Auxiliary Material for the Slides "Calculational Design of [In]Correctness Transformational Program Logics by Abstract Interpretation" at POPL 2024, London

PATRICK COUSOT

We study transformational program logics for correctness and incorrectness that we extend to explicitly handle both termination and nontermination. We show that the logics are abstract interpretations of the right image transformer for a natural relational semantics covering both finite and infinite executions. This understanding of logics as abstractions of a semantics facilitates their comparisons through their respective abstractions of the semantics (rather that the much more difficult comparison through their formal proof systems). More importantly, the formalization provides a calculational method for constructively designing the sound and complete formal proof system by abstraction of the semantics. As an example, we extend Hoare logic to cover all possible behaviors of nondeterministic programs and design a new precondition (in)correctness logic.

CCS Concepts: • **Theory of computation → Logic and verification**; **Axiomatic semantics**.

Additional Key Words and Phrases: program logic, transformer, semantics, correctness, incorrectness, termination, nontermination, abstract interpretation

ACM Reference Format:
Patrick Cousot. 2024. Auxiliary Material for the Slides "Calculational Design of [In]Correctness Transformational Program Logics by Abstract Interpretation" at POPL 2024, London. *Proc. ACM Program. Lang.* 8, POPL, Article 7 (January 2024), 15 pages. https://doi.org/10.1145/3632849

This text contains the details of the formal development of Hoare logic, reverse Hoare logic aka incorrectness logic, and Hoare incorrectness logic.

Author's address: Patrick Cousot, pcousot@cims.nyu.edu.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

© 2024 Copyright held by the owner/author(s).
ACM 2475-1421/2024/1-ART7
https://doi.org/10.1145/3632849

1 PROPERTIES OF STRONGEST POSTCONDITIONS

Lemma 1.1 (Composition). $\mathsf{post}(X\,{}^{\circ}_{9}\,Y) = \mathsf{post}(Y) \circ \mathsf{post}(X)$.

Proof of Lem. 1.1.

$$
\begin{array}{ll}
& \mathsf{post}(X\,{}^{\circ}_{9}\,Y) \\
= & \boldsymbol{\lambda} P \bullet \{\sigma'' \mid \exists \sigma \in P \,.\, \langle \sigma,\, \sigma'' \rangle \in X\,{}^{\circ}_{9}\,Y\} \hfill \text{(def. post)} \\
= & \boldsymbol{\lambda} P \bullet \{\sigma'' \mid \exists \sigma \in P \,.\, \exists \sigma' \,.\, \langle \sigma,\, \sigma' \rangle \in X \wedge \langle \sigma',\, \sigma'' \rangle \in Y\} \hfill \text{(def. }{}^{\circ}_{9}\text{)} \\
= & \boldsymbol{\lambda} P \bullet \{\sigma'' \mid \exists \sigma' \,.\, \sigma' \in \{\sigma' \mid \exists \sigma \in P \,.\, \langle \sigma,\, \sigma' \rangle \in X\} \wedge \langle \sigma',\, \sigma'' \rangle \in Y\} \hfill \text{(def. } \exists \text{ and } \in\text{)} \\
= & \boldsymbol{\lambda} P \bullet \{\sigma'' \mid \exists \sigma' \in \mathsf{post}(X)P \,.\, \langle \sigma',\, \sigma'' \rangle \in Y\} \hfill \text{(def. post)} \\
= & \boldsymbol{\lambda} P \bullet \mathsf{post}(Y)(\mathsf{post}(X)P) \hfill \text{(def. post)} \\
= & \mathsf{post}(Y) \circ \mathsf{post}(X) \hfill \text{(def. function composition } \circ\text{)} \quad \square
\end{array}
$$

Lemma 1.2 (test). $\mathsf{post}[\![\mathsf{B}]\!]P = P \cap \mathcal{B}[\![\mathsf{B}]\!]$.

Proof of Lem. 1.2.

$$
\begin{array}{ll}
& \mathsf{post}[\![\mathsf{B}]\!]P \\
= & \{\sigma' \mid \exists \sigma \in P \,.\, \langle \sigma,\, \sigma' \rangle \in [\![\mathsf{B}]\!]\} \hfill \text{(def. post)} \\
= & \{\sigma \mid \sigma \in P \wedge \sigma \in \mathcal{B}[\![\mathsf{B}]\!]\} \hfill \text{(def. } [\![\mathsf{B}]\!] \triangleq \{\langle \sigma,\, \sigma \rangle \mid \sigma \in \mathcal{B}[\![\mathsf{B}]\!]\}\text{)} \\
= & P \cap \mathcal{B}[\![\mathsf{B}]\!] \hfill \text{(def. intersection } \cup\text{)} \quad \square
\end{array}
$$

Lemma 1.3 (Strongest postcondition). $\mathcal{T}(\mathsf{S}) = \alpha_{\mathrm{G}} \circ \mathsf{post}[\![\mathsf{S}]\!] = \{\langle P,\, \mathsf{post}[\![\mathsf{S}]\!]P \rangle \mid P \in \wp(\Sigma)\}$.

Proof of Lem. 1.3.

$$
\begin{array}{ll}
& \mathcal{T}(\mathsf{S}) \\
= & \alpha_{\mathrm{G}} \circ \mathsf{post} \circ \alpha_{\not\perp} \circ \alpha_{C}(\{[\![\mathsf{S}]\!]_{\perp}\}) \hfill \text{(def. } \mathcal{T}\text{)} \\
= & \alpha_{\mathrm{G}} \circ \mathsf{post} \circ \alpha_{\not\perp}([\![\mathsf{S}]\!]_{\perp}) \hfill \text{(def. } \alpha_{C}\text{)} \\
= & \alpha_{\mathrm{G}} \circ \mathsf{post}([\![\mathsf{S}]\!]_{\perp} \cap (\Sigma \times \Sigma)) \hfill \text{(def. } \alpha_{\not\perp}\text{)} \\
= & \alpha_{\mathrm{G}} \circ \mathsf{post}[\![\mathsf{S}]\!] \hfill \text{(def. (1) of the angelic semantics } [\![\mathsf{S}]\!]\text{)} \\
= & \{\langle P,\, \mathsf{post}[\![\mathsf{S}]\!]P \rangle \mid P \in \wp(\Sigma)\} \hfill \text{(def. } \alpha_{\mathrm{G}}\text{)} \quad \square
\end{array}
$$

Lemma 1.4 (Strongest postcondition over approximation).

$$\mathcal{T}_{\mathrm{HL}}(\mathsf{S}) \;\triangleq\; \mathsf{post}(\supseteq.\subseteq) \circ \mathcal{T}(\mathsf{S}) \;=\; \{\langle P,\, Q \rangle \mid \mathsf{post}[\![\mathsf{S}]\!]P \subseteq Q\} \;=\; \mathsf{post}(=,\subseteq) \circ \mathcal{T}(\mathsf{S})$$

Proof of Lem. 1.4.

$$
\begin{array}{ll}
& \mathsf{post}(\supseteq.\subseteq) \circ \mathcal{T}(\mathsf{S}) \\
= & \mathsf{post}(\supseteq.\subseteq)(\mathcal{T}(\mathsf{S})) \hfill \text{(def. function composition } \circ\text{)} \\
= & \mathsf{post}(\supseteq.\subseteq)(\{\langle P,\, \mathsf{post}[\![\mathsf{S}]\!]P \rangle \mid P \in \wp(\Sigma)\}) \hfill \text{(Lem. 1.3)} \\
= & \{\langle P',\, Q' \rangle \mid \exists \langle P,\, Q \rangle \in \{\langle P,\, \mathsf{post}[\![\mathsf{S}]\!]P \rangle \mid P \in \wp(\Sigma)\} \,.\, \langle \langle P,\, Q \rangle,\, \langle P',\, Q' \rangle \rangle \in \supseteq.\subseteq\} \hfill \text{(def. (10) of post)} \\
= & \{\langle P',\, Q' \rangle \mid \exists P \,.\, \langle \langle P,\, \mathsf{post}[\![\mathsf{S}]\!]P \rangle,\, \langle P',\, Q' \rangle \rangle \in \supseteq.\subseteq\} \hfill \text{(def. } \in\text{)} \\
= & \{\langle P',\, Q' \rangle \mid \exists P \,.\, \langle P,\, \mathsf{post}[\![\mathsf{S}]\!]P \rangle \supseteq.\subseteq \langle P',\, Q' \rangle\} \hfill \text{(def. } \in\text{)} \\
= & \{\langle P',\, Q' \rangle \mid \exists P \,.\, P \supseteq P' \wedge \mathsf{post}[\![\mathsf{S}]\!]P \subseteq Q'\} \hfill \text{(def. } \supseteq.\subseteq\text{)} \\
= & \{\langle P',\, Q' \rangle \mid \exists P \,.\, P' \subseteq P \wedge \mathsf{post}[\![\mathsf{S}]\!]P \subseteq Q'\} \hfill \text{(def. } \supseteq\text{)}
\end{array}
$$

$= \{\langle P', Q'\rangle \mid \mathsf{post}[\![\mathtt{S}]\!]P' \subseteq Q'\}$

$\wr(\subseteq)$ by Galois connection (12), post is increasing so that $P' \subseteq P \wedge \mathsf{post}[\![\mathtt{S}]\!]P \subseteq Q'$ implies $\mathsf{post}[\![\mathtt{S}]\!]P' \subseteq \mathsf{post}[\![\mathtt{S}]\!]P \wedge \mathsf{post}[\![\mathtt{S}]\!]P \subseteq Q'$ hence $\mathsf{post}[\![\mathtt{S}]\!]P' \subseteq Q'$ by transitivity; $(\supseteq)$ take $P = P'\wr$

$= \{\langle P', Q'\rangle \mid \exists P \,.\, P' = P \wedge \mathsf{post}[\![\mathtt{S}]\!]P \subseteq Q'\}$ $\quad\wr$def. $=\wr$

$= \{\langle P', Q'\rangle \mid \exists P \,.\, \langle P, \mathsf{post}[\![\mathtt{S}]\!]P\rangle =,\subseteq \langle P', Q'\rangle\}$ $\quad\wr$def. $=,\subseteq\wr$

$= \{\langle P', Q'\rangle \mid \exists P \,.\, \langle\langle P, \mathsf{post}[\![\mathtt{S}]\!]P\rangle, \langle P', Q'\rangle\rangle \in =,\subseteq\}$ $\quad\wr$def. $\in\wr$

$= \{\langle P', Q'\rangle \mid \exists\langle P, Q\rangle \in \{\langle P, \mathsf{post}[\![\mathtt{S}]\!]P\rangle \mid P \in \wp(\Sigma)\} \,.\, \langle\langle P, Q\rangle, \langle P', Q'\rangle\rangle \in =,\subseteq\}$ $\quad\wr$def. $\in\wr$

$= \{\langle P', Q'\rangle \mid \exists\langle P, Q\rangle \in \mathcal{T}(\mathtt{S}) \,.\, \langle\langle P, Q\rangle, \langle P', Q'\rangle\rangle \in =,\subseteq\}$ $\quad\wr$Lem. 1.3$\wr$

$= \mathsf{post}(=,\subseteq)(\mathcal{T}(\mathtt{S}))$ $\quad\wr$def. (10) of post$\wr$

$= \mathsf{post}(=,\subseteq) \circ \mathcal{T}(\mathtt{S})$ $\quad\wr$def. function composition $\circ\wr$ $\square$

For simplicity, we consider conditional iteration `W = while (B) S` with no `break`.

Lemma 1.5 (Commutation). *$\mathsf{post} \circ F'^{e} = \bar{F}^{e} \circ \mathsf{post}$ where $\bar{F}^{e}(X) \triangleq \mathsf{id} \mathbin{\dot\cup} (\mathsf{post}([\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!]^{e}) \circ X)$ and $F'^{e} \triangleq \boldsymbol{\lambda} X \bullet \mathsf{id} \cup (X \mathbin{⨾} [\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!]^{e})$, $X \in \wp(\Sigma \times \Sigma)$ by (70).*

Proof of Lem. 1.5.

$\mathsf{post}(F'^{e}(X))$ $\quad\wr$where $X \in \wp(\Sigma)\wr$

$= \mathsf{post}(\mathsf{id} \cup (X \mathbin{⨾} [\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!]^{e}))$ $\quad\wr$def. $F^{e}\wr$

$= \mathsf{post}(\mathsf{id}) \mathbin{\dot\cup} \mathsf{post}(X \mathbin{⨾} [\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!]^{e})$ $\quad\wr$join preservation in Galois connection (12)$\wr$

$= \mathsf{id} \mathbin{\dot\cup} (\mathsf{post}([\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!]^{e}) \circ \mathsf{post}(X))$ $\quad\wr$def. post and composition Lem. 1.1$\wr$

$= \bar{F}^{e}(\mathsf{post}(X))$ $\quad\wr$def. $\bar{F}^{e}\wr$ $\square$

Lemma 1.6 (Pointwise commutation). *$\forall X \in \wp(\Sigma) \to \wp(\Sigma) \,.\, \forall P \in \wp(\Sigma) \,.\, \bar{F}^{e}(X)P \triangleq \bar{\bar{F}}^{e}_{P}(X(P))$ where $\bar{\bar{F}}^{e}_{P}(X) \triangleq P \cup \mathsf{post}([\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!]^{e})X$.*

Proof of Lem. 1.6.

$\bar{F}^{e}(X)P$

$= (\mathsf{id} \mathbin{\dot\cup} (\mathsf{post}([\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!]^{e}) \circ X))P$ $\quad\wr$def. $\bar{F}^{e}\wr$

$= \mathsf{id}(P) \cup (\mathsf{post}([\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!]^{e}) \circ X)(P)$ $\quad\wr$pointwise def. $\dot\cup$ and function composition $\circ\wr$

$= P \cup \mathsf{post}([\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!]^{e})(X(P))$ $\quad\wr$def. identity id and function application$\wr$

$= \bar{\bar{F}}^{e}_{P}(X(P))$ $\quad\wr$def. $\bar{\bar{F}}^{e}_{P}(X) \triangleq P \cup \mathsf{post}([\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!]^{e})X\wr$ $\square$

Theorem 1.7 (Iteration strongest postcondition). *$\mathsf{post}[\![\mathtt{W}]\!]P = \mathsf{post}[\![\neg\mathtt{B}]\!](\mathsf{lfp}^{\subseteq} \bar{\bar{F}}^{e}_{P})$ where $\bar{\bar{F}}^{e}_{P}(X) \triangleq P \cup \mathsf{post}([\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!]^{e})X$.*

Proof of Th. 1.7.

$\mathsf{post}[\![\mathtt{W}]\!]$

$= \mathsf{post}(\mathsf{lfp}^{\subseteq} F^{e} \mathbin{⨾} [\![\neg\mathtt{B}]\!])$ $\quad\wr$def. (49) of $[\![\mathtt{W}]\!]$ in absence of `break`$\wr$

$= \mathsf{post}[\![\neg\mathtt{B}]\!] \circ \mathsf{post}(\mathsf{lfp}^{\subseteq} F^{e})$ $\quad\wr$composition Lem. 1.1$\wr$

$= \mathsf{post}[\![\neg\mathtt{B}]\!] \circ \mathsf{post}(\mathsf{lfp}^{\subseteq} F'^{e})$ $\quad\wr$since $\mathsf{lfp}^{\subseteq} F^{e} = \mathsf{lfp}^{\subseteq} F'^{e}$ in (70)$\wr$

$= \mathsf{post}[\![\neg\mathtt{B}]\!](\mathsf{lfp}^{\subseteq} \bar{F}^{e})$ $\quad\wr$commutation Lem. 1.5 and fixpoint abstraction Th. II.2.2$\wr$

$= \ \mathsf{post}[\![\neg\mathtt{B}]\!] \circ \boldsymbol{\lambda} P \bullet \mathsf{lfp}^{\subseteq} \bar{\bar{F}}_P^e$

$\wr$pointwise commutation Lem. 1.6 and pointwise abstraction Cor. II.2.2$\int$ $\square$

Corollary 1.8 (Conditional iteration strongest postcondition graph). $\mathcal{T}(\mathtt{W}) = \{\langle P, \mathsf{post}[\![\neg\mathtt{B}]\!](\mathsf{lfp}^{\subseteq} \bar{\bar{F}}_P^e)\rangle \mid P \in \wp(\Sigma)\}$ *where* $\bar{\bar{F}}_P^e(X) \triangleq P \cup \mathsf{post}([\![\mathtt{B}]\!] \,\mathring{,}\, [\![\mathtt{S}]\!]^e)X$.

Proof of Cor. 1.8.

$\mathcal{T}(\mathtt{W})$

$= \ \alpha_{\mathrm{G}} \circ \mathsf{post}([\![\mathtt{W}]\!])$ $\wr$Lem. 1.3$\int$

$= \ \alpha_{\mathrm{G}} \circ \mathsf{post}[\![\neg\mathtt{B}]\!] \circ \boldsymbol{\lambda} P \bullet \mathsf{lfp}^{\subseteq} \bar{\bar{F}}_P^e$ $\wr$Th. 1.7$\int$

$= \ \{\langle P, \mathsf{post}[\![\neg\mathtt{B}]\!](\mathsf{lfp}^{\subseteq} \bar{\bar{F}}_P^e)\rangle \mid P \in \wp(\Sigma)\}$ $\wr$def. (7) of $\alpha_{\mathrm{G}}$$\int$ $\square$

2 CALCULATIONAL DESIGN OF HOARE LOGIC HL

2.1 Calculational Design of Hoare Logic Theory

THEOREM 2.1 (THEORY OF HOARE LOGIC HL).

$$\begin{array}{rcl}\mathcal{T}_{\mathrm{HL}}(\mathtt{W}) & \triangleq & \mathsf{post}(\supseteq.\subseteq) \circ \mathcal{T}(\mathtt{W}) \\ & = & \{\langle P,\,Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \langle I \cap \mathcal{B}[\![\mathtt{B}]\!],\, I\rangle \in \mathcal{T}_{HL}(\mathtt{S}) \wedge (I \cap \neg\mathcal{B}[\![\mathtt{B}]\!]) \subseteq Q\}\end{array}$$

PROOF OF TH. 2.1 .

$\mathcal{T}_{\mathrm{HL}}(\mathtt{W})$

$= \mathsf{post}(\supseteq.\subseteq) \circ \mathcal{T}(\mathtt{W})$ ≀def. $\mathcal{T}_{\mathrm{HL}}$≀

$= \mathsf{post}(=,\subseteq) \circ \mathcal{T}(\mathtt{W})$ ≀Lem. 1.4≀

$= \{\langle P',\,Q'\rangle \mid \langle P,\,Q\rangle \in \mathcal{T}(\mathtt{W}) \,.\, \langle P,\,Q\rangle =,\subseteq \langle P',\,Q'\rangle\}$ ≀def. post≀

$= \{\langle P',\,Q'\rangle \mid \langle P,\,Q\rangle \in \mathcal{T}(\mathtt{W}) \,.\, P = P' \wedge Q \subseteq Q'\}$ ≀component wise def. $=,\subseteq$≀

$= \{\langle P,\,Q'\rangle \mid \exists Q \,.\, \langle P,\,Q\rangle \in \mathcal{T}(\mathtt{W}) \,.\, Q \subseteq Q'\}$ ≀def. $=$≀

$= \{\langle P,\,Q'\rangle \mid \exists Q \,.\, \mathsf{post}[\![\neg\mathtt{B}]\!](\mathsf{lfp}^{\subseteq}\,\bar{\bar{F}}^{e}_{P}) \subseteq Q \wedge Q \subseteq Q'\}$ ≀Th. 1.7≀

$= \{\langle P,\,Q'\rangle \mid \exists Q \,.\, \mathsf{post}[\![\neg\mathtt{B}]\!](\mathsf{lfp}^{\subseteq}\,\bar{\bar{F}}^{e}_{P}) \subseteq Q'\}$
≀($\subseteq$) $\exists Q \,.\, \mathsf{post}[\![\neg\mathtt{B}]\!](\mathsf{lfp}^{\subseteq}\,\bar{\bar{F}}^{e}_{P}) \subseteq Q \wedge Q \subseteq Q'$ and transitivity;
($\supseteq$) take $Q = Q'$≀

$= \{\langle P,\,Q'\rangle \mid \exists Q \,.\, \mathsf{lfp}^{\subseteq}\,\bar{\bar{F}}^{e}_{P} \subseteq Q \wedge \mathsf{post}[\![\neg\mathtt{B}]\!](Q) \subseteq Q'\}$
≀($\subseteq$) take $Q = \mathsf{lfp}^{\subseteq}\,\bar{\bar{F}}^{e}_{P}$; ($\supseteq$) $\mathsf{post}[\![\neg\mathtt{B}]\!]$ is increasing by (12)≀

$= \{\langle P,\,Q'\rangle \mid \exists Q \,.\, \exists I \,.\, \bar{\bar{F}}^{e}_{P}(I) \subseteq I \wedge I \subseteq Q \wedge \mathsf{post}[\![\neg\mathtt{B}]\!](Q) \subseteq Q'\}$ ≀Park fixpoint induction Th. II.3.1≀

$= \{\langle P,\,Q'\rangle \mid \exists I \,.\, \bar{\bar{F}}^{e}_{P}(I) \subseteq I \wedge \mathsf{post}[\![\neg\mathtt{B}]\!](I) \subseteq Q'\}$
≀($\subseteq$) $I \subseteq Q$ implies $\mathsf{post}[\![\neg\mathtt{B}]\!](I) \subseteq \mathsf{post}[\![\neg\mathtt{B}]\!](Q)$ since $\mathsf{post}[\![\neg\mathtt{B}]\!]$ is increasing by (12) hence $\mathsf{post}[\![\neg\mathtt{B}]\!](I) \subseteq Q'$ by transitivity;
($\supseteq$) take $Q = I$≀

$= \{\langle P,\,Q\rangle \mid \exists I \,.\, P \cup \mathsf{post}([\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!]^{e})(I) \subseteq I \wedge \mathsf{post}[\![\neg\mathtt{B}]\!](I) \subseteq Q\}$ ≀renaming, def. $\bar{\bar{F}}^{e}_{P}$≀

$= \{\langle P,\,Q\rangle \mid \exists I \,.\, P \cup \mathsf{post}([\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!])(I) \subseteq I \wedge \mathsf{post}[\![\neg\mathtt{B}]\!](I) \subseteq Q\}$ ≀$[\![\mathtt{S}]\!]^{e} = [\![\mathtt{S}]\!]$ in absence of `breaks`≀

$= \{\langle P,\,Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \mathsf{post}([\![\mathtt{B}]\!] \mathbin{⨾} [\![\mathtt{S}]\!])I \subseteq I \wedge \mathsf{post}[\![\neg\mathtt{B}]\!](I) \subseteq Q\}$ ≀def. $\subseteq$ and $\cup$≀

$= \{\langle P,\,Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \mathsf{post}[\![\mathtt{S}]\!](\mathsf{post}[\![\mathtt{B}]\!]I) \subseteq I \wedge \mathsf{post}[\![\neg\mathtt{B}]\!](I) \subseteq Q\}$ ≀composition Lem. 1.1≀

$= \{\langle P,\,Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \mathsf{post}[\![\mathtt{S}]\!](I \cap \mathcal{B}[\![\mathtt{B}]\!]) \subseteq I \wedge (I \cap \neg\mathcal{B}[\![\mathtt{B}]\!]) \subseteq Q\}$ ≀test Lem. 1.2≀

$= \{\langle P,\,Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \langle I \cap \mathcal{B}[\![\mathtt{B}]\!],\, I\rangle \in \{\langle P,\,Q\rangle \mid \mathsf{post}[\![\mathtt{S}]\!]P \subseteq Q\} \wedge (I \cap \neg\mathcal{B}[\![\mathtt{B}]\!]) \subseteq Q$ ≀def. $\in$≀

$= \{\langle P,\,Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \langle I \cap \mathcal{B}[\![\mathtt{B}]\!],\, I\rangle \in \mathsf{post}(=,\subseteq) \circ \mathcal{T}(\mathtt{S}) \wedge (I \cap \neg\mathcal{B}[\![\mathtt{B}]\!]) \subseteq Q$ ≀Lem. 1.4≀

$= \{\langle P,\,Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \langle I \cap \mathcal{B}[\![\mathtt{B}]\!],\, I\rangle \in \mathcal{T}_{\mathrm{HL}}(\mathtt{S}) \wedge (I \cap \neg\mathcal{B}[\![\mathtt{B}]\!]) \subseteq Q$ ≀Lem. 1.4≀ □

2.2 Hoare logic rules

Theorem 2.2 (Hoare rules for conditional iteration).

$$\frac{P \subseteq I,\ \{I \cap \mathcal{B}[\![\mathtt{B}]\!]\}\,\mathtt{S}\,\{I\},\ (I \cap \neg\mathcal{B}[\![\mathtt{B}]\!]) \subseteq Q}{\{P\}\,\mathtt{while\ (B)\ S}\,\{Q\}} \tag{1}$$

Proof of Th. 2.2. We write $\{P\}\,\mathtt{S}\,\{Q\} \triangleq \langle P,\ Q\rangle \in \mathcal{T}_{\mathrm{HL}}(\mathtt{S})$;

By structural induction (`S` being a strict component of `while (B) S`), the rule for $\{P\}\,\mathtt{S}\,\{Q\}$ have already been defined;

By Aczel method, the (constant) fixpoint $\mathsf{lfp}^{\subseteq}\,\boldsymbol{\lambda} X \bullet S$ is defined by $\{\frac{\varnothing}{c} \mid c \in S\}$;

So for `while (B) S` we have an axiom $\dfrac{\varnothing}{\{P\}\,\mathtt{while\ (B)\ S}\,\{Q\}}$ with side condition $P \subseteq I,\ \{I \cap \mathcal{B}[\![\mathtt{B}]\!]\}\,\mathtt{S}\,\{I\},\ (I \cap \neg\mathcal{B}[\![\mathtt{B}]\!]) \subseteq Q$;

Traditionally, the side condition is written as a premiss, to get (1).

3 CALCULATIONAL DESIGN OF REVERSE HOARE AKA INCORRECTNESS LOGIC (IL)

3.1 Calculational Design of Reverse Hoare aka Incorrectness Logic Theory

THEOREM 3.1 (THEORY OF IL).

$$\begin{aligned}\mathcal{T}_{IL}(\mathtt{W}) &\triangleq \mathsf{post}(\subseteq,\supseteq)\circ\mathcal{T}(\mathtt{W})\\ &= \{\langle P,\ Q\rangle \mid \exists\langle J^n,\ n\in\mathbb{N}\rangle\ .\ J^0 = P \wedge \langle J^n\cap\mathcal{B}[\![\mathtt{B}]\!],\ J^{n+1}\rangle \in \mathcal{T}_{IL}(\mathtt{S}) \wedge Q \subseteq (\bigcup_{n\in\mathbb{N}} J^n)\cap\mathcal{B}[\![\neg\mathtt{B}]\!]\}\end{aligned}$$

PROOF OF TH. 3.1.

$$\mathcal{T}_{\mathrm{IL}}(\mathtt{W})$$

$= \mathsf{post}(\subseteq,\supseteq)\circ\mathcal{T}(\mathtt{W})$ ⦃def. $\mathcal{T}_{\mathrm{IL}}$⦄

$= \{\langle P,\ Q\rangle \mid Q \subseteq \mathsf{post}[\![\mathtt{W}]\!]P\}$ ⦃$\subseteq$-order dual of Lem. 1.4⦄

$= \{\langle P,\ Q\rangle \mid Q \subseteq \mathsf{post}[\![\neg\mathtt{B}]\!](\mathsf{lfp}^{\subseteq}\,\bar{\bar{F}}^{e}_{P})\}$ ⦃Th. 1.7 where $\bar{\bar{F}}^{e}_{P}(X) \triangleq P\cup\mathsf{post}([\![\mathtt{B}]\!]\,;\,[\![\mathtt{S}]\!]^{e})X$⦄

$= \{\langle P,\ Q\rangle \mid \exists I\ .\ Q \subseteq \mathsf{post}[\![\neg\mathtt{B}]\!](I) \wedge I \subseteq \mathsf{lfp}^{\subseteq}\,\bar{\bar{F}}^{e}_{P}\}$

⦃($\subseteq$) Take $I = \mathsf{lfp}^{\subseteq}\,\bar{\bar{F}}^{e}_{P}$ and reflexivity;
($\supseteq$) By Galois connection (12), $\mathsf{post}[\![\neg\mathtt{B}]\!]$ is increasing so $Q \subseteq \mathsf{post}[\![\neg\mathtt{B}]\!](I) \subseteq \mathsf{post}[\![\neg\mathtt{B}]\!](\mathsf{lfp}^{\subseteq}\,\bar{\bar{F}}^{e}_{P})$ and transitivity⦄

$= \{\langle P,\ Q\rangle \mid \exists I\ .\ Q \subseteq \mathsf{post}[\![\neg\mathtt{B}]\!](I) \wedge \exists\langle J^n,\ n<\omega\rangle\ .\ J^0 = \varnothing \wedge J^{n+1} \subseteq \bar{\bar{F}}^{e}_{P}(J^n) \wedge I \subseteq \bigcup_{n<\omega} J^n\}$

⦃fixpoint underapproximation Th. II.3.6⦄

$= \{\langle P,\ Q\rangle \mid \exists\langle J^n,\ n<\omega\rangle\ .\ J^0 = \varnothing \wedge J^{n+1} \subseteq \bar{\bar{F}}^{e}_{P}(J^n) \wedge Q \subseteq \mathsf{post}[\![\neg\mathtt{B}]\!](\bigcup_{n<\omega} J^n)\}$

⦃($\subseteq$) By Galois connection (12), $\mathsf{post}[\![\neg\mathtt{B}]\!]$ is increasing so $Q \subseteq \mathsf{post}[\![\neg\mathtt{B}]\!](I) \subseteq \mathsf{post}[\![\neg\mathtt{B}]\!](\bigcup_{n<\omega} J^n)$ and transitivity;
($\supseteq$) take $I = \bigcup_{n<\omega} J^n$⦄

$= \{\langle P,\ Q\rangle \mid \exists\langle J^n,\ n<\omega\rangle\ .\ J^0 = \varnothing \wedge J^{n+1} \subseteq (P\cup\mathsf{post}([\![\mathtt{B}]\!]\,;\,[\![\mathtt{S}]\!]^{e})(J^n)) \wedge Q \subseteq \mathsf{post}[\![\neg\mathtt{B}]\!](\bigcup_{n<\omega} J^n)\}$

⦃def. $\bar{\bar{F}}^{e}_{P}$⦄

$= \{\langle P,\ Q\rangle \mid \exists\langle J^n,\ 1\leqslant n<\omega\rangle\ .\ J^1 = P \wedge J^{n+1} \subseteq \mathsf{post}([\![\mathtt{B}]\!]\,;\,[\![\mathtt{S}]\!]^{e})(J^n) \wedge Q \subseteq \mathsf{post}[\![\neg\mathtt{B}]\!](\bigcup_{1\leqslant n<\omega} J^n)\}$

⦃getting rid of $J^0 = \varnothing$⦄

$= \{\langle P,\ Q\rangle \mid \exists\langle J^n,\ n\in\mathbb{N}\rangle\ .\ J^0 = P \wedge J^{n+1} \subseteq \mathsf{post}([\![\mathtt{B}]\!]\,;\,[\![\mathtt{S}]\!]^{e})(J^n) \wedge Q \subseteq \mathsf{post}[\![\neg\mathtt{B}]\!](\bigcup_{n\in\mathbb{N}} J^n)\}$

⦃changing $n+1$ to n⦄

$= \{\langle P,\ Q\rangle \mid \exists\langle J^n,\ n\in\mathbb{N}\rangle\ .\ J^0 = P \wedge J^{n+1} \subseteq \mathsf{post}[\![\mathtt{S}]\!]^{e}(J^n\cap\mathcal{B}[\![\mathtt{B}]\!]) \wedge Q \subseteq (\bigcup_{n\in\mathbb{N}} J^n)\cap\mathcal{B}[\![\neg\mathtt{B}]\!]\}$

⦃Lem. 1.2⦄

$= \{\langle P,\ Q\rangle \mid \exists\langle J^n,\ n\in\mathbb{N}\rangle\ .\ J^0 = P \wedge \langle J^n\cap\mathcal{B}[\![\mathtt{B}]\!],\ J^{n+1}\rangle \in \{\langle P',\ Q'\rangle \mid Q' \subseteq \mathsf{post}[\![\mathtt{S}]\!]^{e})P)\} \wedge Q \subseteq (\bigcup_{n\in\mathbb{N}} J^n)\cap\mathcal{B}[\![\neg\mathtt{B}]\!]\}$ ⦃def. $\in$⦄

$= \{\langle P,\ Q\rangle \mid \exists\langle J^n,\ n\in\mathbb{N}\rangle\ .\ J^0 = P \wedge \langle J^n\cap\mathcal{B}[\![\mathtt{B}]\!],\ J^{n+1}\rangle \in \mathcal{T}_{\mathrm{IL}}(\mathtt{S}) \wedge Q \subseteq (\bigcup_{n\in\mathbb{N}} J^n)\cap\mathcal{B}[\![\neg\mathtt{B}]\!]\}$ ⦃def. $\mathcal{T}_{\mathrm{IL}}$⦄

□

3.2 Calculational design of IL rules

$$\frac{J^0 = P,\ [J^n \cap \mathcal{B}[\![\mathtt{B}]\!]]\ \mathtt{S}\ [J^{n+1}],\ Q \subseteq (\bigcup_{n\in\mathbb{N}} J^n) \cap \mathcal{B}[\![\neg\mathtt{B}]\!]}{[P]\ \mathtt{while\ (B)\ S}\ [Q]} \tag{2}$$

Proof. We write $[P]\,\mathtt{S}\,[Q] \triangleq \langle P,\ Q\rangle \in \mathcal{T}_{\mathrm{IL}}(\mathtt{S})$;

By structural induction ($\mathtt{S}$ being a strict component of $\mathtt{while\ (B)\ S}$), the rule for $[P]\,\mathtt{S}\,[Q]$ have already been defined;

By Aczel method, the (constant) fixpoint $\mathsf{lfp}^{\subseteq}\, \boldsymbol{\lambda} X \bullet S$ is defined by $\{\frac{\varnothing}{c} \mid c \in S\}$;

So for $\mathtt{while\ (B)\ S}$ we have an axiom $\dfrac{\varnothing}{\{P\}\ \mathtt{while\ (B)\ S}\ \{Q\}}$ with side condition $J^0 = P,\ [J^n \cap \mathcal{B}[\![\mathtt{B}]\!]]\ \mathtt{S}\ [J^{n+1}],\ Q \subseteq (\bigcup_{n\in\mathbb{N}} J^n) \cap \mathcal{B}[\![\neg\mathtt{B}]\!]$;

Traditionally, the side condition is written as a premiss, to get (2).

4 CALCULATIONAL DESIGN OF HOARE INCORRECTNESS LOGIC

4.1 Calculational Design of Hoare Incorrectness Logic Theory

THEOREM 4.1 (EQUIVALENT DEFINITIONS OF $\overline{\text{HL}}$ THEORIES).

$$\mathcal{T}_{\overline{HL}}(\mathtt{S}) \quad \triangleq \quad \mathsf{post}(\subseteq,\supseteq)\circ\alpha^{\neg}\circ\mathcal{T}_{HL}(\mathtt{S}) \quad = \quad \alpha^{\neg}\circ\mathcal{T}_{HL}(\mathtt{S})$$

Observe that Th. 4.1 shows that post$(\subseteq,\supseteq)$ can be dispensed with. This implies that the consequence rule is useless for Hoare incorrectness logic.

PROOF OF TH. 4.1.

$$\begin{array}{ll}
\mathcal{T}_{\overline{\text{HL}}}(\mathtt{S}) \ = \ \mathsf{post}(\subseteq,\supseteq)\circ\alpha^{\neg}\circ\mathcal{T}_{\text{HL}}(\mathtt{S}) & \wr\text{def. } \mathcal{T}_{\overline{\text{HL}}}\wr \\
= \mathsf{post}((\subseteq,\supseteq)(\neg\{\langle P,\ Q\rangle \mid \mathsf{post}[\![\mathtt{S}]\!]P\subseteq Q\}) & \wr\text{Lem. 1.4 and def. (30) of } \alpha^{\neg}\wr \\
= \mathsf{post}(\subseteq,\supseteq)(\{\langle P,\ Q\rangle \mid \neg(\mathsf{post}[\![\mathtt{S}]\!]P\subseteq Q)\}) & \wr\text{def. } \neg\wr \\
= \mathsf{post}(\subseteq,\supseteq)(\{\langle P,\ Q\rangle \mid \mathsf{post}[\![\mathtt{S}]\!]P\cap\neg Q\neq\varnothing\}) & \wr\text{def. } \subseteq \text{ and } \neg\wr \\
= \{\langle P',\ Q'\rangle \mid \exists\langle P,\ Q\rangle\in\{\langle P,\ Q\rangle \mid \mathsf{post}[\![\mathtt{S}]\!]P\cap\neg Q\neq\varnothing\}\ .\ \langle P,\ Q\rangle \subseteq,\supseteq \langle P',\ Q'\rangle\} & \wr\text{def. post}\wr \\
= \{\langle P',\ Q'\rangle \mid \exists\langle P,\ Q\rangle\ .\ \mathsf{post}[\![\mathtt{S}]\!]P\cap\neg Q\neq\varnothing \wedge \langle P,\ Q\rangle \subseteq,\supseteq \langle P',\ Q'\rangle\} & \wr\text{def. } \in\wr \\
= \{\langle P',\ Q'\rangle \mid \exists\langle P,\ Q\rangle\ .\ \mathsf{post}[\![\mathtt{S}]\!]P\cap\neg Q\neq\varnothing \wedge P\subseteq P' \wedge Q\supseteq Q'\} & \wr\text{component wise def. of } \subseteq,\supseteq\wr \\
= \{\langle P',\ Q'\rangle \mid \exists Q\ .\ \mathsf{post}[\![\mathtt{S}]\!]P'\cap\neg Q\neq\varnothing \wedge Q\supseteq Q'\} &
\end{array}$$

$\wr$($\subseteq$) if $P \subseteq P'$ then $\mathsf{post}[\![\mathtt{S}]\!]P \subseteq \mathsf{post}[\![\mathtt{S}]\!]P'$ by (12) so that $\mathsf{post}[\![\mathtt{S}]\!]P\cap\neg Q\neq\varnothing$ implies $\mathsf{post}[\![\mathtt{S}]\!]P'\cap\neg Q\neq\varnothing$;
($\supseteq$) conversely, if $\exists Q\ .\ \mathsf{post}[\![\mathtt{S}]\!]P'$, then $\exists P\ .\ \mathsf{post}[\![\mathtt{S}]\!]P\cap\neg Q\neq\varnothing\wedge P\subseteq P'$ by choosing $P = P'$. $\wr$

$$= \{\langle P',\ Q'\rangle \mid \mathsf{post}[\![\mathtt{S}]\!]P'\cap\neg Q'\neq\varnothing\}$$

$\wr$($\subseteq$) if $Q\supseteq Q'$ then $\neg Q'\supseteq\neg Q$ so $\mathsf{post}[\![\mathtt{S}]\!]P'\cap\neg Q\neq\varnothing$ implies $\mathsf{post}[\![\mathtt{S}]\!]P'\cap\neg Q'\neq\varnothing$;
($\supseteq$) conversely $\mathsf{post}[\![\mathtt{S}]\!]P'\cap\neg Q'\neq\varnothing$ implies $\exists Q\ .\ \mathsf{post}[\![\mathtt{S}]\!]P'\cap\neg Q\neq\varnothing\wedge Q\supseteq Q'$ by choosing $Q = Q'$. $\wr$

$$\begin{array}{ll}
= \{\langle P,\ Q\rangle \mid \neg(\mathsf{post}[\![\mathtt{S}]\!]P\subseteq Q)\} & \wr\text{def. } \subseteq \text{ and } \neg\wr \\
= \alpha^{\neg}\circ\mathcal{T}_{\text{HL}}(\mathtt{S}) & \wr\text{def. } \alpha^{\neg} \text{ and } \mathcal{T}_{\text{HL}} \text{ for Hoare logic}\wr \quad \square
\end{array}$$

THEOREM 4.2 (THEORY OF $\overline{\text{HL}}$). `W = while (B) S`

$$\begin{array}{rl}
\mathcal{T}_{\overline{HL}}(\mathtt{W}) \ = & \{\langle P,\ Q\rangle \mid \exists n\geqslant 1\ .\ \exists\langle\sigma_i\in I,\ i\in[1,n]\rangle\ .\ \sigma_1\in P\ \wedge \\
& \forall i\in[1,n[\ .\ \langle\mathcal{B}[\![\mathtt{B}]\!]\cap\{\sigma_i\},\ \neg\{\sigma_{i+1}\}\rangle\in\mathcal{T}_{\overline{HL}}(\mathtt{S})\wedge\sigma_n\notin\mathcal{B}[\![\mathtt{B}]\!]\wedge\sigma_n\notin Q\}
\end{array}$$

PROOF OF TH. 4.2.

$$\begin{array}{ll}
\mathcal{T}_{\overline{\text{HL}}}(\mathtt{W}) & \\
= \{\langle P,\ Q\rangle \mid \mathsf{post}[\![\neg\mathtt{B}]\!](\mathsf{lfp}^{\subseteq}\bar{\bar{F}}^{e}_{P})\cap\neg Q\neq\varnothing\} & \wr\text{Lem. 1.3, where } \bar{\bar{F}}^{e}_{P}(X)\triangleq P\cup\mathsf{post}([\![\mathtt{B}]\!]\,{\scriptstyle\fatsemi}\,[\![\mathtt{S}]\!]^{e})X\wr \\
= \{\langle P,\ Q\rangle \mid \mathsf{lfp}^{\subseteq}\bar{\bar{F}}^{e}_{P}\cap\mathsf{pre}[\![\neg\mathtt{B}]\!](\neg Q)\neq\varnothing\} & \wr\text{(39.d)}\wr
\end{array}$$

$= \{\langle P,\ Q\rangle \mid \exists I\in\wp(\Sigma)\ .\ \bar{\bar{F}}^{e}_{P}(I)\subseteq I\wedge\exists\langle W,\ \leqslant\rangle\in\mathfrak{Wf}\ .\ \exists\nu\in I\to W\ .\ \exists\langle\sigma_i\in I,\ i\in[1,\infty]\rangle\ .\ \sigma_1\in\bar{\bar{F}}^{e}_{P}(\varnothing)\wedge\forall i\in[1,\infty]\ .\ \sigma_{i+1}\in\bar{\bar{F}}^{e}_{P}(\{\sigma_i\})\wedge\forall i\in[1,\infty]\ .\ (\sigma_i\neq\sigma_{i+1})\Rightarrow(\nu(\sigma_i)>\nu(\sigma_{i+1})\wedge\forall i\in[1,\infty]\ .\ (\nu(\sigma_i)\ngtr\nu(\sigma_{i+1})\Rightarrow\{\sigma_i\}\cap\mathsf{pre}[\![\neg\mathtt{B}]\!](\neg Q)\neq 0\}$ $\wr$induction principle Th. H.3$\wr$

$= \{\langle P,\ Q\rangle \mid \exists I\in\wp(\Sigma)\ .\ P\subseteq I\wedge\mathsf{post}([\![\mathtt{B}]\!]\,{\scriptstyle\fatsemi}\,[\![\mathtt{S}]\!]^{e})I\subseteq I\wedge\exists\langle W,\ \leqslant\rangle\in\mathfrak{Wf}\ .\ \exists\nu\in I\to W\ .\ \exists\langle\sigma_i\in I,\ i\in[1,\infty]\rangle\ .\ \sigma_1\in P\wedge\forall i\in[1,\infty]\ .\ (\sigma_{i+1}\in P\vee\{\sigma_{i+1}\}\subseteq\mathsf{post}([\![\mathtt{B}]\!]\,{\scriptstyle\fatsemi}\,[\![\mathtt{S}]\!]^{e})\{\sigma_i\})\wedge\forall i\in[1,\infty]\ .\ (\sigma_i\neq\sigma_{i+1})\Rightarrow(\nu(\sigma_i)>\nu(\sigma_{i+1})\wedge\forall i\in[1,\infty]\ .\ (\nu(\sigma_i)\ngtr\nu(\sigma_{i+1})\Rightarrow\sigma_i\in\mathsf{pre}[\![\neg\mathtt{B}]\!](\neg Q)\}$

$\wr$def. $\bar{\bar{F}}^{e}_{P}(X)\triangleq P\cup\mathsf{post}([\![\mathtt{B}]\!]\,{\scriptstyle\fatsemi}\,[\![\mathtt{S}]\!]^{e})X$, $\subseteq$, and post, which is $\varnothing$-strict$\wr$

$= \{\langle P,\ Q\rangle \mid \exists I \in \wp(\Sigma)\ .\ P \subseteq I \wedge \mathsf{post}(\llbracket \mathtt{B}\rrbracket \mathbin{⨾} \llbracket \mathtt{S}\rrbracket^e)I \subseteq I \wedge \exists\langle W,\ \preccurlyeq\rangle \in \mathfrak{Wf}\ .\ \exists \nu \in I \to W\ .\ \exists\langle \sigma_i \in I,\ i \in [1,\infty]\rangle\ .\ \sigma_1 \in P \wedge \forall i \in [1,\infty]\ .\ \{\sigma_{i+1}\} \subseteq \mathsf{post}(\llbracket \mathtt{B}\rrbracket \mathbin{⨾} \llbracket \mathtt{S}\rrbracket^e)\{\sigma_i\} \wedge \forall i \in [1,\infty]\ .\ (\sigma_i \neq \sigma_{i+1}) \Rightarrow (\nu(\sigma_i) > \nu(\sigma_{i+1}) \wedge \forall i \in [1,\infty]\ .\ (\nu(\sigma_i) \not> \nu(\sigma_{i+1}) \Rightarrow \sigma_i \in \mathsf{pre}\llbracket\neg\mathtt{B}\rrbracket(\neg Q)\}$

$\wr$since if $\sigma_{i+1} \in P$, we can equivalently consider the sequence $\langle \sigma_j \in I,\ j \in [i+1,\infty]\rangle$$\wr$

$= \{\langle P,\ Q\rangle \mid \exists I \in \wp(\Sigma)\ .\ P \subseteq I \wedge \mathsf{post}(\llbracket \mathtt{B}\rrbracket \mathbin{⨾} \llbracket \mathtt{S}\rrbracket^e)I \subseteq I \wedge \exists n \geqslant 1\ .\ \exists\langle \sigma_i \in I,\ i \in [1,n]\rangle\ .\ \sigma_1 \in P \wedge \forall i \in [1,n[\ .\ \{\sigma_{i+1}\} \subseteq \mathsf{post}(\llbracket \mathtt{B}\rrbracket \mathbin{⨾} \llbracket \mathtt{S}\rrbracket^e)\{\sigma_i\} \wedge \sigma_n \in \mathsf{pre}\llbracket\neg\mathtt{B}\rrbracket(\neg Q)\}$

$\wr$($\subseteq$) By $\langle W,\ \preccurlyeq\rangle \in \mathfrak{Wf}$, $\nu \in I \to W$, $\forall i \in [1,\infty]\ .\ (\sigma_i \neq \sigma_{i+1}) \Rightarrow (\nu(\sigma_i) > \nu(\sigma_{i+1})$, the sequence is ultimately stationary at some rank n. For then on, $\sigma_{i+1} = \sigma_i$, $i \geqslant n$ and so $\nu(\sigma_i) = \nu(\sigma_{i+1})$. Therefore $\forall i \in [1,\infty]\ .\ (\nu(\sigma_i) \not> \nu(\sigma_{i+1}) \Rightarrow \sigma_i \notin Q$ implies that $\sigma_n \in \mathsf{pre}\llbracket\neg\mathtt{B}\rrbracket(\neg Q)$;

($\supseteq$) Conversely, from $\langle \sigma_i \in I,\ i \in [1,n]\rangle$ we can define $W = \{\sigma_i \mid i \in [1,n]\} \cup \{-\infty\}$ with $-\infty < \sigma_i < \sigma_{i+1}$ and $\nu(x) = (\!| x \in \{\sigma_i \mid i \in [1,n]\ ?\ x \mathbin{:} -\infty |\!)$ and the sequence $\langle \sigma_j \in I,\ j \in [1,\infty]\rangle$ repeats σ_n ad infimum for $j \geqslant n$.$\wr$

$= \{\langle P,\ Q\rangle \mid \exists I \in \wp(\Sigma)\ .\ P \subseteq I \wedge \mathsf{post}(\llbracket \mathtt{B}\rrbracket \mathbin{⨾} \llbracket \mathtt{S}\rrbracket^e)I \subseteq I \wedge \exists n \geqslant 1\ .\ \exists\langle \sigma_i \in I,\ i \in [1,n]\rangle\ .\ \sigma_1 \in P \wedge \forall i \in [1,n[\ .\ \{\sigma_{i+1}\} \subseteq \mathsf{post}(\llbracket \mathtt{B}\rrbracket \mathbin{⨾} \llbracket \mathtt{S}\rrbracket^e)\{\sigma_i\} \wedge \sigma_n \notin \mathcal{B}\llbracket\mathtt{B}\rrbracket \wedge \sigma_n \notin Q\}$ $\wr$def. pre$\wr$

$= \{\langle P,\ Q\rangle \mid \exists n \geqslant 1\ .\ \exists\langle \sigma_i \in I,\ i \in [1,n]\rangle\ .\ \sigma_1 \in P \wedge \forall i \in [1,n[\ .\ \{\sigma_{i+1}\} \subseteq \mathsf{post}(\llbracket \mathtt{B}\rrbracket \mathbin{⨾} \llbracket \mathtt{S}\rrbracket^e)\{\sigma_i\} \wedge \sigma_n \notin \mathcal{B}\llbracket\mathtt{B}\rrbracket \wedge \sigma_n \notin Q\}$ $\wr$$I$ is not used and can always be chosen to be $\Sigma$$\wr$

$= \{\langle P,\ Q\rangle \mid \exists n \geqslant 1\ .\ \exists\langle \sigma_i \in I,\ i \in [1,n]\rangle\ .\ \sigma_1 \in P \wedge \forall i \in [1,n[\ .\ \mathsf{post}(\llbracket \mathtt{B}\rrbracket \mathbin{⨾} \llbracket \mathtt{S}\rrbracket^e)\{\sigma_i\} \cap \{\sigma_{i+1}\} \neq \varnothing \wedge \sigma_n \notin \mathcal{B}\llbracket\mathtt{B}\rrbracket \wedge \sigma_n \notin Q\}$ $\wr$since $x \in X \Leftrightarrow X \cap \{x\} \neq \varnothing$$\wr$

$= \{\langle P,\ Q\rangle \mid \exists n \geqslant 1\ .\ \exists\langle \sigma_i \in I,\ i \in [1,n]\rangle\ .\ \sigma_1 \in P \wedge \forall i \in [1,n[\ .\ \mathsf{post}(\llbracket \mathtt{B}\rrbracket \mathbin{⨾} \llbracket \mathtt{S}\rrbracket^e)\{\sigma_i\} \cap \neg(\neg\{\sigma_{i+1}\}) \neq \varnothing \wedge \sigma_n \notin \mathcal{B}\llbracket\mathtt{B}\rrbracket \wedge \sigma_n \notin Q\}$ $\wr$def. $\neg X = \Sigma \setminus X$$\wr$

$= \{\langle P,\ Q\rangle \mid \exists n \geqslant 1\ .\ \exists\langle \sigma_i \in I,\ i \in [1,n]\rangle\ .\ \sigma_1 \in P \wedge \forall i \in [1,n[\ .\ \neg(\mathsf{post}(\llbracket \mathtt{B}\rrbracket \mathbin{⨾} \llbracket \mathtt{S}\rrbracket^e)\{\sigma_i\} \subseteq (\neg\{\sigma_{i+1}\})) \wedge \sigma_n \notin \mathcal{B}\llbracket\mathtt{B}\rrbracket \wedge \sigma_n \notin Q\}$ $\wr\neg(X \subseteq Y) \Leftrightarrow (X \cap \neg Y \neq \varnothing$$\wr$

$= \{\langle P,\ Q\rangle \mid \exists n \geqslant 1\ .\ \exists\langle \sigma_i \in I,\ i \in [1,n]\rangle\ .\ \sigma_1 \in P \wedge \forall i \in [1,n[\ .\ \neg(\mathsf{post}(\llbracket \mathtt{S}\rrbracket^e)(\mathcal{B}\llbracket\mathtt{B}\rrbracket \cap \{\sigma_i\}) \subseteq (\neg\{\sigma_{i+1}\})) \wedge \sigma_n \notin \mathcal{B}\llbracket\mathtt{B}\rrbracket \wedge \sigma_n \notin Q\}$ $\wr$def. post, $\llbracket\mathtt{B}\rrbracket$, and $⨾$$\wr$

$= \{\langle P,\ Q\rangle \mid \exists n \geqslant 1\ .\ \exists\langle \sigma_i \in I,\ i \in [1,n]\rangle\ .\ \sigma_1 \in P \wedge \forall i \in [1,n[\ .\ \langle \mathcal{B}\llbracket\mathtt{B}\rrbracket \cap \{\sigma_i\},\ \neg\{\sigma_{i+1}\}\rangle \in \{\langle P,\ Q\rangle \mid \neg(\mathsf{post}(\llbracket \mathtt{S}\rrbracket^e)P \subseteq Q)\} \wedge \sigma_n \notin \mathcal{B}\llbracket\mathtt{B}\rrbracket \wedge \sigma_n \notin Q\}$ $\wr$def. $\in$$\wr$

$= \{\langle P,\ Q\rangle \mid \exists n \geqslant 1\ .\ \exists\langle \sigma_i \in I,\ i \in [1,n]\rangle\ .\ \sigma_1 \in P \wedge \forall i \in [1,n[\ .\ \langle \mathcal{B}\llbracket\mathtt{B}\rrbracket \cap \{\sigma_i\},\ \neg\{\sigma_{i+1}\}\rangle \in \mathcal{T}_{\overline{\mathrm{HL}}}(\mathtt{S}) \wedge \sigma_n \notin \mathcal{B}\llbracket\mathtt{B}\rrbracket \wedge \sigma_n \in Q\}$ $\wr$def. $\mathcal{T}_{\overline{\mathrm{HL}}}(\mathtt{S})$$\wr$ □

4.2 Calculational Design of $\overline{\mathrm{HL}}$ Proof Rules

Theorem 4.3 ($\overline{\mathrm{HL}}$ rules for conditional iteration). `W = while (B) S`

$$\frac{\exists\langle \sigma_i \in I,\ i \in [1,n]\rangle\ .\ \sigma_1 \in P \wedge \forall i \in [1,n[\ .\ (\!| \mathcal{B}\llbracket\mathtt{B}\rrbracket \cap \{\sigma_i\} |\!)\ \mathtt{S}\ (\!| \neg\{\sigma_{i+1}\} |\!) \wedge \sigma_n \notin \mathcal{B}\llbracket\mathtt{B}\rrbracket \wedge \sigma_n \notin Q}{(\!| P |\!)\ \mathtt{while\ (B)\ S}\ (\!| Q |\!)} \tag{3}$$

Proof of (3). We write $(\!| P |\!)\ \mathtt{S}\ (\!| Q |\!) \triangleq \langle P,\ Q\rangle \in \overline{\mathrm{HL}}(\mathtt{S})$;

By structural induction ($\mathtt{S}$ being a strict component of `while (B) S`), the rule for $(\!| P |\!)\ \mathtt{S}\ (\!| Q |\!)$ have already been defined;

By Aczel method, the (constant) fixpoint $\mathsf{lfp}^{\subseteq}\, \boldsymbol{\lambda} X \bullet S$ is defined by $\{\frac{\varnothing}{c} \mid c \in S\}$;

So for `while (B) S` we have an axiom $\dfrac{\varnothing}{(\!| P |\!)\ \mathtt{while\ (B)\ S}\ (\!| Q |\!)}$ with side condition $\exists\langle \sigma_i \in I,\ i \in [1,n]\rangle\ .\ \sigma_1 \in P \wedge \forall i \in [1,n[\ .\ (\!| \mathcal{B}\llbracket\mathtt{B}\rrbracket \cap \{\sigma_i\} |\!)\ \mathtt{S}\ (\!| \neg\{\sigma_{i+1}\} |\!) \wedge \sigma_n \notin \mathcal{B}\llbracket\mathtt{B}\rrbracket \wedge \sigma_n \notin Q$ where $(\!| \mathcal{B}\llbracket\mathtt{B}\rrbracket \cap \{\sigma_i\} |\!)\ \mathtt{S}\ (\!| \neg\{\sigma_{i+1}\} |\!)$ is well-defined by structural induction;

Traditionally, the side condition is written as a premiss, to get (3). □

This is nothing but debugging formalized as a logic since $\langle \sigma_i \in I,\ i \in [1, n] \rangle$ is a finite iteration in the loop starting with P true and finishing with Q false, which is obviously a counter example to Hoare triple $\{P\}$ `while (B) S` $\{Q\}$. Notice that recursively $(\!| \mathcal{B}[\![\mathtt{B}]\!] \cap \{\sigma_i\} |\!)\, \mathtt{S}\, (\!| \{\sigma_{i+1}\} |\!)$ enforces the execution of the loop body `S` to start in state σ_i and terminate in state σ_{i+1}.

5 COMPARISON OF INCORRECTNESS LOGIC AND HOARE INCORRECTNESS LOGIC

Lemma 5.1 (IL is sufficient but not necessary for incorrectness). *Assuming* $Q \neq \Sigma$.

$$\begin{array}{rcl} \neg(\{P\}\,\mathsf{S}\{Q\}) & \Leftrightarrow & \mathsf{post}(R)P \cap \neg Q \neq \varnothing \\ & \Leftrightarrow & \exists \sigma \in P \,.\, \exists \sigma' \notin Q \,.\, \langle \sigma,\, \sigma' \rangle \in [\![\mathsf{S}]\!] \\ & \Leftrightarrow & P \cap \mathsf{pre}[\![\mathsf{S}]\!]\neg Q \neq \varnothing \\ & \overset{\not\Rightarrow}{\Leftarrow} & \forall \sigma' \notin Q \,.\, \exists \sigma \in P \,.\, \langle \sigma,\, \sigma' \rangle \in [\![\mathsf{S}]\!] \\ & \Leftrightarrow & [P]\mathsf{S}[\neg Q] \end{array} \tag{4}$$

Proof of Lem. 5.1.

$\neg(\{P\}\,\mathsf{S}\{Q\})$

$\Leftrightarrow \neg(\mathsf{post}[\![\mathsf{S}]\!]P \subseteq Q)$ ≀Lem. 1.4≀

$\Leftrightarrow \mathsf{post}[\![\mathsf{S}]\!]P \cap \neg Q \neq \varnothing$ ≀De Morgan≀

$\Leftrightarrow \exists \sigma \in P \,.\, \exists \sigma' \notin Q \,.\, \langle \sigma,\, \sigma' \rangle \in [\![\mathsf{S}]\!]$ ≀def. $\cap$ and $\varnothing$≀

$\Leftrightarrow P \cap \mathsf{pre}[\![\mathsf{S}]\!]\neg Q \neq \varnothing$ ≀def. pre≀

$[P]\mathsf{S}[\neg Q]$ ≀reverse Hoare aka incorrectness logic≀

$\Leftrightarrow \neg Q \subseteq \mathsf{post}[\![\mathsf{S}]\!]P$ ≀def. triple≀

$\Leftrightarrow \neg Q \subseteq \{\sigma' \mid \exists \sigma \in P \,.\, \langle \sigma,\, \sigma' \rangle \in [\![\mathsf{S}]\!]\}$ ≀def. post≀

$\Leftrightarrow \forall \sigma' \notin Q \,.\, \exists \sigma \in P \,.\, \langle \sigma,\, \sigma' \rangle \in [\![\mathsf{S}]\!]$ ≀def. $\subseteq$ and $\neg$≀

$\overset{\not\Leftarrow}{\Rightarrow} \exists \sigma \in P \,.\, \exists \sigma' \,.\, \langle \sigma,\, \sigma' \rangle \in [\![\mathsf{S}]\!] \wedge \sigma' \notin Q$

≀($\Rightarrow$) Assume $\neg Q \neq \varnothing$ so pick $\sigma_0 \in \neg Q$. Then, by hypothesis, $\exists \sigma_1 \in P \,.\, \langle \sigma_0,\, \sigma_1 \rangle \in [\![\mathsf{S}]\!]$ proving $\exists \sigma \in P \,.\, \exists \sigma' \,.\, \langle \sigma,\, \sigma' \rangle \in [\![\mathsf{S}]\!] \wedge \sigma' \notin Q$ with $\sigma = \sigma_0$ and $\sigma' = \sigma_1$;
($\not\Leftarrow$) If $\neg Q = \varnothing$ i.e. $Q = \Sigma$ then $\forall \sigma' \notin Q \,.\, \exists \sigma \in P \,.\, \langle \sigma,\, \sigma' \rangle \in [\![\mathsf{S}]\!]$ is vacuously true while $\exists \sigma' \,.\, \sigma' \notin Q$ hence $\exists \sigma \in P \,.\, \exists \sigma' \,.\, \langle \sigma,\, \sigma' \rangle \in [\![\mathsf{S}]\!] \wedge \sigma' \notin Q$ is false≀ □

Lemma 5.2 (Proving Hoare incorrectness with IL).

$$\begin{array}{rcl} \neg(\{P\}\,\mathsf{S}\{Q\}) & \Leftrightarrow & \exists R \in \wp(\Sigma) \,.\, [P]\,\mathsf{S}\,[R] \wedge R \cap \neg Q \neq \varnothing \\ & \Leftrightarrow & \exists \sigma \in \Sigma \,.\, [P]\,\mathsf{S}\,[\{\sigma\}] \wedge \sigma \notin Q \end{array} \tag{5}$$

Proof of Lem. 5.2.

$\neg(\{P\}\,\mathsf{S}\{Q\})$ ≀def. incorrect Hoare triple≀

$\Leftrightarrow \exists \sigma \in P \,.\, \exists \sigma' \notin Q \,.\, \langle \sigma,\, \sigma' \rangle \in [\![\mathsf{S}]\!]$ ≀lem. 5.1≀

$\Leftrightarrow \exists \sigma \notin Q \,.\, \exists \sigma' \in P \,.\, \langle \sigma',\, \sigma \rangle \in [\![\mathsf{S}]\!]$ ≀commutativity and renaming≀

$\Leftrightarrow \exists \sigma \in \Sigma \,.\, \exists \sigma' \in P \,.\, \langle \sigma',\, \sigma \rangle \in [\![\mathsf{S}]\!] \wedge \sigma \notin Q$ ≀def. $\exists$≀

$\Leftrightarrow \exists \sigma \in \Sigma \,.\, \forall \sigma'' \in \{\sigma\} \,.\, \exists \sigma' \in P \,.\, \langle \sigma',\, \sigma'' \rangle \in [\![\mathsf{S}]\!] \wedge \sigma \notin Q$ ≀def. $\in$≀

$\Leftrightarrow \exists \sigma \in \Sigma \,.\, [P]\,\mathsf{S}\,[\{\sigma\}] \wedge \sigma \notin Q$ ≀def. IL≀

$\Leftrightarrow \exists R \in \wp(\Sigma) \,.\, [P]\,\mathsf{S}\,[R] \wedge R \cap \neg Q \neq \varnothing$

≀($\subseteq$) take $R = \{\sigma\}$;
($\supseteq$) since $R \cap \neg Q \neq \varnothing$, we have $\exists \sigma \in R \,.\, \sigma \notin Q$ and $[P]\,\mathsf{S}\,[\{\sigma\}]$ since otherwise we would have $\neg(\forall \sigma'' \in \{\sigma\} \,.\, \exists \sigma' \in P \,.\, \langle \sigma'',\, \sigma' \rangle \in [\![\mathsf{S}]\!]) \Leftrightarrow \forall \sigma' \in P \,.\, \langle \sigma,\, \sigma' \rangle \notin [\![\mathsf{S}]\!])$, in contradiction with $[P]\,\mathsf{S}\,[R]$ and $\sigma \in R$. ≀ □