Design of program logics by abstract interpretation

Patrick Cousot
Courant Institute
New York University

Principle

Semantics

abstraction ↓

Theory of the Logic

isomorphism ↓

Proof system of the Logic

Foundations of Exact Abstract Interpretation

- Everything is simple but fixpoints (for iteration and recursion)
- Properties (defined in extension) are complete lattices
- Increasing functions on complete lattices have fixpoint
- The exact abstraction of a fixpoint is a fixpoint

- A fixpoint on a complete lattice can be expressed by a deductive system (a generalization of Peter Aczel on powersets)

Tarski fixpoint theorem

Theorem 15.6 An increasing function $f \in L \xrightarrow{\nearrow} L$ on a complete lattice $\langle L, \sqsubseteq, \bot, \top, \sqcap, \sqcup \rangle$ has a least fixpoint $\mathsf{lfp}^{\sqsubseteq} f = \bigsqcap \{x \in L \mid f(x) \sqsubseteq x\}$.

DAVID PARK'S FIXPOINT INDUCTION

$$\mathrm{lfp}^{\sqsubseteq} F \sqsubseteq P$$

$$\Longleftrightarrow \quad \exists I \,.\, F(I) \sqsubseteq I \;\wedge\; I \sqsubseteq P$$

sound and complete by Tarski's fixpoint theorem

AN INTERMEZZO ON THE NATURALS

Application: proofs by recurrence on naturals

$$\mathbb{N} = \mathrm{lfp}^{\subseteq} F \qquad F(X) = \{0\} \cup \{n+1 \mid n \in X\}$$

$\mathbb{N} \subseteq P$

$\Leftrightarrow \mathrm{lfp}^{\subseteq} F \subseteq P$

$\Leftarrow \exists I.\ F(I) \subseteq I \wedge I \subseteq P$ fixpoint induction

$\Leftarrow \exists I.\ \{0\} \subseteq I \wedge \{n+1 \mid n \in I\} \subseteq I \wedge I \subseteq P$

$\Leftarrow \exists I.\ 0 \in I \wedge \forall n.\ n \in I \Rightarrow n+1 \in I \wedge I \subseteq P$

which is recurrence

$$\frac{I(0),\ I(n) \Rightarrow I(n+1)}{\forall n \in \mathbb{N}.\ I(n)}$$

where P may need to be strengthened to I to be provable

Non standard models of arithmetic

- Peano : $0 \in \mathbb{N}$ $\quad \forall n \in \mathbb{N}.\ n+1 \in \mathbb{N}$
- standard model : $0 < 1 < 2 < \dots$
- Skolem non-standard model : $0 < 1 < 2 < \dots < -2 < -1 < 0 < 1 < 2 < \dots$
- Solution : the models of the naturals are those for which proof by recurrence is valid
- This eliminates $0 < 1 < 2 < \dots$ $\dots < -2 < -1 < 0 < 1 < 2 < \dots$
- The fixpoint definition : "the smallest set S such that $0 \in S$ and $\forall n \in S.\ n+1 \in S$" is simpler.

GALOIS CONNECTIONS

Galois connections

- Given posets $\langle \mathscr{C}, \sqsubseteq \rangle$ (the *concrete domain*) and $\langle \mathscr{A}, \preccurlyeq \rangle$ (the *abstract domain*), the pair $\langle \alpha, \gamma \rangle$ of functions $\alpha \in \mathscr{C} \to \mathscr{A}$ (the *lower adjoint* or *abstraction*) and $\gamma \in \mathscr{A} \to \mathscr{C}$ (the *upper-adjoint* or *concretization*) is a *Galois connection* (GC) if and only if

$$\forall P \in \mathscr{C} \,.\, \forall \overline{P} \in \mathscr{A} \,.\, \alpha(P) \preccurlyeq \overline{P} \Leftrightarrow P \sqsubseteq \gamma(\overline{P}) \tag{11.1}$$

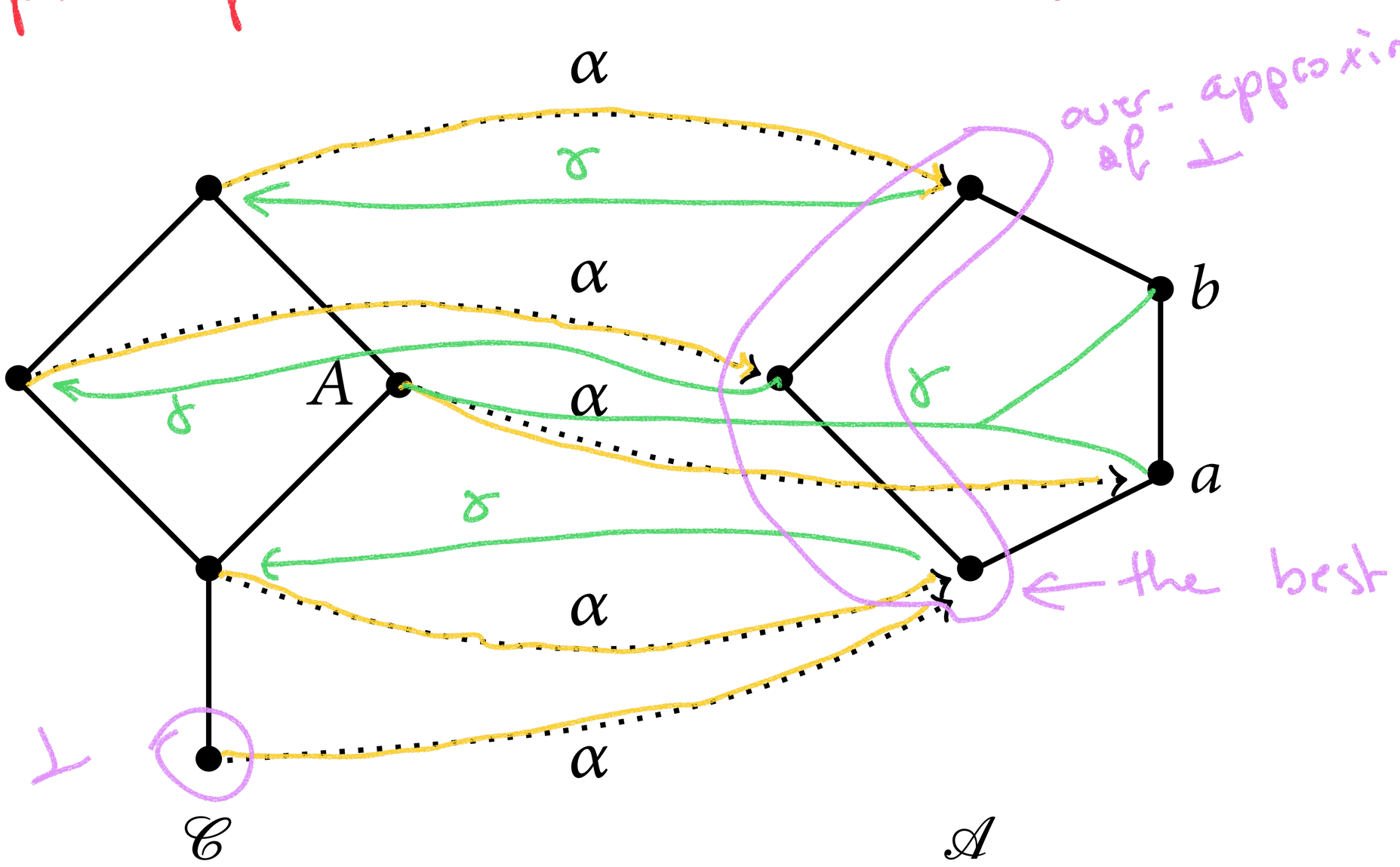
  which we write

$$\langle \mathscr{C}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathscr{A}, \preccurlyeq \rangle \,.$$

idea $\forall x \in \mathscr{C}. \alpha(x)$ is the best/$\preccurlyeq$-most precise element of $\mathscr{A}$ over-approximating x.

en.wikipedia.org/wiki/Galois_connection

Example of Galois connection



FIXPOINT ABSTRACTION

Fixpoint abstraction

- $\mathscr{C}$ is a concrete domain
- $f \in \mathscr{C} \xrightarrow{\nearrow} \mathscr{C}$ is an increasing concrete transformer
- $\langle \mathscr{C}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathscr{A}, \preccurlyeq \rangle$ is an abstraction into $\mathscr{A}$
- Problem: abstract $\mathrm{lfp}^{\sqsubseteq} f$
  - first abstract the concrete transformer f into an abstract transformer $\overline{f} \in \mathscr{A} \xrightarrow{\nearrow} \mathscr{A}$
  - then abstract $\alpha(\mathrm{lfp}^{\sqsubseteq} f)$ into $\mathrm{lfp}^{\preccurlyeq} \overline{f}$.
  - This abstraction may be

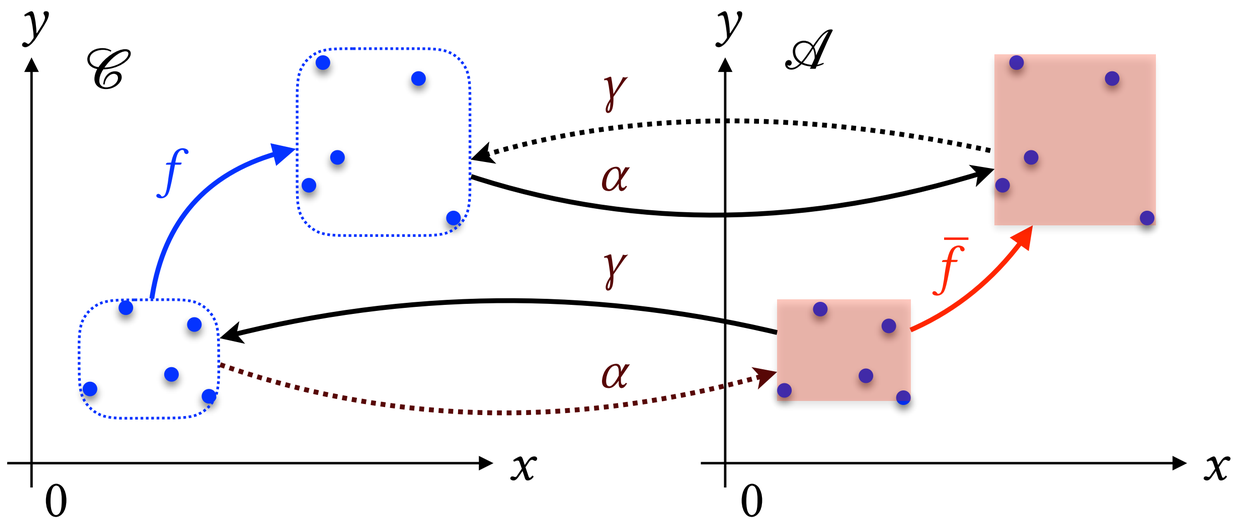
(1) • *exact* i.e. $\alpha(\mathrm{lfp}^{\sqsubseteq} f) = \mathrm{lfp}^{\preccurlyeq} \overline{f}$

(2) • or *sound* but imprecise, in which case we get an overapproximation $\alpha(\mathrm{lfp}^{\sqsubseteq} f) \preccurlyeq \mathrm{lfp}^{\preccurlyeq} \overline{f}$.

(2) is for static analysis, not studied in this presentation

Transformer abstraction

- To abstract a fixpoint $\alpha(\mathrm{lfp}^{\sqsubseteq}\ f)$, we first abstract its transformer f.



Theorem (18.3, transformer abstraction) If $\langle \mathscr{C}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathscr{A}, \preccurlyeq \rangle$ then $\langle \mathscr{C} \xrightarrow{\nearrow} \mathscr{C}, \dot{\sqsubseteq} \rangle \underset{\vec{\alpha}}{\overset{\vec{\gamma}}{\leftrightarrows}} \langle \mathscr{A} \xrightarrow{\nearrow} \mathscr{A}, \dot{\preccurlyeq} \rangle$ where $\dot{\sqsubseteq}$ and $\dot{\preccurlyeq}$ are pointwise (i.e. $f \dot{\sqsubseteq} g$ if and only if $\forall x \in \mathscr{C} \ .\ f(x) \sqsubseteq g(x)$), $\vec{\alpha}(f) = \alpha \circ f \circ \gamma$, and $\vec{\gamma}(\overline{f}) = \gamma \circ \overline{f} \circ \alpha$.

Exact fixpoint abstraction

Theorem (18.23, exact fixpoint abstraction in a complete lattice) Assume that $\langle \mathscr{C}, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ and $\langle \mathscr{A}, \preccurlyeq, 0, 1, \curlyvee, \curlywedge \rangle$ are complete lattices, $f \in \mathscr{C} \stackrel{\nearrow}{\longrightarrow} \mathscr{C}$ is increasing, $\langle \mathscr{C}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathscr{A}, \preccurlyeq \rangle$, $\overline{f} \in \mathscr{A} \stackrel{\nearrow}{\longrightarrow} \mathscr{A}$ is increasing, and $\alpha \circ f = \overline{f} \circ \alpha$ (*commutation property*). Then $\alpha(\mathsf{lfp}^{\sqsubseteq} f) = \mathsf{lfp}^{\preccurlyeq} \overline{f}$.

FIXPOINT DEFINITIONS

Fixpoint definition

Definition 16.4 The fixpoint definition of $D \in \wp(\mathbb{U})$ by a $\subseteq$-increasing function $F \in \wp(\mathbb{U}) \xrightarrow{\nearrow} \wp(\mathbb{U})$ is $D \triangleq \mathsf{lfp}^{\subseteq} F$.

DEDUCTIVE DEFINITIONS (Hilbert systems)

Deductive definition

- A deductive definition of $D \in \wp(\mathbb{U})$ is given by a set of *inference rules* $R = \left\{ \frac{P_i}{c_i} \mid i \in \Delta \right\}$
- $P_i \in \wp_f(\mathbb{U})$ is the *finite*(*) *premise* and $c_i \in \mathbb{U}$ is the *conclusion* of the rule.
- A rule $\frac{P_i}{c_i} \in R$ states that if $P_i \subseteq D$ then $c_i \in D$.
- If $P_i = \varnothing$, the rule is called an *axiom* and states that $c_i \in D$.

(*) if premises infinite proofs must be transfinite.

en.wikipedia.org/wiki/Deductive_reasoning
en.wikipedia.org/wiki/Hilbert_system
en.wikipedia.org/wiki/Axiom
en.wikipedia.org/wiki/Rule_of_inference

Example : odd naturals

Fixpoint definition

$$\mathcal{O} = \mathrm{lfp}^{\subseteq} F \quad \text{where} \quad F(X) = \{1\} \cup \{n+2 \mid n \in X\}$$

Deductive definition

$$\frac{}{1 \in \mathcal{O}} \qquad \frac{n \in \mathcal{O}}{n+2 \in \mathcal{O}}$$

$1 \to 3 \to 5 \quad \text{so} \quad 5 \in \mathcal{O}$

$6 \leftarrow 4 \leftarrow 2 \leftarrow 0$!?! so $6 \notin \mathcal{O}$

The two definitions are <u>equivalent</u>

proof

- A proof of p by rules R is a finite sequence $t_0 \dots t_n$ of elements of $\mathbb{U}$ such that
  - each $t_i, i \in [0, n]$ is deduced from $t_0 \dots t_{i-1}$ by application of a rule of R
  - $t_n = p$.

- Formally

Definition 16.7
is-provable$(p, R) \triangleq \exists t_0 \dots t_n \in \mathbb{U} \,.\, (\forall i \in [0, n] \,.\, \exists \frac{P}{c} \in R \,.\, P \subseteq \{t_0, \dots, t_{i-1}\} \wedge t_i = c) \wedge t_n = p$.

en.wikipedia.org/wiki/Mathematical_proof
en.wikipedia.org/wiki/Formal_proof

Deductive definition

Definition 16.10 (deductive definition) The deductive definition of $D \in \wp(\mathbb{U})$ by a deductive system of rules $\frac{P}{c} \in R$ is $D \triangleq \{p \in \mathbb{U} \mid \text{is-provable}(p, R)\}$.

FIXPOINT DEFINITION EQUIVALENT TO A DEDUCTIVE DEFINITION

A deductive definition can be expressed as a fixpoint definition and conversely.

Consequence operator

For a deductive definition by rules $R = \left\{ \frac{P_i}{c_i} \mid i \in \Delta \right\}$, define

- the *consequence operator* $F_R(X) \triangleq \{c \mid \exists \frac{P}{c} \in R \,.\, P \subseteq X\}$
- $F_R(X)$ is the set of consequences provable by R when X has already been proved
- The consequence operator F_R does not necessarily preserve joins but is increasing

Equivalence of the deductive and fixpoint definitions

Theorem 16.12 We have $D = \{p \in \mathbb{U} \mid \text{is-provable}(p, R)\} = \text{lfp}^{\subseteq} F_R$ where $F_R(X) \triangleq \{c \mid \exists \frac{P}{c} \in R \,.\, P \subseteq X\}$ is the *consequence operator* of R.

Theorem 16.12 may not hold when considering rules which premises can be infinite sets.

DEDUCTIVE DEFINITIO EQUIVALENT TO A FIXPOINT DEFINITION

Equivalence of the fixpoint and deductive definitions

Theorem 16.16 For a fixpoint definition $\mathsf{lfp}^{\subseteq} F$ define $R = \left\{ \frac{P}{c} \mid P \subseteq \mathbb{U} \wedge c \in F(P) \right\}$. Then $F = F_R$ so $\mathsf{lfp}^{\subseteq} F_R = \mathsf{lfp}^{\subseteq} F$.

Note that if R turns out to have finite premises only, then $\{p \in \mathbb{U} \mid \text{is-provable}(p, R)\} = \mathsf{lfp}^{\subseteq} F_R$.

NATURAL SEMANTICS

(one of the possible semantics which abstraction yield a program logic, forget about non-termination, so too abstract e.g. to prove termination)

structural natural semantics

- assignment $S ::= {}^{\ell} x := A;$

$$S^N[\![S]\!] = \{ \langle \rho, \rho[x \leftarrow v] \rangle \mid v \in \mathcal{A}[\![A]\!]\rho \}$$

- skip $S ::= \ell \text{ skip}$

$$S^N[\![S]\!] = \{ \langle \rho, \rho \rangle \mid \rho \in \mathbb{E} \}$$

Structural natural semantics

- conditional $S ::= \mathbf{if}^{\ell}(B)\ S_t\ \mathbf{else}\ S_f$

$$S^N[\![S]\!] = \{\langle \rho, \rho \rangle \mid \mathcal{B}[\![B]\!]\rho = tt\} \circ S^N[\![S_t]\!]$$
$$\cup \{\langle \rho, \rho \rangle \mid \mathcal{B}[\![B]\!]\rho = ff\} \circ S^N[\![S_f]\!]$$

where

$$R \circ R' = \{\langle x, z \rangle \mid \exists y : \langle x, y \rangle \in R \wedge \langle y, z \rangle \in R'\}$$

Structural natural semantics

- Sequential composition $S ::= S\ell_1 ; S_2$

$$S^N[\![S]\!] = S^N[\![S\ell_1]\!] \circ S^N[\![S_2]\!]$$

where

$$R \circ R' = \{ \langle x, z \rangle \mid \exists y. \langle x, y \rangle \in R \wedge \langle y, z \rangle \in R' \}$$

Structural natural semantics

- iteration $S = \text{while}^{\ell}(B)\ S_t$ $\qquad \ell = at[\![S]\!]$

$$S^N[\![S]\!] = \text{lfp}_I^{\subseteq} F^N[\![S]\!] \text{ in}$$
$$I = \{\langle \rho, \rho' \rangle \mid \mathcal{B}[\![B]\!]\rho' = \text{ff}\}$$

$$F^N[\![S]\!]X = \{\langle \rho, \rho \rangle \mid \rho \in \mathbb{E}\}$$
$$\{\langle \rho, \rho' \rangle \in X \mid \mathcal{B}[\![B]\!]\rho' = \text{tt}\} \circ S^N[\![S_t]\!]$$

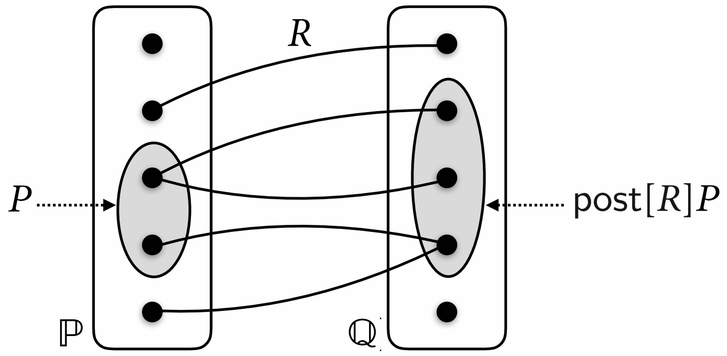
EXAMPLES OF ABSTRACTIONS :
TRANSFORMERS

Property transformers

- Isomorphic abstractions of relations (e.g.(in)finitary relational semantics)
- the *post-image* of a preproperty/precondition $P \in \wp(\mathbb{P})$ by relation $R \in \wp(\mathbb{P} \times \mathbb{Q})$ is $\mathrm{post}[R]P \in \wp(\mathbb{Q})$ such that

$$\mathrm{post}[R] \quad \triangleq \quad P \mapsto \{y \in \mathbb{Q} \mid \exists x \in P \,.\, \langle x,\ y\rangle \in R\} \tag{12.2}$$

(This is also called the *right-image* of P by R, also written $R[P]$ or even $R(P)$.)



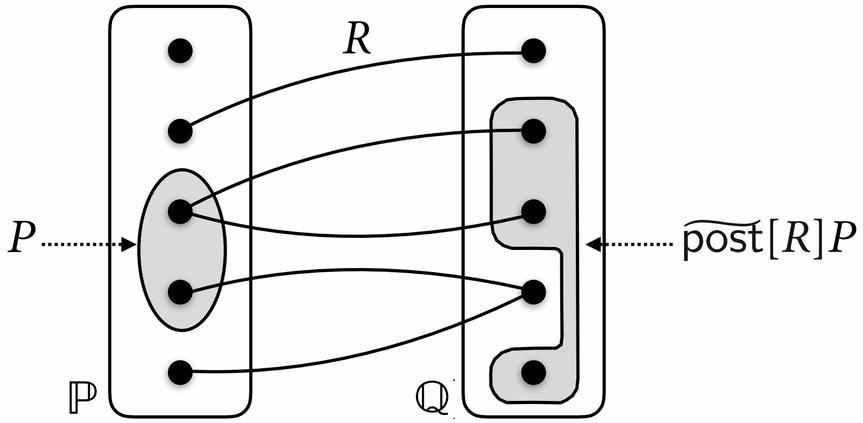
- $\langle \wp(\mathbb{P} \times \mathbb{Q}),\ \subseteq\rangle \underset{\mathrm{post}}{\overset{\mathrm{post}^{-1}}{\twoheadleftarrow\!\!\twoheadrightarrow}} \langle \wp(\mathbb{P}) \xrightarrow{\sqcup} \wp(\mathbb{Q}),\ \dot{\subseteq}\rangle$

where $\mathrm{post}^{-1}[T] \triangleq \{\langle x,\ y\rangle \in \mathbb{P} \times \mathbb{Q} \mid y \in T(\{x\})\}$

Property transformers

- The *dual post-image* of a preproperty $P \in \wp(\mathbb{P})$ by relation R is $\widetilde{\mathsf{post}}[R]P \in \wp(\mathbb{Q})$ such that

$$\begin{aligned} \widetilde{\mathsf{post}}[R] &\triangleq \neg \circ \mathsf{post}[R] \circ \neg \,^{1} \\ &= P \mapsto \{y \in \mathbb{Q} \mid \forall x \in \mathbb{P} \,.\, \langle x,\, y\rangle \in R \Rightarrow x \in P\} \end{aligned} \tag{12.3}$$



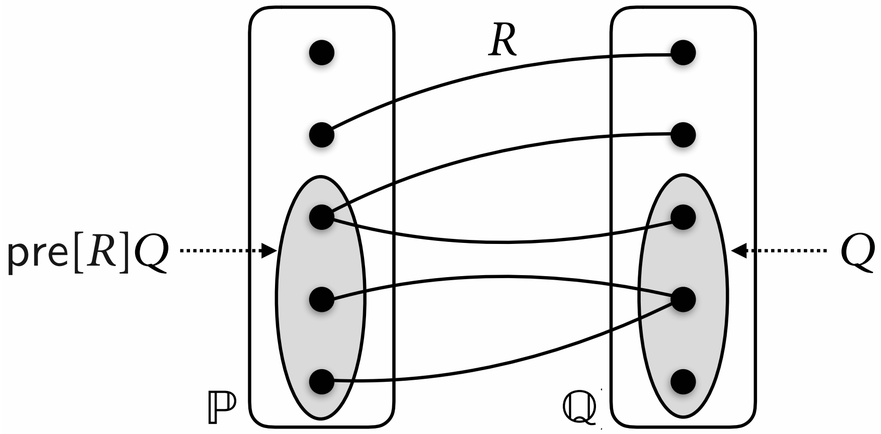
[1] We write $\neg P$ for $\mathbb{P} \smallsetminus P$ and $\neg Q$ for $\mathbb{Q} \smallsetminus Q$, the ambiguity being solved by considering the powerset to which the negated property belongs.

Property transformers

- The *pre-image* of a postproperty $Q \in \wp(\mathbb{Q})$ by relation $R \in \wp(\mathbb{P} \times \mathbb{Q})$ is $\mathrm{pre}[R]Q \in \wp(\mathbb{P})$ such that

$$\mathrm{pre}[R] \triangleq \mathrm{post}[R^{-1}] = Q \mapsto \{x \in \mathbb{P} \mid \exists y \in Q \,.\, \langle x,\ y\rangle \in R\} \tag{12.11}$$

(This is also called the *left-image* of P by R, also written $R^{-1}[P]$ or $R^{-1}(P)$.)



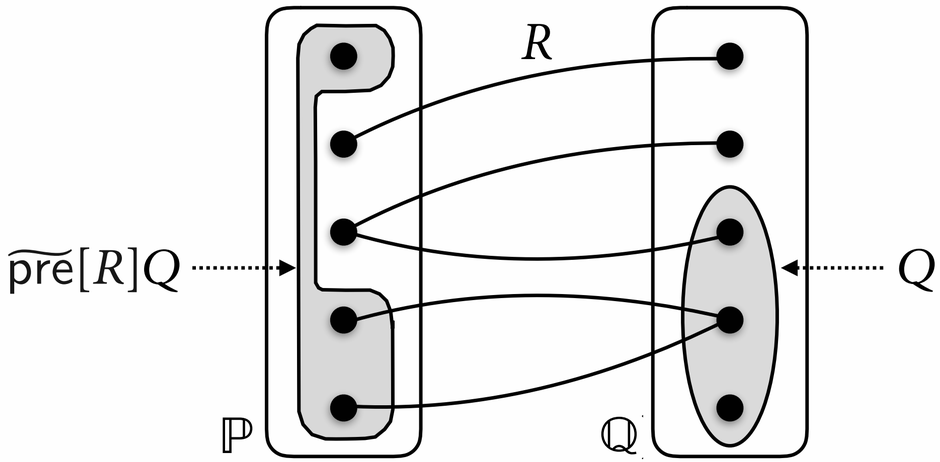
- $\langle \wp(\mathbb{P} \times \mathbb{Q}),\ \subseteq\rangle \underset{\mathrm{pre}}{\overset{\mathrm{pre}^{-1}}{\twoheadleftarrow\!\!\twoheadrightarrow}} \langle \wp(\mathbb{Q}) \xrightarrow{\sqcap} \wp(\mathbb{P}),\ \dot{\subseteq}\rangle$

where $\mathrm{pre}^{-1}[T] = \{\langle x,\ y\rangle \in \mathbb{P} \times \mathbb{Q} \mid x \in T(\{y\})\}$

Property transformers

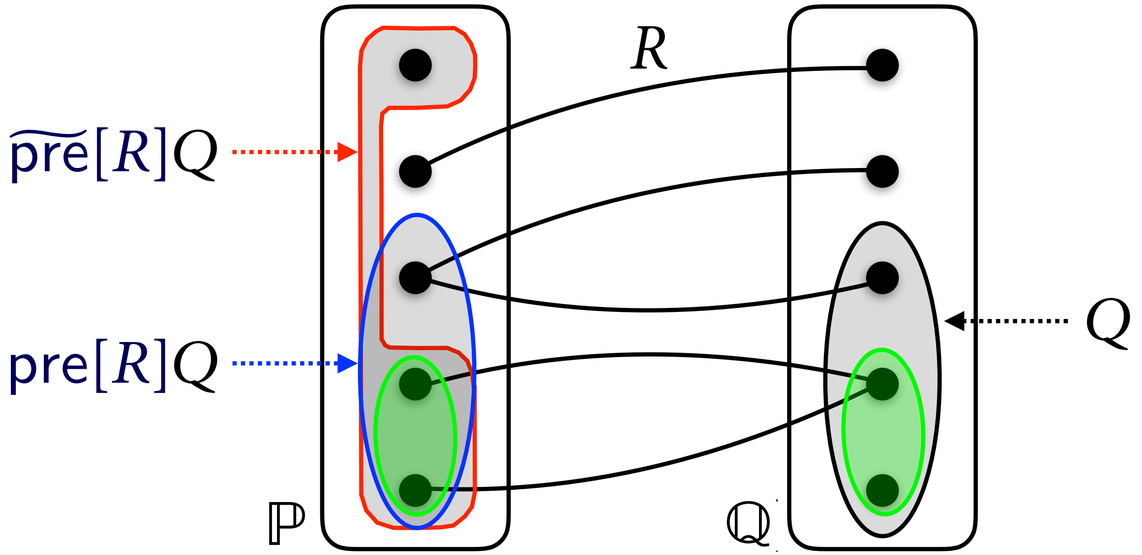
- The *dual pre-image* of a postproperty $Q \in \wp(\mathbb{Q})$ by relation $R \in \wp(\mathbb{P} \times \mathbb{Q})$ is is $\widetilde{\mathsf{pre}}[r]Q \in \wp(\mathbb{P})$ such that

$$\widetilde{\mathsf{pre}}[R] \triangleq \neg \circ \mathsf{pre}[R] \circ \neg = \widetilde{\mathsf{post}}[R^{-1}] \tag{12.12}$$
$$= Q \mapsto \{x \in \mathbb{P} \mid \forall y \in \mathbb{Q} \,.\, \langle x, y \rangle \in R \Rightarrow y \in Q\}$$



Weakest precondition

- $\mathrm{pre}[R]Q \wedge \widetilde{\mathrm{pre}}[R]Q$



- If $P \subseteq \mathrm{pre}[R]Q \wedge \widetilde{\mathrm{pre}}[R]Q$ then it is guaranteed to reach Q from P through R

Galois connections between property transformers

If $R \in \wp(\mathbb{P} \times \mathbb{Q})$, we have the following Galois connections

$$\langle \wp(\mathbb{P}),\ \subseteq \rangle \underset{\mathsf{post}[R]}{\overset{\widetilde{\mathsf{pre}}[R]}{\leftrightarrows}} \langle \wp(\mathbb{Q}),\ \subseteq \rangle \tag{12.22}$$

$$\langle \wp(\mathbb{Q}),\ \subseteq \rangle \underset{\mathsf{pre}[R]}{\overset{\widetilde{\mathsf{post}}[R]}{\leftrightarrows}} \langle \wp(\mathbb{P}),\ \subseteq \rangle \tag{12.23}$$

ABSTRACTION OF A RELATIONAL OR NATURAL SEMANTICS TO AN ASSERTIONAL LOGICS

Abstraction

- Relational semantics:

$$s \in \wp(\Sigma \times \Sigma')$$

(or $\wp(\mathbb{E} \times \mathbb{E}_\perp)$)

- Transformer:

$$\langle \wp(\Sigma), \subseteq \rangle \underset{\widetilde{tr}[\![s]\!]}{\overset{tr[\![s]\!]}{\rightleftarrows}} \langle \wp(\Sigma'), \subseteq \rangle$$

- Assertional logic:

$$\langle \wp(\Sigma \times \Sigma'), \subseteq \rangle \underset{\alpha^{\subseteq}_{\ell}}{\overset{\gamma^{\subseteq}_{\ell}}{\rightleftarrows}} \langle \{ \{P\}\, s\, \{Q\} \mid P \in \wp(\Sigma) \wedge Q \in \wp(\Sigma') \}, \subseteq \rangle$$

$$\alpha^{s}_{\ell}(S) = \{ \{P\}\, s\, \{Q\} \mid tr[s]\, P \subseteq Q \}$$

or dual/inverse

Assertional Logics

Hoare logic

$$\{\{P\}\, S\, \{Q\} \mid \mathrm{post}\,(S^{\mathcal{N}}[\![S]\!])\, P \subseteq Q\}$$

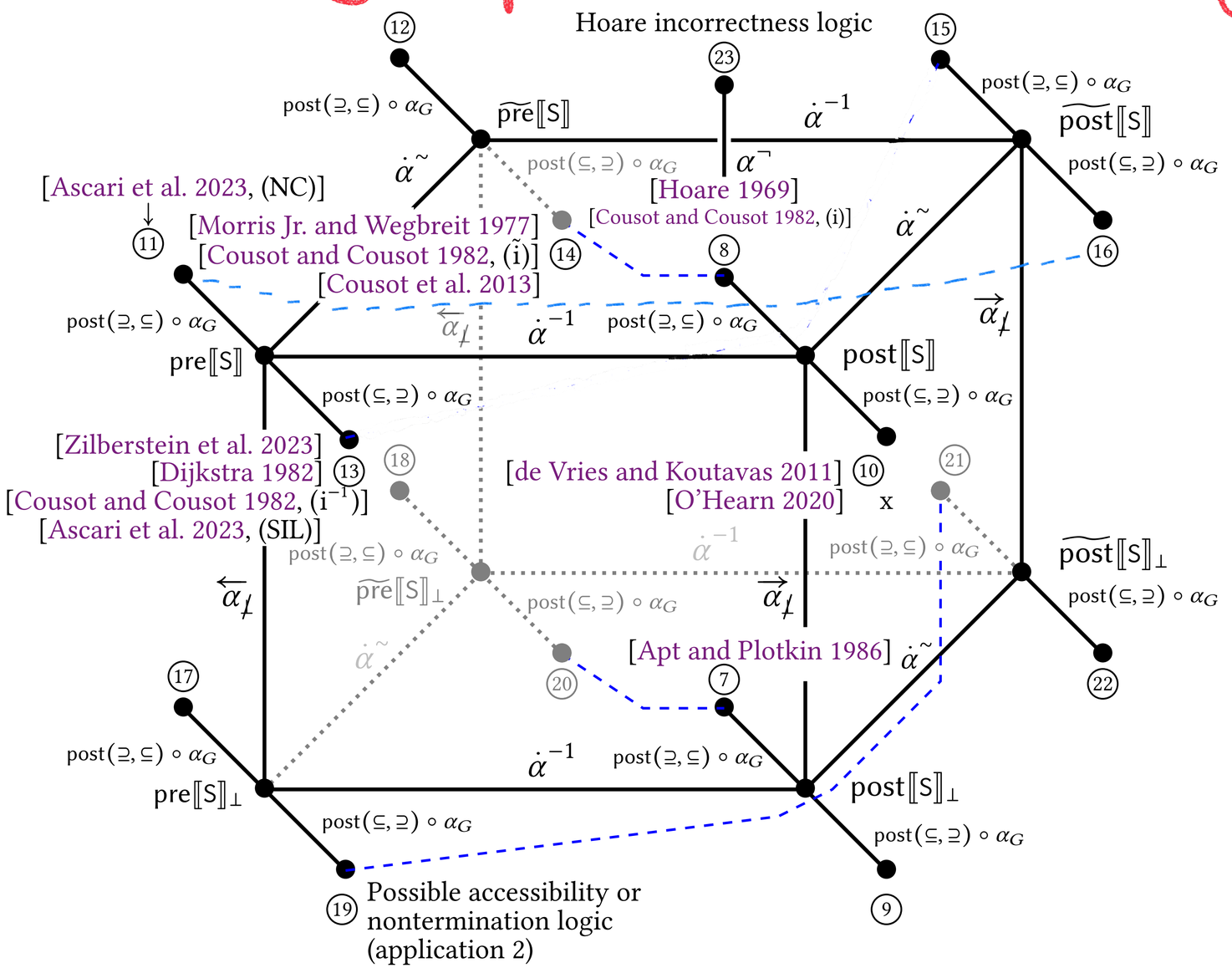
Subgoal induction logic

$$\{\{P\}\, S\, \{Q\} \mid P \subseteq \widetilde{\mathrm{pre}}\,(S^{\mathcal{N}}[\![S]\!])\, Q\}$$

Incorrectness logic

$$\{\{P\}\, S\, \{Q\} \mid Q \subseteq \mathrm{post}\,(S^{\mathcal{N}}[\![S]\!])\, P\}$$

Taxonomy of assertional logics



CALCULATIONAL DESIGN OF LOGICS

Calculational design method

- Given the relational semantics $S[\![s]\!]$ calculate $tr[S[\![s]\!]]$ by structural induction on s (in fixpoint form)
- Then calculate $\{\langle P, Q\rangle \mid tr[S[\![s]\!]]\, P \subseteq Q\}$ (in fixpoint form for iteration)
- Calculate the proof system

CALCULATIONAL DESIGN OF HOARE LOGIC

Hoare logic

- assignment $S ::= x := A;$

$$S^N[\![S]\!] = \{ \langle \rho, \rho[x \leftarrow v] \rangle \mid v \in \mathcal{A}[\![A]\!]\rho \}$$

$$post[S^N[\![S]\!]]P = \{ \rho' \mid \exists \rho \in P. \langle \rho, \rho' \rangle \in S^N[\![S]\!] \}$$
$$= \{ \rho[x \leftarrow v] \mid \rho \in P, v \in \mathcal{A}[\![A]\!]\rho \}$$

$$H[\![S]\!] = \{ \{P\} S \{Q\} \mid post[S^N[\![S]\!]]P \subseteq Q \}$$
$$= \{ \{P\} S \{Q\} \mid \{ \rho[x \leftarrow v] \mid \rho \in P \wedge v \in \mathcal{A}[\![A]\!]\rho \} \subseteq Q \}$$

- assignment $S ::= x := A;$ (cont'd)

$$H[\![S]\!] = \{ \{P\}\, S\, \{Q\} \mid \{\rho[x \leftarrow \sigma] \mid \rho \in P \wedge \sigma \in \mathcal{A}[\![A]\!]\rho\} \subseteq Q \}$$

characterized by the following deductive system

$$\frac{}{\{P\}\, x := A;\, \{\{\rho[x \leftarrow \sigma] \mid \rho \in P \wedge \sigma \in \mathcal{A}[\![A]\!]\rho\}}$$

$$\frac{\{P\}\, S\, \{Q\}}{\{P\}\, S\, \{Q'\}}\ Q \subseteq Q'$$

right consequence rule

Hoare Logic

- conditional $S ::= \text{if } (B)\ S_t$

$$S^N[\![S]\!] = \{\langle \rho, \rho\rangle \mid \mathcal{B}[\![B]\!]\rho = ff\} \cup \{\langle \rho, \rho\rangle \mid \mathcal{B}[\![B]\!]\rho = tt\} \circ S^N[\![S_t]\!]$$

$$\text{post}\, S^N[\![S]\!]\, P = \{\rho' \mid \exists \rho \in P.\ \langle \rho, \rho'\rangle \in S^N[\![S]\!]\}$$

$$= \{\rho \in P \mid \mathcal{B}[\![B]\!]\rho = ff\} \cup \{\rho' \mid \exists \rho \in P.\ \mathcal{B}[\![B]\!]\rho = tt \wedge \langle \rho, \rho'\rangle \in S^{df}[\![S_t]\!]\}$$

$$= \{\rho \mid \exists \rho \in P \cap \{\rho \mid \mathcal{B}[\![B]\!]\rho = tt\} \wedge \langle \rho, \rho'\rangle \in S^N[\![S_t]\!]\}$$

$$= \{\rho \in P \mid \mathcal{B}[\![B]\!]\rho = ff\} \cup \text{post}[S^N[\![S_t]\!]](P \cap \{\rho \mid \mathcal{B}[\![B]\!]\rho = tt\})$$

Hoare logic

- conditional $S ::= \texttt{if}\ (B)\ S_t$ (continued)

$$H[\![S]\!] = \{\{P\}\, S\, \{Q\} \mid post[S^N[\![S]\!]]P \subseteq Q\}$$

$$= \{\{P\}\, S\, \{Q\} \mid \{\rho \in P \mid \mathcal{B}[\![B]\!]\rho = ff\}\} \subseteq Q\} \cup$$

$$\{\{P\}\, S\, \{Q\} \mid post[S^t[\![S_t]\!]](P \cap \{\rho \mid \mathcal{B}[\![B]\!]\rho = tt\})\}$$

$$\subseteq Q$$

$$= \{\{P\}\, S\, \{Q\} \mid \{\rho \in P \mid \mathcal{B}[\![B]\!]\rho = ff\} \subseteq Q\} \cup$$

$$\{\{P\}\, S\, \{Q\} \mid \{P \cap \{\rho \mid \mathcal{B}[\![B]\!]\rho = ff\}\}\ S_t\ \{Q\}\}$$

Hoare logic

- conditional $S ::= \mathtt{if}\ (B)\ S_t$

$$H[\![S]\!] = \{\{P\}\,S\,\{Q\} \mid P \cap \{\rho \mid \mathcal{B}[\![B]\!]\rho = \mathit{ff}\} \subseteq Q\} \cup \{\{P\}\,S\,\{Q\} \mid \{P \cap \{\rho \mid \mathcal{B}[\![B]\!]\rho = \mathit{tt}\}\}\,S_t\,\{Q\}\}$$

$$\neg B = \{\rho \mid \mathcal{B}[\![B]\!]\rho = \mathit{ff}\} \qquad B = \{\rho \mid \mathcal{B}[\![B]\!]\rho = \mathit{tt}\}$$

$$\frac{\emptyset}{\{P\}\,\mathtt{if}(B)\,S_t\,\{Q\}} \qquad \frac{P \cap \neg B \subseteq Q \qquad \{P \cap B\}\,S_t\,\{Q\}}{\text{side conditions}}$$

Hoare logic

- sequential composition $sl ::= sl_1 ; s_2$

$$S^N[\![sl]\!] = S^N[\![sl_1]\!] \circ S^N[\![s_2]\!]$$

$$\text{post}\, S^N[\![sl]\!] P = \{\rho' \mid \exists \rho \in P.\ \langle \rho, \rho' \rangle \in S^N[\![sl]\!] P\}$$

$$= \{\rho' \mid \exists \rho \in P.\ \exists \rho''.\ \langle \rho, \rho'' \rangle \in S^N[\![sl_1]\!] \wedge \langle \rho'', \rho' \rangle \in S^N[\![s_2]\!]\}$$

$$= \{\rho' \mid \exists \rho'' \in \text{post}\, S^N[\![sl_1]\!] P.\ \langle \rho'', \rho' \rangle \in S^N[\![s_2]\!]\}$$

$$= \text{post}\, S^N[\![s_2]\!] (\text{post}\, S^N[\![sl_1]\!] P)$$

- $\circ$ is function composition $f \circ g(x) = f(g(x))$

• sequential composition $Sl ::= Sl_1 ; S_2$

$$H[\![Sl]\!] = \{\{P\}\, Sl\, \{Q\} \mid post^N[\![Sl]\!]P \subseteq Q\}$$

$$= \{\{P\}\, Sl\, \{Q\} \mid post(S^N[\![S_2]\!])(post(S^N[\![Sl_1]\!]P) \subseteq Q\}$$

$$= \{\{P\}\, Sl\, \{Q\} \mid \exists R.\ post(S^N[\![Sl_1]\!]P \subseteq R \wedge post(S^N[\![S_2]\!]R) \subseteq Q\}$$

$$= \{\{P\}\, Sl\, \{Q\} \mid \exists R.\ \{P\}\, Sl_1\, \{R\} \wedge \{R\}\, S_2\, \{Q\}\}$$

Proof system

$$\frac{\varnothing}{\{P\}\, Sl\, \{Q\}} \quad \exists R.\ \{P\}\, Sl_1\, \{R\} \wedge \{R\}\, S_2\, \{Q\}$$

- sequential composition $\delta\ell ::= \varepsilon$

$$S^N[\![\varepsilon]\!] = \{\langle \rho, \rho \rangle \mid \rho \in \mathbb{E}\}$$

$$\mathrm{post}\, S^N[\![\varepsilon]\!]\, P = \{\rho' \mid \exists \rho \in P.\ \langle \rho, \rho' \rangle \in S^N[\![\varepsilon]\!]\}$$

$$= \{\rho' \mid \exists \rho \in P.\ \rho' = \rho\} = P$$

$$M[\![\varepsilon]\!] = \{\{P\}\varepsilon\{Q\} \mid \mathrm{post}\, S^N[\![\varepsilon]\!]\, P \subseteq Q\}$$

$$= \{\{P\}\varepsilon\{Q\} \mid P \subseteq Q\}$$

proof system

$$\frac{\varnothing}{\{P\}\,\varepsilon\,\{P\}} \qquad \frac{\varnothing}{\{P\}\,\varepsilon\,\{Q\}}\ P \subseteq Q$$

Hoare logic

- iteration $S ::= \texttt{while}\ (B)\ S_b$

$$S^N[\![S]\!] = \text{lfp}^{\subseteq} I = \text{lfp}^{\subseteq} F^N[\![S]\!] \text{ in}$$
$$= \{\langle \rho, \rho' \rangle \in I \mid \mathcal{B}[\![B]\!]\rho' = \text{ff}\}$$

$$F^N[\![S]\!]X = \{\langle \rho, \rho \rangle \mid \rho \in \mathbb{E}\} \cup \{\langle \rho, \rho' \rangle \in X \mid \mathcal{B}[\![B]\!]\rho' = \text{tt}\} \circ S^N[\![S_t]\!]$$

iteration $S = \texttt{while}\ (B)\ S_b$

$\mathrm{post}[S^N[\![S]\!]]\,P$

$= \mathrm{post}[\{\langle \rho, \rho' \rangle \in \mathrm{lfp}^{\subseteq} F^N[\![S]\!] \mid \mathcal{B}[\![B]\!]\rho' = \mathit{ff}\}][P]$

$= \{\rho' \mid \exists \rho \in P.\ \langle \rho, \rho' \rangle \in \mathrm{lfp}^{\subseteq} F^N[\![S]\!] \wedge \mathcal{B}[\![B]\!]\rho' = \mathit{ff}\}$

$= \{\rho' \mid \mathcal{B}[\![B]\!]\rho' = \mathit{ff} \wedge \rho' \in \mathrm{post}[\mathrm{lfp}^{\subseteq} F^N[\![S]\!]]P\}$

$= \mathrm{post}[\mathrm{lfp}^{\subseteq} F^N[\![S]\!]]P \cap \neg B$

$= \alpha_P(\mathrm{lfp}^{\subseteq} F^N[\![S]\!]) \cap \neg B$

$\neg B = \{\rho' \mid \mathcal{B}[\![B]\!]\rho' = \mathit{ff}\}$

where $\alpha_P = \lambda X.\ \mathrm{post}[X]P$

We use exact function abstraction:

Theorem (18.23, exact fixpoint abstraction in a complete lattice) Assume that $\langle \mathscr{C}, \sqsubseteq, \bot, \top, \sqcup, \sqcap \rangle$ and $\langle \mathscr{A}, \preccurlyeq, 0, 1, \curlyvee, \curlywedge \rangle$ are complete lattices, $f \in \mathscr{C} \longrightarrow \mathscr{C}$ is increasing, $\langle \mathscr{C}, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \mathscr{A}, \preccurlyeq \rangle$, $\overline{f} \in \mathscr{A} \longrightarrow \mathscr{A}$ is increasing, and $\alpha \circ f = \overline{f} \circ \alpha$ (*commutation property*). Then $\alpha(\mathrm{lfp}^{\sqsubseteq} f) = \mathrm{lfp}^{\preccurlyeq} \overline{f}$.

$$\alpha_P(F^N[\![S]\!](X)) = \overline{F}(\alpha_P(X))$$

$$\forall P.\ \underbrace{\mathrm{pair}}_{\alpha}(F^N[\![S]\!]X)P = \underbrace{\overline{F}}_{\overline{f}}(\underbrace{\mathrm{pair}(X)P}_{\alpha})$$

By calculational design

$S = \texttt{while}(B)\ S_b$

$$
\begin{aligned}
&post(F^N[\![S]\!]X)P \\
&= post(\{\langle\rho,\rho\rangle \mid \rho\in E\} \cup \{\langle\rho,\rho'\rangle\in X \mid \mathcal{B}[\![B]\!]\rho' = tt\} \circ S^N[\![S_b]\!])P \\
&= post(\{\langle\rho,\rho\rangle \mid \rho\in E\})P \cup \\
&\quad post(S^N[\![S_b]\!])(post(\{\langle\rho,\rho'\rangle\in X \mid \mathcal{B}[\![B]\!]\rho' = tt\})P) \\
&= P \cup post(S^N[\![S_b]\!])(\{\rho' \mid \exists \rho\in P.\ \langle\rho,\rho'\rangle\in X \wedge \mathcal{B}[\![B]\!]\rho' = tt\}) \\
&= P \cup post(S^N[\![S_b]\!])(post(X)P \cap \{\rho' \mid \mathcal{B}[\![B]\!]\rho' = tt\}) \\
&= P \cup post(S^N[\![S_b]\!])(post(X)P \cap B) \\
&= P \cup post(S^N[\![S_b]\!])(\alpha_P(X) \cap B) \\
&= \bar{F}_P[\![S]\!](\alpha_P(X))
\end{aligned}
$$

$B = \{\rho \mid \mathcal{B}[\![B]\!]\rho = tt\}$

$\bar{F}[\![S]\!]X = P \cup post(S^N[\![S_b]\!])(X \cap B)$

S = while (B) S_b

Therefore

$$\begin{aligned}
&\mathrm{post}[\![S^N[\![S]\!]]\!]\rho \\
&= \mathrm{post}[\{\langle\rho,\rho'\rangle \in \mathrm{lfp}^{\subseteq} F^N[\![S]\!] \mid \mathcal{B}[\![B]\!]\rho' = tt\}]\rho \\
&= \mathrm{post}[\mathrm{lfp}^{\subseteq} F^N[\![S]\!]]\rho \cap \neg B \\
&= \mathrm{lfp}^{\subseteq} \bar{F}_\rho[\![S]\!] \cap \neg B
\end{aligned}$$

$\neg B = \{\rho \mid \mathcal{B}[\![B]\!]\rho = ff\}$

Moore logic

$$\begin{aligned}
M[\![S]\!] &= \{\{P\}\, S\, \{Q\} \mid \mathrm{post}[S^N[\![S]\!]P] \subseteq Q\} \\
&= \{\{P\}\, S\, \{Q\} \mid \mathrm{lfp}^{\subseteq} \bar{F}_P[\![S]\!] \cap \neg B \subseteq Q\} \\
&= \{\{P\}\, S\, \{Q\} \mid \mathrm{lfp}^{\subseteq} \bar{F}_P[\![S]\!] \subseteq B \cup Q\} \\
&= \{\{P\}\, S\, \{Q\} \mid \exists I.\ \bar{F}_P[\![S]\!]I \subseteq I \wedge I \subseteq B \cup Q\}
\end{aligned}$$

fixpoint induction

$$= \{\{P\}\,S\,\{Q\} \mid \exists I.\ P \cup \mathrm{pair}(S^N[\![S_b]\!])(I \cap B) \subseteq I \wedge I \subseteq \mathcal{S} \cup Q\}$$

$$= \{\{P\}\,S\,\{Q\} \mid \exists I.\ P \subseteq I \wedge \{I \cap B\}\,S_b\,\{I\} \wedge I \cap \neg B \subseteq Q\}$$

Proof rules

$$\frac{\emptyset}{\{I\}\ \mathtt{while}\ (B)\ S\ \{I \cap \neg B\}}\ \{I \cap B\}\,S_b\,\{I\}$$ Hoare iteration rule

$$\frac{\{P\}\,S\,\{Q\}}{\{P'\}\,S\,\{Q'\}}\ P \subseteq Q,\ Q \subseteq Q'$$ consequence rule

ON THE "AXIOMATIC SEMANTICS"

Is Hoare logic a definition of the semantics of a programming language (so called "axiomatic semantics")

NO

because it does not eliminate non standard semantics !!!

(same problem as Peano)

Non standard trace semantics

States : Σ

S^0 : $[0, n] \to \Sigma$, $n \in \mathbb{N}$ ⟼ finite traces
$\mathbb{N} \to \Sigma$ ⟼ infinite traces

$S^1 = S^0 \cup (-\mathbb{N} \to \Sigma)$ ⟼ traces that terminate but never start

$S^2 = S^1 \cup (\mathbb{Z} \to \Sigma)$ ⟼ traces that never start and never terminate

- while $(x < 0)$ $x := x+1$;

  standard $\{-n \dots 0 \mid n \in \mathbb{N}^+\} \cup \{n \mid n \in \mathbb{N}\}$

  non-standard $= \cup \{\dots -2 -1 0\}$

- while(true) $x := x+1$;

  standard $\{n\ n+1 \dots \mid n \in \mathbb{Z}^+$

  non-standard $= \cup \{\dots -2 -1\ 0\ 1\ 2 \dots\}$

- For all traces in both standard and non-standard cases, Hoare's iteration rule is satisfied (for the invariant which is the set of states on this trace)

The axiomatic semantics has non-standard models

- not a well-defined semantics
- solution for while (B) s :
  the strongest invariant is

$$\mathrm{lfp}^{\subseteq} \lambda X . B \cup \cup \{ \gamma \mid \{X\} s \{\gamma\} \}$$

- this is <u>not</u> expressible in Hoare Logic

$\Rightarrow$ The axiomatic semantics is ambiguous!

ON INCORRECTNESS LOGIC

Incorrectness logic

$\{[P]\, S\, [Q] \mid Q \subseteq \mathrm{post}\, [\![S]\!]^{\mathrm{e}}\, P\}$

- The calculational design is essentially the same as for total correctness Hoare logic. The difference is on while iteration
  - total Hoare logic : for all traces s.t. after $[\![S]\!]$ is reached (variant function)
  - incorrectness logic : exists a trace s.t. after $[\![S]\!]$ is reached (variant function)

Incorrectness Logic is not Hoare incorrectness

$$\neg(\{P\}\,\mathtt{S}\,\{Q\}) \not\Rightarrow\Leftarrow [P]\,\mathtt{S}\,[\neg Q] \qquad (0)$$

$$\Leftrightarrow \exists R \in \wp(\Sigma)\,.\,[P]\,\mathtt{S}\,[R] \wedge R \cap \neg Q \neq \emptyset \qquad (1)$$

$$\Leftrightarrow \exists \sigma \in \Sigma\,.\,[P]\,\mathtt{S}\,[\{\sigma\}] \wedge \sigma \notin Q \qquad (2)$$

(0) $\neg(\{\mathsf{true}\}\,\mathtt{x} = 0\{\mathtt{x} \neq 0 \wedge \mathtt{x} \neq 1\})$ holds but not $[\mathsf{true}]\,\mathtt{x} = 0[\mathtt{x} = 0 \vee \mathtt{x} = 1]$.

(1) this is not a formula of incorrectness logic

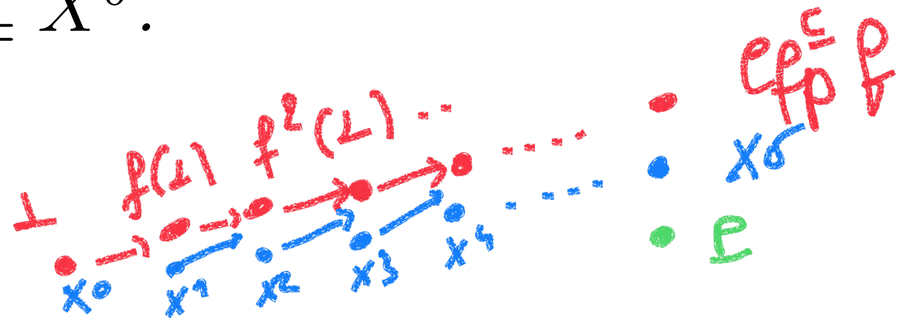
(2) a counter example is sufficient (and necessary)

proof in :

Patrick Cousot:
On the Design of Program Logics. On the Pursuit of Insight and Elegance 2026: 92-106

Induction principle

Theorem 3 (Fixpoint Under Approximation by Transfinite Iterates). *Let $f \in L \xrightarrow{i} L$ be an increasing function on a CPO $\langle L, \sqsubseteq, \bot, \sqcup \rangle$ (i.e. every increasing chain in L has a least upper bound in L, including $\bot = \sqcup\emptyset$). $P \in L$ is a fixpoint under approximation, i.e. $P \sqsubseteq \mathsf{lfp}^{\sqsubseteq} f$, if and only if there exists an increasing transfinite sequence $\langle X^\delta, \delta \in \mathbb{O} \rangle$ such that $X^0 = \bot$, $X^{\delta+1} \sqsubseteq f(X^\delta)$ for successor ordinals, $\bigsqcup_{\delta<\lambda} X^\delta$ exists for limit ordinals λ such that $X^\lambda \sqsubseteq \bigsqcup_{\delta<\lambda} X^\delta$, and $\exists \delta \in \mathbb{O} \,.\, P \sqsubseteq X^\delta$.*



Calculational design $\mathtt{W} = \mathtt{while(B)S}$

$S^{IL}[\![\mathtt{W}]\!]$

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

$= \ldots$

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

Proof rule :

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

$S^{IL}[\![\omega]\!]$

$$
\begin{aligned}
&= \{\langle P, Q\rangle \mid \exists \langle P', Q'\rangle \in \{\langle P'', \mathsf{post}[\![\mathtt{W}]\!]P''\rangle \mid P'' \in \wp(\Sigma)\} \,.\, P' \subseteq P \wedge Q \subseteq Q'\} \\
&= \{\langle P, Q\rangle \mid \exists P', Q', P'' \,.\, P' = P'' \wedge Q' = \mathsf{post}[\![\mathtt{W}]\!]P'' \wedge P' \subseteq P \wedge Q \subseteq Q'\} \\
&\qquad\qquad \wr\text{def. } \in\int \\
&= \{\langle P, Q\rangle \mid \exists P' \,.\, P' \subseteq P \wedge Q \subseteq \mathsf{post}[\![\mathtt{W}]\!]P'\} \qquad \wr\text{def. } =\int \\
&= \{\langle P, Q\rangle \mid Q \subseteq \mathsf{post}[\![\mathtt{W}]\!]P\} \\
&\quad \wr(\subseteq)\ \mathsf{post}[\![\mathtt{W}]\!] \text{ increasing and transitivity; } (\supseteq) \text{ take } P' = P \text{ and reflexivity}\int \\
&= \{\langle P, Q\rangle \mid Q \subseteq \mathsf{post}[\![\neg \mathtt{B}]\!](\mathsf{lfp}^{\subseteq} F'_P)\} \ \ \wr(5) \text{ with } F'_P(X) \triangleq P \cup \mathsf{post}([\![\mathtt{B}]\!] \fatsemi [\![\mathtt{S}]\!])X\int \\
&= \{\langle P, Q\rangle \mid \exists I \,.\, Q \subseteq \mathsf{post}[\![\neg \mathtt{B}]\!](I) \wedge I \subseteq \mathsf{lfp}^{\subseteq} F'_P\} \\
&\quad \wr(\subseteq)\quad \text{Take } I = \mathsf{lfp}^{\subseteq} F'_P \text{ and reflexivity;} \\
&\quad\ (\supseteq)\quad \text{By Galois connection } \langle \wp(\mathcal{X}), \subseteq\rangle \underset{\mathsf{post}(r)}{\overset{\widetilde{\mathsf{pre}}(r)}{\leftrightarrows}} \langle \wp(\mathcal{Y}), \subseteq\rangle, \mathsf{post}[\![\neg \mathtt{B}]\!] \text{ is} \\
&\quad \text{increasing so } Q \subseteq \mathsf{post}[\![\neg \mathtt{B}]\!](I) \subseteq \mathsf{post}[\![\neg \mathtt{B}]\!](\mathsf{lfp}^{\subseteq} F'_P) \text{ and transitivity}\int \\
&= \{\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 = \emptyset \wedge J^{n+1} \subseteq F'_P(J^n) \wedge I \subseteq \\
&\quad \bigcup_{n<\omega} J^n\} \qquad\qquad \wr\text{fixpoint under approximation Th. II.3.6}\int
\end{aligned}
$$

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

$\wr(\subseteq)$ By Galois connection $\langle \wp(\mathcal{X}), \subseteq\rangle \underset{\mathsf{post}(r)}{\overset{\widetilde{\mathsf{pre}}(r)}{\leftrightarrows}} \langle \wp(\mathcal{Y}), \subseteq\rangle$ $\mathsf{post}[\![\neg \mathtt{B}]\!]$ 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 $I = \bigcup_{n<\omega} J^n \int$

$= \{\langle P, Q\rangle \mid \exists\langle J^n, n < \omega\rangle \,.\, J^0 = \emptyset \wedge J^{n+1} \subseteq (P \cup \mathsf{post}([\![\mathtt{B}]\!] \fatsemi [\![\mathtt{S}]\!])(J^n)) \wedge Q \subseteq \mathsf{post}[\![\neg \mathtt{B}]\!](\bigcup_{n<\omega} J^n)\}$ $\wr$def. $F'_P\int$

$= \{\langle P, Q\rangle \mid \exists\langle J^n, 1 \leqslant n < \omega\rangle \,.\, J^1 = P \wedge J^{n+1} \subseteq \mathsf{post}([\![\mathtt{B}]\!] \fatsemi [\![\mathtt{S}]\!])(J^n) \wedge Q \subseteq \mathsf{post}[\![\neg \mathtt{B}]\!](\bigcup_{1\leqslant n<\omega} J^n)\}$ $\wr$getting rid of $J^0 = \emptyset\int$

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

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

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

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

HOARE LOGIC OF INCORRECTNESS

Meare incorrectness

$$\neg \{P\} S \{Q\}$$

$$= \neg \left(post[S] P \subseteq Q \right)$$

$$= \neg \left(\{ \rho' \mid \exists \rho \in P . \langle \rho, \rho' \rangle \in S \} \subseteq Q \right)$$

$$= \exists \rho \in P . \exists \rho' . \langle \rho, \rho' \rangle \in S \wedge \rho' \notin Q$$

$$= \exists \rho \in P \cap \{ \rho \mid \exists \rho' . \langle \rho, \rho' \rangle \in S \wedge \rho' \in \neg Q \}$$

$$= P \cap pre[S] \neg Q \neq \emptyset$$

Induction principle

Theorem 4 (Non empty intersection with abstraction of least fixpoint). *Assume that (1)* $\langle L, \sqsubseteq, \bot, \top, \sqcap, \sqcup \rangle$ *is an atomic complete lattice; (2)* $f \in L \to L$ *preserves nonempty joins* $\sqcup$*; (3)* $\langle L, \sqsubseteq \rangle \underset{\alpha}{\overset{\gamma}{\leftrightarrows}} \langle \bar{L}, \preceq, \curlywedge \rangle$*; (4)* $\bar{Q} \in \bar{L} \setminus \{0\}$ *where* $0 \triangleq \alpha(\bot)$*; (5) There exists an inductive invariant* $I \in L$ *of* f *(i.e.* $f(I) \sqsubseteq I$*); (6)* $\langle W, \leqslant \rangle$ *is a well-founded set and* $\nu \in \mathsf{atoms}(I) \to W$ *is a (variant) function; (7) There exists a sequence* $\langle a_i \in \mathsf{atoms}(I),\ i \in [1, \infty] \rangle$ *that (7.a)* $a_1 \in f(\bot)$*, (7.b)* $\forall i \in [1, \infty]\ .\ a_{i+1} \in \mathsf{atoms}(f(a_i))$*, (7.c)* $\forall i \in [1, \infty]\ .\ (a_i \neq a_{i+1}) \Rightarrow (\nu(a_i) > \nu(a_{i+1}))$*, (7.d)* $\forall i \in [1, \infty]\ .\ (\nu(a_i) \not> \nu(a_{i+1}) \Rightarrow \alpha(a_i) \curlywedge \bar{Q} \neq 0$*; Then, hypotheses (1) to (7) imply* $\alpha(\mathsf{lfp}^{\sqsubseteq} f) \curlywedge \bar{Q} \neq 0$*. Conversely (1) to (4) and* $\mathsf{lfp}^{\sqsubseteq} f \sqcap \gamma(\bar{Q}) \neq \bot$ *imply (5) to (7).*

Calculational design

$\mathtt{W} = \mathtt{while}(\mathtt{B})\mathtt{S}$

$\mathcal{S}^{\overline{\mathrm{HL}}}[\![\mathtt{W}]\!]$

$$
\begin{aligned}
&\triangleq \{\langle P, Q\rangle \mid \neg(\mathsf{post}[\![\mathtt{W}]\!]P \subseteq Q)\} && \text{〖def. } \alpha^{\neg}\text{〗}\\
&= \{\langle P, Q\rangle \mid \mathsf{post}[\![\mathtt{W}]\!]P \cap \neg Q \neq \emptyset\} && \text{〖def. } \subseteq \text{ and } \neg\text{〗}\\
&= \{\langle P, Q\rangle \mid \mathsf{post}[\![\neg\mathtt{B}]\!](\mathsf{lfp}^{\subseteq} F'_P) \cap \neg Q \neq \emptyset\} && \text{〖(5), } F'_P(X) \triangleq P \cup \mathsf{post}([\![\mathtt{B}]\!] \fatsemi [\![\mathtt{S}]\!])X\text{〗}\\
&= \{\langle P, Q\rangle \mid \mathsf{lfp}^{\subseteq} F'_P \cap \mathsf{pre}[\![\neg\mathtt{B}]\!](\neg Q) \neq \emptyset\}\\
& && \text{〖}\mathsf{post}(R)P \cap Q \neq \emptyset \Leftrightarrow P \cap \mathsf{pre}(R)Q \neq \emptyset\text{〗}\\
&= \{\langle P, Q\rangle \mid \exists I \in \wp(\Sigma)\ .\ F'_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,\\
&\quad i \in [1,\infty]\rangle\ .\ \sigma_1 \in F'_P(\emptyset) \wedge \forall i \in [1,\infty]\ .\ \sigma_{i+1} \in F'_P(\{\sigma_i\}) \wedge \forall i \in [1,\infty]\ .\\
&\quad (\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\\
&\quad \mathsf{pre}[\![\neg\mathtt{B}]\!](\neg Q) \neq 0\} && \text{〖induction principle Th. 4〗}\\
&= \{\langle P, Q\rangle \mid \exists I \in \wp(\Sigma)\ .\ P \subseteq I \wedge \mathsf{post}([\![\mathtt{B}]\!] \fatsemi [\![\mathtt{S}]\!])I \subseteq I \wedge \exists\langle W, \leqslant\rangle \in \mathfrak{Wf}\ .\ \exists \nu \in\\
&\quad 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\\
&\quad \mathsf{post}([\![\mathtt{B}]\!] \fatsemi [\![\mathtt{S}]\!])\{\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\\
&\quad [1,\infty]\ .\ (\nu(\sigma_i) \not> \nu(\sigma_{i+1}) \Rightarrow \sigma_i \in \mathsf{pre}[\![\neg\mathtt{B}]\!](\neg Q)\}
\end{aligned}
$$

$$\wr\text{def. } F'_P(X) \triangleq P \cup \mathsf{post}(\llbracket \mathtt{B} \rrbracket \fatsemi \llbracket \mathtt{S} \rrbracket)X, \subseteq, \text{and } \mathsf{post}, \text{which is } \emptyset\text{-strict}\int$$

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

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

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

$\wr(\subseteq)$ By $\langle W,\ \leqslant\rangle \in \mathfrak{Wf}$, $\nu \in I \to W$, $\forall i \in [1,\infty]\ .\ (\sigma_i \neq \sigma_{i+1}) \Rightarrow (\nu(\sigma_i) > \nu(\sigma_{i+1}))$, 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 $\sigma_n \in \mathsf{pre}[\![\neg \mathtt{B}]\!](\neg Q)$;

$(\supseteq)$ 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 $\nu(x) = (\!|\, x \in \{\sigma_i \mid i \in [1,n]\}\ ?\ x : -\infty \,|\!)$ and the sequence $\langle \sigma_j \in I,\ j \in [1,\infty]\rangle$ repeats σ_n ad infimum for $j \geqslant n$.$\int$

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

$$\wr\text{def. } \mathsf{pre}\int$$

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

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

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

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

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

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

$$= \{\langle P, Q\rangle \mid \exists n \geqslant 1 \,.\, \exists\langle \sigma_i \in I,\, i \in [1,n]\rangle \,.\, \sigma_1 \in P \wedge \forall i \in [1,n[\,.\, \langle \underline{\mathcal{B}}\llbracket \mathtt{B} \rrbracket \cap \{\sigma_i\}, \neg\{\sigma_{i+1}\}\rangle \in \overline{\mathfrak{I}^{\mathfrak{HL}}}\llbracket \mathtt{S} \rrbracket \wedge \sigma_n \notin \mathcal{B}\llbracket \mathtt{B} \rrbracket \wedge \sigma_n \in Q\}$$
$$\wr \text{def. } \overline{\mathfrak{I}^{\mathfrak{HL}}}\llbracket \mathtt{S} \rrbracket\int \qquad \square$$

Hoare incorrectness proof rule ω = while(B)s

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

which is ..... ?!?

Hoare incorrectness proof rule

$\mathtt{w} = \mathtt{while(B)s}$

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

which is debugging !

THE END, THANK YOU