Calculational Design of [In]Correctness Transformational Program Logics by Abstract Interpretation

Patrick Cousot

Courant Institute, New York University

Objective

Method to design program transformational logics

Transformational logic = Hoare style logics {P} S {Q}

Method to design a program transformational logics

1. Define the natural relational semantics $[\![\mathsf{S}]\!]_\perp$ of the programming language (in structural fixpoint form)

Method to design a program transformational logics

1. Define the natural relational semantics $[\![S]\!]_\perp$ of the programming language (in structural fixpoint form)
2. Define the theory of the logics as an abstraction $\alpha(\{[\![S]\!]_\perp\})$ of the collecting semantics $\{[\![S]\!]_\perp\}$ (strongest (hyper) property)

Theory of a logic = the subset of all true formulas

Method to design a program transformational logics

1. Define the natural relational semantics $[\![S]\!]_{\perp}$ of the programming language (in structural fixpoint form)
2. Define the theory of the logics as an abstraction $\alpha(\{[\![S]\!]_{\perp}\})$ of the collecting semantics $\{[\![S]\!]_{\perp}\}$ (strongest (hyper) property)
3. Calculate the theory $\alpha(\{[\![S]\!]_{\perp}\})$ in structural fixpoint form by fixpoint abstraction

Theory of a logic = the subset of all true formulas

Method to design a program transformational logics

1. Define the natural relational semantics $[\![S]\!]_\perp$ of the programming language (in structural fixpoint form)
2. Define the theory of the logics as an abstraction $\alpha(\{[\![S]\!]_\perp\})$ of the collecting semantics $\{[\![S]\!]_\perp\}$ (strongest (hyper) property)
3. Calculate the theory $\alpha(\{[\![S]\!]_\perp\})$ in structural fixpoint form by fixpoint abstraction
4. Calculate the proof system by fixpoint induction and Aczel correspondence between fixpoints and deductive systems

Theory of a logic = the subset of all true formulas

Two simple examples*:

Hoare (HL) and reverse Hoare aka incorrectness (IL) logics

* not in the paper (where the examples are more complicated).

General Idea

HL = strongest postcondition abstraction of the collecting semantics
+ over approximating consequence abstraction
} theory

+ over approximating fixpoint induction
+ Aczel correspondence fixpoint ⇹ proof system
} proof system

General Idea

HL = strongest postcondition abstraction of the collecting semantics
+ over approximating consequence abstraction
+ over approximating fixpoint induction
+ Aczel correspondence fixpoint ⇹ proof system

} theory
} proof system

IL = strongest postcondition abstraction of the collecting semantics
+ under approximating consequence abstraction
+ under approximating fixpoint induction
+ Aczel correspondence fixpoint ⇹ proof system

} theory
} proof system

1. Angelic relational semantics $[\![\mathtt{S}]\!]^e$

- Syntax*:

$$\mathtt{S} \in \mathbb{S} ::= \mathtt{x\ =\ A} \mid \mathtt{skip} \mid \mathtt{S;S} \mid \mathtt{if\ (B)\ S\ else\ S} \mid \mathtt{while\ (B)\ S} \mid \mathtt{x\ =\ [}a\mathtt{,}b\mathtt{]} \mid \mathtt{break}$$

- States: Σ

ends

- Angelic relational semantics: $[\![\mathtt{S}]\!]^e \in \wp(\Sigma \times \Sigma)$

* plus unbounded nondeterminism, breaks, and nontermination $\perp$ in the paper.

1. Angelic relational semantics $[\![\mathtt{S}]\!]$ (in deductive form)

- Notations using judgements:
  - $\sigma \vdash \mathtt{S} \overset{e}{\Rightarrow} \sigma'$ for $\langle \sigma, \sigma' \rangle \in [\![\mathtt{S}]\!]^e$
  - $\sigma \vdash \mathtt{while(B)\ S} \overset{i}{\Rightarrow} \sigma'$ for σ leads to σ' after 0 or more iterations

1. Angelic relational semantics $[\![S]\!]$ (in deductive form)

- Notations using judgements:
  - $\sigma \vdash \mathtt{S} \overset{e}{\Rightarrow} \sigma'$ for $\langle \sigma, \sigma' \rangle \in [\![\mathtt{S}]\!]^e$
  - $\sigma \vdash \mathtt{while(B)\ S} \overset{i}{\Rightarrow} \sigma'$ for σ leads to σ' after 0 or more iterations
- Semantics of the conditional iteration* $\mathtt{W} = \mathtt{while(B)\ S}$:

$$\text{(a)}\quad \sigma \vdash \mathtt{W} \overset{i}{\Rightarrow} \sigma \qquad\qquad \text{(b)}\quad \frac{\mathcal{B}[\![\mathtt{B}]\!]\sigma, \quad \sigma \vdash \mathtt{S} \overset{e}{\Rightarrow} \sigma', \quad \sigma' \vdash \mathtt{W} \overset{i}{\Rightarrow} \sigma''}{\sigma \vdash \mathtt{W} \overset{i}{\Rightarrow} \sigma''} \tag{2}$$

$$\text{(a)}\quad \frac{\sigma \vdash \mathtt{W} \overset{i}{\Rightarrow} \sigma', \quad \mathcal{B}[\![\neg\mathtt{B}]\!]\sigma'}{\sigma \vdash \mathtt{W} \overset{e}{\Rightarrow} \sigma'} \tag{3}$$

* plus breaks, and co-induction for nontermination $\perp$ in the paper.

1. Angelic relational semantics $[\![S]\!]$ (in fixpoint form)

- Semantics of the conditional iteration* $\texttt{W} = \texttt{while(B) S}$:

$$F^e(X) \triangleq \mathsf{id} \cup ([\![\mathsf{B}]\!] \mathbin{;} [\![\mathsf{S}]\!]^e \mathbin{;} X), \quad X \in \wp(\Sigma \times \Sigma) \tag{49}$$

$$[\![\texttt{while (B) S}]\!]^e \triangleq \mathsf{lfp}^{\subseteq} F^e \mathbin{;} [\![\neg\mathsf{B}]\!] \quad \text{(no break)} \tag{51}$$

- Derived using Aczel correspondence between deductive systems and set-theoretic fixpoints, see Ex. II.5.1

Aczel correspondence between deductive systems and fixpoints

- **Rules:** $\dfrac{P}{c}$ ($\mathcal{U}$ universe, $P \in \wp_{\text{fin}}(\mathcal{U})$ premiss, $c \in \mathcal{U}$ conclusion, $\dfrac{\varnothing}{c}$ axiom)

Aczel correspondence between deductive systems and fixpoints

- Rules: $\dfrac{P}{c}$ ($\mathcal{U}$ universe, $P \in \wp_{\mathrm{fin}}(\mathcal{U})$ premiss, $c \in \mathcal{U}$ conclusion, $\dfrac{\varnothing}{c}$ axiom)
- Deductive system : $R = \left\{ \dfrac{P_i}{c_i} \;\middle|\; i \in \Delta \right\}, \quad R \in \wp(\wp_{\mathrm{fin}}(\mathcal{U}) \times \mathcal{U})$

Aczel correspondence between deductive systems and fixpoints

- Rules: $\frac{P}{c}$ ($\mathcal{U}$ universe, $P \in \wp_{\mathrm{fin}}(\mathcal{U})$ premiss, $c \in \mathcal{U}$ conclusion, $\frac{\varnothing}{c}$ axiom)
- Deductive system : $R = \left\{ \frac{P_i}{c_i} \;\middle|\; i \in \Delta \right\}$, $R \in \wp(\wp_{\mathrm{fin}}(\mathcal{U}) \times \mathcal{U})$
- Subset of the universe $\mathcal{U}$ defined by R:

proof theoretic ↓

$$\{t_n \in \mathcal{U} \mid \exists t_1, \ldots, t_{n-1} \in \mathcal{U} \;.\; \forall k \in [1, n] \;.\; \exists \frac{P}{c} \in R \;.\; P \subseteq \{t_1, \ldots, t_{k-1}\} \wedge t_k = c\}$$

$$= \quad \mathsf{lfp}^{\subseteq}\, F(R)$$

← model theoretic (gfp for coinduction)

$$F(R)X \;\triangleq\; \left\{c \;\middle|\; \exists \frac{P}{c} \in R \;.\; P \subseteq X\right\}$$

← consequence operator

Aczel correspondence between deductive systems and fixpoints

- Rules: $\frac{P}{c}$ ($\mathcal{U}$ universe, $P \in \wp_{\mathrm{fin}}(\mathcal{U})$ premiss, $c \in \mathcal{U}$ conclusion, $\frac{\emptyset}{c}$ axiom)

- Deductive system : $R = \left\{\frac{P_i}{c_i} \,\middle|\, i \in \Delta\right\}$, $R \in \wp(\wp_{\mathrm{fin}}(\mathcal{U}) \times \mathcal{U})$

- Subset of the universe $\mathcal{U}$ defined by R:

proof theoretic ↓

$$\{t_n \in \mathcal{U} \mid \exists t_1, \ldots, t_{n-1} \in \mathcal{U} \,.\, \forall k \in [1, n] \,.\, \exists \frac{P}{c} \in R \,.\, P \subseteq \{t_1, \ldots, t_{k-1}\} \wedge t_k = c\}$$

$$= \operatorname{lfp}^{\subseteq} F(R)$$

← model theoretic (gfp for coinduction)

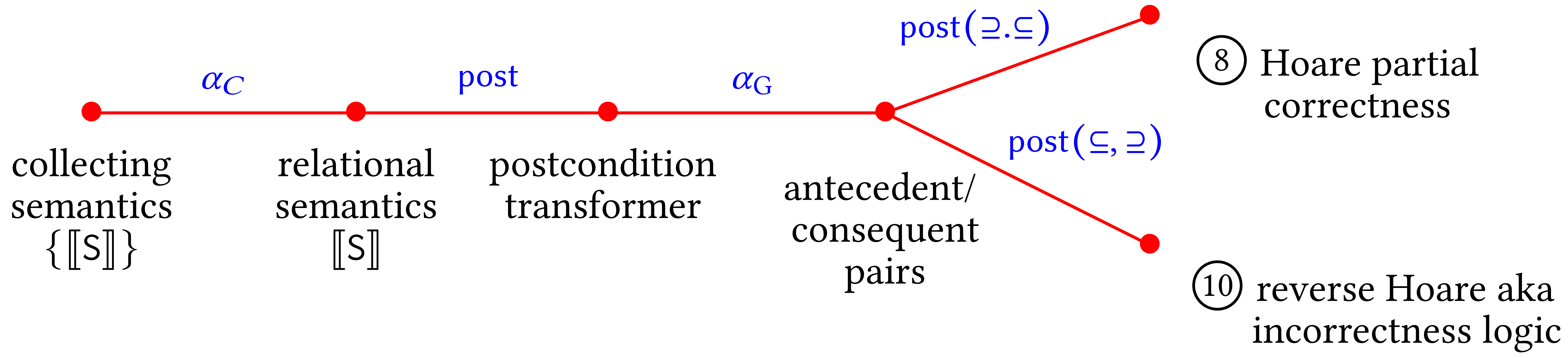
$$F(R)X \triangleq \left\{c \,\middle|\, \exists \frac{P}{c} \in R \,.\, P \subseteq X\right\}$$

← consequence operator

- Deductive system defining $\operatorname{lfp}^{\subseteq} F$: $R_F \triangleq \left\{\frac{P}{c} \,\middle|\, P \subseteq \mathcal{U} \wedge c \in F(P)\right\}$

2. Abstraction (much simplified)

- The composition of these abstractions is



- This is an oversimplification of Fig. 1 of the paper, forgetting about nontermination including total correctness and relational predicates

2. Abstraction (much simplified)

- Hyper properties to properties abstraction:

$$\langle \wp(\wp(\Sigma \times \Sigma)),\ \subseteq \rangle \xrightleftharpoons[\alpha_C]{\gamma_C} \langle \wp(\Sigma \times \Sigma),\ \subseteq \rangle \qquad \alpha_C(P) \triangleq \bigcup P \qquad \gamma_C(S) \triangleq \wp(S)$$

2. Abstraction (much simplified)

- Hyper properties to properties abstraction:

$$\langle \wp(\wp(\Sigma \times \Sigma)),\ \subseteq\rangle \underset{\alpha_C}{\overset{\gamma_C}{\leftrightarrows}} \langle \wp(\Sigma \times \Sigma),\ \subseteq\rangle \qquad \alpha_C(P) \triangleq \bigcup P \qquad \gamma_C(S) \triangleq \wp(S)$$

- Post-image isomorphism:

$$\langle \wp(\Sigma \times \Sigma),\ \subseteq\rangle \underset{\text{post}}{\overset{\widetilde{\text{pre}}}{\leftrightarrows}} \langle \wp(\Sigma) \to \wp(\Sigma),\ \subseteq\rangle \quad \text{post}(R) \triangleq \boldsymbol{\lambda} P \bullet \{\sigma' \mid \exists \sigma \in P \land \langle\sigma,\ \sigma'\rangle \in R\}$$

$$\widetilde{\text{pre}}(R) \triangleq \boldsymbol{\lambda} X \bullet \{\sigma \mid \forall \sigma' \in Q\ .\ \langle\sigma,\ \sigma'\rangle \in R\}$$

2. Abstraction (much simplified)

- Hyper properties to properties abstraction:

$$\langle \wp(\wp(\Sigma \times \Sigma)), \subseteq \rangle \xleftarrow[\alpha_C]{\gamma_C} \langle \wp(\Sigma \times \Sigma), \subseteq \rangle \qquad \alpha_C(P) \triangleq \bigcup P \qquad \gamma_C(S) \triangleq \wp(S)$$

- Post-image isomorphism:

$$\langle \wp(\Sigma \times \Sigma), \subseteq \rangle \xleftarrow[\text{post}]{\widetilde{\text{pre}}} \langle \wp(\Sigma) \to \wp(\Sigma), \subseteq \rangle \quad \text{post}(R) \triangleq \boldsymbol{\lambda} P \bullet \{\sigma' \mid \exists \sigma \in P \wedge \langle \sigma, \sigma' \rangle \in R\}$$

$$\widetilde{\text{pre}}(R) \triangleq \boldsymbol{\lambda} X \bullet \{\sigma \mid \forall \sigma' \in Q \,.\, \langle \sigma, \sigma' \rangle \in R\}$$

- Graph isomorphism (a function is isomorphic to its graph, which is a function relation):…/…

$$\langle \wp(\Sigma) \to \wp(\Sigma), = \rangle \xleftarrow[\alpha_{\mathrm{G}}]{\gamma_{\mathrm{G}}} \langle \wp_{\mathrm{fun}}(\wp(\Sigma) \times \wp(\Sigma)), = \rangle \quad f \in \wp(\Sigma) \to \wp(\Sigma)$$

$$\alpha_{\mathrm{G}}(f) = \{\langle P, f(P) \rangle \mid P \in \wp(\Sigma)\}$$

$$\gamma_{\mathrm{G}}(R) \triangleq \boldsymbol{\lambda} P \bullet (Q \textit{ such that } \langle P, S \rangle \in R)$$

2. Abstraction (much simplified)

- Strongest postcondition logic theory (common to HL and IL with no consequence rule):

$$\begin{array}{rcl}\mathcal{T}(\mathsf{S}) & \triangleq & \alpha_{\mathrm{G}} \circ \mathrm{post} \circ \alpha_C(\{[\![\mathsf{S}]\!]\}) \\ & = & \{\langle P,\ \mathrm{post}[\![\mathsf{S}]\!]P\rangle \mid P \in \wp(\Sigma)\}\end{array}$$

2. Abstraction (much simplified)

- Strongest postcondition logic theory (common to HL and IL with no consequence rule):

$$\begin{aligned} \mathcal{T}(\mathtt{S}) &\triangleq \alpha_{G} \circ \mathrm{post} \circ \alpha_{C}(\{[\![\mathtt{S}]\!]\}) \\ &= \{\langle P,\ \mathrm{post}[\![\mathtt{S}]\!]P\rangle \mid P \in \wp(\Sigma)\} \end{aligned}$$

- Notation: $\{\,P\,\}\,\mathtt{S}\,\{\,Q\,\} \triangleq \langle P,\ Q\rangle \in \mathcal{T}(\mathtt{S})$
- The next step is to express this theory in fixpoint form

2. Abstraction (much simplified)

- The abstraction of a fixpoint is a fixpoint (POPL 79)

THEOREM II.2.1 (FIXPOINT ABSTRACTION). *If* $\langle C, \sqsubseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle A, \preceq\rangle$ *is a Galois connection between complete lattices* $\langle C, \sqsubseteq\rangle$ *and* $\langle A, \preceq\rangle$, $f \in C \xrightarrow{i} C$ *and* $\bar{f} \in A \xrightarrow{i} A$ *are increasing and commuting, that is,* $\alpha \circ f = \bar{f} \circ \alpha$, *then* $\alpha(\mathsf{lfp}^{\sqsubseteq} f) = \mathsf{lfp}^{\preceq} \bar{f}$ *(while semi-commutation* $\alpha \circ f \preceq \bar{f} \circ \alpha$ *implies* $\alpha(\mathsf{lfp}^{\sqsubseteq} f) \preceq \mathsf{lfp}^{\preceq} \bar{f}$*).*

2. Abstraction (much simplified)

- The abstraction of a fixpoint is a fixpoint (POPL 79)

THEOREM II.2.1 (FIXPOINT ABSTRACTION). *If* $\langle C, \sqsubseteq\rangle \xrightleftharpoons[\alpha]{\gamma} \langle A, \preceq\rangle$ *is a Galois connection between complete lattices* $\langle C, \sqsubseteq\rangle$ *and* $\langle A, \preceq\rangle$, $f \in C \xrightarrow{i} C$ *and* $\bar{f} \in A \xrightarrow{i} A$ *are increasing and commuting, that is,* $\alpha \circ f = \bar{f} \circ \alpha$, *then* $\alpha(\mathsf{lfp}^{\sqsubseteq} f) = \mathsf{lfp}^{\preceq} \bar{f}$ *(while semi-commutation* $\alpha \circ f \preceq \bar{f} \circ \alpha$ *implies* $\alpha(\mathsf{lfp}^{\sqsubseteq} f) \preceq \mathsf{lfp}^{\preceq} \bar{f}$*).*

- We get a fixpoint definition of the theory of strongest postconditions logics (common to HL and IL with no consequences at all)
- For the iteration `W = while (B) S` :

$$\mathcal{T}(\mathtt{W}) \triangleq \{\langle P, \mathsf{post}[\![\neg\mathtt{B}]\!](\mathsf{lfp}^{\subseteq} \boldsymbol{\lambda} X \bullet P \cup \mathsf{post}([\![\mathtt{B}]\!] \fatsemi [\![\mathtt{S}]\!]^{e})X)\rangle \mid P \in \wp(\Sigma)\}$$

1 PROPERTIES OF STRONGEST POSTCONDITIONS

LEMMA 1.1 (COMPOSITION). $\mathsf{post}(X \fatsemi Y) = \mathsf{post}(Y) \circ \mathsf{post}(X)$.

PROOF OF LEM. 1.1.

$\mathsf{post}(X \fatsemi Y)$

$= \boldsymbol{\lambda} P \bullet \{\sigma'' \mid \exists \sigma \in P \,.\, \langle \sigma, \sigma'' \rangle \in X \fatsemi Y\}$ ⟅def. post⟆

$= \boldsymbol{\lambda} P \bullet \{\sigma'' \mid \exists \sigma \in P \,.\, \exists \sigma' \,.\, \langle \sigma, \sigma' \rangle \in X \wedge \langle \sigma', \sigma'' \rangle \in Y\}$ ⟅def. $\fatsemi$⟆

$= \boldsymbol{\lambda} P \bullet \{\sigma'' \mid \exists \sigma' \,.\, \sigma' \in \{\sigma' \mid \exists \sigma \in P \,.\, \langle \sigma, \sigma' \rangle \in X\} \wedge \langle \sigma', \sigma'' \rangle \in Y\}$ ⟅def. $\exists$ and $\in$⟆

$= \boldsymbol{\lambda} P \bullet \{\sigma'' \mid \exists \sigma' \in \mathsf{post}(X)P \,.\, \langle \sigma', \sigma'' \rangle \in Y\}$ ⟅def. post⟆

$= \boldsymbol{\lambda} P \bullet \mathsf{post}(Y)(\mathsf{post}(X)P)$ ⟅def. post⟆

$= \mathsf{post}(Y) \circ \mathsf{post}(X)$ ⟅def. function composition $\circ$⟆ ☐

LEMMA 1.2 (TEST). $\mathsf{post}\llbracket \mathtt{B} \rrbracket P = P \cap \mathcal{B}\llbracket \mathtt{B} \rrbracket$.

PROOF OF LEM. 1.2.

$\mathsf{post}\llbracket \mathtt{B} \rrbracket P$

$= \{\sigma' \mid \exists \sigma \in P \,.\, \langle \sigma, \sigma' \rangle \in \llbracket \mathtt{B} \rrbracket\}$ ⟅def. post⟆

$= \{\sigma \mid \sigma \in P \wedge \sigma \in \mathcal{B}\llbracket \mathtt{B} \rrbracket\}$ ⟅def. $\llbracket \mathtt{B} \rrbracket \triangleq \{\langle \sigma, \sigma \rangle \mid \sigma \in \mathcal{B}\llbracket \mathtt{B} \rrbracket\}$⟆

$= P \cap \mathcal{B}\llbracket \mathtt{B} \rrbracket$ ⟅def. intersection $\cup$⟆ ☐

LEMMA 1.3 (STRONGEST POSTCONDITION). $\mathcal{T}(\mathtt{S}) = \alpha_{\mathrm{G}} \circ \mathsf{post}\llbracket \mathtt{S} \rrbracket = \{\langle P,\ \mathsf{post}\llbracket \mathtt{S} \rrbracket P \rangle \mid P \in \wp(\Sigma)\}$.

PROOF OF LEM. 1.3.

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

$= \alpha_{\mathrm{G}} \circ \mathsf{post} \circ \alpha_{\not\perp} \circ \alpha_{C}(\{\llbracket \mathtt{S} \rrbracket_{\perp}\})$ ⟅def. $\mathcal{T}$⟆

$= \alpha_{\mathrm{G}} \circ \mathsf{post} \circ \alpha_{\not\perp}(\llbracket \mathtt{S} \rrbracket_{\perp})$ ⟅def. α_{C}⟆

$= \alpha_{\mathrm{G}} \circ \mathsf{post}(\llbracket \mathtt{S} \rrbracket_{\perp} \cap (\Sigma \times \Sigma))$ ⟅def. $\alpha_{\not\perp}$⟆

$= \alpha_{\mathrm{G}} \circ \mathsf{post}\llbracket \mathtt{S} \rrbracket$ ⟅def. (1) of the angelic semantics $\llbracket \mathtt{S} \rrbracket$⟆

$= \{\langle P,\ \mathsf{post}\llbracket \mathtt{S} \rrbracket P \rangle \mid P \in \wp(\Sigma)\}$ ⟅def. α_{G}⟆ ☐

LEMMA 1.4 (STRONGEST POSTCONDITION OVER APPROXIMATION).

$$\mathcal{T}_{\mathrm{HL}}(\mathtt{S}) \quad \triangleq \quad \mathsf{post}(\supseteq,\subseteq) \circ \mathcal{T}(\mathtt{S}) \quad = \quad \{\langle P, Q \rangle \mid \mathsf{post}\llbracket \mathtt{S} \rrbracket P \subseteq Q\} \quad = \quad \mathsf{post}(=,\subseteq) \circ \mathcal{T}(\mathtt{S})$$

PROOF OF LEM. 1.4.

$\mathsf{post}(\supseteq,\subseteq) \circ \mathcal{T}(\mathtt{S})$

$= \mathsf{post}(\supseteq,\subseteq)(\mathcal{T}(\mathtt{S}))$ ⟅def. function composition $\circ$⟆

$= \mathsf{post}(\supseteq,\subseteq)(\{\langle P,\ \mathsf{post}\llbracket \mathtt{S} \rrbracket P \rangle \mid P \in \wp(\Sigma)\})$ ⟅Lem. 1.3⟆

$= \{\langle P', Q' \rangle \mid \exists \langle P, Q \rangle \in \{\langle P,\ \mathsf{post}\llbracket \mathtt{S} \rrbracket P \rangle \mid P \in \wp(\Sigma)\} \,.\, \langle \langle P, Q \rangle, \langle P', Q' \rangle \rangle \in \supseteq,\subseteq\}$ ⟅def. (10) of post⟆

$= \{\langle P', Q' \rangle \mid \exists P \,.\, \langle \langle P,\ \mathsf{post}\llbracket \mathtt{S} \rrbracket P \rangle, \langle P', Q' \rangle \rangle \in \supseteq,\subseteq\}$ ⟅def. $\in$⟆

$= \{\langle P', Q' \rangle \mid \exists P \,.\, \langle P,\ \mathsf{post}\llbracket \mathtt{S} \rrbracket P \rangle \supseteq,\subseteq \langle P', Q' \rangle\}$ ⟅def. $\in$⟆

$= \{\langle P', Q' \rangle \mid \exists P \,.\, P \supseteq P' \wedge \mathsf{post}\llbracket \mathtt{S} \rrbracket P \subseteq Q'\}$ ⟅def. $\supseteq,\subseteq$⟆

$= \{\langle P', Q' \rangle \mid \exists P \,.\, P' \subseteq P \wedge \mathsf{post}\llbracket \mathtt{S} \rrbracket P \subseteq Q'\}$ ⟅def. $\supseteq$⟆

$= \{\langle P', Q' \rangle \mid \mathsf{post}\llbracket \mathtt{S} \rrbracket P' \subseteq Q'\}$

⟅($\subseteq$) by Galois connection (12), post is increasing so that $P' \subseteq P \wedge \mathsf{post}\llbracket \mathtt{S} \rrbracket P \subseteq Q'$ implies $\mathsf{post}\llbracket \mathtt{S} \rrbracket P' \subseteq \mathsf{post}\llbracket \mathtt{S} \rrbracket P \wedge \mathsf{post}\llbracket \mathtt{S} \rrbracket P \subseteq Q'$ hence $\mathsf{post}\llbracket \mathtt{S} \rrbracket P' \subseteq Q'$ by transitivity;
($\supseteq$) take $P = P'$⟆

$= \{\langle P', Q' \rangle \mid \exists P \,.\, P' = P \wedge \mathsf{post}\llbracket \mathtt{S} \rrbracket P \subseteq Q'\}$ ⟅def. $=$⟆

$= \{\langle P', Q' \rangle \mid \exists P \,.\, \langle P,\ \mathsf{post}\llbracket \mathtt{S} \rrbracket P \rangle =,\subseteq \langle P', Q' \rangle\}$ ⟅def. $=,\subseteq$⟆

$= \{\langle P', Q' \rangle \mid \exists P \,.\, \langle \langle P,\ \mathsf{post}\llbracket \mathtt{S} \rrbracket P \rangle, \langle P', Q' \rangle \rangle \in =,\subseteq\}$ ⟅def. $\in$⟆

$= \{\langle P', Q' \rangle \mid \exists \langle P, Q \rangle \in \{\langle P,\ \mathsf{post}\llbracket \mathtt{S} \rrbracket P \rangle \mid P \in \wp(\Sigma)\} \,.\, \langle \langle P, Q \rangle, \langle P', Q' \rangle \rangle \in =,\subseteq\}$ ⟅def. $\in$⟆

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

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

$= \mathsf{post}(=,\subseteq) \circ \mathcal{T}(\mathtt{S})$ ⟅def. function composition $\circ$⟆ ☐

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* $\bar{F}^{e}(X) \triangleq \mathrm{id} \,\dot{\cup}\, (\mathsf{post}(\llbracket \mathtt{B} \rrbracket \fatsemi \llbracket \mathtt{S} \rrbracket^{e}) \circ X)$ *and* $F'^{e} \triangleq \boldsymbol{\lambda} X \bullet \mathrm{id} \cup (X \fatsemi \llbracket \mathtt{B} \rrbracket \fatsemi \llbracket \mathtt{S} \rrbracket^{e})$, $X \in \wp(\Sigma \times \Sigma)$ *by (70).*

PROOF OF LEM. 1.5.

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

$= \mathsf{post}(\mathrm{id} \cup (X \fatsemi \llbracket \mathtt{B} \rrbracket \fatsemi \llbracket \mathtt{S} \rrbracket^{e}))$ ⟅def. F^{e}⟆

$= \mathsf{post}(\mathrm{id}) \,\dot{\cup}\, \mathsf{post}(X \fatsemi \llbracket \mathtt{B} \rrbracket \fatsemi \llbracket \mathtt{S} \rrbracket^{e})$ ⟅join preservation in Galois connection (12)⟆

$= \mathrm{id} \,\dot{\cup}\, (\mathsf{post}(\llbracket \mathtt{B} \rrbracket \fatsemi \llbracket \mathtt{S} \rrbracket^{e}) \circ \mathsf{post}(X))$ ⟅def. post and composition Lem. 1.1⟆

$= \bar{F}^{e}(\mathsf{post}(X))$ ⟅def. $\bar{F}^{e}$⟆ ☐

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* $\bar{\bar{F}}^{e}_{P}(X) \triangleq P \cup \mathsf{post}(\llbracket \mathtt{B} \rrbracket \fatsemi \llbracket \mathtt{S} \rrbracket^{e})X$.

PROOF OF LEM. 1.6.

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

$= (\mathrm{id} \,\dot{\cup}\, (\mathsf{post}(\llbracket \mathtt{B} \rrbracket \fatsemi \llbracket \mathtt{S} \rrbracket^{e}) \circ X))P$ ⟅def. $\bar{F}^{e}$⟆

$= \mathrm{id}(P) \cup (\mathsf{post}(\llbracket \mathtt{B} \rrbracket \fatsemi \llbracket \mathtt{S} \rrbracket^{e}) \circ X)(P)$ ⟅pointwise def. $\dot{\cup}$ and function composition $\circ$⟆

$= P \cup \mathsf{post}(\llbracket \mathtt{B} \rrbracket \fatsemi \llbracket \mathtt{S} \rrbracket^{e})(X(P))$ ⟅def. identity id and function application⟆

$= \bar{\bar{F}}^{e}_{P}(X(P))$ ⟅def. $\bar{\bar{F}}^{e}_{P}(X) \triangleq P \cup \mathsf{post}(\llbracket \mathtt{B} \rrbracket \fatsemi \llbracket \mathtt{S} \rrbracket^{e})X$⟆ ☐

THEOREM 1.7 (ITERATION STRONGEST POSTCONDITION). $\mathsf{post}\llbracket \mathtt{W} \rrbracket P = \mathsf{post}\llbracket \neg\mathtt{B} \rrbracket(\mathsf{lfp}^{\subseteq}\, \bar{\bar{F}}^{e}_{P})$ *where* $\bar{\bar{F}}^{e}_{P}(X) \triangleq P \cup \mathsf{post}(\llbracket \mathtt{B} \rrbracket \fatsemi \llbracket \mathtt{S} \rrbracket^{e})X$.

PROOF OF TH. 1.7.

$\mathsf{post}\llbracket \mathtt{W} \rrbracket$

$= \mathsf{post}(\mathsf{lfp}^{\subseteq}\, F^{e} \fatsemi \llbracket \neg\mathtt{B} \rrbracket)$ ⟅def. (49) of $\llbracket \mathtt{W} \rrbracket$ in absence of `break`⟆

$= \mathsf{post}\llbracket \neg\mathtt{B} \rrbracket \circ \mathsf{post}(\mathsf{lfp}^{\subseteq}\, F^{e})$ ⟅composition Lem. 1.1⟆

$= \mathsf{post}\llbracket \neg\mathtt{B} \rrbracket \circ \mathsf{post}(\mathsf{lfp}^{\subseteq}\, F'^{e})$ ⟅since $\mathsf{lfp}^{\subseteq}\, F^{e} = \mathsf{lfp}^{\subseteq}\, F'^{e}$ in (70)⟆

$= \mathsf{post}\llbracket \neg\mathtt{B} \rrbracket(\mathsf{lfp}^{\subseteq}\, \bar{F}^{e})$ ⟅commutation Lem. 1.5 and fixpoint abstraction Th. II.2.2⟆

$= \mathsf{post}\llbracket \neg\mathtt{B} \rrbracket \circ \boldsymbol{\lambda} P \bullet \mathsf{lfp}^{\subseteq}\, \bar{\bar{F}}^{e}_{P}$

⟅pointwise commutation Lem. 1.6 and pointwise abstraction Cor. II.2.2⟆ ☐

COROLLARY 1.8 (CONDITIONAL ITERATION STRONGEST POSTCONDITION GRAPH). $\mathcal{T}(\mathtt{W}) = \{\langle P,\ \mathsf{post}\llbracket \neg\mathtt{B} \rrbracket(\mathsf{lfp}^{\subseteq}\, \bar{\bar{F}}^{e}_{P}) \rangle \mid P \in \wp(\Sigma)\}$ *where* $\bar{\bar{F}}^{e}_{P}(X) \triangleq P \cup \mathsf{post}(\llbracket \mathtt{B} \rrbracket \fatsemi \llbracket \mathtt{S} \rrbracket^{e})X$.

PROOF OF COR. 1.8.

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

$= \alpha_{\mathrm{G}} \circ \mathsf{post}(\llbracket \mathtt{W} \rrbracket)$ ⟅Lem. 1.3⟆

$= \alpha_{\mathrm{G}} \circ \mathsf{post}\llbracket \neg\mathtt{B} \rrbracket \circ \boldsymbol{\lambda} P \bullet \mathsf{lfp}^{\subseteq}\, \bar{\bar{F}}^{e}_{P}$ ⟅Th. 1.7⟆

$= \{\langle P,\ \mathsf{post}\llbracket \neg\mathtt{B} \rrbracket(\mathsf{lfp}^{\subseteq}\, \bar{\bar{F}}^{e}_{P}) \rangle \mid P \in \wp(\Sigma)\}$ ⟅def. (7) of α_{G}⟆ ☐

3. Approximation

- The component wise approximation:

$$\langle x, y \rangle \sqsubseteq, \preceq \langle x', y' \rangle \quad \triangleq \quad x \sqsubseteq x' \wedge y \preceq y'$$

3. Approximation

- The component wise approximation:

$$\langle x,\ y\rangle \sqsubseteq,\leq \langle x',\ y'\rangle \quad \triangleq \quad x \sqsubseteq x' \wedge y \leq y'$$

- The over approximation abstraction for HL:

$$\mathsf{post}(\subseteq,\supseteq) \quad = \quad \boldsymbol{\lambda} R \bullet \{\langle P,\ Q\rangle \mid \exists \langle P',\ Q'\rangle \in R\ .\ P \subseteq P' \wedge Q' \subseteq Q\}$$

$$\mathcal{T}_{\mathrm{HL}}(\mathsf{S}) \quad \triangleq \quad \mathsf{post}(\supseteq.\subseteq) \circ \mathcal{T}(\mathsf{S})$$

3. Approximation

- The component wise approximation:

$$\langle x,\ y\rangle \sqsubseteq, \preceq \langle x',\ y'\rangle \quad \triangleq \quad x \sqsubseteq x' \wedge y \preceq y'$$

- The over approximation abstraction for HL:

$$\text{post}(\subseteq, \supseteq) \quad = \quad \lambda R \bullet \{\langle P,\ Q\rangle \mid \exists\langle P',\ Q'\rangle \in R \,.\, P \subseteq P' \wedge Q' \subseteq Q\}$$

$$\mathcal{T}_{\text{HL}}(\text{S}) \quad \triangleq \quad \text{post}(\supseteq.\subseteq) \circ \mathcal{T}(\text{S})$$

- The (order dual) under approximation abstraction for IL:

$$\text{post}(\supseteq, \subseteq) \quad = \quad \lambda R \bullet \{\langle P,\ Q\rangle \mid \exists\langle P',\ Q'\rangle \in R \,.\, P' \subseteq P \wedge Q \subseteq Q'\}$$

$$\mathcal{T}_{RL}(\text{S}) \quad \triangleq \quad \text{post}(\subseteq, \supseteq) \circ \mathcal{T}(\text{S})$$

- Shows what it shared by HL and IL: all but the consequence rule (?)

4. Fixpoint induction

- Deriving the proof system at this stage by Aczel correspondence would be great!
- A common part and different consequence rules for HL and IL

4. Fixpoint induction

- Deriving the proof system at this stage by Aczel correspondence would be great!
- A common part and different consequence rules for HL and IL
- But then the HL proof system for iteration would be
  1. Prove strongest postconditions (⋙⋙⋙ total correctness)
  2. Approximate with a consequence rule to get partial correctness
- This is sound and complete

4. Fixpoint induction

- Deriving the proof system at this stage by Aczel correspondence would be great!
- A common part and different consequence rules for HL and IL
- But then the HL proof system for iteration would be
  1. Prove strongest postconditions (⋙⋙⋙ total correctness)
  2. Approximate with a consequence rule to get partial correctness
- This is sound and complete
- But too demanding $\Longrightarrow$ not so great!
- What we miss is fixpoint induction

4. Fixpoint induction

Theorem II.3.1 (Park fixpoint over approximation) *Let* $\langle L, \sqsubseteq, \bot, \top, \sqcup, \sqcap\rangle$ *be a complete lattice,* $f \in L \xrightarrow{i} L$ *be increasing, and* $p \in L$*. Then* $\mathsf{lfp}^{\sqsubseteq} f \sqsubseteq p$ *if and only if* $\exists i \in L \,.\, f(i) \sqsubseteq i \wedge i \sqsubseteq p$.

4. Fixpoint induction

THEOREM II.3.6 (FIXPOINT UNDER APPROXIMATION BY TRANSFINITE ITERATES) *Let* $f \in L \xrightarrow{i} L$ *be an increasing function on a* CPO $\langle L, \sqsubseteq, \bot, \sqcup \rangle$. $P \sqsubseteq \mathsf{lfp}^{\sqsubseteq} f$, *if and only if there exists an increasing transfinite sequence* $\langle X^\delta, \delta \in \mathbb{O} \rangle$ *such that*

(1) $X^0 = \bot$,

(2) $X^{\delta+1} \sqsubseteq f(X^\delta)$ *for successor ordinals,*

(3) $\bigsqcup_{\delta<\lambda} X^\delta$ *exists for limit ordinals* λ *such that* $X^\lambda \sqsubseteq \bigsqcup_{\delta<\lambda} X^\delta$, *and*

(4) $\exists \delta \in \mathbb{O} \,.\, P \sqsubseteq X^\delta$.

δ bounded by ω for continuous f.

5. Calculational design of HL

- Theory of HL (for iteration):

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

5. Calculational design of HL

- Theory of HL (for iteration):

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

- HL proof system:

THEOREM 3 (HOARE RULES FOR CONDITIONAL ITERATION).

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

2.1 Calculational Design of Hoare Logic Theory

Theorem 2.1 (Theory of Hoare logic HL).

$$\mathcal{T}_{HL}(\texttt{W}) \triangleq \mathsf{post}(\supseteq,\subseteq) \circ \mathcal{T}(\texttt{W})$$
$$= \{\langle P,\ Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \langle I \cap \mathcal{B}\llbracket\texttt{B}\rrbracket,\ I\rangle \in \mathcal{T}_{HL}(\texttt{S}) \wedge (I \cap \neg\mathcal{B}\llbracket\texttt{B}\rrbracket) \subseteq Q\}$$

Proof of Th. 2.1 .

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

$= \mathsf{post}(\supseteq,\subseteq) \circ \mathcal{T}(\texttt{W})$ ⟅def. $\mathcal{T}_{\mathrm{HL}}$⟆

$= \mathsf{post}(=,\subseteq) \circ \mathcal{T}(\texttt{W})$ ⟅Lem. 1.4⟆

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

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

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

$= \{\langle P,\ Q'\rangle \mid \exists Q \,.\, \mathsf{post}\llbracket\neg\texttt{B}\rrbracket(\mathsf{lfp}^{\subseteq}\, \bar{\bar{\bar{F}}}{}^{e}_{P}) \subseteq Q \wedge Q \subseteq Q'\}$ ⟅Th. 1.7⟆

$= \{\langle P,\ Q'\rangle \mid \exists Q \,.\, \mathsf{post}\llbracket\neg\texttt{B}\rrbracket(\mathsf{lfp}^{\subseteq}\, \bar{\bar{\bar{F}}}{}^{e}_{P}) \subseteq Q'\}$
⟅($\subseteq$) $\exists Q \,.\, \mathsf{post}\llbracket\neg\texttt{B}\rrbracket(\mathsf{lfp}^{\subseteq}\, \bar{\bar{\bar{F}}}{}^{e}_{P}) \subseteq Q \wedge Q \subseteq Q'$ and transitivity;
($\supseteq$) take $Q = Q'$⟆

$= \{\langle P,\ Q'\rangle \mid \exists Q \,.\, \mathsf{lfp}^{\subseteq}\, \bar{\bar{\bar{F}}}{}^{e}_{P} \subseteq Q \wedge \mathsf{post}\llbracket\neg\texttt{B}\rrbracket(Q) \subseteq Q'\}$
⟅($\subseteq$) take $Q = \mathsf{lfp}^{\subseteq}\, \bar{\bar{\bar{F}}}{}^{e}_{P}$; ($\supseteq$) $\mathsf{post}\llbracket\neg\texttt{B}\rrbracket$ is increasing by (12)⟆

$= \{\langle P,\ Q'\rangle \mid \exists Q \,.\, \exists I \,.\, \bar{\bar{\bar{F}}}{}^{e}_{P}(I) \subseteq I \wedge I \subseteq Q \wedge \mathsf{post}\llbracket\neg\texttt{B}\rrbracket(Q) \subseteq Q'\}$ ⟅Park fixpoint induction Th. II.3.1⟆

$= \{\langle P,\ Q'\rangle \mid \exists I \,.\, \bar{\bar{\bar{F}}}{}^{e}_{P}(I) \subseteq I \wedge \mathsf{post}\llbracket\neg\texttt{B}\rrbracket(I) \subseteq Q'\}$
⟅($\subseteq$) $I \subseteq Q$ implies $\mathsf{post}\llbracket\neg\texttt{B}\rrbracket(I) \subseteq \mathsf{post}\llbracket\neg\texttt{B}\rrbracket(Q)$ since $\mathsf{post}\llbracket\neg\texttt{B}\rrbracket$ is increasing by (12) hence $\mathsf{post}\llbracket\neg\texttt{B}\rrbracket(I) \subseteq Q'$ by transitivity;
($\supseteq$) take $Q = I$⟆

$= \{\langle P,\ Q\rangle \mid \exists I \,.\, P \cup \mathsf{post}(\llbracket\texttt{B}\rrbracket \,⨾\, \llbracket\texttt{S}\rrbracket^{e})(I) \subseteq I \wedge \mathsf{post}\llbracket\neg\texttt{B}\rrbracket(I) \subseteq Q\}$ ⟅renaming, def. $\bar{\bar{\bar{F}}}{}^{e}_{P}$⟆

$= \{\langle P,\ Q\rangle \mid \exists I \,.\, P \cup \mathsf{post}(\llbracket\texttt{B}\rrbracket \,⨾\, \llbracket\texttt{S}\rrbracket)(I) \subseteq I \wedge \mathsf{post}\llbracket\neg\texttt{B}\rrbracket(I) \subseteq Q\}$ ⟅$\llbracket\texttt{S}\rrbracket^{e} = \llbracket\texttt{S}\rrbracket$ in absence of `break`s⟆

$= \{\langle P,\ Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \mathsf{post}(\llbracket\texttt{B}\rrbracket \,⨾\, \llbracket\texttt{S}\rrbracket)I \subseteq I \wedge \mathsf{post}\llbracket\neg\texttt{B}\rrbracket(I) \subseteq Q\}$ ⟅def. $\subseteq$ and $\cup$⟆

$= \{\langle P,\ Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \mathsf{post}\llbracket\texttt{S}\rrbracket(\mathsf{post}\llbracket\texttt{B}\rrbracket I) \subseteq I \wedge \mathsf{post}\llbracket\neg\texttt{B}\rrbracket(I) \subseteq Q\}$ ⟅composition Lem. 1.1⟆

$= \{\langle P,\ Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \mathsf{post}\llbracket\texttt{S}\rrbracket(I \cap \mathcal{B}\llbracket\texttt{B}\rrbracket) \subseteq I \wedge (I \cap \neg\mathcal{B}\llbracket\texttt{B}\rrbracket) \subseteq Q\}$ ⟅test Lem. 1.2⟆

$= \{\langle P,\ Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \langle I \cap \mathcal{B}\llbracket\texttt{B}\rrbracket,\ I\rangle \in \{\langle P,\ Q\rangle \mid \mathsf{post}\llbracket\texttt{S}\rrbracket P \subseteq Q\} \wedge (I \cap \neg\mathcal{B}\llbracket\texttt{B}\rrbracket) \subseteq Q$ ⟅def. $\in$⟆

$= \{\langle P,\ Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \langle I \cap \mathcal{B}\llbracket\texttt{B}\rrbracket,\ I\rangle \in \mathsf{post}(=,\subseteq) \circ \mathcal{T}(\texttt{S}) \wedge (I \cap \neg\mathcal{B}\llbracket\texttt{B}\rrbracket) \subseteq Q$ ⟅Lem. 1.4⟆

$= \{\langle P,\ Q\rangle \mid \exists I \,.\, P \subseteq I \wedge \langle I \cap \mathcal{B}\llbracket\texttt{B}\rrbracket,\ I\rangle \in \mathcal{T}_{\mathrm{HL}}(\texttt{S}) \wedge (I \cap \neg\mathcal{B}\llbracket\texttt{B}\rrbracket) \subseteq Q$ ⟅Lem. 1.4⟆ □

2.2 Hoare logic rules

Theorem 2.2 (Hoare rules for conditional iteration).

$$\frac{P \subseteq I,\ \ \{I \cap \mathcal{B}\llbracket\texttt{B}\rrbracket\}\,\texttt{S}\,\{I\},\ \ (I \cap \neg\mathcal{B}\llbracket\texttt{B}\rrbracket) \subseteq Q}{\{P\}\,\texttt{while (B) S}\,\{Q\}} \tag{1}$$

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

By structural induction (S being a strict component of `while (B) S`), the rule for $\{P\}\,\texttt{S}\,\{Q\}$ 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 $\dfrac{\varnothing}{\{P\}\,\texttt{while (B) S}\,\{Q\}}$ with side condition $P \subseteq I,\ \{I \cap \mathcal{B}\llbracket\texttt{B}\rrbracket\}\,\texttt{S}\,\{I\},\ (I \cap \neg\mathcal{B}\llbracket\texttt{B}\rrbracket) \subseteq Q$;

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

Sound and complete by construction

Machine checkable, if not machine checked!

Surprised to find a variant of HL proof system

We also have (post is increasing):

$$\mathcal{T}_{\mathrm{HL}}(\mathtt{S}) \quad = \quad \mathrm{post}(=, \subseteq) \circ \mathcal{T}(\mathtt{S})$$

yields the sound and complete proof system:

$\subseteq$ comes from Th. II.3.1

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

Surprised to find a variant of HL proof system

We also have (post is increasing):

$$\mathcal{T}_{\mathrm{HL}}(\mathtt{S}) \quad = \quad \mathrm{post}(=, \subseteq) \circ \mathcal{T}(\mathtt{S})$$

yields the sound and complete proof system:

$\subseteq$ comes from Th. II.3.1

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

no need for Hoare left consequence rule (but for iteration):

~~If $\vdash P\{Q\}R$ and $\vdash S \supset P$ then $\vdash S\{Q\}R$~~

5. Calculational design of IL

- Theory of IL (for iteration):

$$\mathcal{T}_{IL}(\mathtt{W}) \triangleq \text{post}(\subseteq.\supseteq) \circ \mathcal{T}(\mathtt{W})$$

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

5. Calculational design of IL

- Theory of IL (for iteration):

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

- IL proof system:

THEOREM 5 (IL RULES FOR CONDITIONAL ITERATION).

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

(similar to O'Hearn backward variant since the consequence rule can also be separated)

Calculational design of IL

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).

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

Proof of Th. 3.1.

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

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

$= \{\langle P,\ Q\rangle \mid Q \subseteq \mathsf{post}[\![\mathtt{W}]\!]P\}$ ≀⊆-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 $\bar{\bar{F}}^e_P(X) \triangleq P \cup \mathsf{post}([\![\mathtt{B}]\!] \,⨾\, [\![\mathtt{S}]\!]^e)X$≀

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

≀(⊆) Take $I = \mathsf{lfp}^{\subseteq}\,\bar{\bar{F}}^e_P$ and reflexivity;
(⊇) 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≀

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

≀(⊆) 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;
(⊇) 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. ∈≀

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

□

3.2 Calculational design of IL rules

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

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

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 $\frac{\varnothing}{\{P\}\,\mathtt{while\ (B)\ S}\,\{Q\}}$ 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).

Much more in the paper

Much more in the paper

- Bi-inductive relational semantics with `break` and non termination ($\bot$), for termination and nontermination proofs

Fig. 3. Taxonomy of assertional logics.

Much more in the paper

- Bi-inductive relational semantics with `break` and non termination ($\perp$), for termination and nontermination proofs
- Many more abstractions and combinations → hundreds of transformational logics theories (including property negations, proofs by contradictions, backward logics, etc.)

Fig. 3. Taxonomy of assertional logics

Much more in the paper

- Bi-inductive relational semantics with `break` and non termination (⊥), for termination and nontermination proofs

- Many more abstractions and combinations → hundreds of transformational logics theories (including property negations, proofs by contradictions, backward logics, etc.)

- Taxonomies based on theory abstractions (not proof systems)

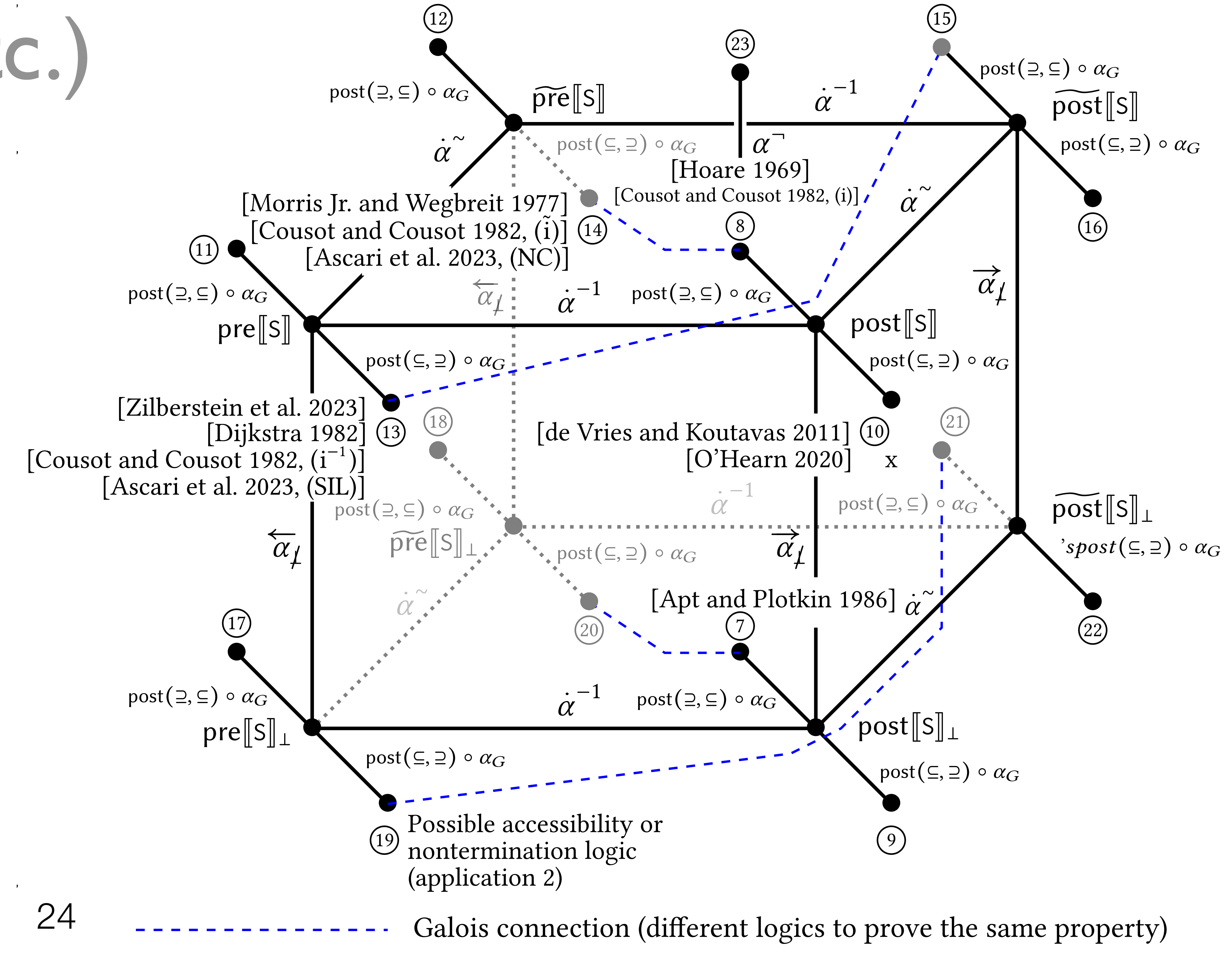


Fig. 3. Taxonomy of assertional logics

Much more in the paper

- Many more fixpoint induction principles (including $P \sqsubseteq \mathsf{lfp}^{\sqsubseteq} F$, $\mathsf{lfp}^{\sqsubseteq} F \sqsubseteq P$, $P \sqsubseteq \mathsf{gfp}^{\sqsubseteq} F$, $\mathsf{gfp}^{\sqsubseteq} F \sqsubseteq P$, $\mathsf{lfp}^{\sqsubseteq} F \sqcap P \neq \emptyset$, $\mathsf{gfp}^{\sqsubseteq} F \sqcap P \neq \emptyset$, etc)

Much more in the paper

- Example 1: calculational design of a logic for partial correctness + total correctness + non termination

$$\{\ n = \underline{n} \wedge f = 1\ \}$$

```
while (n!=0) { f = f * n; n = n - 1;}
```

$$\{\ (\underline{n} \geqslant 0 \wedge f = !\underline{n}) \vee (\underline{n} < 0 \wedge n = f = \bot)\ \}$$

Much more in the paper

- Example II: calculational design of an incorrectness logic including non termination

Much more in the paper

- Example II: calculational design of an incorrectness logic including non termination

- A specification for factorial:

$$\{\ n \in [-\infty, \infty] \wedge f \in [1, 1]\ \}$$

```
while (n!=0) { f = f * n; n = n - 1;}
```

$$\{\ f \in [1, \infty]\ \}$$

- False alarm $f \in [-\infty, 0]$ with a (totally imprecise) interval analysis

Much more in the paper

- Example II: calculational design of an incorrectness logic including non termination

- A specification for factorial:

$$\{\ n \in [-\infty, \infty] \wedge f \in [1, 1]\ \}$$

```
while (n!=0) { f = f * n; n = n - 1;}
```

$$\{\ f \in [1, \infty]\ \}$$

- False alarm $f \in [-\infty, 0]$ with a (totally imprecise) interval analysis

- The alarm is false by nontermination, not provable with IL

About incorrectness

- IL is not Hoare incorrectness logic (sufficient, not necessary)

$$
\begin{array}{rcl}
\neg(\{P\}\,\mathtt{S}\{Q\}) & \overset{\not\Rightarrow}{\Leftarrow} & [P]\mathtt{S}[\neg Q] \\
& \Leftrightarrow & \exists R \in \wp(\Sigma)\,.\,[P]\,\mathtt{S}\,[R] \wedge R \cap \neg Q \neq \emptyset \\
& \Leftrightarrow & \exists \sigma \in \Sigma\,.\,[P]\,\mathtt{S}\,[\{\sigma\}] \wedge \sigma \notin Q
\end{array}
$$

- The logic $\mathcal{T}_{\overline{HL}}(\mathtt{W}) \triangleq \mathrm{post}(\subseteq, \supseteq) \circ \alpha^{\neg} \circ \mathcal{T}_{HL}(\mathtt{W}) = \alpha^{\neg} \circ \mathcal{T}_{HL}(\mathtt{W})$ can be calculated by the design method (and does not need a consequence rule)

Calculational design of Hoare incorrectness logic $\overline{\text{HL}}$

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).

$$\mathcal{T}_{\overline{HL}}(\texttt{W}) \triangleq \text{post}(\subseteq,\supseteq)\circ\alpha^{\neg}\circ\mathcal{T}_{HL}(\texttt{W}) = \alpha^{\neg}\circ\mathcal{T}_{HL}(\texttt{W}) \qquad \texttt{W = while (B) S}$$

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.

$\mathcal{T}_{\overline{\text{HL}}}(\texttt{W}) = \text{post}(\subseteq,\supseteq)\circ\alpha^{\neg}\circ\mathcal{T}_{\text{HL}}(\texttt{W})$ $\quad$ $\wr$def. $\mathcal{T}_{\overline{\text{HL}}}$$\wr$

$= \text{post}((\subseteq,\supseteq)(\neg\{\langle P,\,Q\rangle \mid \text{post}[\![\texttt{W}]\!]P\subseteq Q\})$

$\wr$Lem. 1.4 and def. (30) of $\alpha^{\neg}$$\wr$

$= \text{post}(\subseteq,\supseteq)(\{\langle P,\,Q\rangle \mid \neg(\text{post}[\![\texttt{W}]\!]P\subseteq Q)\})$ $\quad$ $\wr$def. $\neg$$\wr$

$= \text{post}(\subseteq,\supseteq)(\{\langle P,\,Q\rangle \mid \text{post}[\![\texttt{W}]\!]P\cap\neg Q\neq\varnothing\})$ $\quad$ $\wr$def. $\subseteq$ and $\neg$$\wr$

$= \{\langle P',\,Q'\rangle \mid \exists\langle P,\,Q\rangle\in\{\langle P,\,Q\rangle \mid \text{post}[\![\texttt{W}]\!]P\cap\neg Q\neq\varnothing\}\,.\,\langle P,\,Q\rangle \subseteq,\supseteq \langle P',\,Q'\rangle\}$ $\quad$ $\wr$def. post$\wr$

$= \{\langle P',\,Q'\rangle \mid \exists\langle P,\,Q\rangle\,.\,\text{post}[\![\texttt{W}]\!]P\cap\neg Q\neq\varnothing\wedge\langle P,\,Q\rangle \subseteq,\supseteq \langle P',\,Q'\rangle\}$ $\quad$ $\wr$def. $\in$$\wr$

$= \{\langle P',\,Q'\rangle \mid \exists\langle P,\,Q\rangle\,.\,\text{post}[\![\texttt{W}]\!]P\cap\neg Q\neq\varnothing\wedge P\subseteq P'\wedge Q\supseteq Q'\}$ $\quad$ $\wr$component wise def. of $\subseteq,\supseteq$$\wr$

$= \{\langle P',\,Q'\rangle \mid \exists Q\,.\,\text{post}[\![\texttt{W}]\!]P'\cap\neg Q\neq\varnothing\wedge Q\supseteq Q'\}$

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

$= \{\langle P',\,Q'\rangle \mid \text{post}[\![\texttt{W}]\!]P'\cap\neg Q'\neq\varnothing\}$

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

$= \{\langle P,\,Q\rangle \mid \neg(\text{post}[\![\texttt{W}]\!]P\subseteq Q)\}$ $\quad$ $\wr$def. $\subseteq$ and $\neg$$\wr$

$= \alpha^{\neg}\circ\mathcal{T}_{\text{HL}}(\texttt{W})$ $\quad$ $\wr$def. $\alpha^{\neg}$ and $\mathcal{T}_{\text{HL}}$ for Hoare logic$\wr$ $\square$

THEOREM 4.2 (THEORY OF $\overline{\text{HL}}$).

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

PROOF OF TH. 4.2.

$\mathcal{T}_{\overline{\text{HL}}}(\texttt{W})$

$= \{\langle P,\,Q\rangle \mid \text{post}[\![\neg\texttt{B}]\!](\text{lfp}^{\subseteq}\,\bar{\bar{F}}^{e}_{P})\cap\neg Q\neq\varnothing\}$ $\quad$ $\wr$Lem. 1.3, where $\bar{\bar{F}}^{e}_{P}(X)\triangleq P\cup\text{post}([\![\texttt{B}]\!]\,\mathbin{;}\,[\![\texttt{S}]\!]^{e})X$$\wr$

$= \{\langle P,\,Q\rangle \mid \text{lfp}^{\subseteq}\,\bar{\bar{F}}^{e}_{P}\cap\text{pre}[\![\neg\texttt{B}]\!](\neg Q)\neq\varnothing\}$ $\quad$ $\wr$(39.d)$\wr$

$= \{\langle P,\,Q\rangle \mid \exists I\in\wp(\Sigma)\,.\,\bar{\bar{F}}^{e}_{P}(I)\subseteq I\wedge\exists\langle W,\,\preccurlyeq\rangle\in\mathfrak{Wf}\,.\,\exists\nu\in I\to W\,.\,\exists\langle\sigma_i\in I,\,i\in[1,\infty]\rangle\,.\,\sigma_1\in\bar{\bar{F}}^{e}_{P}(\varnothing)\wedge\forall i\in[1,\infty]\,.\,\sigma_{i+1}\in\bar{\bar{F}}^{e}_{P}(\{\sigma_i\})\wedge\forall i\in[1,\infty]\,.\,(\sigma_i\neq\sigma_{i+1})\Rightarrow(\nu(\sigma_i)>\nu(\sigma_{i+1})\wedge\forall i\in[1,\infty]\,.\,(\nu(\sigma_i)\not>\nu(\sigma_{i+1})\Rightarrow\{\sigma_i\}\cap\text{pre}[\![\neg\texttt{B}]\!](\neg Q)\neq 0\}$ $\quad$ $\wr$induction principle Th. H.3$\wr$

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

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

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

$\wr$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$

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

$\wr$($\subseteq$) 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 $\sigma_n\in\text{pre}[\![\neg\texttt{B}]\!](\neg Q)$;
($\supseteq$) 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 $\nu(x)=(\!|\,x\in\{\sigma_i\mid i\in[1,n]\ \text{?}\ x\ \text{:}\ -\infty\,|\!)$ and the sequence $\langle\sigma_j\in I,\ j\in[1,\infty]\rangle$ repeats σ_n ad infimum for $j\geqslant n$.$\wr$

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

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

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

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

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

$= \{\langle P,\,Q\rangle \mid \exists n\geqslant 1\,.\,\exists\langle\sigma_i\in I,\,i\in[1,n]\rangle\,.\,\sigma_1\in P\wedge\forall i\in[1,n[\,.\,\neg(\text{post}([\![\texttt{S}]\!]^{e})(\mathcal{B}[\![\texttt{B}]\!]\cap\{\sigma_i\})\subseteq(\neg\{\sigma_{i+1}\}))\wedge\sigma_n\notin\mathcal{B}[\![\texttt{B}]\!]\wedge\sigma_n\notin Q\}$ $\quad$ $\wr$def. post, $[\![\texttt{B}]\!]$, and $\mathbin{;}$$\wr$

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

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

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

THEOREM 4.3 ($\overline{\text{HL}}$ RULES FOR CONDITIONAL ITERATION).

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

PROOF OF (3). We write $(\!|P|\!)\,\texttt{S}\,(\!|Q|\!)\triangleq\langle P,\,Q\rangle\in\overline{\text{HL}}(\texttt{S})$;
By structural induction (S being a strict component of `while (B) S`), the rule for $(\!|P|\!)\,\texttt{S}\,(\!|Q|\!)$ have already been defined;
By Aczel method, the (constant) fixpoint $\text{lfp}^{\subseteq}\,\lambda X\bullet S$ is defined by $\{\frac{\varnothing}{c}\mid c\in S\}$;
So for `while (B) S` we have an axiom $\dfrac{\varnothing}{(\!|P|\!)\,\texttt{while (B) S}\,(\!|Q|\!)}$ with side condition $\exists\langle\sigma_i\in I,\,i\in[1,n]\rangle\,.\,\sigma_1\in P\wedge\forall i\in[1,n[\,.\,(\!|\mathcal{B}[\![\texttt{B}]\!]\cap\{\sigma_i\}|\!)\,\texttt{S}\,(\!|\neg\{\sigma_{i+1}\}|\!)\wedge\sigma_n\notin\mathcal{B}[\![\texttt{B}]\!]\wedge\sigma_n\notin Q$ where $(\!|\mathcal{B}[\![\texttt{B}]\!]\cap\{\sigma_i\}|\!)\,\texttt{S}\,(\!|\neg\{\sigma_{i+1}\}|\!)$ is well-defined by structural induction;
Traditionally, the side condition is written as a premiss, to get (3). $\square$

Conclusion

A transformational logic is
an abstract interpretation of
a natural relational semantics

The End, Thank You

- slides + calculational design + recording are **online** on my web page (https://cs.nyu.edu/~pcousot/)
- paper + appendix = 1 clickable file on **Zenodo** https://zenodo.org/records/10439109

DOI 10.5281/zenodo.10439108.

