamma\})]\!] \subseteq \mathsf{vars}[\![\vartheta_0(\mathcal{V}_\mathrm{t})]\!]$ which, by the preinvariant (**??**), is included in $\mathsf{dom}(T_0)$. By Lemma **??** and **??**, $\mathsf{dom}(T_{i=1}) \subseteq \mathsf{dom}(T_i)$, $i = 1, \ldots, n$ so that, by transitivity, $\mathsf{dom}(T_0) \subseteq \mathsf{dom}(T_n) = \mathsf{dom}(T)$. Therefore $\mathsf{vars}[\![\vartheta'(\mathcal{V}_\mathrm{t} \setminus \{\gamma\})]\!] \subseteq \mathsf{dom}(T)$;
  - Since $\vartheta'(\mathcal{V}_\mathrm{t}) = \vartheta'(\{\gamma\}) \cup \vartheta'(\mathcal{V}_\mathrm{t} \setminus \{\gamma\})$, we conclude that $\mathsf{vars}[\![\vartheta'(\mathcal{V}_\mathrm{t})]\!] = \mathsf{vars}[\![\vartheta'(\{\gamma\}) \cup \vartheta'(\mathcal{V}_\mathrm{t} \setminus \{\gamma\})]\!] = \mathsf{vars}[\![\vartheta'(\{\gamma\})]\!] \cup \mathsf{vars}[\![\vartheta'(\mathcal{V}_\mathrm{t} \setminus \{\gamma\})]\!] \subseteq \mathsf{dom}(\vartheta') \cup \mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta')$;
- If $\mathsf{lub}'$ terminates at (**??.??**) then the postinvariant directly follows from the preinvariant of (**??**) since $T = T_0$ and $\vartheta' = \vartheta_0$;
- Finally, if $\mathsf{lub}'$ terminates at (**??.??**), there are two subcases.
  - We have $\mathsf{vars}[\![\vartheta'(\{\gamma\})]\!] = \mathsf{vars}[\![\beta[\gamma \leftarrow \vartheta_0](\{\gamma\})]\!] = \mathsf{vars}[\![\{\beta\}]\!] = \{\beta\} \subseteq \mathsf{dom}(\langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0]) = \mathsf{dom}(T)$;

– Moreover $\mathsf{vars}[\![\vartheta'(\mathcal{V}_t \setminus \{\gamma\})]\!] = \mathsf{vars}[\![\beta[\gamma \leftarrow \vartheta_0](\mathcal{V}_t \setminus \{\gamma\})]\!] = \mathsf{vars}[\![\vartheta_0(\mathcal{V}_t \setminus \{\gamma\})]\!] \subseteq \mathsf{vars}[\![\vartheta_0(\mathcal{V}_t)]\!] \subseteq \mathsf{dom}(T_0)$, by the preinvariant of (??). But $\mathsf{dom}(T_0) \subseteq \mathsf{dom}(T_0) \cup \{\beta\} = \mathsf{dom}(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0]) = \mathsf{dom}(T)$, proving the postinvariant of vars-codom-substitution0 by transitivity;

– We conclude since vars preserves joins. □

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

**Lemma 30** For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}' \in \mathbf{T}^\nu, T_0, T \in \wp(\mathcal{V}_t \times \mathbf{T}^\nu \times \mathbf{T}^\nu)$, and $\vartheta_0, \vartheta_1^0, \vartheta_2^0, \vartheta' \in \mathcal{V}_t \nrightarrow \mathbf{T}^\nu$, 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

$$\vartheta_1^0(\boldsymbol{\tau}') = \boldsymbol{\tau}_1 \wedge \vartheta_2^0(\boldsymbol{\tau}') = \boldsymbol{\tau}_2. \qquad (??) \quad \square$$

**Proof of Lemma ??** For the first call at (??.??), (??) 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 (??). Then (??) holds before the recursive calls (??.??), …, (??.??) since the induction hypothesis $\vartheta_j^0(\boldsymbol{\tau}') = \boldsymbol{\tau}_j$, $\boldsymbol{\tau}' = f(\boldsymbol{\tau}_1', \ldots, \boldsymbol{\tau}_n')$ by the test (??.??) which is false, $\boldsymbol{\tau}_j = f(\boldsymbol{\tau}_j^1, \ldots, \boldsymbol{\tau}_j^n)$ by the test (??.??) which is true, and (48.30) imply that $\vartheta_j^0(\boldsymbol{\tau}') = \vartheta_j^0(f(\boldsymbol{\tau}_1', \ldots, \boldsymbol{\tau}_n')) = f(\vartheta_j^0(\boldsymbol{\tau}_1'), \ldots, \vartheta_j^0(\boldsymbol{\tau}_n')) = f(\boldsymbol{\tau}_j^1, \ldots, \boldsymbol{\tau}_j^n) = \boldsymbol{\tau}_j$ and therefore $\vartheta_j^0(\boldsymbol{\tau}_i') = \boldsymbol{\tau}_j^i$, $j = 1, \ldots, n$. We conclude by induction on the sequence of calls to lub′. □

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

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

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

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

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

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

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

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

- In case (**??.??**), we have $T = T_n$ and $\vartheta_n$ which satisfy the postinvariant of (**??**), as shown above.
- In case (**??.??**), the postinvariant is $\forall j = 1,2 \;.\; \forall \alpha \in \mathsf{dom}(f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0]) \;.\; \vartheta^0_j(\alpha) = \overline{\varsigma}_j(T_n)(f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\alpha))$.
  - If $\alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\}$, we must show that $\vartheta^0_j(\alpha) = \overline{\varsigma}_j(T_n)(\vartheta_0(\alpha))$.
    By Lemma **??**, $\forall \alpha \in \mathsf{dom}(T_{i-1}) \;.\; T_{i-1}(\alpha) = T_i(\alpha)$, $i = 1, \ldots, n$ so that, by transitivity, $\forall \alpha \in \mathsf{dom}(T_0) \;.\; T_0(\alpha) = T_n(\alpha)$. Therefore, by (**??**), for all $\beta \in \mathsf{dom}(T_0)$, $\overline{\varsigma}_j(T_0)\beta \triangleq \mathsf{let}\ \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle = T_0(\beta)\ \mathsf{in}\ \boldsymbol{\tau}_j = \mathsf{let}\ \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle = T_n(\beta)\ \mathsf{in}\ \boldsymbol{\tau}_j = \overline{\varsigma}_j(T_n)\beta$. By Lemma **??**, $\mathsf{vars}[\![\vartheta_0(\mathbb{V}_{\mathbb{t}})]\!] \subseteq \mathsf{dom}(T_0)$ so, in particular, $\forall \alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\} \;.\; \mathsf{vars}[\![\vartheta_0(\alpha)]\!] \subseteq \mathsf{dom}(T_0)$. This implies that $\forall \alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\} \;.\; \forall \beta \in \mathsf{vars}[\![\vartheta_0(\alpha)]\!] \;.\; \overline{\varsigma}_j(T_0)\beta = \overline{\varsigma}_j(T_n)\beta$. By (48.30) and (48.30), we infer that $\forall \alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\} \;.\; \overline{\varsigma}_j(T_0)\boxtimes_0(\boxtimes) = \overline{\varsigma}_j(T_n)\boxtimes_0(\boxtimes)$. By the preinvariant of (**??**), we have $\forall \alpha \in \mathsf{dom}(\vartheta_0) \;.\; \vartheta^0_j(\alpha) = \overline{\varsigma}_j(T_0)(\vartheta_0(\alpha))$. Therefore, by transitivity, $\vartheta^0_j(\alpha) = \overline{\varsigma}_j(T_n)(\vartheta_0(\alpha))$.
  - Otherwise $\alpha = \gamma$, in which case we must show that $\vartheta^0_j(\gamma) = \overline{\varsigma}_j(T_n)(f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n))$. By Lemma **??**, (48.42) of Lemma 48.40, and (**??.??**), we have $\vartheta^0_j(\gamma) = \vartheta^0_j(\boldsymbol{\tau}') = \boldsymbol{\tau}_j = \overline{\varsigma}_j(T)(\boldsymbol{\tau}) = \overline{\varsigma}_j(T)(f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n))$.
- In case (**??.??**), the postinvariant of (**??**) immediately follows from the preinvariant since $T = T_0$ and $\vartheta' = \vartheta_0$;
- In case (**??.??**), we must show that $\forall j = 1,2 \;.\; \forall \alpha \in \mathsf{dom}(\beta[\gamma \leftarrow \vartheta_0]) \;.\; \vartheta^0_j(\alpha) = \overline{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])(\beta[\gamma \leftarrow \vartheta_0](\alpha))$. There are two cases.
  - If $\alpha = \gamma$ then we must prove that $\vartheta^0_j(\gamma) = \overline{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])(\beta)$, that is, by (**??**), $\vartheta^0_j(\gamma) = \boldsymbol{\tau}_j$. It is not possible that $\gamma \in \mathsf{dom}(\vartheta_0)$ since otherwise, we would have $\forall \beta \in \mathsf{dom}(T_0) \;.\; T_0(\beta) \neq \langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle$ since the test (**??.??**) is $\mathsf{ff}$ and $\boldsymbol{\tau}' = \gamma \in \mathbb{V}_{\mathbb{t}}$ by Lemma **??**, which is in contradiction with (the contrapositive of) Lemma **??**. Therefore $\vartheta_0(\gamma) = \gamma$ by (48.30). It follows that we have to prove that $\vartheta^0_j(\vartheta_0(\gamma)) = \boldsymbol{\tau}_j$, which directly follows from the preinvariant of (**??**);
  - Otherwise, $\alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\}$ and we must show that $\vartheta^0_j(\alpha) = \overline{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])(\vartheta_0(\alpha))$. The test (**??.??**) implies $\beta \notin \mathsf{dom}(T_0)$ and so $\beta \notin \mathsf{vars}[\![\vartheta_0(\alpha)]\!]$ since $\mathsf{vars}[\![\vartheta_0(\mathbb{V}_{\mathbb{t}})]\!] \subseteq \mathsf{dom}(T_0)$ by (**??**) of Lemma **??**. Therefore, by (**??**), $\forall \gamma \in \mathsf{vars}[\![\vartheta_0(\alpha)]\!] \;.\; \overline{\varsigma}_j(T_0)(\gamma) = \overline{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2 \rangle[\beta \leftarrow T_0])(\gamma)$. It follows, by (48.30) and (48.30), that $\overline{\varsigma}_j(T_0)(\vartheta_0(\alpha)) = \overline{\varsigma}_j(\langle \boldsymbol{\tau}_1,$

$\boldsymbol{\tau}_2\rangle[\beta \leftarrow T_0])(\vartheta_0(\alpha))$. We conclude, by the preinvariant (??) and transitivity that $\overline{\varsigma}_j(\langle \boldsymbol{\tau}_1, \boldsymbol{\tau}_2\rangle[\beta \leftarrow T_0])(\vartheta_0(\alpha)) = \vartheta_j^0(\alpha)$. □

**Lemma 34** For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^v$, $T_0, T \in \wp(\mathbb{V}_t \times \mathbf{T}^v \times \mathbf{T}^v)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V}_t \nrightarrow \mathbf{T}^v$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$ 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.

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

**Proof of Lemma ??** The proof of (??) is by induction on the sequence of calls to $\mathsf{lub}'$ and, for any given call, by recurrence to handle the recursive calls at (??.??), (??.??),…, (??.??), 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 (??.??), we have $\mathsf{dom}(\vartheta') = \mathsf{dom}(f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0]) = \mathsf{dom}(\vartheta_0) \cup \{\gamma\} = \mathsf{dom}(\vartheta_0) \cup \mathbb{vars}[\![\boldsymbol{\tau}']\!]$ since $\vartheta' = \gamma$ by the test (??.??);
- In case (??.??), we have $\mathsf{dom}(\vartheta_i) = \mathsf{dom}(\vartheta_{i-1}) \cup \mathbb{vars}[\![\boldsymbol{\tau}^i]\!]$, $i = 1, \dots, n$, by induction hypothesis on the sequence of calls to $\mathsf{lub}'$. It follows that $\mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta_n) = \mathsf{dom}(\vartheta_0) \cup \bigcup_{i=1}^n \mathbb{vars}[\![\boldsymbol{\tau}^i]\!] = \mathsf{dom}(\vartheta_0) \cup \mathbb{vars}[\![f(\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^n)]\!] = \mathsf{dom}(\vartheta_0) \cup \mathbb{vars}[\![\boldsymbol{\tau}']\!]$;
- In case (??.??), we have $\vartheta' = \beta[\gamma \leftarrow \vartheta_0]$ so $\mathsf{dom}(\vartheta') = \mathsf{dom}(\vartheta_0) \cup \{\gamma\} = \mathsf{dom}(\vartheta_0) \cup \mathbb{vars}[\![\boldsymbol{\tau}']\!]$ since $\boldsymbol{\tau}' = \gamma$ by Lemma ??;
- Finally, in case (??.??), $\mathsf{dom}(\vartheta') = \mathsf{dom}(\beta[\gamma \leftarrow \vartheta_0]) = \mathsf{dom}(\vartheta_0) \cup \{\gamma\} = \mathsf{dom}(\vartheta_0) \cup \mathbb{vars}[\![\boldsymbol{\tau}']\!]$ since $\boldsymbol{\tau}' = \gamma$ by Lemma ??. □

**Lemma 36** For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}'^0, \boldsymbol{\tau}^{n-1}, \boldsymbol{\tau}^n, \boldsymbol{\tau}^{m-1}.\boldsymbol{\tau}^m \in \mathbf{T}^v$, $T_n, T_m \in \wp(\mathbb{V}_t \times \mathbf{T}^v \times \mathbf{T}^v)$, 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 (??.??) 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 ??, this also holds for calls to $\mathsf{lub}'$ independently of the other two parameters. □

**Proof of Lemma ??** By (??) in Lemma ??, Lemma ??, (??.??), …, (??.??), and (??.??), …, (??.??) and recurrence, the successive calls of $\mathsf{lub}$ and $\mathsf{lub}'$ 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 **??**, the reasoning is the same for $\mathsf{lub}'$). The only possible executions are the following.

- If one execution follows the true branch of (48.68.1), so does the other since they have the same parameters. By recurrence and induction on the sequence of calls for (48.68.2), …, (48.68.4) with $\forall \alpha \in \mathsf{dom}(T_{i-1})\ .\ T_{i-1}(\alpha) = T_i(\alpha)$, $i = 1, \ldots, n$, we have $\boldsymbol{\tau}^k = f(\boldsymbol{\tau}^{1\,k}, \ldots, \boldsymbol{\tau}^{n\,k}) = f(\boldsymbol{\tau}^{1\,m}, \ldots, \boldsymbol{\tau}^{n\,m}) = \boldsymbol{\tau}^m$;
- If both calls go through (48.68.7) then obviously $\boldsymbol{\tau}^k = \boldsymbol{\tau}^m = \beta$;
- Both calls cannot go through (48.68.9) since the first ones (which is $\langle \boldsymbol{\tau}^k, T_k \rangle = \mathsf{lub}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_{k-1})$) that goes through (48.68.9) will add $\beta$ 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) since $\mathsf{dom}(T_k) \subseteq \mathsf{dom}(T_{m-1})$ with $\beta \in \mathsf{dom}(T_{m-1})$ so that $\boldsymbol{\tau}^k = \boldsymbol{\tau}^m = \beta$. □

**Lemma 37** For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^v$, $T_0, T \in \wp(\mathbb{V}_{\mathbb{t}} \times \mathbf{T}^v \times \mathbf{T}^v)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V}_{\mathbb{t}} \rightarrow\!\!\!\!\!\!+\ \mathbf{T}^v$, if $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0)$ is (recursively) called from the main call $\mathsf{lub}'(\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \varnothing, \boldsymbol{\tau}_0', \boldsymbol{\varepsilon})$ with hypothesis $\vartheta_1(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_1^0 \wedge \vartheta_2(\boldsymbol{\tau}_0') = \boldsymbol{\tau}_2^0$ and returns $\langle \boldsymbol{\tau},\ T,\ \vartheta' \rangle$, then the following postinvariant holds after the call.

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

**Proof of Lemma ??** The proof of (**??**) is by induction on the sequence of calls to $\mathsf{lub}'$ and, for any given call, by recurrence to handle the recursive calls at (**??.??**), (**??.??**),…, (**??.??**), 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 (**??.??**), we have $\forall \alpha \in \mathsf{dom}(\vartheta_0) \setminus \{\gamma\}\ .\ \vartheta_0(\alpha) = f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\alpha) = \vartheta'(\alpha)$.

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

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

**Lemma 39** For all $\boldsymbol{\tau}_1^0, \boldsymbol{\tau}_2^0, \boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \boldsymbol{\tau}_0', \boldsymbol{\tau}', \boldsymbol{\tau} \in \mathbf{T}^\vee$, $T_0, T \in \wp(\mathbb{V}_{\mathbb{t}} \times \mathbf{T}^\vee \times \mathbf{T}^\vee)$, and $\vartheta_0, \vartheta_1, \vartheta_2, \vartheta' \in \mathbb{V}_{\mathbb{t}} \nrightarrow \mathbf{T}^\vee$, 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.

$$\vartheta'(\boldsymbol{\tau}') = \boldsymbol{\tau} \qquad (??)$$ □

**Proof of Lemma ??** The proof of (??) is by induction on the sequence of calls to $\mathsf{lub}'$ and, for any given call, by recurrence to handle the recursive calls at (??.??), (??.??),…, (??.??), 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 (??.??), we have $\vartheta'(\boldsymbol{\tau}') = f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n)[\gamma \leftarrow \vartheta_0](\gamma) = f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n) = \boldsymbol{\tau}$;
- In case (??.??), we handle (??.??), …, (??.??) by recurrence.
  - For the basis at (??.??), we have $\mathsf{dom}(\vartheta_1) = \mathsf{dom}(\vartheta_0) \cup \mathbb{vars}[\![\boldsymbol{\tau}_1']\!]$ by (??) of Lemma ??, and $\vartheta_1(\boldsymbol{\tau}_1') = \boldsymbol{\tau}^1$, by induction on the sequence of calls to $\mathsf{lub}'$;
  - Assume, by recurrence hypothesis, that for the $i^{\text{th}}$ call (??.??), …, (??.??), $i \in [1, n[$, we have

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

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

2. By (??) of Lemma ??, we have $\forall \alpha \in \mathsf{dom}(\vartheta_i)\ .\ \vartheta_i(\alpha) = \vartheta_{i+1}(\alpha)$ so that by recurrence hyp. (??), $\forall j \in [1, i+1]\ .\ \forall \alpha \in \mathsf{dom}(\vartheta_j)\ .\ \vartheta_{i+1}(\alpha) = \vartheta_i(\alpha) = \vartheta_j(\alpha)$
3. By (??)., $\forall j \in [1, i+1]\ .\ \mathsf{vars}[\![\boldsymbol{\tau}'_j]\!] \subseteq \mathsf{dom}(\vartheta_j) \subseteq \mathsf{dom}(\vartheta_{i+1})$ and by (??)., $\forall \alpha \in \mathsf{dom}(\vartheta_j)\ .\ \vartheta_{i+1}(\alpha) = \vartheta_j(\alpha)$ 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 $\mathsf{lub}'$. 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, (??) 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 (??.??), 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 ??, 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 (??.??), by (??.??) and Lemma ??, we have $\vartheta'(\boldsymbol{\tau}') = \beta[\gamma \leftarrow \vartheta_0](\gamma) = \beta = \boldsymbol{\tau}$. □

**Proof of Theorem 48.72** By Lemma ??, $[\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)]_{\simeq^\nu}$ is a $\preceq_{\simeq^\nu}$-upper-bound of $[\boldsymbol{\tau}_1]_{\simeq^\nu}$ and $[\boldsymbol{\tau}_2]_{\simeq^\nu}$. By Lemma ??, so is $[\mathsf{lgc}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)]_{\simeq^\nu}$.

Now if $[\boldsymbol{\tau}']_{\simeq^\nu}$ is any $\preceq_{\simeq^\nu}$-upper-bound of $[\boldsymbol{\tau}_1]_{\simeq^\nu}$ and $[\boldsymbol{\tau}_2]_{\simeq^\nu}$ then by Exercise 48.16, $\exists \vartheta_1, \vartheta_2\ .\ \vartheta_1(\boldsymbol{\tau}') = \boldsymbol{\tau}_1 \wedge \vartheta_2(\boldsymbol{\tau}') = \boldsymbol{\tau}_2$, which is the precondition (??.??). It follows that the call to $\mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \varnothing, \boldsymbol{\tau}', \boldsymbol{\varepsilon}, \varnothing)$ terminates (by Lemma ?? and ??) 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 (??) of Lemma ??). By Exercise 48.16, this means that $\mathsf{lgc}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2) \preceq_{\simeq^\nu} [\boldsymbol{\tau}']_{\simeq^\nu}$. This proves by Lemma ?? that $\mathsf{lgc}(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2)$ is the $\preceq_{\simeq^\nu}$-least upper-bound of $[\boldsymbol{\tau}_1]_{\simeq^\nu}$ and $[\boldsymbol{\tau}_2]_{\simeq^\nu}$. □

$$
\begin{array}{l}
\mathsf{let\ rec\ lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, T_0, \boldsymbol{\tau}', \vartheta_0) = \qquad (17)\\
\quad \mathsf{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)\ \mathsf{then} \qquad (??)\\
\quad\quad \mathsf{if}\ \boldsymbol{\tau}' = \gamma \in \mathbb{V}_{\mathbb{t}}\ \mathsf{then} \qquad (??)\\
\quad\quad\quad \mathsf{let}\ \langle \boldsymbol{\tau}^1,\ T_1 \rangle = \mathsf{lub}(\boldsymbol{\tau}_1^1, \boldsymbol{\tau}_2^1, T_0)\ \mathsf{in} \qquad (??)\\
\quad\quad\quad\quad \mathsf{let}\ \langle \boldsymbol{\tau}^2,\ T_2 \rangle = \mathsf{lub}(\boldsymbol{\tau}_1^2, \boldsymbol{\tau}_2^2, T_1)\ \mathsf{in} \qquad (??)\\
\quad\quad\quad\quad\quad \ldots \qquad \ldots\\
\quad\quad\quad\quad\quad\quad \mathsf{let}\ \langle \boldsymbol{\tau}^n,\ T_n \rangle = \mathsf{lub}(\boldsymbol{\tau}_1^n, \boldsymbol{\tau}_2^n, T_{n-1})\ \mathsf{in} \qquad (??)\\
\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 \qquad (??)\\
\quad\quad \mathsf{else}\ /^*\ \boldsymbol{\tau}' = f(\boldsymbol{\tau}_1', \ldots, \boldsymbol{\tau}_n')\ ^*/ \qquad (??)\\
\quad\quad\quad \mathsf{let}\ \langle \boldsymbol{\tau}^1,\ T_1,\ \vartheta_1 \rangle = \mathsf{lub}'(\boldsymbol{\tau}_1^1, \boldsymbol{\tau}_2^1, T_0, \boldsymbol{\tau}_1', \vartheta_0)\ \mathsf{in} \qquad (??)\\
\quad\quad\quad\quad \mathsf{let}\ \langle \boldsymbol{\tau}^2,\ T_2,\ \vartheta_2 \rangle = \mathsf{lub}'(\boldsymbol{\tau}_1^2, \boldsymbol{\tau}_2^2, T_1, \boldsymbol{\tau}_2', \vartheta_1)\ \mathsf{in} \qquad (??)\\
\quad\quad\quad\quad\quad \ldots \qquad \ldots\\
\quad\quad\quad\quad\quad\quad \mathsf{let}\ \langle \boldsymbol{\tau}^n,\ T_n,\ \vartheta_n \rangle = \mathsf{lub}'(\boldsymbol{\tau}_1^n, \boldsymbol{\tau}_2^n, T_{n-1}, \boldsymbol{\tau}_n', \vartheta_{n-1})\ \mathsf{in} \qquad (??)\\
\quad\quad\quad\quad\quad\quad\quad \langle f(\boldsymbol{\tau}^1, \ldots, \boldsymbol{\tau}^n),\ T_n,\ \vartheta_n \rangle \qquad (??)\\
\quad\quad \mathsf{elsif}\ \exists \beta \in \mathsf{dom}(T_0)\ .\ T_0(\beta) = \langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle\ \mathsf{then} \quad /^*\ \boldsymbol{\tau}' = \gamma \in \mathbb{V}_{\mathbb{t}}\ ^*/ \qquad (??)\\
\quad\quad\quad \langle \beta,\ T_0,\ \vartheta_0 \rangle \qquad (??)\\
\quad\quad \mathsf{else\ let}\ \beta \in \mathbb{V}_{\mathbb{t}} \setminus \mathsf{dom}(T_0)\ \mathsf{in} \quad /^*\ \boldsymbol{\tau}' = \gamma \in \mathbb{V}_{\mathbb{t}}\ ^*/ \qquad (??)\\
\quad\quad\quad \langle \beta,\ \langle \boldsymbol{\tau}_1,\ \boldsymbol{\tau}_2 \rangle [\beta \leftarrow T_0],\ \beta[\gamma \leftarrow \vartheta_0] \rangle \qquad (??)\\
\mathsf{let\ lcg}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2) = \qquad (??)\\
\quad \mathsf{if}\ \boldsymbol{\tau}_1 = \overline{\varnothing}^{\nu}\ \mathsf{then}\ \boldsymbol{\tau}_2 \qquad (??)\\
\quad \mathsf{elsif}\ \boldsymbol{\tau}_2 = \overline{\varnothing}^{\nu}\ \mathsf{then}\ \boldsymbol{\tau}_1 \qquad (??)\\
\quad \mathsf{else} \quad /^*\ \mathsf{assume}\ \exists \vartheta_1, \vartheta_2\ .\ \vartheta_1(\boldsymbol{\tau}') = \boldsymbol{\tau}_1 \wedge \vartheta_2(\boldsymbol{\tau}') = \boldsymbol{\tau}_2\ ^*/ \qquad (??)\\
\quad\quad \mathsf{let}\ \langle \boldsymbol{\tau},\ T,\ \vartheta' \rangle = \mathsf{lub}'(\boldsymbol{\tau}_1, \boldsymbol{\tau}_2, \varnothing, \boldsymbol{\tau}', \varepsilon, \varnothing)\ \mathsf{in}\ \boldsymbol{\tau} \quad /^*\ \vartheta'(\boldsymbol{\tau}') = \boldsymbol{\tau}\ ^*/ \qquad (??)
\end{array}
$$

Figure 18: The modified least upper bound algorithm